ISA Delhi Section

International Society of Automation
Delhi Section

PETROLEUM & POWER AUTOMATION MEET 2023

" AUTOMATION for I.I.O.T "

(Industry, Innovation, Operation & Transformation)




12th and 13th May 2023

(FRIDAY & SATURDAY)

Venue: Hotel Eros, Nehru Place, New Delhi

e - Souvenir

2023
STRENGTHENING THE
GREEN RESOLVE

Realising the vision of Net-Zero emissions by 2046 for a better future

As the Energy of India, IndianOil is committed to catalyse the country's ambitious journey to reach Net-Zero emissions by 2070. The Corporation is investing over Rs. 2 Trillion in phases across various initiatives covering the entirety of our operations, particularly in our refineries. IndianOil is focusing on greener avenues of renewable energy, green hydrogen, City Gas Distribution, Compressed Biogas, and Electric Vehicles. The year 2023 is being devoted towards accelerating green innovations to bring about a sustainable and better dawn for the energy sector in India.

Determined to Strengthen the Green Resolve

ISA DELHI SECTION

ASIA PACIFIC DISTRICT

Message

It gives me immense pleasure to note that the International Society of Automation (ISA) - Delhi section is organizing the "Petroleum and Power Automation Meet" focused on the latest developments in Automation Technology in the Energy Sector, with the theme: "AUTOMATION for I.I.O.T - INDUSTRY INNOVATION OPERATIONS TRANSFORMATION" (IIOT) on 12th & 13th May 2023 in New Delhi.

With the advent of smart technologies such as the Industrial Internet of Things (IIoT) and cyber-physical systems in the era of digitalization and automation, industries across the globe are transforming their business processes to adapt to the growing needs of integrating advanced technologies in their existing systems to make it more efficient and responsive. This transformation is visible through increased productivity across industries with the help of data-driven decision-making, prospective planning to align the supply chain network, and investment in Research & Development.

This forum will enable learning from the diverse experiences of peers and industry experts from the Power and Petroleum & Natural Gas sectors in the areas pertaining to digitalization and automation to promote sustainable business solutions in times to come. The symposium also intends to engage stakeholders such as Automation service Providers/manufacturers, system integrators, consultants, R&D Organizations, academicians, and others for an invigorating exchange of ideas, the latest trends and knowledge of the rapidly growing instrumentation and automation sector, and the challenges associated thereof with its large-scale implementation.

I wish the conference a great success.

Regards,

VARTIKA SHUKLA
C&MD, EIL

ISA DELHI SECTION

ASIA PACIFIC DISTRICT

Message

I am pleased to know that ISA Delhi Section is organizing *Petroleum & Power Automation Meet (PPAM-2023)* on May 12-13, 2023, at New-Delhi based on the theme '***Automation for I.I.O.T'.*** It must be mentioned at the onset, that the theme is very apt and perfectly tuned with the need of hour. Alongside, industry automation, a focus on automation excellence towards net zero with efficient use of sustainable, renewable, green energy sources must also figure on our work radar.

Energy & Power Sectors are critical contributors for the growth and development of a country. Due to the rapidly transforming global scenario and the responsibility of the present generation to ensure a safe, clean & green environment for future generations; there is an urgent need to adopt sustainable solutions for operation of industrial plants. Similarly, the energy sector too is briskly in pursuit of alternate clean & green energy sources and deeply involved in working out the workable nuances of balanced demand and supply situation. It is the automation technology that may help reducing this gap as well as become a major factor in meeting the sustainability needs of the petroleum and power sector in India. A shift in energy scenario with the support of new technologies for optimized solutions & operations are the order of the day. The country at this juncture is looking at new vistas to make itself reliant, sustainable, and economical, on all fronts.

As evident from the recently concluded Saksham-2023, the energy sector of India is committed to *Energy Conservation towards Net Zero*. In order to satisfy the future requirements, there is a need to go for rapid capacity addition using all the possible energy options including hydro, nuclear, and renewable resources. It is worthy to note that automated system in the energy sector, now must play a bigger role than in the past to ensure increased availability, reliability, safety, and stability of assets of the petroleum and power plants. The COVID pandemic put many questions before the world. Indeed, new solutions do emerge with new problems; and as we embrace new technologies using Cloud Engineering, AI based adaptive maintenance, ML & data Analysis, IIOT and Remote Process Automation (RPA); we also need to emphasize issues like cyber security to protect our intellectual property, data, and database.

PPAM-2023 is a good opportunity for the control and instrumentation professionals to enhance individual technical expertise. I appreciate this initiative as it offers a vital platform for experts to publish relevant technical papers and benefits professionals with wide spectrum of knowledge exchange on topics covering the vistas of industry, innovation, operations & transformation.

I convey best wishes for the success of the event.

Best Regards,
Ms. Sukla Mistry
Director (Refineries), IndianOil

ISA DELHI SECTION

ASIA PACIFIC DISTRICT

Message

It gives me immense pleasure to be a part of International Society of Automation (ISA) - Delhi section's "Petroleum and Power Automation Meet" being held on 12th & 13th May 2023. International Society of Automation (ISA) is a non-profit Organization dedicated to building a better world through automation ensuring safety, security, availability & reliability.

The noble theme "AUTOMATION for I.I.O.T - INDUSTRY INNOVATION OPRERATIONS TRANSFORMATION" of ISA's Delhi Chapter will address key challenges of energy sector. Adoption of AI/ML, Robotics, IIoT, Digitalization along with cyber security are key to increasing productivity without compromising on safety and security meeting regulatory requirements.

With India's energy demand set to grow rapidly, transition to clean energy will help India emerge as a global leader with a cleaner, greener & sustainable energy mix supporting net zero.

I am happy that the two-day symposium has rich & meaningful content and a powerful context in this regard. Contribution from technology owners, service providers and stakeholders will definitely help in addressing the key challenges of energy sector.

My best wishes to the participants and for success of PPAM-2023.

Director (Projects)
NTPC Limited

ISA DELHI SECTION

ASIA PACIFIC DISTRICT

Message

I am happy to note that International Society of Automation (ISA) - Delhi section is organizing "Petroleum and Power Automation Meet" focused on the latest developments in Automation Technology in the Energy Segment, with the theme: " AUTOMATION for I.I.O.T - INDUSTRY INNOVATION OPRERATIONS TRANSFORMATION" (IIOT) on 12th & 13th May 2023 with a vision and mission to take Instrumentation and Automation to global heights and acquire a numero-uno position in Petroleum and Power Segments in Indian Industry.

The Oil & Gas Sector an important energy provider to nation faces challenges from ever increasing demand for high productivity, improved operational efficiency, increased safety and security meeting regulatory requirements. Today's automation is fully equipped to face the challenges by adopting latest technological advancements without compromising operational safety.

This industry demands adoption of Plant Intelligence digital solutions like IOT, Industry 4.0 and big data analytics that help to connect and integrate the systems that work in isolation. It is necessary to connect the plant floor with the enterprise level that will give real time plant information and enhance productivity.

I believe that the engagement and involvement of various stake holders including technology providers and developers would certainly help in achieving the roadmap for implementing strategies for automation and digital solutions so essential for a world-class Petroleum and Natural Gas utility.

I wish the symposium for their success.

(Rajiv Agarwal),
Director (Technical)
Engineers India Limited.

ISA DELHI SECTION

ASIA PACIFIC DISTRICT

Message

I appreciate the efforts of ISA Delhi section for organizing the Petroleum and Power Automation Meet on 12 and 13 May 2023 in Delhi. I am also humbled and honored to be the keynote address at this event. The theme of the event this year is Industry, Innovation, Operation and Transformation. And I believe a perfectly apt subject for the industrialist and technology providers like yourselves to leverage through discussion and utilize the opportunity to share the industry challenges and learn best practices from each other.

Digital transformation for an industrial process involves using technology solutions to improve productivity, enhance operational performance, and augment customer experience. By deploying the right and scalable digital solutions, one can achieve better energy optimization and management, increased operational efficiency, and asset reliability, leading to reduced downtime and preventing loss of production. Leveraging decades of innovation and expertise in digitalization, Emerson can support the right approach for industries to build digital and sustainable solutions right from the inception stage, and we've seen repeatedly how a practical approach that generates short-term wins with measurable gains can be replicated for enterprise-wide impact.

Year over year ISA Delhi has provided a platform for exchange of expertise and knowledge sharing through multiple such avenues. And it provides immense opportunities for automation professionals to be engaged with the industry and share the latest developments in the automation arena. I am looking forward for highly interactive and engaged sessions where all the industry experts and technology providers would be contributing their best.

With Warm Regards

Anil Bhatia

Vice President & Managing Director,
Emerson - India

ISA DELHI SECTION

ASIA PACIFIC DISTRICT

Message

It is with great pleasure that I acknowledge the organization of the annual Petroleum and Power Automation Meet by the ISA Delhi Section, scheduled to take place on May 12th and 13th, 2023. This remarkable initiative by the ISA Delhi section contributes significantly to fostering synergy among Power and Petroleum Industry Professionals in India regarding Automation Technology. I commend the ISA Delhi section for their efforts in bringing together key players in the energy, Oil and Gas sector such as EIL, IOCL, NPCIL, NTPC, amongst many others, as well as major engineering and private consulting companies including Urban Infrastructure companies and more. Events of this nature serve a pivotal purpose in deepening comprehension of industry expectations, novel technological advancements, and the obstacles confronted by both the Automation Industry and end users.

Innovation, Industry 4.0, and digitization are critical for the energy industry. They drive operational efficiency, sustainability, and transformation, which are vital for achieving India's sustainability goals. With Industry 4.0, the integration of digital technologies optimizes operations, improves resource management, and enhances productivity. Digitization revolutionizes the energy sector, enabling smarter grid management, efficient energy distribution, and decentralized renewable energy solutions. By embracing these advancements, the industry reduces environmental impact, minimizes greenhouse gas emissions, and promotes economic growth, contributing to a greener and more sustainable future.

The Meet will provide participants with access to industry knowledge and expertise, networking opportunities with professionals from diverse backgrounds, a platform to showcase products and solutions, and insights into industry expectations and challenges. This will enable them to stay updated, make informed decisions, foster collaboration, explore business opportunities, enhance brand visibility, and develop innovative strategies to address industry challenges, contributing to future professional growth and business development in the automation field.

I extend my best wishes for the success of the Petroleum and Power Automation Meet 2023.

With best Regards

Anil Kumar,
MD,
Royal Haskoning DHV

ISA DELHI SECTION

ASIA PACIFIC DISTRICT

Message

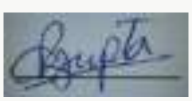
It is my immense pleasure to be part of ISA-D organized Symposium (Conference & Exhibition) under the Title Petroleum and Power Automation (PPA) meet on the theme “AUTOMATION for I.I.O.T” (Industry, Innovation, Operation & Transformation) and the Souvenir being brought out to commemorate this occasion.

Since its inception in year 2000, ISA-D had been promoting latest Technologies in Process Automation through regularly conducting monthly Technical Meets, PPA Meets and imparting Technical Training. ISA-D has emerged as a forum of choice for End users, Consultants, EPC’s, System Integrators, Suppliers, Contractors, and Students. ISA-D is now venturing beyond the boundary of Automation into the areas important for Hydrocarbon Industry in keeping with the key role automation professionals are playing in the industry.

This year’s theme “AUTOMATION for I.I.O.T” (Industry, Innovation, Operation & Transformation) is in keeping with the Prime Ministers vision of Transforming the country through Innovation and Make in India. Professionals, who are expert in their fields will be deliberating the latest Technologies available, through Presentations and Lecture-Demonstrations.

I solicit your co-operation to enable ISA-D to keep on contributing more effectively in enriching the life of all professionals who are part of it. I convey my best wishes for the success of PPA Meet.

With best Regards



(Rajiv Gupta)
Hony. President
ISA Delhi Section

ISA DELHI SECTION

ASIA PACIFIC DISTRICT

Message

The dynamics of Energy Sector are changing at a rapid rate, the quest for having sustainable & environmentally friendly solutions, and advent of new technologies like AI / ML / Data Science etc. are pushing the envelope to new frontiers. The national and international organizations in this sector are facing new challenges but at the same time they are putting lot of effort in developing their expertise to have efficient and sustainable solutions. ***Petroleum and Power Automation Meet (PPAM) 2023***, like its predecessor the past, will offer new opportunities to the professionals in automation field associated with Oil & Gas and Power sectors. This knowledge sharing event has potential to add value to the professional skills covering the automation horizon - as evident from this year theme "***Automation for I.I.O.T***" (Industry, Innovation, Operation, Transformation) and which shall showcase the innovation in respective work areas.

The efforts being put by team of ISA Delhi Section for such a focused event "Petroleum & Power Automation Meet 2023" on 12th & 13th May 2023 at Delhi are commendable. Automation is the key enabler for increased productivity, efficiency, reliability & safety of Oil & Gas and Power industry.

It is also note-worthy that through such seminars, ISA Delhi Section is striving to facilitate the realization of world class production facilities in India. The efforts are also contributing to developing core expertise in various facets of automation which are in turn enhancing our value. Our Petroleum and Power industries have the one of the best facilities of global standards, the mutual co-operation between ISA & Industry is helping them to keep pace with development as they happen.

It is a good opportunity for the automation professionals to attend this conference and enhance their knowledge & expertise. ISA provides platform to all the stake holders for mutual value addition.

I feel privileged for being a part of the ISA team hosting this mega event. I expect all the fellow members of ISA Delhi and participants would feel the same. Let us come together and make this event a success.

With best Regards

Raj

Raja Sekhar Gudipaty,
Hon. Secretary , ISA - Delhi

ISA DELHI SECTION

ASIA PACIFIC DISTRICT

Message

Continuous technological innovations coupled with evolution of sustainable automation solutions have become essential in all sectors of industries across the globe adopting various green technologies with an ultimate aim of achieving “Net zero”. This would be possible with the utilization of appropriate data analytic tools and digitalization of various workflows, thereby analyzing the data for improved and faster decision making.

We believe that sharing of knowledge on latest technological update amongst all stakeholders in the relevant sectors and discussing the same in a common forum generates opportunities for learning and creates synergy in understanding. ISA Delhi section has always been instrumental in creating such platform for automation sectors and fraternity since its inception through organizing flagship mega events.

To keep pace with ever-increasing expectations from automation industry with the appropriate utilization of technologies along with latest analytical tools like Artificial intelligence / Machine Learning and without compromising cyber-security, this two days Conference and Exhibition (Petroleum and Power Automation Meet’ 2023) titled “Automation for I.I.O.T” (Industry, innovation, Operation and Transformation) is organized by ISA-Delhi section involving all the Instrumentation Professionals viz Energy (Petroleum and Power), Process (Chemical and Fertilizer), Infrastructure (Building and Water/Waste Water) Industry in India.

We are sure that such an important conference will help all ISA professionals and delegates, working in numerous fields and providing expertise in diverse areas to nearly any technological field in use today, in synchronizing their knowledge with the industry demand. We have received an overwhelming response from industry while receiving the papers from automation fraternity. All the papers for the event have been carefully reviewed and selected by a team of experts from various sectors of industries.

I really feel honored to get the responsibility and delighted to be part of the ISA Delhi Section Team organizing this Conference & exhibition. I would like to convey my sincere thanks to all ISA members who have worked relentlessly to make this event a grand success.

Looking forward for a happy learning for all of us with an interactive session ahead during the event.

With best Regards

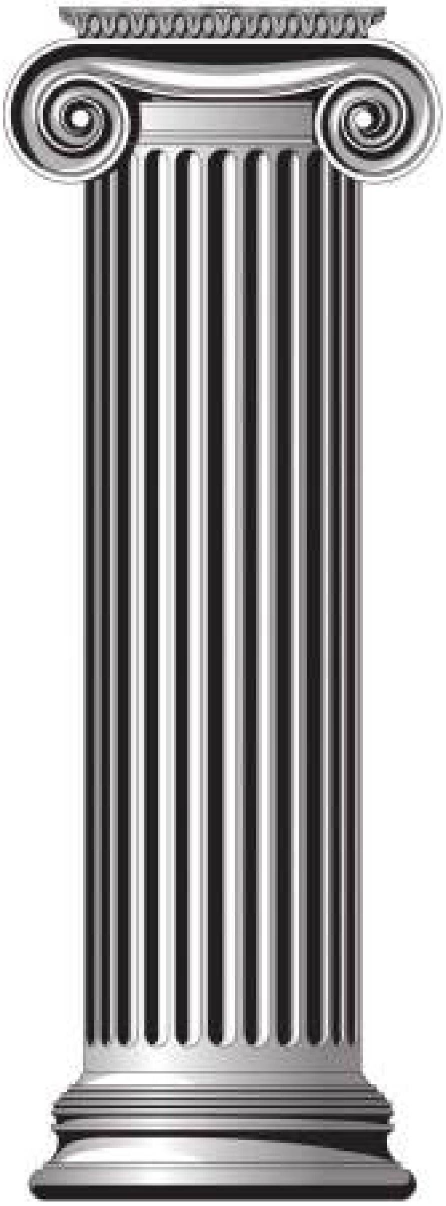
Mnandi

Mainak Nandi
Convenor, PPAM - 2023

The International Society of Automation (ISA)

Founded in 1945, the International Society of Automation (ISA) is a leading, global, non-profit organization that is setting the standard for automation by helping over 30,000 worldwide members and other professionals to meet, interact and share their knowledge. Based in Research Triangle Park, North Carolina, ISA is organised into 14 districts and hundreds of sections across the world. The Southeast Asia region is designated as District-14 and within this district, the Delhi Section is an active organization drawing members from the entire spectrum of automation industry across Power, Oil & Gas, Metallurgy, Chemicals & Fertilizers including the Engineering fraternity from Consultants, EPC Contractors, Automation Component Suppliers & Equipment Manufacturers, System Integrators, and many other industries.

ISA Delhi Section



ISA has been involved in promoting emerging technologies across the globe by a variety of ways such as:

- Developing and updating standards for existing & evolving technologies in automation related fields.
- Publication of Textbooks, handbooks, journals, proceedings etc. on a wide array of automation related subjects from primary field sensors to integrated automation and management systems for various kinds of plants & processes.
- Facilitating Interface & interaction with other agencies like IEC, IEEE, EPRI, ASME and others to develop and maintain automation related standards with regular updating, keeping pace with the march of technology in various fields.
- Organising Training, Seminars/Workshops, Webinars and Exhibitions.
- Carrying out certification programs for technicians, engineers, and senior professionals.
- Recognizing the talented and the dedicated professionals in the field of Automation through various honours and awards
- Enabling Interaction with Student members, formation of student section and annual scholarships, competitions etc. are many interesting student programs of the ISA.

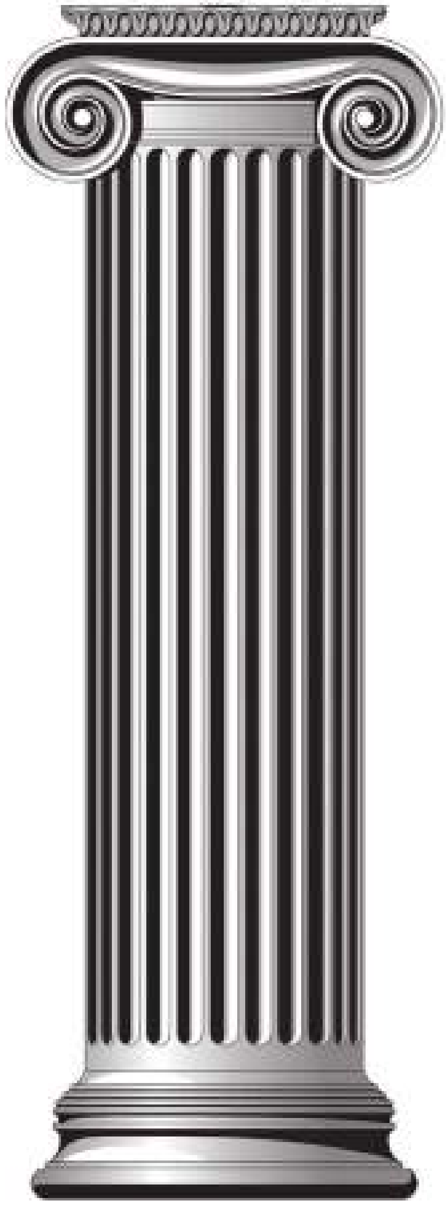
The ISA Delhi Section - ISA(D)

ISA Delhi Section has now completed its more than two decades of successful presence in the country. With the core aim of providing highest levels of technical engagements for its members who are from all over the automation industry domains of Plant and Process Automation. In the post COVID-19 years i.e. 2021 and 2022 ISA Delhi Section had taken many initiatives including the first ever Building Automation Tech-Talk, A Virtual Two Day Symposium on Industrial Automation TOTAL2021 and also a Hybrid Cyber Security Seminar. Regular Monthly technical exchanges on diverse topics were also organised for the benefit of all members of ISA (D), thereby increasing the knowledge base & technical capabilities of members.

Currently, ISA Delhi Section holds the second largest Membership Strength in the Asia Pacific District that covers a diverse number of professionals from Engineering Companies, EPC Entities, End Users, System Integrators, Instrumentation and Automation Component Manufactures, Licensors and Consulting Companies, Traders and Equipment Suppliers, Academia, and Students from Engineering Colleges. Such a gathering of Domain Experts, Designers and Users being the core strength of the Section has provided a value-add platform among the industry.

Our Executive Board members also carry forward the spirit of leading by example to conduct the activities and programs of the Section thereby providing the much-needed synergy of all the stakeholders. We are also proud to be the one of the most active Sections that gives opportunity for new leaders to emerge and showcase their passion for technology.

ISA Delhi Section



ISA Standards

Practical Solutions from Industry Experts

ISA Standards help automation professionals streamline processes and improve industry safety, efficiency, and profitability. Over 150 standards reflect the expertise from over 4,000 industry experts around the world. Since 1949, ISA has been recognized as the expert source for automation and control systems consensus industry standards.

Key Features, Advantages, and Benefits of Standards

Realize a direct return on investment by

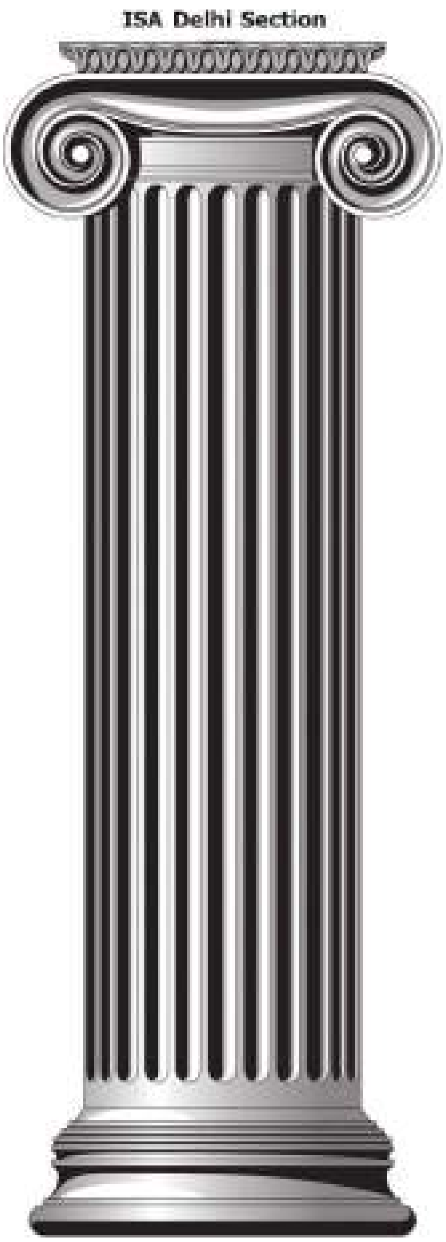
- Lowering installation and start-up costs.
- Reducing need to maintain large inventories.
- Enabling interchangeability of components
- Improving design with less “custom” effort.
- Increasing safety.

Use of standards in industry

- Improves communication.
- Provides practical application of expert knowledge.
- Represents years of experience and avoids necessity of starting each project from ground up.

Standards help you achieve operational excellence by

- Improving performance.
- Lowering maintenance costs.
- Reducing downtime.
- Enhancing operability.
- Saving money



ISA's Role in Developing Standards

More than 4,000 individuals cooperating with more than 140 committees, subcommittees, working groups and task forces are involved in ISA standards. They're developing standards in areas as diverse as ensuring the safety of electrical equipment used in hazardous locations to cost-savings for interfaces between industrial process control computers and subsystems.

How a Standard Saves Money

ISA's batch control standard illustrates how using a standard cuts cost. Food, pharmaceutical and specialty chemical companies build factories with increasingly sophisticated computer-driven automation. The batch standard ISA developed-ANSI/ISA-88.00.01 - shaves as much as 30 percent off the cost of designing the system and software used in these plants. ANSI/ISA-88.00.01 sets out a blueprint that engineers can use to make portions of the code interchangeable, which is less expensive than designing each piece from the ground up.

The savings extend beyond the facility's design, though. By using the batch standard, companies save as much as 10 to 15 percent off the typical cost of meeting Food and Drug Administration criteria for the reliability of automation equipment.

How a Standard Saves Lives

Other ISA standards focus on safety. ISA has developed standards for the performance requirements of toxic gas detectors, standards to keep electrical equipment from igniting flammable material and standards to ensure safety at nuclear power plants.

And some ISA standards can help an entire industry combine cost savings and safety. The most popular ISA standard is ANSI/ISA-5.1, Instrumentation Symbols and Identification. Developed in 1949 and most recently revised in 2009, these symbols are used in blueprints for everything from power plants to factories. If every contractor on a project knows the standard symbols, there are fewer communication problems that could lead to costly delays or safety problems.

Using Standards to Help Your Business Expand Globally

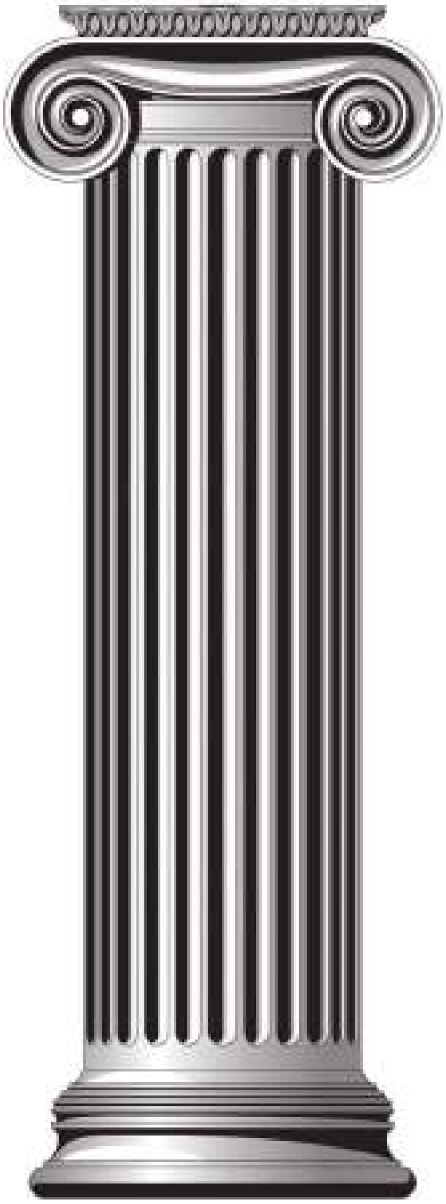
Your company has a product that's taken the United States by storm; now you want to expand globally. But there is a hitch or, as the engineers might tell you, a "technical barrier to trade.'' Your company's product, or the process by which it's made, doesn't meet international standards.

Many ISA standards are also international standards, and our committees strive to stay current with evolving global standards. ISA administers three committees for the International Electro technical Commission (IEC), which is one of the two most widely recognized international standards groups, along with International Organization for Standardization (ISO).

How Your Company Can Take Advantage of ISA's Standards

- Buy ISA standards and train your employees to follow it.
- Help set a standard. ISA's committees are eager for help. Both voting and non-voting memberships are available. Voting members must have their employers' approval, in part because attending at least one meeting a year is expected. But we're cutting down on the time demands of committee membership by encouraging members to do a great deal of their work via e-mail. Non-voting members supply input but are not required to attend meetings. Apply online to volunteer.

ISA Delhi Section



Students

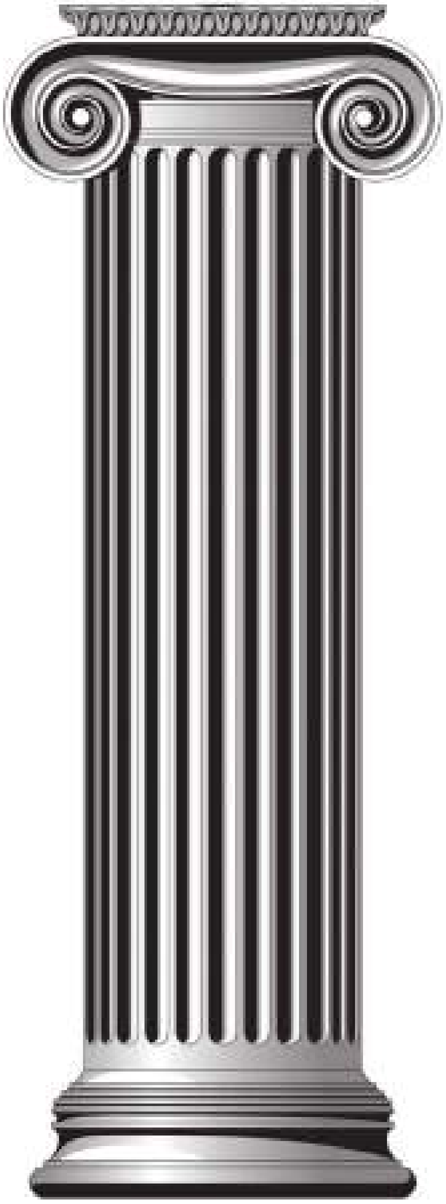
Students can come to automation from a variety of backgrounds and academic programs. It is sometimes difficult for you to find programs that concentrate on automation as a career or specialty. This potential variety can create challenges for students like you that are not seen in many areas of studies.

The essence of automation is that it is a multidisciplinary art, not a single discipline. You are required to know a lot about many things to function as an automation professional. Automation studies are rarely centred in one department. Automation students and faculty on a campus could come from any number of engineering areas. That means that published findings could appear in several journals and presented at a myriad of scientific conventions. This diversification makes it extremely difficult for students to stay current on the newest findings. It also means that you need to have a very open outlook on what will make you a good automation professional.

The ISA web site helps students more easily stay current on research without attending numerous expensive conventions or wading through non-automation related literature for the useful gems. Also, students can find the conferences they should attend to both gain information and networking possibilities, which can lead to job possibilities.

The ISA web site contains the Automation Body of Knowledge, from the very basics of sensors and controls to the most detailed industrial networking, enterprise integration, cyber security, and safety information. When you have digested that Body of Knowledge, you will be ready to be a Certified Automation Professional, and you can find the tutorials and test materials here to help you.

ISA Delhi Section



The ISA Mentor Program for Young Professionals and Students

ISA's Mentor Program enables young professional ISA Members and Student Members to access the wisdom and expertise of seasoned ISA Members, while it offers veteran ISA professionals the chance to share their wisdom and make a difference in someone's career. A mentor can give a young professional guidance in his or her career or help a student determine if automation and control is the right path to follow.

ISA's Mentor Program is an online program, so there are no meetings to attend and there is no travel. ISA Members from all over the world can participate, and the relationship can develop and progress at the convenience of the mentor and protégé.

ISA Members are encouraged to register and participate in the program as mentors. Find out more about becoming a mentor.

ISA's younger Members and Student Members are urged to use this valuable Member benefit. Find out more about getting an ISA Mentor and how to select a mentor.

Executive Committee Members (2022-23)

S.No	Name	Position	E-mail Address	Mobile No.
1	Mr.Rajiv Gupta	President	rajivra1212@gmail.com	9818341262
2	Mr. M K Srivastava	President Elect	mksrivastava01@ntpc.co.in	9650991053
3	Mr. Alok Agarwal	Vice President	alok.agarwal@mcdermott.com	9911998292
4	Mr. Raja Sekhar Gudipaty	Secretary	rs.gudipaty@gmail.com	7206055509
5	Mr. Anupam Srivastava	Treasurer	anupam.srivastava@emerson.com	9873079003
6	Mr. S Mahesh Kumar	Society Delegate	s.mahesh.kumar@eil.co.in	9868105971
7	Mr. Arun Gupta	Alt. Delegate	arung@indure.com	9818102784
8	Mr. Prateek Singh	Program Chair	singhp2@indianoil.in	8377808113
9	Mr. Sarvesh Sharma	Program Chair	sarvesh.sharma@eil.co.in	9810339665
10	Mr. Anil Choudhary	Education Chair	anil@noclesys.com	9310016949
11	Mr. Sukumar Mohapatra	Membership Chair	sukumarmohapatra@ntpc.co.in	9650998369
12	Mr. Sachin Kr. Agarwal	Membership Chair	sachin.agrawal@eil.co.in	9958092991
13	Mr. Sanjay Kumar	Membership Chair	ersanjay1996@gmail.com	9891271003
14	Mr. Surinder Paul Tandon	Newsletter Editor	tandonsp@indianoil.in	9937012734
15	Mr. Rajat Goyal	Newsletter Editor	rajatgoyal06@gmail.com	9818953473
16	Mr. Amit Singh	WebMaster	amit.singh@dtl.gov.in	9999533927
17	Mr. Rishi Gaurav	WebMaster	rishig@indianoil.in	9717171047
18	Mr. H S Kalsi	Exhibit Chair	hskalsi18@gmail.com	9811771819
19	Mr. R D Kushwaha	Exhibit Chair	rdkushwaha@noclesys.com	9899158323
20	Mr. Sandeep Gupta	Marketing Chair	totalsolutionsco@yahoo.co.in	9868255848
21	Mr. Ashish Manchanda	Marketing Chair	ashishcontact@yahoo.co.in	9350043430
22	Mr. Kamal Rathore	Marketing Chair	rathorek@indianoil.in	9412280080
23	Mr. Parag Tyagi	Publication Chair	paraag@wissenautomation.com	9310295951
24	Mr. Some Nath Kundu	Publication Chair	somenathkundu@gmail.com	9650997664
25	Mr. Sachin Joshi	Honors & Awards	sachin.joshi@eil.co.in	9650011669

Executive Committee Members (2022-23)

S.No	Name	Position	E-mail Address	Mobile No.
26	Mr. Aman Sagar	Historian	aman_sagar44@yahoo.com	9910555211
27	Mr. Pankaj Gupta	Student Section Liaision	pankajinst@yahoo.com	8506066604
28	Ms. Anuja Thukral	Student Section Liaision	anuja.thukral@gmail.com	9310221033
29	Mr. Manish Kumar	Section Division Liasion	manish.kumar@eil.co.in	9810890933
30	Mr. Gaurav Mittal	Standards & Practices	mittalg@indianoil.in	9996644332
31	Mr. Arupjyoti Saikia	Standards & Practices	arupjyoti.saikia@eil.co.in	9910066741
32	Mr. Sushil Kumar	Past President	sushil@gail.co.in	9871004983
33	Mr. Rohit Bhardwaj	Chief Patron	rohit_iocl@yahoo.co.in	9873149991
34	Mr. S K Dhawan	Patron	sk.dhawan28@gmail.com	9818686181
35	Mr. Prasenjit Pal	Patron	prasenjit@ntpc.co.in	9650991122
36	Mr. S K Bardhan	Patron	bardhansk@yahoo.co.in	7838000016
37	Mr. R K Bassi	Sr. Advisor	rkbassi@yahoo.com	9810005826
38	Ms. R Priyamvada	Sr. Advisor	r.priyamvada@yahoo.com	9312229961
39	Mr. Dharmender Singhal	Sr. Advisor	dhsi@topsoe.in	9999387604
40	Mr. Sanjay Raijada	Sr. Advisor	raizadas@indianoil.in	9416500180
41	Mr. S K Tripathi	Sr. Advisor	sanjaykrtripathi@pdilin.com	9868358859
42	Mr. Mainak Nandi	Sr. Advisor	m.nandi@eil.co.in	9971581956
43	Mr. Atish Chakraborty	Sr. Advisor	atish400@gmail.com	9810629360
44	Mr. Ashish Dev	Sr. Advisor	ashisdev@ntpc.co.in	9650999070
45	Mr. R Sarangapani	Sr. Advisor	rsarangapani@ntpc.co.in	9650992571
46	Mr. Ravinder Goyal	Sr. Advisor	rgoyal@eipenviroindia.com	9810181109
47	Mr. S Sudershan Rao	Sr. Advisor	ssrao46@gmail.com	9650011279
48	Mr. Vivek Gupta	Sr. Advisor	vivek_gupta@dcmshriram.com	9829037954
49	Mr. N Vinod	Sr. Advisor	nvinod@indianoil.in	9466702974

Petroleum & Power Automation Meet

PROGRAM DETAILS

DAY-1 12-May-2023

	Inaugural Session			Time	
				FROM	TO
1	Introduction and Welcoming of Chief Guest and Guests of Honour			09:45 AM	9:50 AM
2	Lamp Lighting Ceremony			9:50 AM	9:55 AM
3	Welcome Address by ISA-D President - Mr. Rajiv Gupta	Ex ED(T) - EIL		9:55 AM	10:00 AM
4	Address By Chief Guest and Guest of Honour: Ms. Vartika Shukla - C&MD - Engineers India Ltd. Ms. Sukla Mistry - Director (Refineries) - IOCL Mr. U K Bhattacharya- Director (Projects) - NTPC Mr. Rajiv Agarwal - Director(Technical) - EIL			10:00 AM	11:00 AM
5	Note of Gratitude - Mr. Mainak Nandi - (Convenor PPAM-2023)	GGM - EIL		11:00 AM	11:10 AM
6	Release of e-Souvenir and Inauguration of Exhibition			11:10 AM	
	TEA BREAK AND STALL VISIT			11:15 AM	11:30 AM
	Automation for I.I.O.T.				
	Session -1 :	Organization	Speaker	11:30 AM	1:00 PM
1	KEYNOTE ADDRESS:				
	i. MR. ANIL BHATIA - VICE PRESIDENT & MANAGING DIRECTOR	Emerson Automation Solution			
	ii. MR. ANIL KUMAR - MANAGING DIRECTOR	Royal Haskoning DHV			
2	ARTIFICIAL INTELLIGENCE IN STEAM CRACKING MODELING: A DEEP LEARNING ALGORITHM FOR OPTIMISATION OF FURNACE OPER ATIONS	GAIL	Mr. Manu Mehta Mr. Chirag Gupta		
3	SAFETY AGAINST LIGHTNING	EATON	Mr. Aneesh VN		
4	SUSTAINABILITY TECHNOLOGIES FOR HYDROGEN VALUE CHAIN	EMERSON	Ms Poonam Parmar Mr. Aravind Singla		
	SMART QUIZ SESSION				
	NETWORKING LUNCH BREAK AND STALL VISIT			1:00 PM	2:00 PM
	I - Industry 4.0 & Digitization				
	Session- 2 :	Organization	Speaker	2:00 PM	03:30 PM
	OPENING ADDRESS BY SESSION CHAIR				
1	ONLINE DIGITAL TWIN MODELS FOR PIPELINE INTEGRITY A ND CUSTODY TRANSFER OF NATURAL GAS	GAIL	Mr. Pankaj Gupta Mr. D Sakthiwel		
2	O-PAS - THE PROCESS AUTOMATION OPENS UP	PHOENIX	Mr. Vishal Kumar		
3	POTENTIAL CYBERSECURITY THREATS TO THE DIGITAL POWE R INDUSTRY - FROM SUPPLY CHAIN TO SUBSTATION AND THEIR ZEROTRUST STRATEGIES	TxONE	Mr. Yenting Lee Mr. Debraj Chakraborty		
4	INDUSTRY 5.0: LOOKING INTO THE FUTURE	NTPC	Mr. Alok Kumar Sinha, Mr. P.K Gupta, Mr. Sumit Kumar Haldar		
	SMART QUIZ SESSION				
	TEA BREAK AND STALL VISIT			03 30 PM	04:00 PM
	I - Innovation				
	Session - 3	Organization	Speaker	4:00 PM	5:00 PM
	OPENING ADDRESS BY SESSION CHAIR				
1	NEXT GENERATION CONDITION MONITORING SOLUTION	FORBES MARSHALL	Mr. Mukesh Vyas		
2	MICRO MODULAR SMART SAMPLE CONDITIONING SYSTEM	SPIRARE ENERGY PVT. LTD.	Mr. Chandan Sanyal Mr. Justin Bieber		
3	PHOTONIC MOLECULAR TECHNOLOGY FOR HEALTH MONITORING OF CRITICAL EQUIPMENT USED IN REFINERY AND PIPELINE	PYROTECH	Mr. Biren Shah Mr. Kuldeep Rathore		
4	ENHANCING RELIABILITY & RESILIENCE OF GENERATION THROUGH CYBER SECURITY	NTPC	Mr. Alok Kumar Sinha Mr. Kuldeep Singh Yadav		
	SMART QUIZ SESSION				
	STALL VISIT			5:00 PM	6:00 PM
	NETWORKING DINNER			6:30 PM	9:00 PM

Petroleum & Power Automation Meet

PROGRAM DETAILS

DAY-2 13-May-2023

	O - Operation				
	Session - 4 :	Organization	Speaker	09:30 AM	11:00 AM
	OPENING ADDRESS BY SESSION CHAIR				
1	APPLICATION OF DIGITIZATION IN AUTOMATION OF PROCESS INDUSTRY & CYBER SECURITY CHALLENGES	HMEL	Mr. Kailash Kumar Mr. Shirish Mishra		
2	SECURING OPERATIONAL TECHNOLOGY (OT): ADDRESSING DIGITAL RISKS IN BUSINESS-CRITICAL INFRASTRUCTURES	SCHNEIDER	Mr. Kirankumar Vyas Mr. Priyesh Mistry		
3	CHAT WITH CISOS ON "FRAMEWORK FOR CYBER RESILIENT CRITICAL INFORMATION INFRASTRUCTURE WITH ROADMAP FOR GRC" MODERATOR: MR. SOMENATH KUNDU, DGM & ALT. CISO, NTPC	1. CISO - ONGC 2. CISO - PGCIL 3. CISO - NTPC 4. CISO - IOCL 5. ALT. CISO - EIL 6. CISO - GAIL 7. CISO - NHPC	1. Mr. Paparaju Buddhavarapu 2. Mr. Anand Shankar 3. Mr. Akshaya Kumar Patel 4. Dr. Yask 5. Mr. Jaspreet Bindra 6. Mr. Susheel Kumar 7. Mr. Anirudh Gupta		
	SMART QUIZ SESSION				
	TEA BREAK AND STALL VISIT			11:00 AM	11:15 AM
	Session - 5 :				
	PRESENTATION & DEMO ON 'Digital Twins, Digital worker enablement and optimization'	Rockwell Automation India Ltd.	Mr. Sandeep Redkar & Team	11:15AM	12:00 PM
	T - Transformation				
	Session - 6 :	Organization	Speaker	12:00 PM	1:00 PM
	OPENING ADDRESS BY SESSION CHAIR				
1	DIGITAL TRANSFORMATION OF PROCESS PLANTS - AN INTRO DUCTION TO ETHERNET – APL	P&F	Mr. Binoy Kamath		
2	EARTHQUAKE EARLY WARNING SYSTEM	EIL	Mr. Saikat Bhowal Mr. Javed Akhtar		
3	TRUE TUBE SKIN MEASUREMENT DEVELOPED BY R&D CENTER	WIKA	Mr. Navjyot Singh		
	SMART QUIZ SESSION				
	NETWORKING LUNCH BREAK AND STALL VISIT			01:00 PM	02:00 PM
	TRENDS IN AUTOMATION				
	Session - 7 :	Organization	Speaker	02:00 PM	03:45 PM
	OPENING ADDRESS BY SESSION CHAIR				
1	AUTOMATION OF STRIPPER TRACKING CALCULATIONS IN SCL AIRTECH BASED LLDPE PLANT AT GAIL PATA	GAIL	Mr. Manupati Sravan Kumar Md. Shahid Jamal Mr. Aritra Bhattacharya Mr. Priyanshu Raj		
2	EMERGING TRENDS AND DEVELOPMENTS IN INDUSTRIAL AUTOMATION	RITTAL	Mr. Abhinav Gurkhoo		
3	OPERANTIONAL TRANSFORMATION OF SALAL POWER STATION - A CASE STUDY	NHPC	Mr. Dharmesh Kumar Singh		
4	O-PASTM AND RELIANCE INDUSTRIES LIMITED	RIL	Mr. Divyang Shah Mr. Vaibhav Yagnik		
5	AUTOMATION & CALIBRATION IN IIOT PLATFORM	FLUKE	Mr. Kaushik Thirumalachar Mr. Satyajit Nath		
	SMART QUIZ SESSION				
	TEA BREAK AND STALL VISIT			03:45 PM	4:15 PM
	TAKEAWAYS AND PATH FORWARD				
	Session - 8 :				
1	EXPERTS FROM VARIOUS INDUSTRIES			4:15 PM	4:45 PM
2	FELICITATION TO EXHIBITORS FOLLOWED BY LUCKY DIP DRAW			4:45 PM	5:15 PM
3	VOTE OF THANKS BY SECRETARY - ISA-DELHI	IOCL	Mr. Raja Sekhar Gudipaty	05:15 PM	
	*********** EVENT NEXT ***********				


Take Charge
To take charge and be sure your operations and system are in sync at optimal capacity, you need to be atop autonomy. And to get there, Yokogawa delivers resilient solutions for you, a process using our smart manufacturing and IA2IA (Industrial Automation to Industrial Autonomy), deploying OpreX as our true enabler to achieve total optimization throughout the supply chain. Integrating discrete systems in society, we move together with you toward the system of systems in which everything is intricately connected and goals are achieved beyond those of a single system. Yokogawa. Atop autonomy for the planet.
OpreX™

TECHNICAL PAPERS

TECHNICAL PAPERS
Session 1

Session 1

1. Sustainability Technologies for Hydrogen Value Chain-Emerson
2. Safety Against Lightening-EATON
3. Artificial Learning in Steam Cracking Modelling-GAIL

ARTIFICIAL INTELLIGENCE IN STEAM CRACKING MODELING: A DEEP LEARNING ALGORITHM FOR OPTIMISATION OF FURNACE OPERATIONS

Manu Mehta, Chirag Gupta
GAIL (India) Ltd, Pata

ABSTRACT

The carburizing and coking of ethylene cracking furnace tubes are the important factors that affect the energy efficiency of ethylene production. To realize the diagnosis and prediction of degree of coking in the cracking furnace tubes, and then take corresponding treatment measures, is of paramount importance. One such implementation has been discussed to maximize the furnace run length (optimization of increment in CPR i.e. Coil pressure ratio which is a direct indicator of degree of coking), through a Deep learning (DL) algorithm named Long Short Term Memory (LSTM) network, to further enforce the Industry 4.0 revolution claims that by introducing machine learning/deep learning into these fields, substantial economic and environmental gains can be achieved.

KEYWORDS

Artificial Intelligence, Machine Learning, Deep Learning, Industry 4.0, Real Time Optimization, Digital Twin Model, Optimization.

INTRODUCTION

In Gas Cracker Unit (GCU-II), basic process control philosophy has been employed through Emerson DCS. In a bid to survive and thrive in the digital era, we ought to have a technology platform that enables rapid innovation and response to changing business environment. Hence, one such case study has been presented for furnace operation to predict optimum COT (Coil outlet temperature) for cracking in order to maximize the furnace run length, through various Machine learning/Deep learning (ML/DL) techniques.

AI techniques excel at tackling highly complex and nonlinear problems. Therefore, application of these methods to the modeling of the reactor section of the steam cracking process, which is itself complex and nonlinear, will deliver models that are expected to outperform traditional detailed kinetic models in both execution speed and accuracy.

Steam cracking is a process in which saturated hydrocarbons (alkanes) are broken down into smaller, unsaturated hydrocarbons(alkenes). The steam cracking furnace consists of 3 broad sections: Radiation section, Convection section & Stack section. The most important parameter governing the products of cracking is the temperature at which cracking takes place, and that is kept under control by the coil outlet temperature (COT). Optimization of all the inter related parameters shall involve controls that evaluate trade-offs between increment in CPR (coil pressure ratio) and cracking efficiency and choose the operating conditions which increase furnace yield.

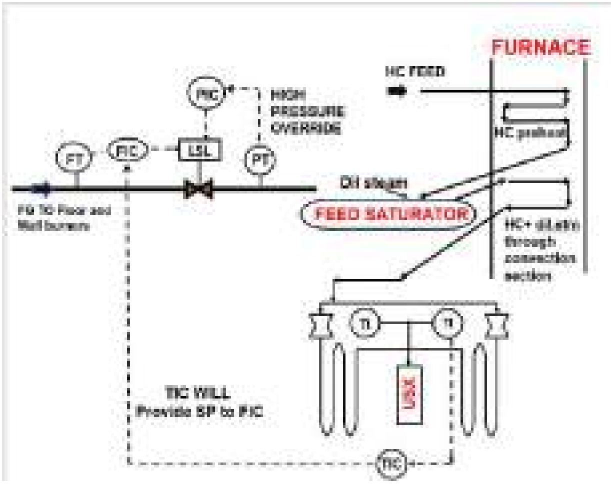
Traditionally, the operators, based on their knowledge, experience and guidelines provided by the licensor have selected these operating conditions. An attempt to thoroughly analyze these complex controls through several algorithms has been presented in this paper. The analysis ensures that sufficient real time data is available to improve on the existing offline guidelines and that the benefit for each scheme justifies its incremental cost.

OVERVIEW OF THE EXISTING & PROPOSED CONTROL SCHEMES

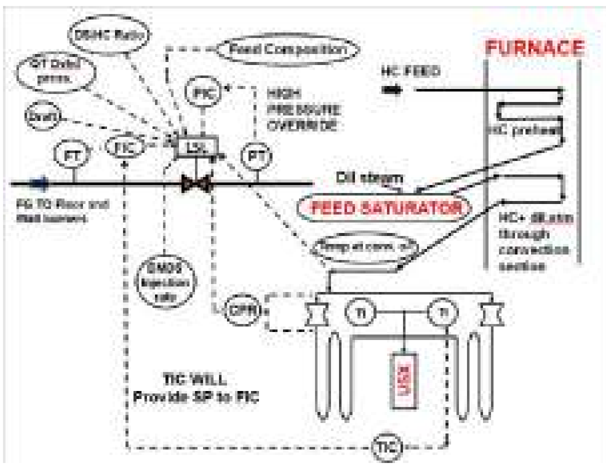
Since coke formation on the inner walls of furnace coils is a highly complex and non-linear process, in order to estimate this parameter we require to delve deep into the chemical engineering involved in this. Some of the reasons as to why we’ve chosen the modeling technique are:

1. However effective, reliable and best in class basic process control strategies are, one thing that they lack is consideration of MIMO, i.e. how multiple input variables can affect multiple output variables and interdependency between them. Also, to some extent, how changes in PID settings of one loop can affect another coupled loop is difficult to infer through basic process control philosophy, this is taken care of by operators based upon their experience and knowledge base.
2. Advanced process control strategies can take care of the point, for instance the case study presented is based upon deep learning framework which considers effect of 10 input variables on 1 output variable. This also can help to better understand and analyze, in real time, various operating ranges of furnace parameters.
3. This strategy can act as a first step to usher into an era of digitalization and complete process automation.

The figures below depict the existing COT control strategy and proposed control strategy.



EXISTING COT CONTROL SCHEME



PROPOSED COT CONTROL SCHEME

METHODS AND DATA ANALYSIS

Step 1: Selection of relevant process parameters for modelling: Based upon empirical studies and information furnished by the licensor, the input parameters which affect the increment in CPR over a run length of furnace are as follows:

a) Feed composition i.e., percentage of each Ethane, Propane and Butane
b) Saturated feed flowrate.
c) COT (Coil outlet temperature)
d) Temperature at convection section outlet.
e) Furnace draft at steady load.
f) Average flowrate of DMDS.
g) Quench tower overhead pressure.
h) Dilution steam to HC ratio in the feed.

Step 2: Data collection and cleaning: The dataset ranges from February 2018 to November 2021. But not all data is relevant, i.e., there are instances where values were not healthy or outside of expected operating range, hence such data has been eliminated. The sampling frequency is 10 minutes, hence 156,405 samples in total. Post data cleaning using various exploratory data analysis tools, the total no. of samples is 148,277.

Step 3: Selection of modeling algorithm:

3.1. TRADITIONAL TIME SERIES TECHNIQUES

There exist a host of techniques which can provide solution for sequential, time-series data, most prominent of which are mentioned below:

a) Traditional algorithms like ARIMA (Auto regressive moving average), ARIMAX (Auto regressive moving average with exogenous inputs), SARIMA (Seasonal ARIMA) and SARIMAX (Seasonal ARIMA with exogenous inputs).
b) State of the art Deep learning algorithms involving LSTMs (Long short-term memory units).

As the name suggests, SARIMAX model is built upon the following facts:

1) The variable which we need to predict dynamically is directly dependent on its own past values that constitutes the AR part (Auto regressive).
2) The MA (Moving average) part indicates that the regression error is actually a linear combination of error terms whose values occurred contemporaneously and at various times in the past.
3) The I (Integrated) indicates that the data values have been replaced with the difference between their values and the previous values.
4) S (Seasonality) signifies that the data is following a certain seasonal trend.
5) X (Exogenous inputs) considers the effect of

external variables/factors on the predicted variable.

The equation describing the aforesaid points is given below:

$$d_t = c + \sum_{n=1}^{p} \alpha_n d_{t-n} + \sum_{n=1}^{q} \theta_n \epsilon_{t-n} + \sum_{n=1}^{r} \beta_n x_{n_t} + \sum_{n=1}^{P} \phi_n d_{t-sn} + \sum_{n=1}^{Q} \eta_n \epsilon_{t-sn} + \epsilon_t$$

The AR (blue), MA (purple), X (green), S (yellow) components are just added together. We can easily tune up or down the complexity of our model by adding or removing terms and switching between raw and differenced (red) data, to create ARMA, SARIMA, ARX etc. models.

Shortcomings of this technique are as follows:

a) The most apparent and visible fallout of using this technique is that it would work very well if the predicted and predictor variables are linearly dependent. But in our case, it is not so, and it was validated by the results we obtained.

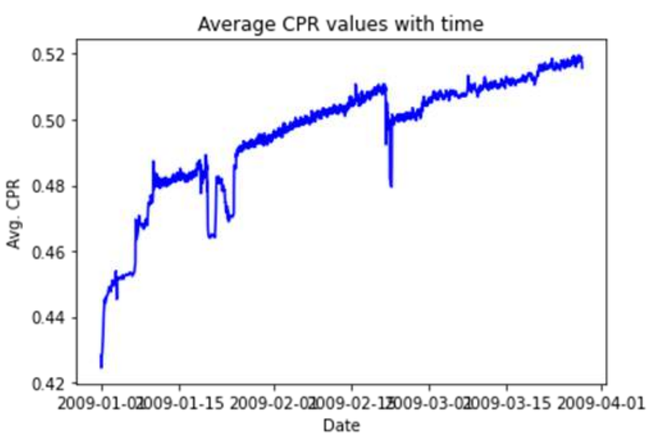


Figure 1

The plot shown above shows the trend of CPR values (total sample count is 9974) collected over a given duration of time (August 2020 to January 2021). 80% of this data was used for training and remaining was tested upon the built model. The plot given below shows the result on testing data (predicted values are shown by blue plot and actual values are in red):

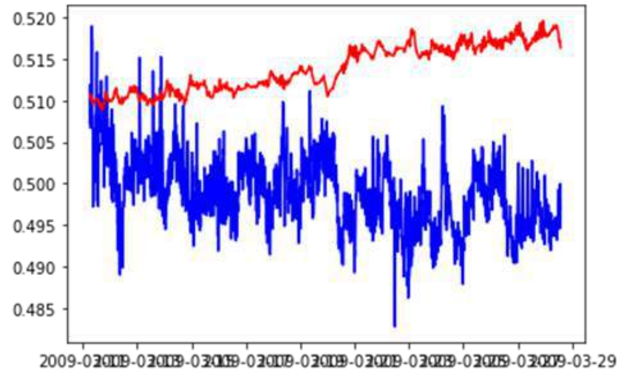


Figure 2

b) This technique can work well if the dataset is relatively small and easy to model. Our case study is a complex process which is highly non-linear.

3.2. DEEP LEARNING TECHNIQUE INVOLVING LSTMs

Long Short Term Memory (LSTM) networks are a type of recurrent neural network capable of learning order dependence in sequence prediction problems, our case study being one of them as increment in CPR is not only dependent on other factors but also time. Unlike the methods discussed above, these networks can capture the dynamicity of the data, hence are suited best for forecasting purposes. A LSTM layer consists of a set of recurrently connected blocks, known as memory blocks. These blocks are analogous to a differentiable version of the memory chips in a digital computer. Diagram shows the same:

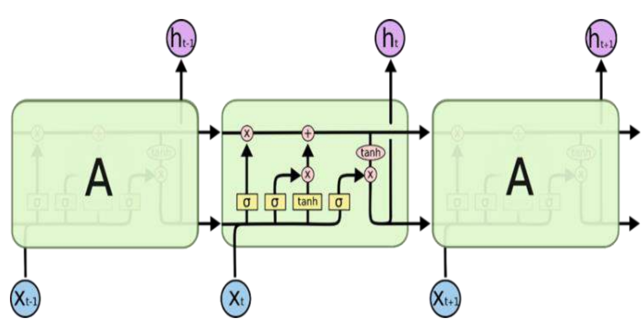


Figure 3 shows the input and outputs of an LSTM for a single timestep. This is one timestep input, output, and the equations for a time unrolled representation. The LSTM has an input x(t) which is the input sequence. h(t-1) and c(t-1) are the inputs from the previous timestep LSTM. o(t) is the output of the LSTM for this timestep. The LSTM also generates the c(t) and h(t) for the consumption of the next time step LSTM.

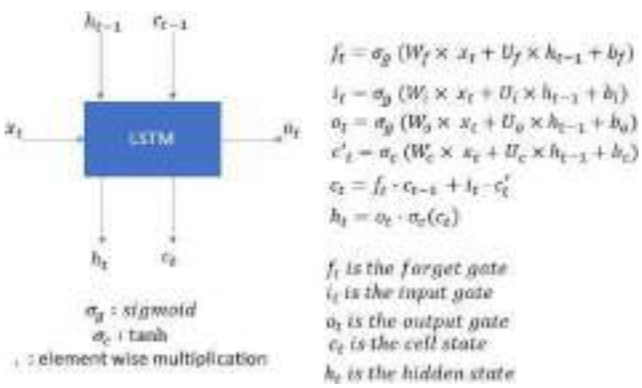


Figure 3

Step 4: Model Development and Accuracy

Our goal is to forecast CPR values 100 minutes into the future given 1440 minutes (24 hours) of historic data consisting of 10 input variables.

```
[ ] class FeedBack(tf.keras.Model):
      def __init__(self, units, out_steps):
        super().__init__()
        self.out_steps = out_steps
        self.units = units
        self.lstm_cell = tf.keras.layers.LSTMCell(units)
        # Also wrap the LSTMCell in an RNN to simplify the `warmup` method.
        self.lstm_rnn = tf.keras.layers.RNN(self.lstm_cell, return_state=True)
        self.dense = tf.keras.layers.Dense(num_features)

[ ] feedback_model = FeedBack(units=32, out_steps=OUT_STEPS)

    def warmup(self, inputs):
      # inputs.shape => (batch, time, features)
      # x.shape => (batch, lstm_units)
      x, *state = self.lstm_rnn(inputs)
      # predictions.shape => (batch, features)
      prediction = self.dense(x)
      return prediction, state

[ ] FeedBack.warmup = warmup

[ ] prediction, state = feedback_model.warmup(w1.example[0])
    prediction.shape

    TensorShape([32, 9])
```

Figure 4

After some pre-processing steps to make the data appropriate in a form to be fed to the network, the core part of the code, the model architecture, is shown in Figure 4.

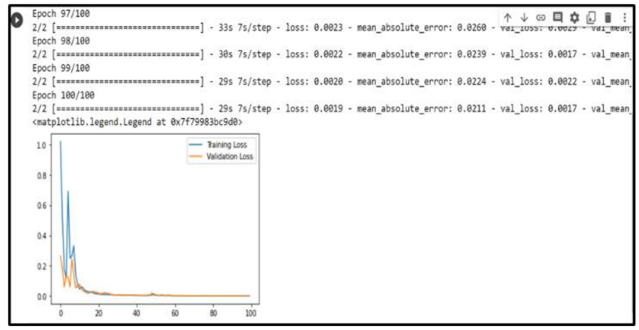


Figure 5

Figure 5 depicts the loss curves for training and validation data in blue and orange colors respectively. Training has been done over 100 epochs with a learning rate of 0.002. Train and validation losses obtained are 0.0019 and 0.0017 respectively.

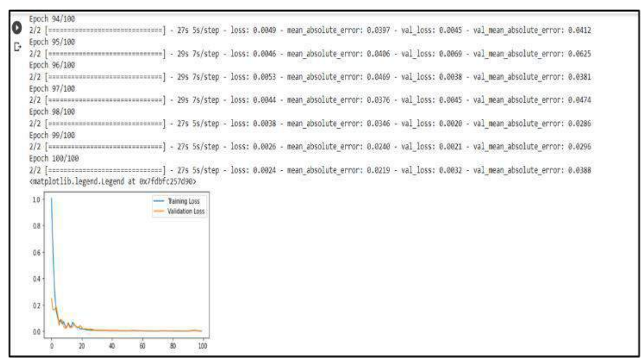


Figure 6

Figure 6 depicts the loss curves for training and validation data in blue and orange colors respectively. Training has been done over 100 epochs with a learning rate of 0.001. Train and validation losses obtained are 0.0024 and 0.0032 respectively.

Based upon the accuracies obtained, model with a learning rate of 0.002 is selected due to lower loss, although both the models achieve highly accurate results.

RESULTS & CONCLUSION

Since a batch of input sequence contains 24 hours of data and the model predicts 100 minutes of data, therefore the actual and predicted values of CPR are shown in the plots below for 92 such batches of unseen input data. Blue plot shows the actual CPR values and the orange plot depicts the model prediction.

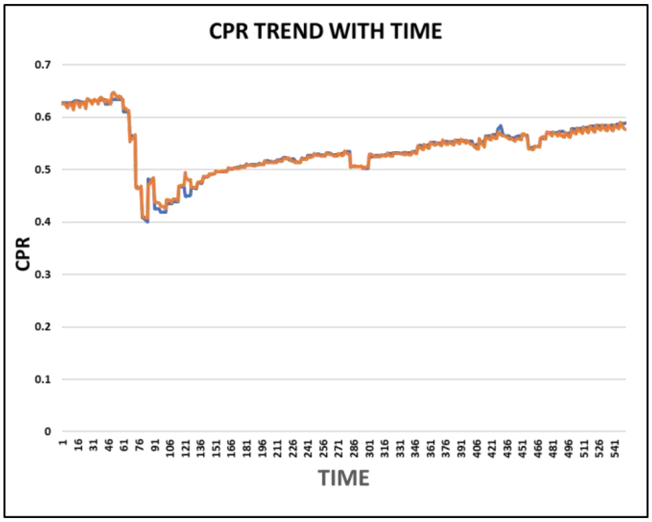


Figure 7

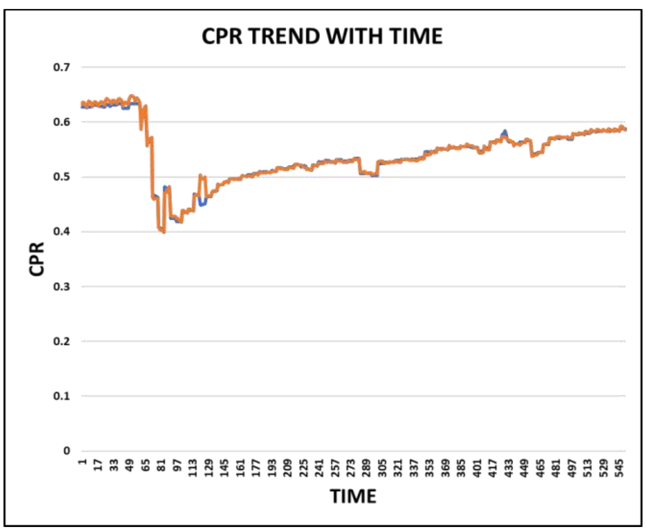


Figure 8

Figures 7 & 8 show the predictions with a learning rate of 0.001 and 0.002 respectively.

Hence, 100 minutes of forecast of CPR values based upon input parameters of past 24 hours has been obtained within limits of modeling accuracy.

Our target is to forecast the values 24 hours into the future, as the best models generally do in real world scenario.

When the model is fully implemented, benefits that it can offer in its advanced stages are:

a) This sort of advanced strategy for control shall enable the operators to push the process out of the comfort zone towards the optimum performance while still honoring the plant operating constraints. For instance, product composition specifications, metallurgical limits of furnace coils.

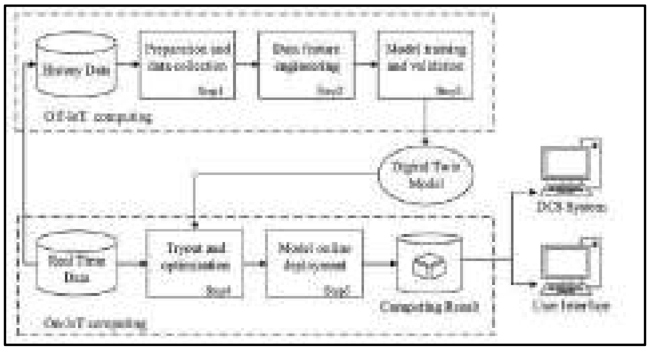
b) Operators would be able to identify what parameters need to be adjusted to balance the tradeoff between the increment in CPR and cracking efficiency and hence the optimum operating range of COT.

c) Advanced control and Real Time Optimization (RTO) benefits are field proven and generate high rates of return on investment. Typical benefits include increased throughput, reduced energy usage, decreased operating costs, increased operating flexibility, and reduced downtime.

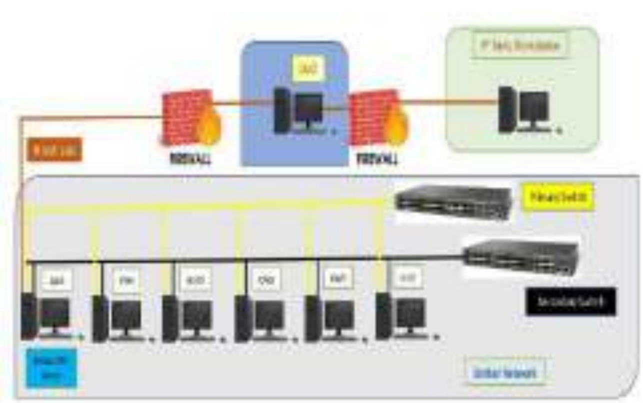
d) Usage of such AI/ML techniques will significantly help in resource planning for shutdown of furnace cells in a predictive manner and improved process safety in form of process watchdog and earlier identification of problems.

RECOMMENDATIONS

The model has been successfully tested in offline environment. To realize its true potential in the form of RTO, integration of Historian data server with the 3rd party server (the server which will be the host of the model) is required. Model deployment pipeline is shown in the figure below:



In line with the pipeline shown, one such architecture has been devised which will be the prototype of our DIGITAL TWIN model:



Real Time Data Collection via OPC

REFERENCES

1. https://www.tensorflow.org/tutorials/structured_data/time_series#next_steps.
2. Otegui, J.L.; Bona, J.D.; Fazzini, P.G. Effect of coking in massive failure of tubes in an ethylene cracking furnace. Eng. Fail. Anal. 2015, 48, 201–209.
3. Albright, L.F.; Marek, J.C. Mechanistic model for formation of coke in pyrolysis units producing ethylene. Ind. Eng. Chem. Res. 1988, 27, 755–759.
4. Applications of artificial neural networks in chemical problems K. Suzuki (Ed.), Artificial neural networks—architectures and applications, InTech, Rijeka (2013), pp. 203-223.
5. H. Lasi, P. Fettke, H.G. Kemper, T. Feld, M. Hoffmann: Industry 4.0 https://link.springer.com/article/10.1007/s12599-014-0334-4

BIOGRAPHIES

Sh. Manu Mehta was born in Meerut, India in the year 1987. He graduated in Instrumentation and Control Engineering from Bharati Vidyapeeth College of Engineering, Delhi. He joined GAIL (India) Ltd. in the year 2009. He also completed MBA in Oil & Gas from UPES, Dehradun in 2015.At present, he is working as Chief Manager, Instrumentation department, Petrochemical Maintenance in GCU-II, Petrochemical Complex, Gail Pata**.** He has myriad experience of over 13 years at Gas Cracker Unit, both old and new plants specific in Gas fired Furnace controls and safety systems as well as steam turbine driven rotating machines.

Sh. Chirag Gupta was born in Delhi, India in the year 1997. He graduated in Instrumentation and Control Engineering from Netaji Subhas Institute of Technology (NSIT), Delhi. He joined GAIL (India) Ltd. in the year 2019. At present, he is working as Senior Engineer, Instrumentation department, Petrochemical Maintenance in GCU-II, Pata Petrochemical Complex, Gail Pata**.**

Setting the Standard for Automation™

ISA Delhi Section

Protection against Lightning

Key applications of Surge protective devices

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

1

Speaker profile

•Aneesh VN Joined Eaton in 2018 and working as Product Line Manager, Eaton- MTL SPDs. He is involved in the development and introduction of Surge protective devices for critical applications in harsh and hazardous environment. Aneesh is a graduate from Kannur University, Kerala in Electrical and Electronics Engineering with more than 17 years of experience in the field of Lightning protection system & Surge Protective Devices. He has conducted many site studies and more than 500 technical presentations to industries which includes Oil& Gas, Process, Chemical, Utilities, Pipeline, Marine, Pharma and Defense

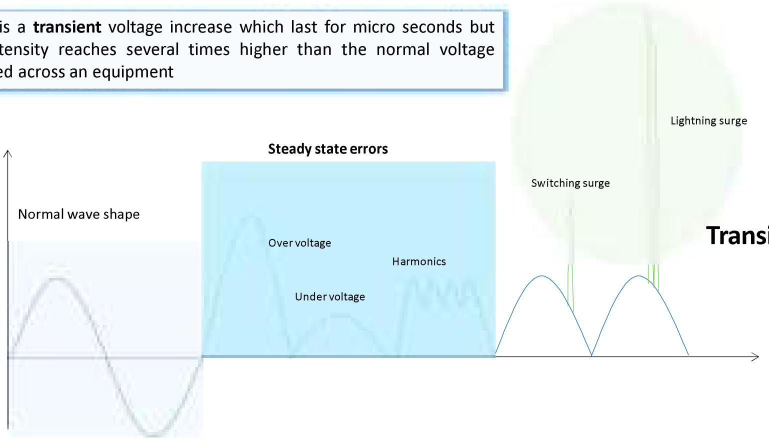
2

Content

1) What is Surge?
2) National and International Standards
3) Definition of Lightning Protection System (LPS)
4) Surge wave shapes
5) Recommendation of SPD in a Process Plant-(Power, Data & Signal)
6) SPD technologies and Operation
7) Common mode and differential mode of protection
8) Application Example- Power , Signal, Data and communication SPDs

What is Surge?

Surge is a **transient** voltage increase which last for micro seconds but the intensity reaches several times higher than the normal voltage supplied across an equipment



Transient Errors

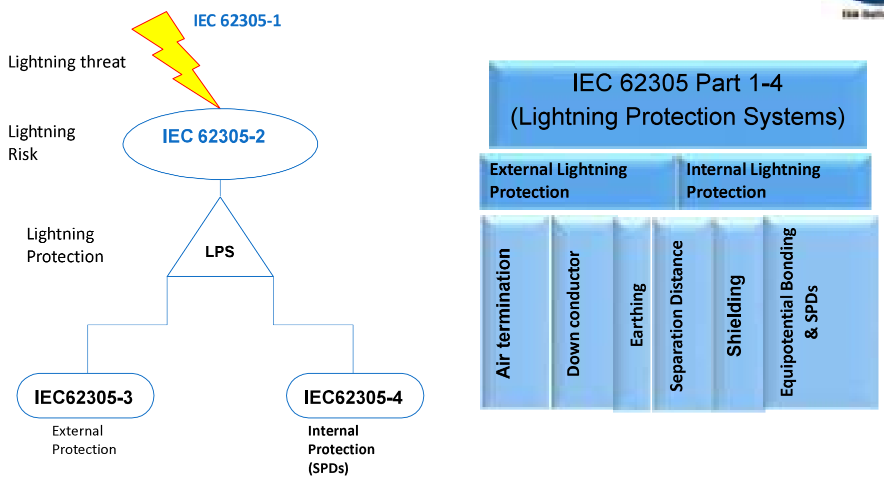
International standards on Lightning & Surge Protection

IEC 62305-1:2010 Protection against lightning – Part 1: General principles
IEC 62305-2:2010 Protection against lightning – Part 2: Risk Management
IEC 62305-3:2010 Protection against lightning- Part 3: Physical damage to structures and life hazard
IEC 62305-4:2010 Protection against lightning – Part 4: Electrical and electronic systems within structures

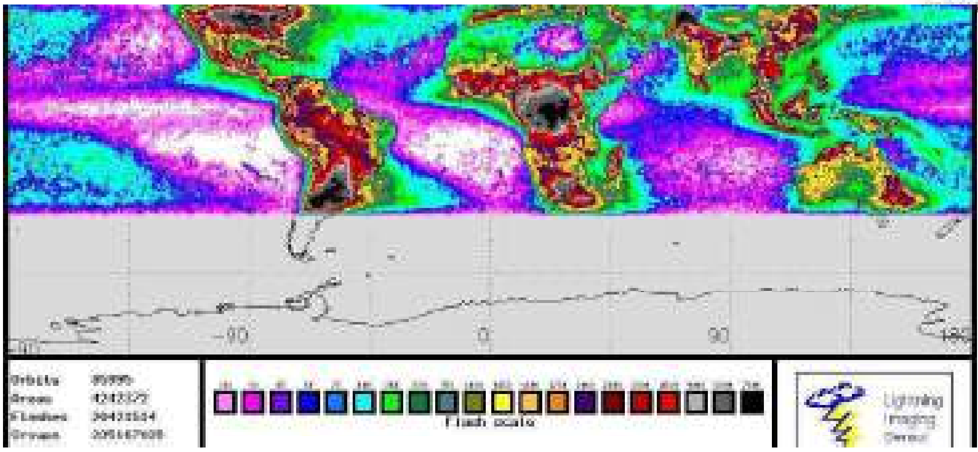
UL96: Standard for Installation Requirements for Lightning Protection Systems
UL1449,5th Edition: Standard for Surge Protective Device
UL497A : Secondary Protectors for Communication circuits
UL497B: Protectors for Data communications and fire alarm circuits

IEC 61643-12:2020 Low-voltage surge protective devices –Part 12: Surge protective devices connected to low-voltage power distribution systems - Selection and application principles
IEC 61643-11:2011 Low-voltage surge protective devices – Part 11: Surge protective devices connected to low-voltage power systems - Requirements and test methods
IEC 61643-22:2015 Low-voltage surge protective devices – Part 22: Surge protective devices connected to telecommunications and signalling networks - Selection and application principles
IEC 61643-21:2000+AMD1:2008+AMD2:2012 Low voltage surge protective devices - Part 21: Surge protective devices connected to telecommunications and signaling networks - Performance requirements and testing methods

Complete Lightning Protection System(LPS)



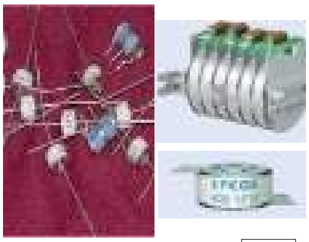
World Lightning Map- NASA



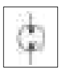
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

7

SPD Technologies



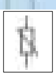
Gas Discharge Tubes (GDT)
Spark Gaps(SG)



Voltage switching device
High surge current
Low capacitance

Low response time
Risk of follow current

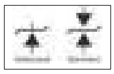
Metal Oxide Varistors (MOV)



Voltage limiting device
High surge current
Faster response time

Limited lightning current capacity
Degradation and leakage current

Silicon Avalanche Diodes(SAD)



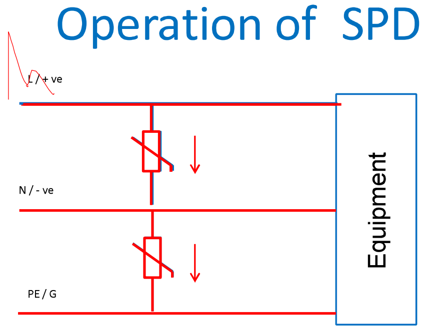
Voltage limiting device
Precise clamping
Faster response time

Limited surge capacity
Not suitable for service entry protection

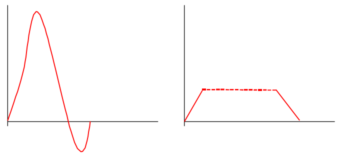
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

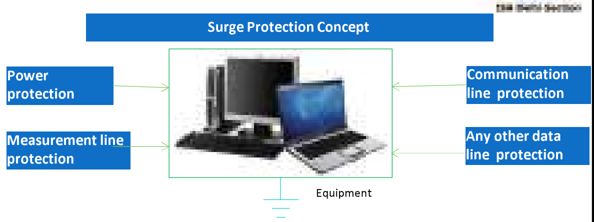
8

Operation of SPD



SPD limits/switches the surge voltage and diverts the surge current.



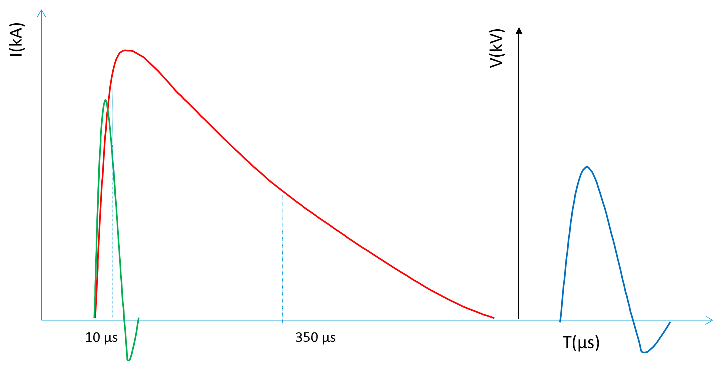


Even the best surge protection device will not be effective, unless all the services connected to the equipment are protected by an SPD

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

9

Different surge wave shapes



10/350µS
Simulated wave shape to demonstrate Partial Lightning current
Source: Lightning strike

8/20µS
Induced effect of lightning current/ Switching surges
Source: Near by lightning
Switching of breakers
Motors
Capacitor bank switching

1.2/50µS
Open circuit voltage wave shape

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

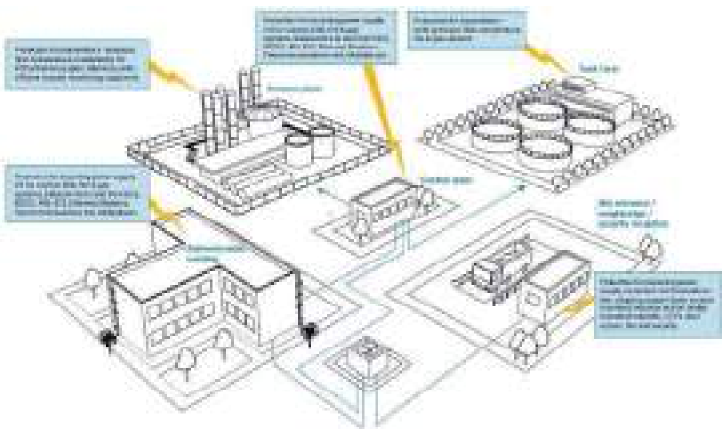
10

Source and damage according to IEC62305

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

11

Schematic illustration of SPDs in process plant



ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

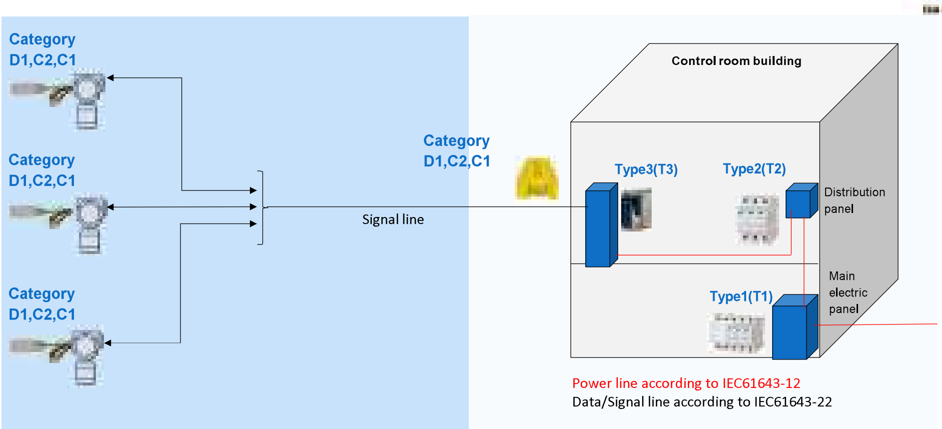
12

Application example of SPDs

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

13

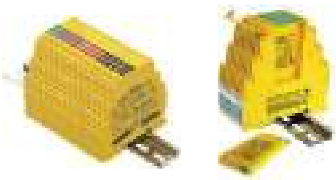
Recommendation of SPDs for Power & Signal



ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

14

Protection Concept in Process environments



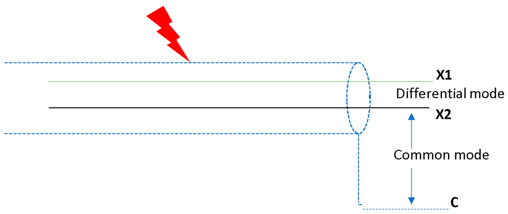
Signal surge protection

For I/Os, Profibus, Modbus, Foundation fieldbus, RTDs.

Transmitter surge protection

For 2 wire, 3 wire, 4 wire , Profibus-PA, Foundation field bus

Common and Differential mode protection

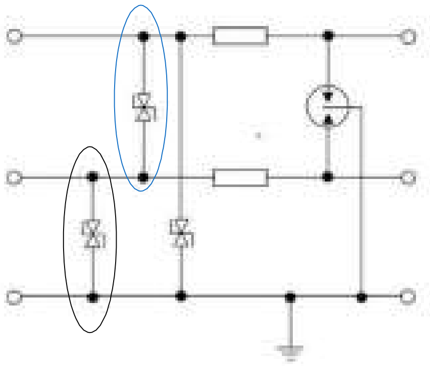


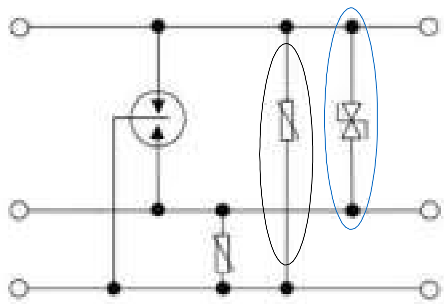
Common mode interference always occurs between signal line and Earth.
Differential model interference always occurs between the signal line

According to IEC61643-21 standards, Common mode (X1-C and X2-C) is must, X1-X2 is optional.

When it comes to the protection, both common mode and differential mode protection is required

Protection topology (Common- Differential mode)



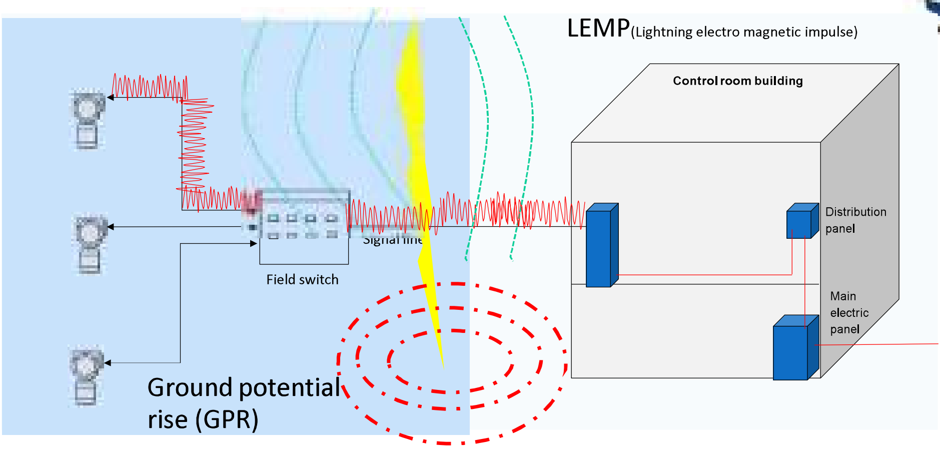


SD Range:Hybrid surge protection for 2 wire , 3 wire application

TP Range:Hybrid 3 stage surge protection for 2 wire , 3 wire,4 wire application

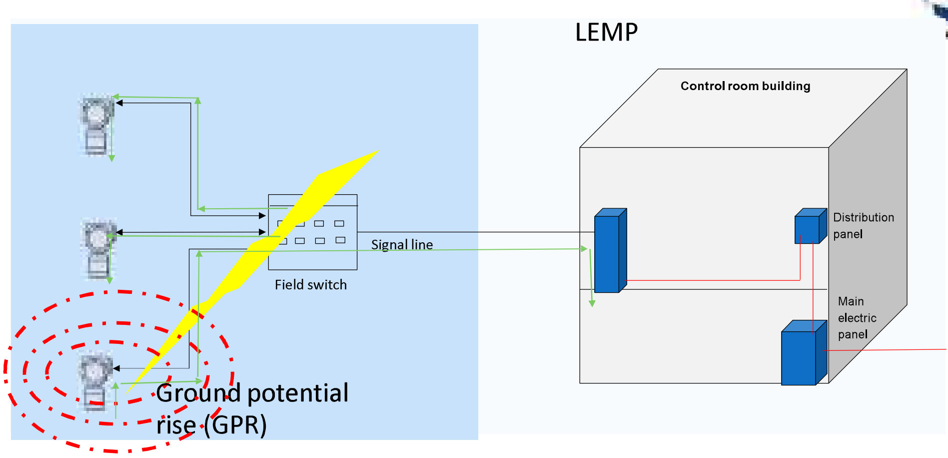
17

LEMP in installations in a plant



18

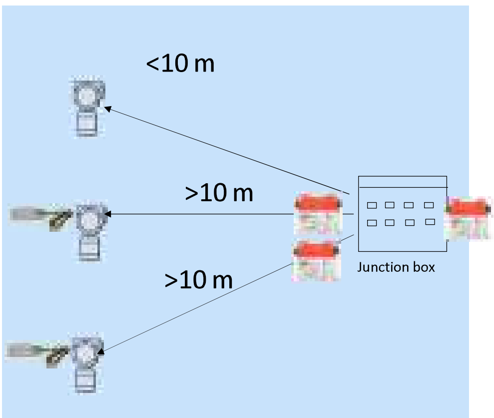
GPR in installations in a plant



ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

19

Protective distance



According to IEC61643-12,
If the distance between the SPD and the equipment to be protected is **too large**, **oscillations** could lead to a voltage at the equipment terminals which is generally up to two times higher than *U*p but, under some circumstances, can even exceed this level

Recommended Protective Distance **<10 meter**

If the protective distance is more than 10 meter, install another SPD close to the equipment

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

20

Power surge protection devices

Type 1 SPD
Main Panel

T1+T2 SPD
100kA(10/350µS)/Phase
Suitable for LPL I-IV

Type 2 SPD
Distribution Board

T2 SPD
I max-40kA(8/20µS)

Type 3 SPD
Equipment level

T3 SPD
240V and 120V versions
Itotal- 20KA(8/20µS)

Signal Surge protection devices

- 7mm, compact SPD with Com& Diff mode protection
- 20KA surge rating
- 07V-55V to suit all I/O applications
- Fuse disconnect, High bandwidth, 3 wire, RTD, PSTN ,120V and 275V versions
- Versions for RS232,RS422, RS485

Field equipment Protection solutions

MTL TP48
4-20mA, 2,3,4 wire

MTL TP32
2wire+Earth ,Profibus-PA/ Foundation fieldbus

MTL TP-AC
4 wire+Earth
100-277V AC+ 4-20mA/Profibus-PA/ Foundation fieldbus

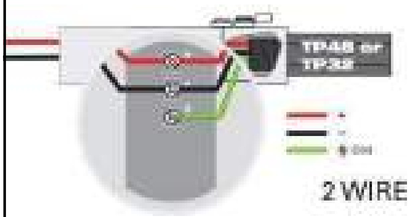
MTL TP-Pipe
2wire+Earth, Series
4-20mA ,FFB/Profibus-PA

MTL 24/7
4wire+Earth,
1pair-10-24V
1pair-RS485

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

23

Specification & Connection details



20KA Surge rating
Common & Differential mode protection
½"NPT,M20, ½"BSP threads
IP66 with SS316 housing

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

24

Communication Surge protection

- Dial up, Leased line,T1,ADSL
- CAT5, CAT5e, CAT6
- POE,POE+ Cameras
- DIN rail mounting/surface mounting

- Foundation™ fieldbus, Profibus PA
- 20KA Surge Protection
- GDT isolation to Shield –Ground

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

25

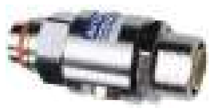
Radio Frequency Surge protection

GT range

DC — 2.5GHz
40KA Surge rating
N,SMA,BNC,TNC

FGT range

DC — 2.5GHz
20KA Surge rating
LMDS/RG 6 and LMDS/RG59 Cable. F connector



RGT range

DC — 4GHz, Replaceable Gas Tubes
7/16, N,BNC,TNC connectors

RGT range

410MHz — 6GHz
Up to 100KA Surge rating
7/16, N type connectors

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

26

Solutions for Zone 2 installations

MTL now offeres a comprehensive range of SPD with protection technique “Increased safety” Ex ec for “Power “ as well as “Signal” Protection. Both SD and SDM ranges are now ATEX and IECEX certified for Ex ec for Zone 2 installation.

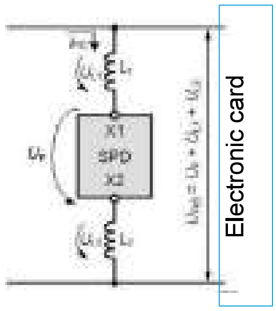
Also We have introduced MA15E for both 110V and 230V application with IECEX and ATEX certified for “Ex ec”

Application : Remote I/O installations

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

27

Installation-Parallel Connection of SPD



Connection of a Parallel SPD

U_{L1} / U_{L2} depends upon the wire length from signal line to SPD.
U_{L1}= L*di/dt
L= 1µH for 1 meter cable length
di/dt- Rate of change of current

1KA/µS surge current induces 1kV voltage on a one-meter wire length.

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

28

Global certification

- MTL SPD product lines carry comprehensive regulatory approvals for harsh and hazardous locations:
  - Global coverage extends market penetration
  - Free download of certificates from MTL website
  - Expert on-board certification resource

Sustainability Technologies for Hydrogen Value Chain

The demand for green H2 is greater than ever before, and many consider it to be one of the most vi - able near-future sources of energy. Addressing the nation on the 75th Independence Day (15th August 2021), Prime Minister Narendra Modi announced the **National Hydrogen Mission** with the aim of making India a hub for the production and export of green hydrogen. This is geared to make India energy independent before the country completes 100 years of its independence in 2047. With proactive collaboration among innovators, entrepreneurs, and government, green hydrogen has the potential to drastically reduce CO2 emissions, fight climate change, and put India on a path towards net-zero energy imports.

The Challenge to meet Sustainability goals while simultaneously improving Safety, Availability, and Profitability in a constrained capital environment is real. At Emerson, we call it the 'dual challenge'. Emerson delivers value with Intelligent Field solutions through pervasive sensing and intelligent edge. Pervasive sensing with a purpose provides tangible business results. Emerson is identifying areas where we can push intelligence to the edge to provide a quick, reliable response. From edge to enterprise from conceptualization all the way through the decommissioning of a facility, Emerson and AspenTech provide software that deliver customer outcomes. We are focused on providing safer and more sustainable operations, increased profitability, and improved reliability.

Recognizing that indeed Hydrogen is a sustainable answer to the growing energy demand, Emerson and AspenTech have come together to provide leadership in Automation and Software technologies for all stages of Hydrogen production, storage, transportation, and use. At production, it starts with enabling electrolysis innovation, improving blue and green hydrogen processes, and also Integrating renewables. We help prioritize investments, evaluate alternatives along overall Hydrogen value chain including feasibility and scaleup options to pursue high value markets.

Emerson and AspenTech are at the forefront of addressing the dual challenge, and we are excited to share our expertise and pioneering leadership in Automation and Software to help industry achieve their sustainability and profitability objectives.

John Rodrigues

Business Leader – Industrial Software

Emerson Automation Solutions, India

Jyotsna Joshi
Business Director

Sustainability and Decarbonisation

Emerson Automation Solutions, India

TECHNICAL PAPERS
Session 2

Session 2

1. Online Digital Twins for Pipeline Integrity - GAIL
2. O-PAS – Phoenix
3. Potential Digital Threats to Power Industry – TxOne
4. Industry 5.0 Looking into the future - NTPC

ONLINE DIGITAL TWIN MODELS FOR PIPELINE INTEGRITY AND CUSTODY TRANSFER OF NATURAL GAS

Pankaj Gupta
GAIL(India)Limited
Noida, India

D Sakthiwel
GAIL(India)Limited
Bengaluru, India

ABSTRACT

Gas Pipeline is the backbone of the energy infrastructure of any country and is going to gain far more importance with the increasing thrust of government towards energy security and self-reliance. With the increasing geographical area under coverage, challenges such as Safety related issues like Third party intrusions & pipeline leaks along with sustainable commercial existence by minimizing the losses on account of Mis-measurements & LAUF Gas accounting. For ensuring safety of the pipeline systems from issues like pipeline leaks, Pipeline industry deploys various pipeline leak detection system using Mass Balancing or Pressure Wave or other principles. However, the accuracy of the leak detection depends upon the accuracy of the associated instrumentation signals like flow, pressure ,temperature and gas quality parameters. More often than not, false positive or negative leak alarms are attributed to reliability and authenticity of the data provided by associated instrumentation system.

Recognizing the imminent need for development of online validation, audit and diagnostic systems which track ,monitor and predict the health of the instruments on their own without intervention of the operators and keep the operator updated in case of any deviations from normal course of operation was felt and a data analytics and diagnostic solution based on the basic principles of science and equipment operational philosophy/algorithms such as USM, GC and Flow Computers has been exploited to gain insight about the equipment operational behavior and prediction of condition of equipment. The solution uses information from relevant standards like : ISO, GPA ,AGA ,API and other relevant techniques like Control charts etc.

Keywords: Virtual Flow Computation, Online Validation and Audit, Digital Twin, Online Diagnostics, Data Acquisition and Aggregation

1. INTRODUCTION

Humongous investments are being done in execution of various pipeline projects so that even far flung geographical areas are also served with clean fuel. With the increasing geographical area under coverage following changes are being faced by pipeline industry:

(i) Safety related issues like Third party intrusions & pipeline leaks:

Pipeline industry deploys various pipeline leak detection system using Mass Balancing or Pressure Wave or other principles. However, the accuracy of the leak detection often depends upon the accuracy of the associated instrumentation system like flow, pressure ,temperature and gas quality parameters measurement. In case of any difficulty in reducing the false leak alarms, it is found challenging to establish the authenticity of data available from the primary instrumentation inputs. Although the Primary Meter (USM, TFM or RPD) is generally calibrated at ISO 17025 accredited flow calibration labs, the secondary instrumentations like pressure, temperature and gas quality instruments are calibrated in house using traceable master instruments. Being electronic devices it is always possible to observe drift in these instruments which may introduce a bias in the measurement and thus the accuracy of leak detection is impacted. An online system which validates the entire measurement system including primary meter and secondary measurement devices for any mis measurement with identification of the possible cause of drift/inaccuracy with recommended solutions to reinstate the measurement accuracy is the need of the hour.

(ii) Commercial issues like gas measurement, reconciliation and LAUF gas accounting:

For big pipeline Network operators, Gas reconciliation and LAUF gas accounting is also a challenge. Gas Reconciliation involves various aspects like measurement of Gas purchased, Gas Sold, System Use Gas and inventory as a stock in pipeline. Thus the network may consist of thousands of gas meters/measurement systems and means/software for determining the pipeline inventory. In case of any discrepancy in any of the gas meters at a given point of time may cost a company huge financial losses if not detected and corrected immediately. Thus a need for such an online DIGITAL TWIN for Virtual Flow Computation which monitors, validates and audits the gas measurement system on real-time basis is the need of the hour.

This paper tries to address the issue and challenges faced above with an ONLINE DIGITAL TWIN MODEL which monitors the gas measurement systems on real-time basis with a frequency as low as fraction of a second(user configurable) which can not only ensure validated flow values to third party software(like leak detection systems) as well as establishing the custody transfer measurement systems accuracy with online validation and diagnostics as per applicable AGA/ISO/GPA /API standards and regulatory requirements.

2. MATERIALS AND METHODS

While designing the system, past experience in handling metering stations was exploited to address the prevailing constraints at any in- service gas metering system. The system does online validation, audit trial and alarm management with following steps:

- (i) Data Acquisition and aggregation
- (ii) Analytical engine for DIGITAL TWIN for each equipment
- (iii) Alarms, Events and Reporting
- (iv) Local and Remote Data Storage

Thus the solution addresses one of the greatest challenge in Natural Gas metering systems in maintaining the accuracy and provide early detection and quick trouble shooting of ensuing problems/failures. This also helps in mis-measurement and thereby unnecessary arbitration between buyers and sellers. Apart from this, with the increased accuracy and confidence in the raw data to the leak detection systems, the accuracy of the detection is expected to increase.

2.1 Challenges in Data Acquisition

Following challenges are faced by any in-service gas metering systems:

- (i) Time stamped data acquisition from different devices like USM, GC and Flow computers at a frequency as low as one second (recommended frequency by API 21.1 for custody transfer measurements algorithms)
- (ii) Different equipment like USM meters, Flow Computers and Gas chromatographs offer different types of communication ports (like TCP/IP, RS 232/485 or a mix for data acquisition by any third party device/software on Modbus protocol.
- (iii) Availability of the requisite data for further analytics ,virtual flow computations, audit and diagnostics in non contagious data registers in different data blocks .
- (iv) Configuration of data with variable scan frequency for each device as data may be required at different frequencies depending upon the intended analytics. For example, Data may be required at a frequency as high as few milli seconds for Virtual Flow Computation and USM diagnostics using DIGITAL TWIN MODEL while for the frequency of data acquision may be few times in a day for Gas Chromatograph diagnostics based on correlation and other statistical analysis .
- (v) At times the configuration of requisite data in a requisite format in flow computers or USM calls for specific software and OEM services also. Thus the equipment which provides the data is often needed to be reconfigured rather than the device/software being capable of accepting the data in whatever form already available.
- (vi) Data aggregation and storage for future retrieval and analysis is also one of the desirable functionality of any such system. System should be able to acquire data and store with user configurable frequency at not only LOCAL storage but also an online REMOTE replica/image of the data being captured locally should be created. Artificial intelligence and Machine Learning tools are more and more being deployed in all fields of application and these models are really data hungry. Larger the available dataset, more accurate the machine learning model. Thus, system for frequent data capture is required for data hungry third party interfaces.

DATA ACQUISITION MODULE IMPLEMENTATION:

Keeping above shortcoming s and requirements in real world scenario in mind, the software has been developed so that no external hardware or drivers are required. Same can run on any Normal Personal Computer with Microsoft OS. Technology stack such as Visual Studio, SQL server and OLEDB have been used for development of software. As different stations may have different number of devices installed due to multiple stream configurations, the software has been designed in modular form so that it can fetch data from multiple devices as per the station requirement. Different data polling frequency can be configured for each device by the operator with engineer privilege through a User Interface.

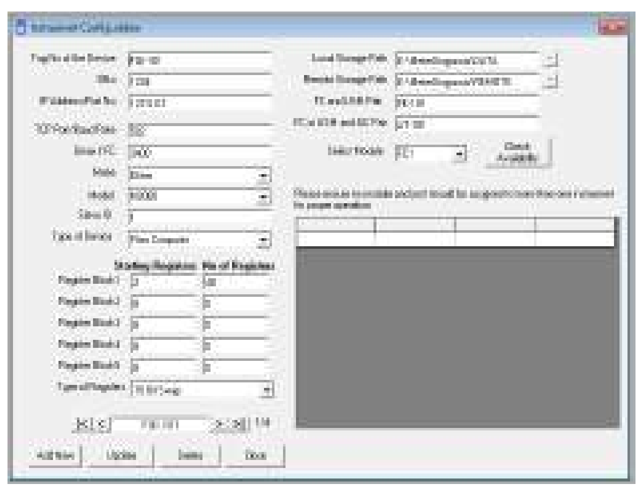


FIGURE 1: GUI FOR INSTRUMENT CONFIGURATION

2.2 Digital Twin and Virtual Flow Computation

Custody transfer of natural gas involves measurement of the gas volume and energy at line or operating conditions and finally converting it to base conditions as per contractual obligations or regulatory requirements. Measurement of gas volume and energy involves various type of devices depending upon the measurement principle involved like orifice meter, turbine or RPD meter , Ultrasonic meters and Gas chromatographs. For conversion of the gas volume or energy to base or standard conditions a Flow computer in compliance with API Chapter 21.1 is deployed. The quantities reported by the Flow computers are used for billing purposes. In case of any mis measurement of any operating parameters like Line Pressure, Line Temperature, Gas flow raw measurement (DP, Velocity, Pulses etc.) or gas composition may result in huge financial loss to either party. Further inaccurate measurement of these parameters impacts the Leak detection system accuracy.

Discussion here is restricted to smart metering stations like USM based metering systems which involve smart devices like USM meters, Flow computers and Gas chromatographs capable of providing data in electronic form.

A Flow computer converts operating condition flow to base conditions in compliance with relevant international Standard/recommendations/reports like AGA, ISO, GPA or API.

Some critical aspects in this conversion process are as under:

(i) Acquisition of operating condition data such as raw low, pressure, temperature and gas composition

(ii) Calculation of compressibility factors or densities at line and base conditions as per AGA-8 detailed characterization equation of state

(iii) Calculation of other parameters such as calibration error curve compensation and Pressure and temperature expansion correction as per AGA-9 calculations, in addition to several other algorithms.

(iv) Calculation of Energy flows and calorific values as per ISO 6976 or GPA 2172/2145.

All these equation of state and algorithms are run in flow computer as per API 21.1 framework. The Software also runs these EOS and calculations as a DIGITAL TWIN of actual flow computer and provides Virtual Flow Computation . Developed software provides online validation of the Flow Computer with theoretical calculated intermediate and final parameters as per applicable standards and compares it online with actual flow being reported by flow computer . Alerts in case of deviations with probable cause of deviations along with recommended measures to correct the mis-measurement conditions are also provided.

DIGITAL TWIN for Virtual Flow Computation incorporates following Equation of states and Calculations:

(i) AGA-8 Detailed Characterization Equation of state

$$Z=1+Bd-D\sum_{n=13}^{18} CnT^{-un} + \sum_{n=13}^{58} CnT^{-un} (b_n - c_n k_n D^{Kn}) D^{bn} \exp(-c_n D^{Kn}) \qquad (1)$$

where d is the molar density of the gas, B is the second virial coefficient, D is the reduced density, Cn are parameters that are functions of composition, and un, bn, cn, and kn are coefficients and exponents as explained in AGA-8 Report.

The reduced density D is related to the molar density d by the equation

$$D = K\, d^{\,3} \qquad (2)$$

where K is the mixture size parameter.

The density can be determined with appropriate iterative procedures. As explained in AGA-8 Report , the values of B, Cn and K are calculated from the composition and temperature of the gas.

The mixture size parameter K for a mixture of N components is calculated as

$$K^5=[\sum_{i}^{N} xiKi^{5/2}]^2 +2\sum_{i=1}^{N-1}\sum_{j=i+1}^{N} xixj\ (K5ij - 1)(KiKj)^{5/2} \qquad (3)$$

where the Kij are binary interaction parameters for size, Ki and Kj are size parameters for the i th and j th components , and xi and xj are mole fractions of components i and j in the gas mixture.

The second virial coefficient B is given by the following equations:

$$B=\sum_{n=1}^{18} a_n T^{-un}\ B^*\ \text{with} \qquad (4)$$

$$B^*=\sum_{i=1}^{n} x_i^2 E_i^{\,un} K_i^3 B^*_{nii} + \sum_{i=1}^{N-1}\sum_{j=i+1}^{N} 2xixj\ [E_{ij}(E_i\, E_i)^{1/2}]^{un} (K_iK_j)^{3/2} B^*_{nij}\ , \qquad (5)$$

$$B^*_{nij} = [G_{ij}(G_i\, G_i)/2 +1-g_n]^{gn} (Q_iQ_j +1-q_n)^{qn} (F_iF_j +1-f_n)^{fn} (S_iS_j +1-s_n)^{sn} (W_iW_j +1-w_n)^{wn} \qquad (6)$$

The coefficients Cn (n=13 to 58) are as under

$$C_n= a_n (G+1-gn)^{gn} (Q^2+1-qn)^{qn}(F+1-fn)^{fn}U^{un} \qquad (7)$$

The mixture parameters F, G, Q, and U are calculated with the following equations, where in the double sums i ranges from 1 to N–1, and each value of j ranges from i+1 to N:

$$U^5=\left[\sum_i^N xiEi^{5/2}\right]^2 +2\sum_{i=1}^{N-1}\sum_{j=i+1}^{N} xixj\,(U^5_{ij}-1)(E_iE_j)^{5/2} \quad (8)$$

$$G=\sum_i^N xiGi+\sum_{i=1}^{N-1}\sum_{j=i+1}^{N} xixj\,(G_{ij}-1)(G_{i+Gj}) \quad (9)$$

$$Q=\sum_i^N xiQi \quad (10)$$

$$F=\sum_i^N xi^2 F_i \quad (11)$$

Further details about theses parameters are provided in AGA Report No -8 Part -I.

DIGITAL TWIN Model executes these calculations within few milliseconds and provides intermediate and final results in terms of line and base compressibility and densities for use in subsequent Modules.

(ii) AGA-9 & AGA-7 Flow calculations

Flow calculations are done by the DIGITAL TWIN Models based on the AGA-9 and AGA-7 calculations. Some USM metering stations are configured with dual streams(pulse based as well serial input for velocity measurement) for ascertaining the health of the meter. Software has DIGITAL TWIN Models to accommodate both such streams.

DIGITAL TWIN model identifies the most common contributors to Mis- measurements which are generally overlooked during configurations or data updation after calibration/Re calibration of the meters. These include error curve compensation algorithms as well as flow compensation due to pressure and temperature variance between the calibration and operating conditions depending upon construction material of the Meter.

As per AGA-9, Different methods of correction for USM errors are deployed either in USM electronics or Flow computers. These include:

(a) Flow weighted Mean Error (FWME) Correction

$$FWME=\frac{\sum_{i=1}^{n}(\frac{qi}{qmax})xEi}{\sum_{i=1}^{n}(\frac{qi}{qmax})} \quad (12)$$

Where SUM is the summation of the individual terms representing each of the test flow points, qi is the actual test flow rate from the reference meter, and Qi/qmax is a weighing factor (wf) for each flow test point, and Ei is the indicated flow rate error (in %) at the actual test flow rate qi

Calibration factor, F is calculated as

$$F=\frac{100}{100+FWME} \quad (13)$$

(b) Polynomial Algorithms

Polynomial algorithms use polynomial functions for approximation of the calibration factor F over the USM's flow range

$$F= a0 + a1 \times q + a2 \times q2 + ... + an \times qn \quad (14)$$

(c) Multi-point/ Piecewise Linear Interpolation

This is the most frequently used correction technique. It uses linear function for calibration factor between adjacent test points i and i+1

$$F= Fi + (Fi+1 - Fi)\, x(\frac{q-qi}{qi+1-qi}) \quad (15)$$

DIGITAL TWIN models capture the correct implementation of these corrections (as per calibration reports issued by ISO 17025 accredited flow calibration Laboratory) and mis-measurements in quantitative terms are reflected online.

Similarly, online quantification of the Mis-measurement due to incorrect or non- implementation of Pressure and thermal expansions are provided.

(iii) Energy Measurement as per applicable Standard

Generally the custody transfer takes place in terms of the energy content of the gas. For determining the energy content of the flowing gas , a Gas Chromatograph is used which analyzes the gas sample and provides information about various constituents of the gas. Further calculations based on applicable standard such as ISO 6976 or GPA 2172/2145 are done on the analyzed sample to determine Various thermodynamic properties like Calorific Value of the gas which in turn determines the energy flow rate.

As explained in ISO 6976, the real-gas calorific value on a volumetric basis, for combustion at temperature t1 and pressure p1 of a gas mixture metered at a temperature t2 and pressure p2 is calculated from the equation

$$H[t1,V(t2,p2)]=\frac{Ho[t1,V(t2,p2)]}{Zmix(t2,p2)} \quad (16)$$

where H[t1 ,V(t2 ,p2)] is the real gas calorific value on a volumetric basis of component j (either superior or inferior) and Ho[t1, V(t2, p2)] is the ideal gas calorific value on a volumetric basis of component j (either superior or inferior)

Zmix(t2 ,p2) is the compression factor at the metering reference conditions.

$$\mathrm{Ho}(t1, V(t2,p2))] = \sum_{j=1}^{N} xj.Hj[t1, V(t2, p2)] \quad (17)$$

$$\rho o(t,p)] = (p/RT) \sum_{j=1}^{N} xj.Mj \quad (18)$$

$$\rho(t,p)] = \frac{\rho o(t,p}{Zmix(t,p)}) \quad (19)$$

$$d^{o} = \sum_{j=1}^{N} xj.Mj\,/Mair \quad (20)$$

$$d(t,p) = d^{o}.\frac{Zair(t,p)}{Zmix(t,p)} \quad (21)$$

where d o is the relative density of the ideal gas and d(t,p) is the relative density of the real gas; Zmix(t,p) is the compression factor of the gas; Zair(t,p) is the compression factor of dry air of standard composition. ρo (t,p) is the density of the ideal gas and ρ (t,p) is the density of the real gas

$$Zmix = 1 - [\textstyle\sum_{j}^{N} xj.\sqrt{bj}]2 \quad (22)$$

where

$$bj = 1 - Zj \quad (23)$$

where $\sqrt{bj}$ is the summation factor

DIGITAL TWIN Model executes these calculation and other routines as per ISO 6976 online and quantifies the Mis-measurements dynamically.

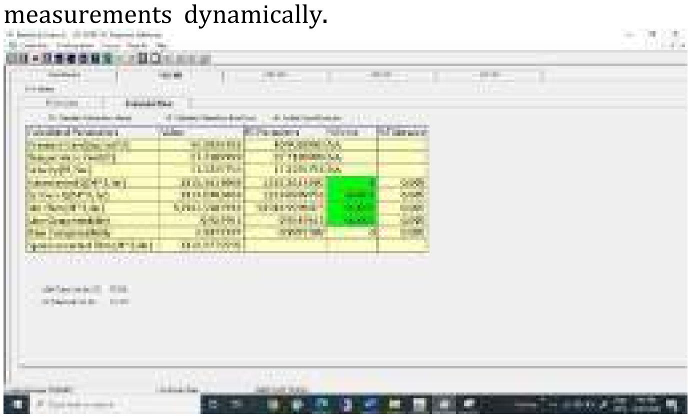


FIGURE 2: ONLINE VIRTUAL FLOW COMPUTATION WITH DATA COMPARISION WITH FLOW COMPUTER

2.3 Digital Twin for Ultrasonic Meters Diagnostics

With the advancement of technology USM meter are becoming smarter day by day. These meters offers various diagnostic parameters which are not only indicative of the health of the meter itself but also help in identifying process related problems like flow profile distortion due to installation problems or incorrect installation operations like partial close valves or valve noise. Generally USM meters have multiple paths. The Software acquires relevant raw data at very high frequency from USM meter and processes the diagnostic parameters which are monitored online and also stored for future retrieval and further extension to other third party applications. These include Parameters like :

(i) Path performance for each path representing healthiness of each path transducers in terms of signal acceptance.

(ii) SOS validation as per AGA- Report 10 and SOS spread as per AGA-Report9 performance requirements.

(iii) Velocity and its profile for each path

(iv) GAIN parameters for each path representing cleanliness and/or contamination of any path transducer, transducer and associated electronics health, in addition to change in process conditions, if any.

(v) Signal to Noise ratio for each transducer representing the transducer and electronics health and the level of noise signal wrt transducer signal for each transducer.

(vi) Profile Factor which provides information about the flow profile in accordance with relationships between different path velocities based on the meter design

(vii) Symmetry and cross flow which also provides information about the flow profile in accordance with defined relationships between different path velocities based on the meter design and transducer configurations in different planes of meters.

(viii) Swirl angle which indicates any swirl phenomenon due to profile distortion

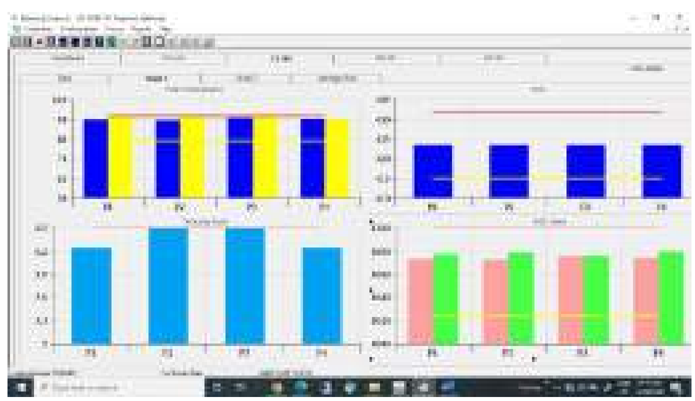


FIGURE 3: DIAGNOSTIC PARAMETERS (PERFORMANCE, AGC, VELOCITY PROFILE, SOS)

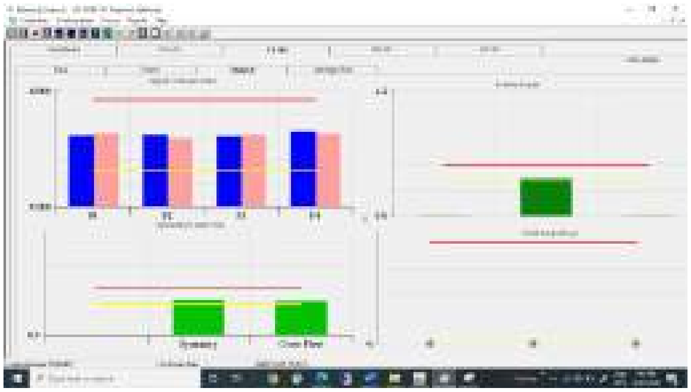


FIGURE 4: DIAGNOSTIC PARAMETERS (SNR, ASYMMETRY, CROSS FLOW, PROFILE FACTOR, SWIRL ANGLE)

(i) Speed of Sound (SOS) Calculation as per AGA 8 Part-I (erstwhile AGA10)

Speed of Sound (SOS) is the most reliable and worldwide used parameters which indicates the health of the ultrasonic meters. If the meter reported SOS and theoretical calculated SOS as per AGA-8 Part-I or erstwhile AGA-10 Report is within the tolerances provided in AGA – 9 , ultrasonic meter can be safely assumed operating within the specified accuracy limits. SOS calculation depends upon the operating pressure, operating temperature and flowing gas composition . Thus if there is no discrepancy in SOS validation, entire measurement system including secondary instrumentation like pressure transmitter, temperature transmitter and gas chromatograph are operating within stated accuracy limits until parameters drift in such a fashion that drift in one parameter compensates the drift in another parameter. Simultaneous drift in these parameters is also captured in DIGITAL TWIN model for flow calculation as well.

DIGITAL TWIN model for SOS validation removes efforts for manual operator intervention in collecting the data manually and then generating the validation report against standard SOS validation software. The validation is done online continuously at a frequency of as low as few milliseconds and provides probable causes and rectification measures thereof in case validation as per AGA-10 fails.

DIGITAL TWIN Model calculates the SOS as per AGA-10 routines from the DETAIL equation of state obtained values through numerical integration of the compressibility factor equation. The equations used for the calculation of thermodynamic properties are implemented through differentiation of the fundamental Helmholtz energy equation.
The equations used for calculating compressibility factor, pressure, and the derivatives of pressure with respect to density and temperature are given in the following equations:

$$Z=\frac{P}{dRT} = 1+\frac{d}{RT}\left[\frac{\partial a^r}{\partial d}\right]_T \tag{24}$$

$$P= d^2 \left(\frac{\partial a}{\partial d}\right)_T \tag{25}$$

$$W^2 = \frac{Cp}{MCv}\left(\frac{\partial P}{\partial d}\right)_T \tag{26}$$

$$c_p = c_v + \frac{T}{d^2}\left(\frac{\partial P}{\partial T}\right)^2_d \left(\frac{\partial d}{\partial T}\right)_T \tag{27}$$

$$c_V = T\left(\frac{\partial S}{\partial T}\right)_d \tag{28}$$

Further details for calculation of the derivatives of the Helmholtz energy required in these equations are provided in AGA -8 Report Part-I .

The results are also saved in LOCAL data storage as well as in REMOTE storage in the form of Reports which may on demand or scheduled.

2.4 Digital Twin for Gas Chromatograph Diagnostics

Inspection of the calibration data generated can give an indication as to whether the equipment and the methods are working satisfactorily. Data generated during the calibration of online gas chromatograph are captured and further analyzed based on the GC design and configuration of columns and valves. System is able to capture any deterioration of the standard calibration gas, operator mistakes while entering the calibration blend in GC configuration, Valve malfunctions etc. System uses methods as described in various applicable standards like ISO 6974, GPA 2198 and GC manufactures manuals.

System also deploys Quality Control Chart which is a statistical tool used to provide a method for distinguishing a pattern of random error or variations from a determined known. The analytical data for a component is plotted on a linear chart over a period of time. The control limit is the mean +/- 3 standard deviations from the mean. Warning limits are established using the mean and +/- 2 standard deviations. For each component in the calibration gas as well as the unnormalized total of the equipment, a control chart is constructed.

FIGURE 5: COMPONENT WISE CONTROL CHART

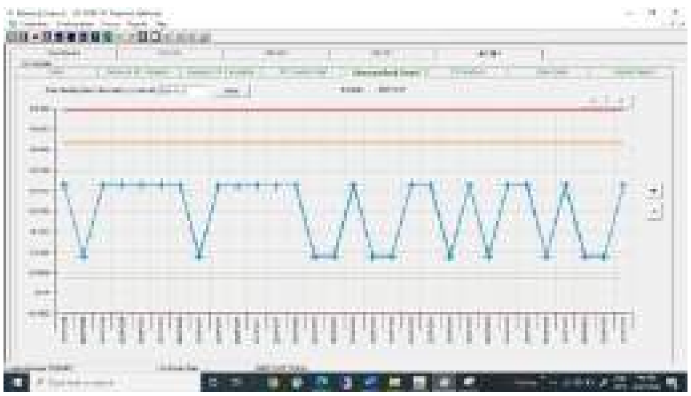


FIGURE 6: CONTROL CHART FOR UNNORMALIZED TOTAL

A standard deviation is defined by the following formula:

$$\text{Standard Deviation} = \frac{\sqrt{n\sum x^2-(\sum x)2}}{\sqrt{n(n-1)}} \qquad (29)$$

Where: n is the number of data points, Σ x2 is the sum of the squares of the data (Σ x)2 is the square of the sum of the data.

Correlation Analysis based on Response Factors (RF) and Molecular weights (MW) is also done for group of components so that highly correlated data indicates proper operation of the equipment along with ensured quality of the standard blend . Any deviation calls for further analysis which is suggested as operator assistance messages with probable cause of such deviations and required actions to be taken.

Analysis is not only done on historical data but also for the Baseline data as well as data just prior to calibration so that no errors or drifts are masked inadvertently. Similarly, retention times are also analyzed for the consistency of the peak detection and peak resolution.

FIGURE 8: RETENTION TIME DRIFT ANALYSIS

Based on the components determined by the GC, Validation of the Calorific value and energy flows are done against ISO 6976 calculations.

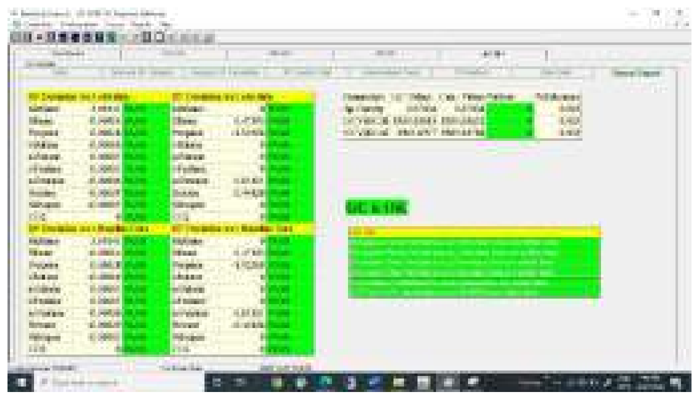


FIGURE 9: OVERALL GC HEALTH DASHBOARD WITH ISO 6976 VALIDATION

3. RESULTS AND DISCUSSION

Keeping in view the requirement of an online Validation, Audit and virtal flow computeaion a DIGITAL TWIN model for complete metering package including USM meters, Gas chromatographs and Flow Computers has been developed. The system provides online validation as per applicable standards or Equipment Manufacturer recommendations thus eliminating need for frequent audits and validations with manual interventions. Local and Remote storage of data for future retrieval and contractual/ regulatory/ company policy compliances . All the Models have been validated rigorously against Sample datasets and results against each applicable standard calculation. Each model is further validated with actual interfacing with live Flow Computers, Gas Chromatographs and USM meters.

With the developed system it is possible to:

1. Minimize the manual intervention in diagnosing the problem and hence no room for biased and irrational decision.

2. Early detection of the problem before it gets reflected in terms of mis-measurement in volume and energy.

3. Suggestive remedies for probable causes of ensuing problems.

4. Online validation and verification of the system which saves time, cost and immediate and handy information.

5. Data repository for each device for every second, which is very useful in mis-measurement handling.

6. Data can also be used for other applications as an input for integration with third party systems for further advanced analytics, if required.

7. Enhancing trust in field signals thereby enhancing leak detection accuracy. As the system can quantify the % error with which the flow meter is operating, this information can be used by third party leak detection systems to assign a weightage or confidence level to the leak alarm.

Entire solution has been developed so that no major modification /Hardware changes is required for implementation. The system is developed as a standard off the shelf package with installation as easy as any other software. For data integration and configuration also no extensive technical expertise is required.

4. CONCLUSION

The Developed DIGITAL TWIN Model for Flow Measurement Systems is one single package addressing multiple problems like timestamped data acquisition at different frequency from different equipment, processing and analyzing the data and validating each equipment against applicable standards with Local and Remote data storage as well as alarm and event logs for future retrieval and audit. Not only problems pertaining to Mis-Measurement in Fiscal Measurement systems are taken care but accuracy of leak detection is also improved as Leak Detection module gets validated data from field instrument

REFERENCES

[1] AGA Report No -8, Part I, Thermodynamic Properties of Natural Gas and Related Gases Using DETAIL and GROSS Equations of State, 2017

[2] Compressibility factors of Natural Gas and other Related Hydrocarbon Gases by K.E.Starling and J.L Savidge, AGA Transmission Committee Report No -8

[3] AGA Report No. 10, Speed of Sound in Natural Gas and Other Related Hydrocarbon Gases

[4] AGA Report No. 09, Measurement of Gas by Multipath Ultrasonic Meters

[5] AGA Report No. 7, Measurement of Natural Gas by Turbine Meters

[6] ISO6976- Natural gas-Calculation of calorific values,density, relative density and Wobbe indices from com;position

[7]ISO6974-1, Natural gas — Determination of composition with defined uncertainty by gas chromatography — Part 1: Guidelines for tailored analysis

[8]GPA Standard 2198-03, Selection, Preparation, Validation, Care and Storage of Natural Gas and Natural Gas Liquids Reference Standard Blends

[9] User Manuals and Other literatures from various Manufacturers of GC, USM and Flow Computers including Emerson Process Management and Elster Instromet

[10] GPA Standard 2261-00, Analysis for Natural Gas and Similar Gaseous Mixtures by Gas Chromatography

[11] Manual of Petroleum Measurement Standards Chapter 21.1, Flow Measurement Using Electronic Metering Systems—Electronic Gas Measurement

Setting the Standard for Automation™

ISA Delhi Section

O-PAS

The Process Automation Opens Up

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

1

What is Open Process Automation ?

- Open Process Automation is an initiative to create a new generation of automation systems with a distinctly different architecture than the Distributed Control Systems (DCS) and Programmable Logic Controllers (PLCs) that are used today for process automation.
- The current drive for Open Process Automation began within ExxonMobil Corporation, where a huge number of older and obsolete DCS installations needed to be replaced. Facing a huge investment over many years, ExxonMobil engineers and managers began to look “outside the box” of existing DCS products and think about how a different class of automation products could improve and simplify their future operations

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

2

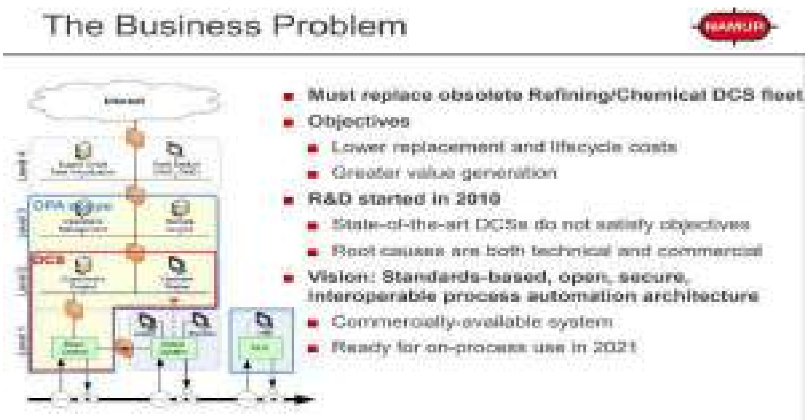
OPAS concepts

- **Interchangeability**: the ability of a component to be replaced by another component without modification
- **Interoperability**: the ability of two or more systems or components to exchange information and to use the information that has been exchanged
- **Portability**: the ease with which a system or component can be transferred from one hardware or software environment to another
- **Modularity**: the degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components

Open Process Automation Forum Goals

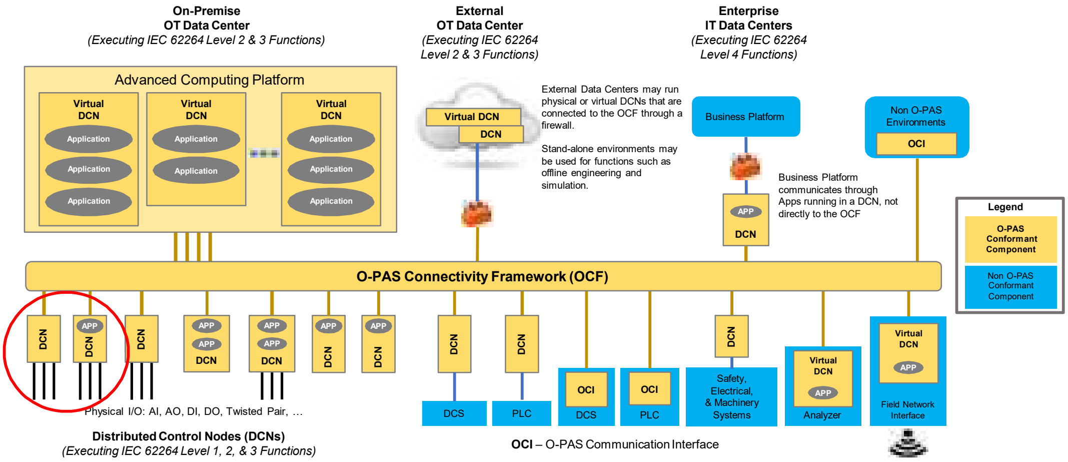
- A standards-based, open, secure, and interoperable process control architecture that:
- Enables access to leading edge capability
- Allows integration of best-in-class components
- Preserves asset owners' application software; Significantly lowers cost of future replacement
- Employs an adaptive intrinsic security model
- Promotes innovation and value creation
- Applies across multiple process industries

Motivation



Source : NAMUR - Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V. Sitz des Vereins: Leverkusen Eintragung: Amtsgericht Köln, VR 18371

OPAF Vision: Open, standards-based, interoperable, secure, process control architecture



O-PAS™ Versions

Version	Year	Theme – Open, multi-vendor control system
V1	2019	Interoperability
V2	2020	Configuration Portability
V2.1	2022	Control Functionality
V3	**2023**	**App Portability, Orchestration & Physical Platform**

Application Portability

Ensures **end users** have the ability to move their apps, whether custom developed or vendor provided, from platform to platform, as well as to use any process automation software, regardless of vendor.

System Orchestration

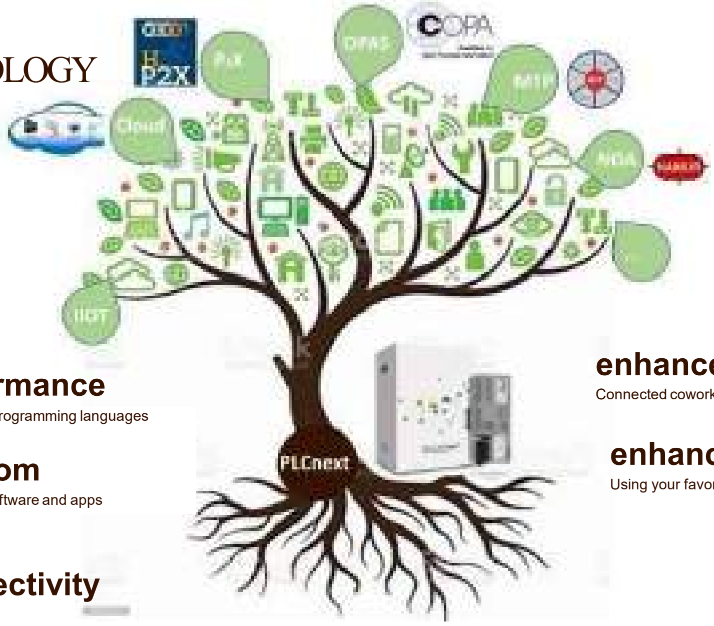
Ensures the ability to select and implement O-PAS certified products from multiple suppliers and to be assured those products will coexist seamlessly in a unified open process automation system.

Physical Platform

Ensures **end users** have the required degree of openness, interchangeability, interoperability and security across platforms within the system.

What Phoenix Contact Offers ?

ToT
TREE OF TECHNOLOGY



enhanced performance
Real-time execution across different programming languages

enhanced freedom
Flexible integration of open source software and apps

enhanced connectivity
Open interfaces and cloud integration

enhanced development
Connected coworking

enhanced convenience
Using your favorite programming tool

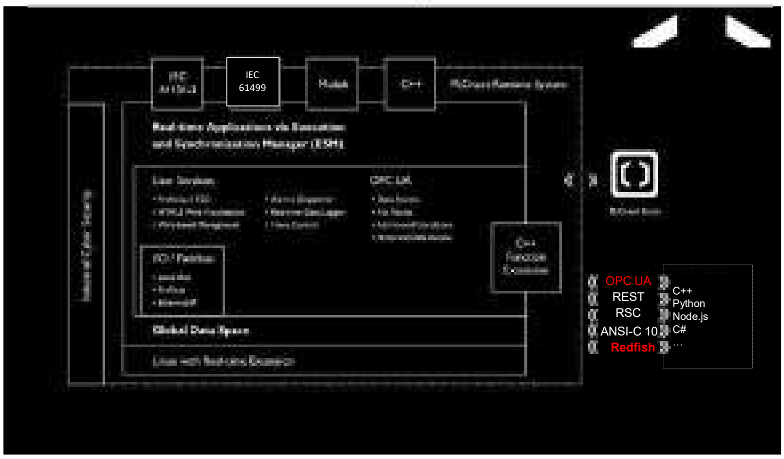
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

9

PLCnext Technology
Designed by PHOENIX CONTACT

PLCnext Runtime System Architecture

PLCnext Runtime System Architecture



- Reduced deployment time through the integration of source software
- Connectivity, security & real-time capability are already implemented
- Future-proof, flexible and secure thanks to continuous updates
- Integration of IEC61131-3, high-level languages and open-source software possible
- Apps from PLCnext Store easy to implement

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

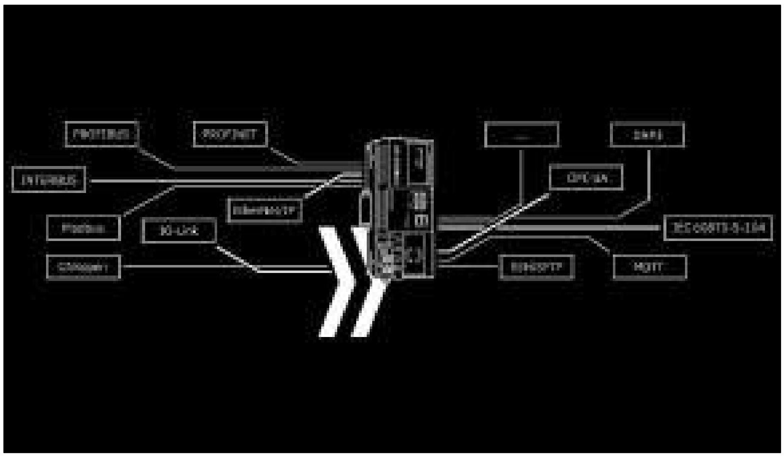
11

10

PLCnext Technology
Designed by PHOENIX CONTACT

enhanced connectivity – Intelligent Networking

Future-proof Connectivity



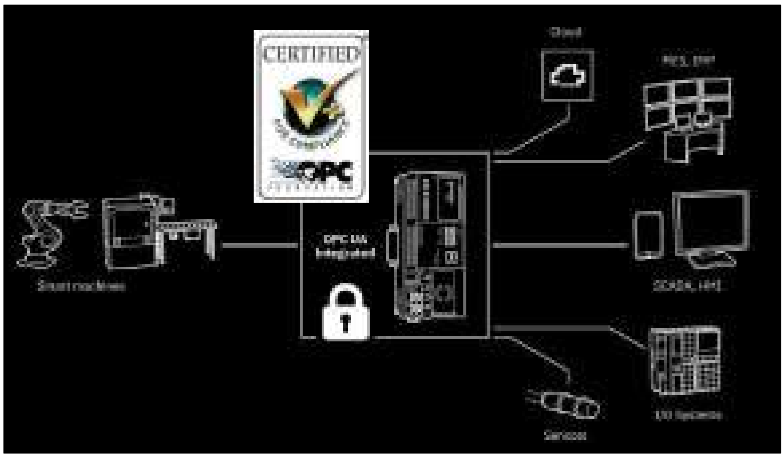
PLCnext Technology enables the integration of current and future interfaces and protocols for open communication in highly networked automation systems.

11

PLCnext Technology
Designed by PHOENIX CONTACT

enhanced connectivity – Intelligent Networking

Integrated OPC UA Client / Server



OPC UA

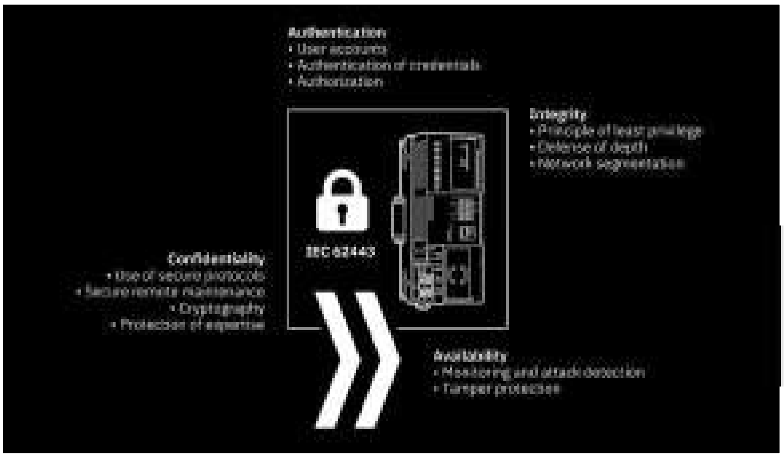
Data Access, Alarms and Conditions, Programs, Historical Access, Global Discovery Server

12

PLCnext Technology
Designed by PHOENIX CONTACT

Applicable Security Laws and Standards

IEC 62443: IT-Security for Industrial Automation



ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

13

PLCnext Technology
Designed by PHOENIX CONTACT

PLCnext Technology – Security

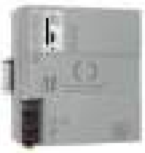
IEC 62443: IT-Security for Industrial Automation

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

14

What Phoenix Contact Offers ….

AXC F 3152



OR

AXC F 2152

IO Service Engine APP

- **OPC UA Client/Server**
- **OPAS Information model**
- **Automatic Bus Detection**
- **Configuration via AML**
- **Redfish**
- **Security**
- **…..**

FB Execution Engine

PLCnext

OR

UNIVERSAL AUTOMATION.ORG

OR

CODESYS

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

15

ExxonMobil Test Bed – Accelerating Transformation

- Vision: Standards-based, open, secure and interoperable DCS architecture

ExxonMobil Prototype in Clinton, NJ

ExxonMobil Test Bed in The Woodlands, TX

2016 – 2018 Proof of Concept → 2018 – 2020 Prototype → 2019 – 2021 Test Bed → 2021 – 2023 Field Trial → 2025 – 2026 Commercial Deployment

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

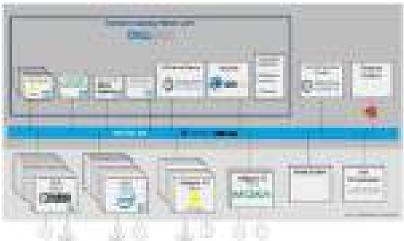
16

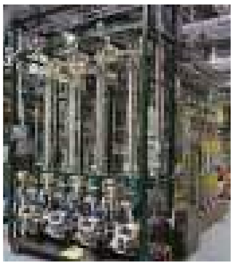
Pilot Project

ExxonMobil

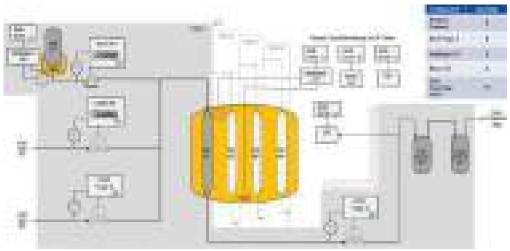
Project Details

- Sandbath reactor with 20 CC catalyst
- Used for evaluating catalyst performance (8 GM/HR liquid feed)
- Hydrocarbon service at process temperature (600°F) and pressure (1200 PSIG)
- Unit includes pumps, reactors, separators and analyzer
- Contains typical process controls (25 control loops)
- Actual I/O count 130 with 500 total points
- Key output of unit operations is data for R&D





OPA Prototype Cabinet



ExxonMobil OPA Prototype System Running Pilot Unit

- Developed Prototype system with unit specific applications
- Biggest challenge related to creating "**system-ness**"
- Migrated from existing DCS
- Completed Site Acceptance Test in January 2020
- Normal unit operations using OPA system
  - Controlling unit paramete
  - Meeting operator expecta

Open Systems Architecture Vision: A system of systems...

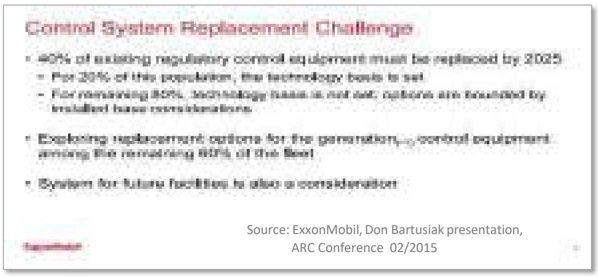
ExxonMobil

Involvement in OPAF

- ExxonMobil is very invested in the success of OPAF since they were at the forefront of initiative
- In addition to the multiple resources devoted to the Forum, they hired Lockheed Martin as a Systems Integrator and Wood PLC as the EPC to test side-by-side functionality discussed in the Forum
- ExxonMobil selected Yokogawa as Systems Integrator for the Test Bed
- They have recently hired Georgia Tech to develop interfaces for connectivity

Phoenix Contact Involvement with ExxonMobil

- OPAF
  - 2017 - Worked with Lockheed Martin and Exxon on Proof of Concept
  - ARC 2019 – Exxon Announcement on Prototype System Architecture
  - PxC worked with Lockheed Martin and ExxonMobil on adding functionality and support for the Prototype



Control System Replacement Challenge

- 40% of existing regulatory control equipment must be replaced by 2025
  - For 20% of this population, the technology basis is set
  - For remaining 80%, technology basis is not set; options are bounded by installed base considerations
- Exploring replacement options for the generation control equipment among the remaining 80% of the fleet
- System for future facilities is also a consideration

Source: ExxonMobil, Don Bartusiak presentation, ARC Conference 02/2015

ExxonMobil OPA Prototype System Running Pilot Unit

- Developed Prototype system with unit specific applications
- Biggest challenge related to creating "**system-ness**"
- Migrated from existing DCS
- Completed Site Acceptance Test in January 2020
- Normal unit operations using OPA system
  - Controlling unit parameters
  - Meeting operator expectations

Accelerating OPA Development with ExxonMobil Test Bed

- Test Bed will support continued testing of components and standards
- Yokogawa is System Integrator working with many suppliers
- ExxonMobil set initial design before engaging Collaboration Partner
- Demonstrate supplier capabilities to produce components aligned with O-PAS™
- Test results will support basis for Field Trials

ExxonMobil OPA Collaboration Partners

- Aligned on need for open process automation systems
- Desire to accelerate development via multiple, parallel field trials
- Each partner will select own System Integrators
- Use O-PAS™ standards as available
- Share non-competitive learnings among collaboration partners
- Collaboration partners developing Test Bed experiments

Collaboration Partners

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

21

COPA QuickStart

- For companies that want to get started with Open Process Automation now
- Pre-assembled OPA system that demonstrates key capabilities
  - Interoperability
  - Best-in-class components
  - Inherently secure
  - Open, standards-based system avoiding vendor lock-in
  - Platform for continuous digital transformation
- Advantages to our approach
  - Fixed cost
  - Integrated learning program to equip engineers and accelerate abilities to leverage the benefits of OPA
  - Continuous improvement thru remote updates
  - Customizable to meet specific needs

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

22

THANK YOU

POTENTIAL CYBERSECURITY THREATS TO THE DIGITAL POWER INDUSTRY - FROM SUPPLY CHAIN TO SUBSTATION AND THEIR ZEROTRUST STRATEGIES

Yenting Lee[a], Debraj Chakraborty[b], Mars Cheng[a], Sheng-Hao Ma[a]
[a] PSIRT and Threat Research of TXOne Networks, Taiwan
[b] TXOne Networks, India

ABSTRACT

Due to the impact of the post-pandemic and Russia-Ukraine war, the risks facing global supply chains have increased dramatically, making it essential for companies to carefully evaluate their supply chain security. However, in the digitally driven trend of the power industry, while it brings efficient operation, it also poses threats to cyber security. This paper will focus on digitized substations and India's most common renewable energy sources (including solar and wind) to analyze potential threats to them and their supply chains. We also propose an effective zerotrust framework to address threats from various attack vectors to keep operations running.

KEYWORDS

Digital Power Industry, Cyber Security, Supply Chain, Substation, Renewable Energy, Zerotrust

INTRODUCTION

No matter the operation of critical infrastructure or the daily needs of people, they all rely on the power industry to provide necessary operational resources. The power industry refers to power generation, management, and retailing. At any stage, cyberattacks could lead to insufficient power supply, causing damage to the national economy and even threatening people's survival. In this paper, we first collect cybersecurity incidents targeting critical infrastructure in 2022. The result is shown in figure-1. It was discovered that attacks targeting the energy industry were the most severe, accounting for approximately 31%. This highlights the necessity for power industry to understand its cybersecurity threats.

In April 2022, the notorious Sandworm group attempted to launch an attack on Ukrainian energy company using the Industroyer2 malware, which is a cyber weapon specifically designed for ICS targeting the power industry. If successful, the malware could directly control circuit breakers, causing multiple substations in Ukraine to be terminated. As shown in figure-1, many cybersecurity incidents are related to the supply chain. For example, Nordex, one of the world's largest wind turbine developers and manufacturers, was forced to shut down its IT systems and remote access to managed turbines due to Conti ransomware attack. Furthermore, like other industries, the power industry is gradually introducing more digital technologies

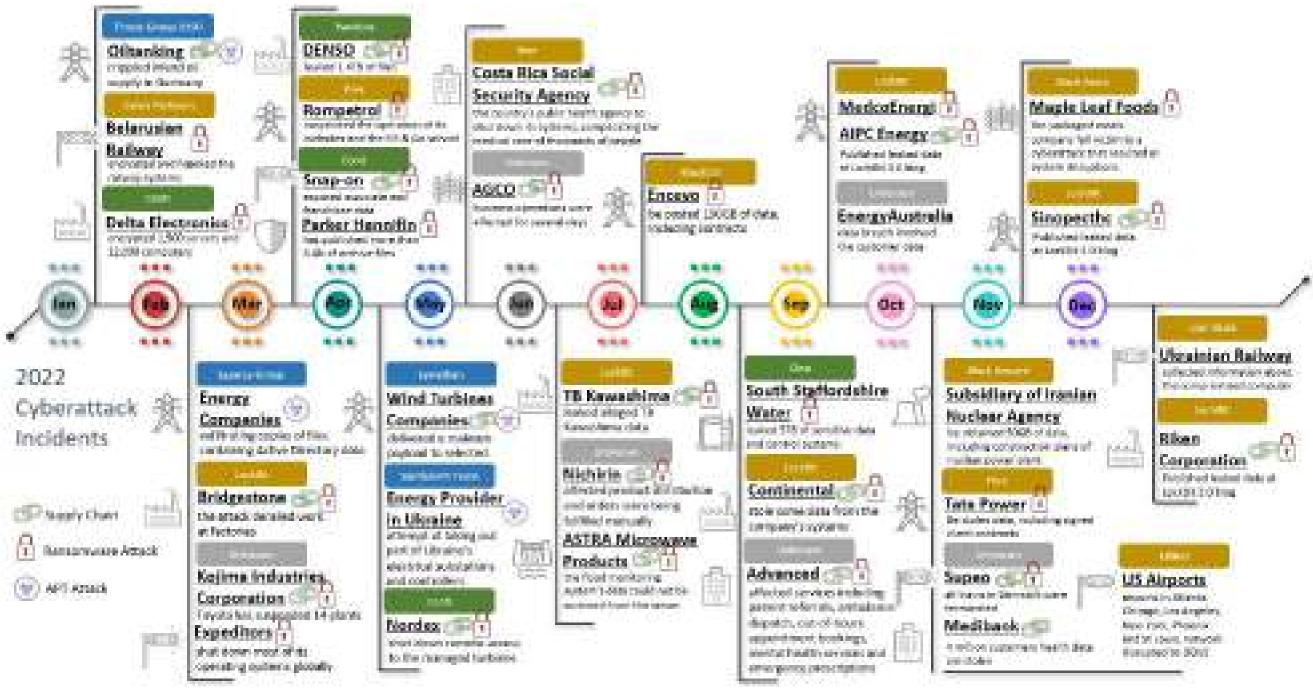


Figure-1. Critical Infrastructure Targeted in 2022 (Show Excerpt Only)

to improve the efficiency of power plants to meet the constantly growing demand for power. To effectively interact various brands of RTUs, IEDs, PLCs, meters, transducers, relays, etc. with monitoring or computing servers, it is essential to adopt a standardized communication protocol [1]. However, in highly interconnected environments, attackers will have more opportunities to launch cyberattacks on the power industry.

POWER INDUSTRY ECOSYSTEM

As previously mentioned, the power industry including power generation, power management, and power retailing. The following will elaborate on the power industry ecosystem with renewable energy:

POWER GENERATION

As shown in the green area of figure-2, power generation forms include thermal, hydro, wind, and solar power. After generating power, the producers can transfer the power to substations through the electric power transmission system. By a series of analysis and management, the power is finally sold to users. in renewable energy, Solar and wind power are the representatives of the highest power production capacity in recent years. However, the characteristics of occupying a large area and often being located in sparsely populated areas, it makes the networked sensors, controllers, actuators, or inverters are exposed to the risk of cyberattacks.

POWER MANAGEMENT

As shown in the yellow area of figure-2, after power generation, power companies need to manage and distribute power through the power grid system. This process involves one or more substations depending on the types of end-users. For instance, residential electricity may need to undergo three voltage reductions before being distributed. Like traditional ICS environments, substations consist of devices such as HMI, IED, and Field Devices. To accurately record the time sequence of events in the power grid system, as

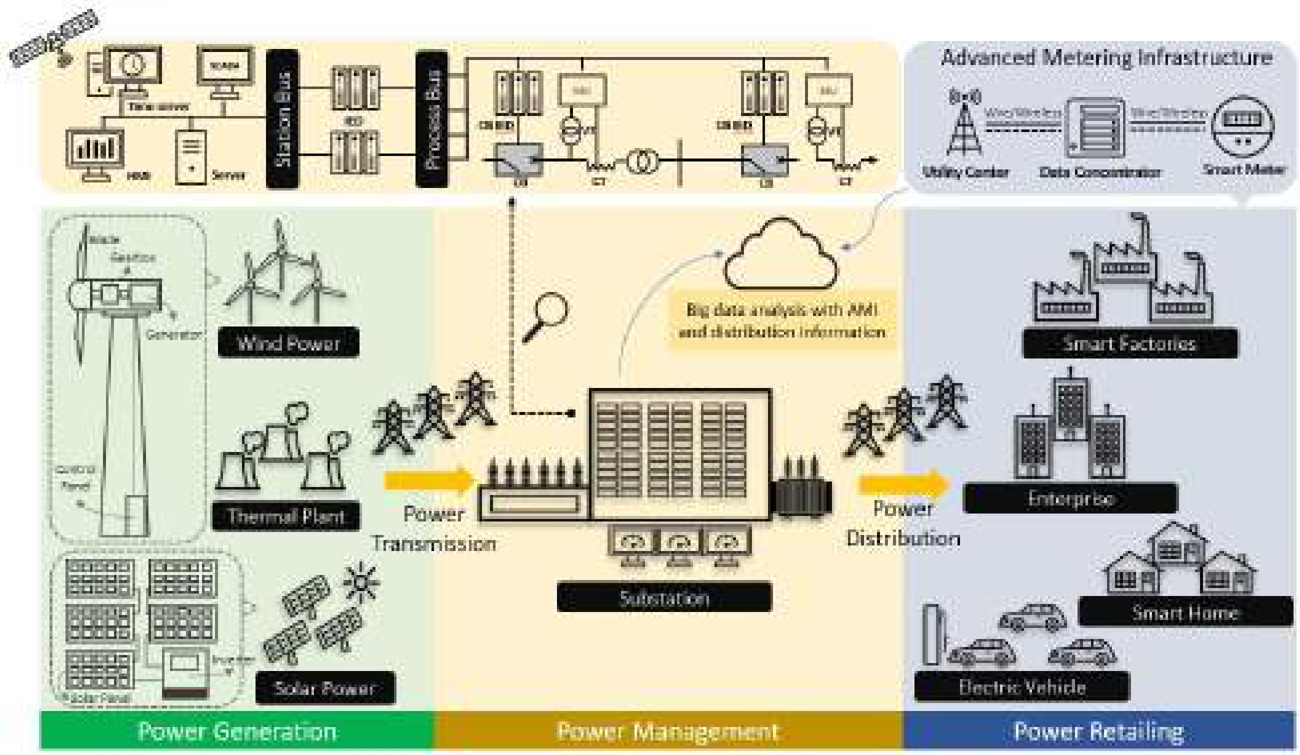


Figure-2. Power Industry Ecosystem

well as to synchronize the voltage and current vectors, Time-Sync devices are also used in substations.

With the development of digitization, power companies also analyze the data of the distribution process for big data analytics to effectively improve operational efficiency. Given the interconnected nature described above, attackers will have more opportunities to launch remote attacks on the ICS environment of power management.

POWER RETAILING

As shown in figure-2 in the blue area, after the power grid operator acquires the power, the next step is to sell it to the user. With the rise of smart factories, smart homes, and electric vehicles (EV), advanced metering infrastructure (AMI) can achieve real-time benefits such as power monitoring, scheduling, and distribution through networked smart meters. As the endpoint devices of AMI are often installed in geographically accessible locations and contain many network nodes, attackers can interfere with the connection between endpoint devices and the Utility Center in unguarded environments. In addition to potentially sending forged data, attackers can also cause the connection to be disrupted.

CYBERSECURITY RISKS

Review the power ecosystem in figure-2. The goal of the power industry is to provide power to consumers, and the equipment manufacturing, power generation, and power management before consumers obtain electricity are interconnected. Therefore, for attackers, it only takes one link in the ecosystem to disrupt the entire system. For example, as of December 31, 2022, about 40.7% of India's electricity comes from renewable energy. If attackers carry out a large-scale cyberattack on renewable energy generation, there is a chance that the shortage of power production will make it impossible to provide stable power to the Indian people due to a lack of sufficient power sources for management.

Given this, MITRE has established a SoT framework for the supply chain to establish trust and stability between enterprises and their supply chains through a series of assessments. When evaluating supply chain vendors, information security governance is an important basis, in addition to vendor reputation, geographical environment, and financial condition. For example, equipment manufacturers or power generators in the ICS environment inevitably face difficult-to-eradicate cybersecurity threats. However, whether they have sufficient countermeasures to ensure the stable supply of their products when facing information security threats is an important issue. Therefore, we will analyze potential cybersecurity threats at various stages of the power industry, and then we also propose zerotrust as a fundamental measure that does not affect the operation of the ICS environment.

POTENTIAL THREATS TO SUBSTAION

Figure-3 shows a schematic diagram of the network architecture of a substation. Like a typical ICS environment, it consists of a controller, HMI, historian, control server, and field devices. Due to the requirement of sub-microsecond level accuracy in power grid operation, a time server is adopted as one of the time synchronization solutions. With the drive towards digitalization, it is often necessary to use a standardized communication protocol to enable efficient communication between devices in both IT and OT environments. OPC-UA is one of the solutions for the substation. In this network architecture, we found the following potential network security threats.

OPC-UA: The mainstream OPC-UA packages currently in use are built on top of .NET Runtime (.NET Framework / .NET Core). However, the default memory stack size of .NET Runtime is limited, and an attacker can cause a stack overflow issue simply by exceeding a level of recursion depth. For example, as shown in CVE-2018-12086, an attacker can cause an OPC Server to crash by sending an ExtensionObject structure of only 64KB in size. Specifically, due to performance considerations, high-frequency APIs such as OpenSecureChannel, GetEndpoints, and FindServers used by OPC Server do not have whitelist authentication mechanisms, as shown in figure-4. Therefore, in CVE-2021-27432, an attacker can impersonate an OPC Client and initiate a FindServersRequest to the server without being restricted by the whitelist, while nesting OPC variables in this request. This will cause the .NET Runtime of the server to call functions too many times and ultimately cause a stack overflow, leading to the OPC Server being shut down. As the OPC server serves as a communication bridge between substation devices, its shutdown will affect the entire environment's operation [2][3].

Time Server: Due to its low cost and high accuracy, GNSS is commonly used as one of the time synchronization solutions in the power industry. However, GNSS signals may be affected by natural changes such as weather or space environment, and attackers also can interfere with the signals using stronger power, causing time synchronization failure in the power grid, and resulting in power outages. To verify that attackers can execute GNSS Spoofing attacks on vulnerable devices using software radio, we used the HackRF tool to spoof GPS location and cause the victim to receive incorrect time information as shown in figure-5. When the time information is incorrect and causes

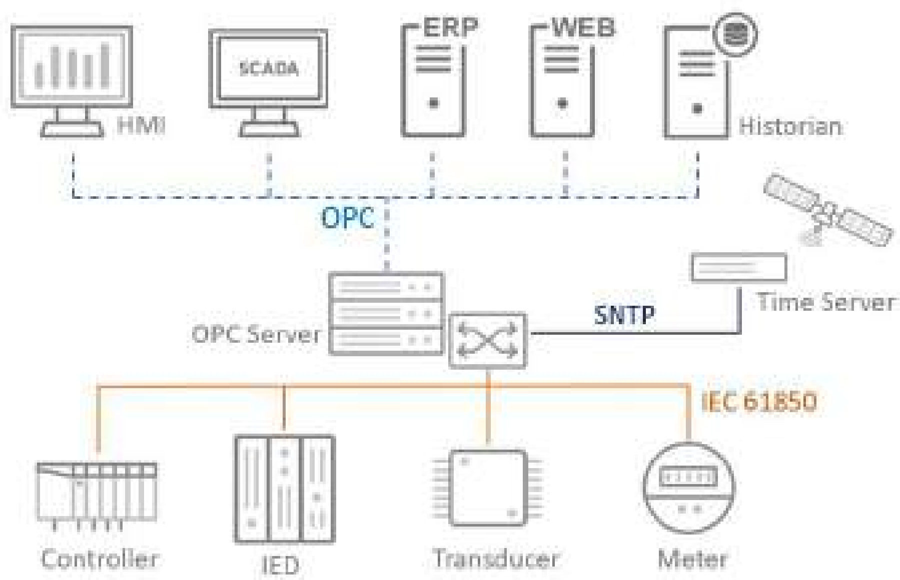


Figure-3. Digital Substation Architecture Sample

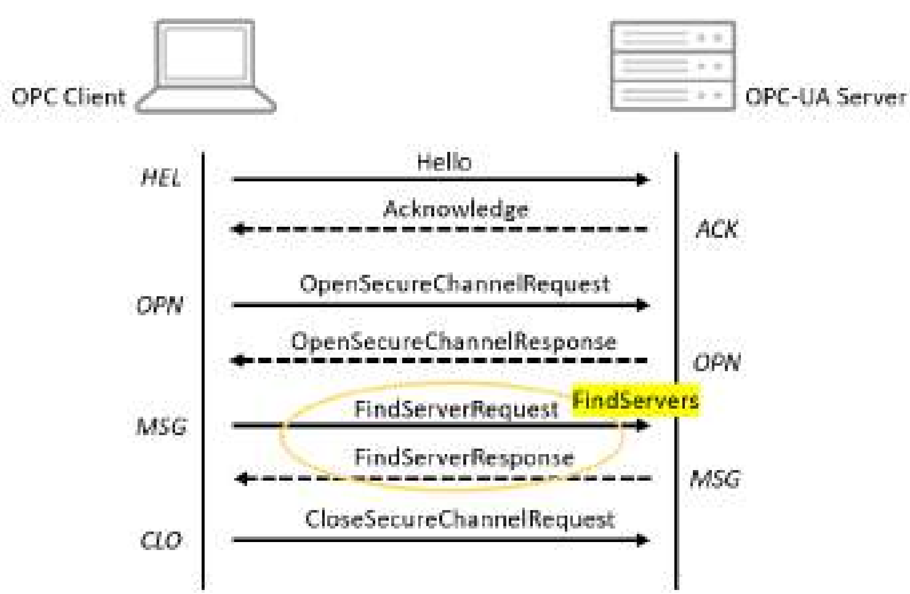


Figure-4. OPC Communication Flow

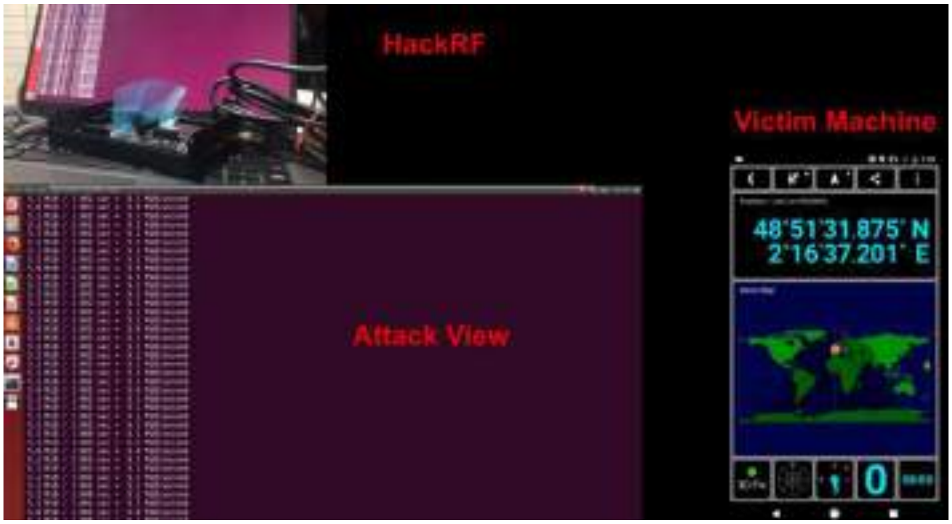


Figure-5. GPS Spoofing Attack

abnormal power supply and demand or frequency in the power grid, it will pose a potential threat of power outages.

IEC 61850: For substations using the IEC 61850 standard, it supports communication protocols such as MMS, GOOSE, SMV, SNTP, and IEEE1588. However, due to the low latency requirements of the IEC 61850 standard, it is difficult to implement data encryption measures (e.g., the maximum latency requirement for the GOOSE protocol is 4ms, and to achieve encryption within 4ms, a high-performance CPU needs to be installed in the IED, which requires redesigning the entire hardware equipment), leading opportunities for attackers to execute attacks such as man-in-the-middle or deception, causing distribution failures in the substation. In addition, the power generation plant's ICS protocols also provide opportunities for attackers to execute communication protocol attacks due to the high-speed transmission requirements. For instance, the Ethernet Global Data (EGD) communication protocol developed by General Electric (GE) uses the UDP protocol of the Ethernet network interface to provide fast data exchange between devices such as PLCs, drive systems, HMI, and SCADA. As this protocol lacks encryption and verification mechanisms, attackers can easily intercept and tamper with packet contents once they have entered the power plant's network.

POTENTIAL THREATS TO RENEWABLE ENERGY

Although renewable energy has been developing rapidly in the past, fossil fuels remain the primary method of power generation for countries due to the characteristics of dispersed energy data and difficult-to-track assets. With the digitalization of the power industry, companies can perform in-depth analysis through real-time information to predict maintenance and reduce downtime, or accurately predict weather and market conditions to make appropriate decisions and provide stable demand. These are all factors promoting the development of renewable energy in the power industry [4]. Among them, solar and wind power generation are the representatives of the highest capacity of renewable energy in recent years, and their structures can be referenced in figure-6 and figure-7, respectively. The following will analyze their potential network security threats.

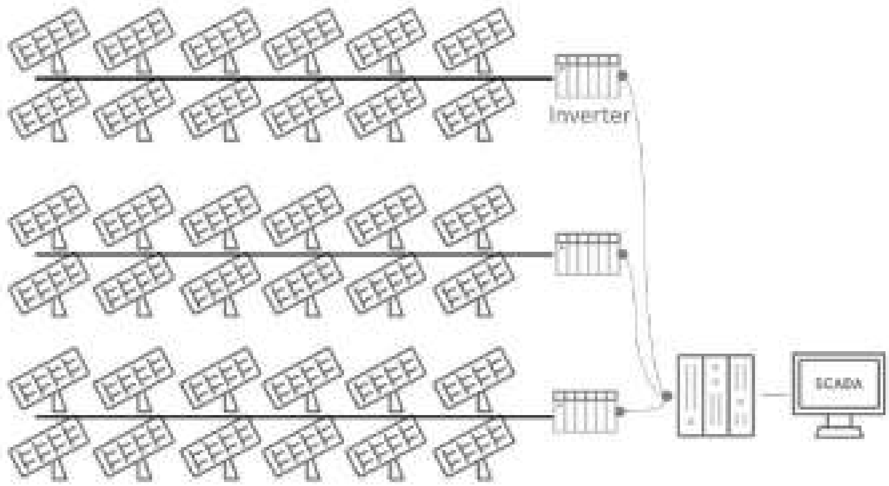


Figure-6. Solar Power Architecture

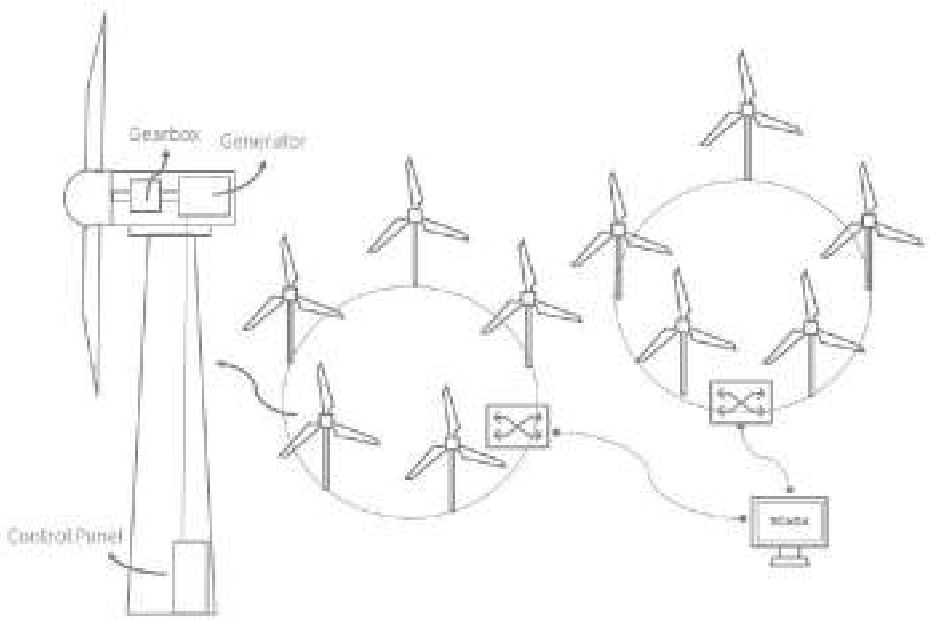


Figure-7. Wind Power Architecture

Solar Power: Solar power is a widely spread and difficult-to-manage power generation method, which includes many endpoint devices exposed outside, such as solar panels and networked inverters. Inverters from different regions can send power generation status to the controller over the network and receive control instructions. The controller then provides information to the back-end SCADA system. As mentioned earlier, inverters are exposed and difficult to be managed, making it easier for attackers to access them and execute large-scale attacks through their network. If the plant does not have alarm devices for damaged equipment, devices that restrict access, or network segmentation, attackers can perform control commands to multiple inverters simultaneously, causing large-scale power outages.

Wind Power: If we observe the internal structure of a wind turbine, in addition to the blades, gearbox, and generator on the top, there is also a networked control panel at the bottom.

Depending on the implementation, this control panel may include an HMI, controller, inverter, etc., and it also provides power information to the backend SCADA system. In real-world environments, wind turbines are often only protected by physical locks, which gives attackers the opportunity to directly break the locks, enter the turbine, and then connect to the SCADA system through the networked devices inside to perform control commands to other turbines.

POTENTIAL THREATS TO POWER EQUIPMENT MANUFACTURING

When it comes to renewable energy, robots inevitably become an asset for most digitalized factories, as they can improve product manufacturing efficiency, accuracy, and the ability to operate in dangerous environments. For example, the world's largest solar photovoltaics manufacturer, Jinkosolar, produces advanced solar cells using mobile robots. KMT Robotic Solutions company also uses robots for drilling and cutting the root end of turbine blades to achieve higher production rates [5]. The basic architecture of robots is shown in figure-8, and operators can perform control instructions to the controller through the pendant or control station (such as executing programs or adjusting parameters), and the controller can control the robot behavior based on the contents of the instructions. Similarly, the controller can receive robot data and provide it to the pendant and control station for operators to analyze or adjust in real-time. In addition to directly modify programs on robots through the pendant or control station, programmers can also use off-line programming (OLP) programs on the Engineer Workstation (EWS), to compile the best execution process through the 3D model in the simulator in an offline state, and then upload the program to the real robots for execution.

Under this architecture, renewable energy equipment manufacturers who use robots can enjoy higher manufacturing efficiency, but it also poses potential cybersecurity threats to their factories.

Controller: To provide operators with the convenience of operating robots through control station, sometimes the controller enables universal remote connection services such as FTP or Web, or APIs defined by the manufacturer. However, we found that the remote connection services they use often do not have appropriate credentials set up, and attackers can even access the controller remotely without authentication if they obtain the tools or API usage methods released by the manufacturer. Through the above methods, attackers can easily upload malicious configuration files or code to the controller, and cause the robot to execute malicious parameters, making the factory unable to continue producing precise products.

Control Station: Robot Operating System (ROS) is an application development framework designed specifically for robots and is widely used in the field of automatic control. With ROS 2 adopting Data Distribution Service (DDS) as the standard for data exchange, CVE-2021-38487 shows that the publish-subscribe communication pattern of this standard poses a threat of amplification attacks [6]. As shown in figure-9, attackers can send custom packets disguised as the victim device to the Control Station, causing the endpoint devices under its jurisdiction to execute amplification attacks on the victim device according to the communication process. By disrupting the victim device's service, the device cannot continue to manufacture products.

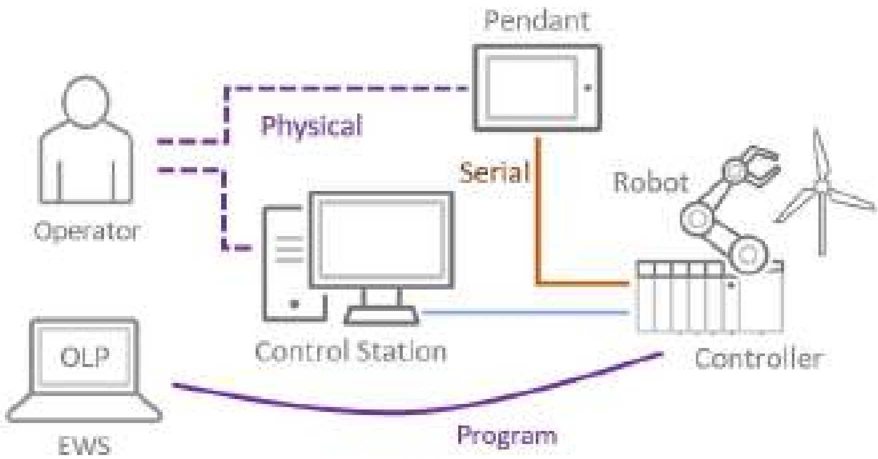


Figure-8. Robot Architecture

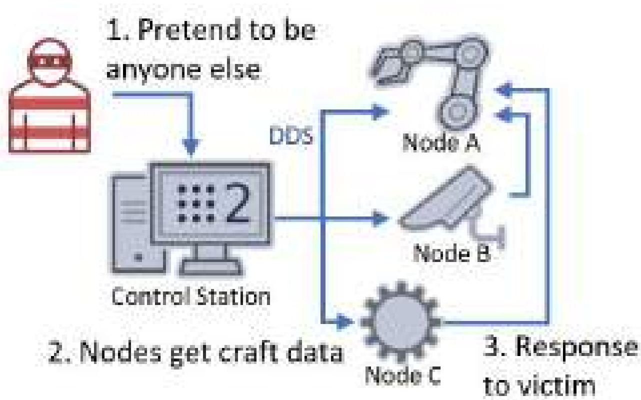


Figure-9. Amplification Attack Targeting Robot

OLP: OLP is a method of programming robots that is independent of the actual robot, using a 3D model in a simulator for offline editing. This helps developers to create the best path for specific tasks in EWS and then upload it to the actual robot for execution. Through our research, we have found that many of these OLP programs developed by various manufacturers are not secure. For example, we have found that some programs have vulnerabilities such as directory traversal, which allows attackers to remotely access any sensitive data in the EWS.

ZEROTRUST COUNTERMEASURE

Based on the analysis of the threats, we can see that the power industry, whether in power generation or management, is exposed to cybersecurity threats in the highly connected digital trend, even though highly connected devices can achieve more efficient operation. In response, we propose the concept of zerotrust - inspect, lock down, segment, and reinforce - for the ICS environment of the power industry.

INSPECT

Before new devices are introduced into the ICS environment, we need to conduct a thorough inspect to ensure that no viruses are hidden within them. Since the initial attack on ICS may come from equipment suppliers or system integrators, power industry operators should conduct malicious program scans for each asset entering the ICS environment and establish a health record for them. For example, if a system integrator's equipment is installed with malicious programs due to the use of vulnerable OLP software, implementing the Inspect step can prevent the malicious program from entering the ICS environment.

LOCK DOWN

Because most ICS critical assets operate in a fixed manner, we can create network rules allow lists to prevent abnormal connection behavior. In the case of digitalized substations using OPC, even if an attacker launches a malicious FindServersRequest that is not restricted by the whitelist to the OPC server, due to the network operation behavior has been locked down, the OPC server will not shutdown.

SEGMENT

This means that networks of different areas or different generator sets need to be isolated from each other to lock the impact of attacks within a specific range. For example, in the case of renewable energy, if an attacker attacks a certain inverter from the outside, due to the network of different areas has been isolated, the attacker can only affect a specific range, avoiding large-scale disasters.

REINFORCE

From the potential cybersecurity threats analyzed earlier, we can see that in the digital power industry, attackers have many opportunities to access its ICS environment. Like most critical infrastructure, there are issues with difficult security updates for control devices, which makes it easy for attackers to further persecute the environment. Therefore, we can use network-level virtual updates to intercept packets when attack features occur, preventing them from actually contacting devices until future conditions allow for updates.

CONCLUSION

In this paper, we analyzed the network architecture of digital substations and the most common renewable energy sources in India and their supply chains. We have discovered multiple potential cybersecurity threats. These threats demonstrate how attackers can infiltrate the ICS environment of the power industry using certain techniques. If attackers successfully exploit these threats, it may cause damage to the national economy and even threaten people's survival. Therefore, based on the discovered threats and the characteristics of ICS, we propose the practice methods of zerotrust. Through these methods, we can mitigate the impact that attackers may have on the power industry and maintain a stable power supply.

ACRONYMS

RTU	Remote Terminal Unit
IED	Intelligent Electronic Device
PLC	Programmable Logic Controller
HMI	Human Machine Interface
SCADA	Supervisory Control And Data Acquisition
EV	Electric Vehicle
AMI	Advanced Metering Infrastructure
EGD	Ethernet Global Data
GE	General Electric
OLP	Off-line Programming
EWS	Engineer Workstation
ROS	Robot Operating System
DDS	Data Distribution Service

REFERENCES

[1] https://page.advantech.com/en/global/industrial-automation/industrial-io/opc-ua

[2] https://nvd.nist.gov/vuln/detail/CVE-2018-12086

[3] https://nvd.nist.gov/vuln/detail/CVE-2021-27432

[4] https://nexusintegra.io/digital-transformation-renewable-energy

[5] https://www.ennomotive.com/robots-automation-renewable-energy

[6] https://nvd.nist.gov/vuln/detail/CVE-2021-38487

BIOGRAPHIES

Yenting Lee is a threat researcher at TXOne Networks, blending experience in ICS/SCADA, cyber offensive and defensive exercises, penetration testing, honeypot, and image processing. Yenting has spoken at several conferences such as FIRST Conference, ICS Cyber Security Conference USA/APAC, CYBERSEC, and InfoSec Taiwan. So far, he has also contributed several white papers and vulnerabilities on the topics of ICS.

Debraj Chakraborty is the Country Sales Manager for TXOne Networks India. He has a blend of Business as well technical expertise in ICS/SCADA cyber security systems in India as well as in the MENA and SEA region. While his stint with a leading Japanese Automation OEM, Debraj contributed to the architect teams ensuring complete cyber resiliency for the customer environment. Debraj is a frequent speaker in several talks around the country as well the cross regions viz: ISA chapters in Delhi / Malaysia / Bahrain / UAE, several cyber security events in ARAMCO / SABIC etc. and events organized by PETRONAS / TNB (Malaysian Power Company). During the pandemic situation he even contributed to several online blogs and e-magazines explaining the need for Cyber Security in environments where the customers had no choice but allow their OEM vendors access their critical systems with the presence of either minimum or even no cyber defense in place.

Mars Cheng is a manager of TXOne Networks PSIRT and threat research team, responsible for coordinating product security and threat research, and is the executive director of Association of Hackers in Taiwan. Mars blends a background and experience in both ICS/SCADA and enterprise cybersecurity systems. Mars has directly contributed to more than ten CVE-IDs, and has had work published in three Science Citation Index (SCI) applied cryptography journals. Before joining TXOne, Cheng was a security engineer at the Taiwan National Center for Cyber Security Technology (NCCST). Mars is a frequent speaker and trainer at several international cyber security conferences such as Black Hat, RSA Conference, DEFCON, SecTor, FIRST, HITB, ICS Cyber Security Conference Asia and USA, HITCON, SINCON, CYBERSEC, and CLOUDSEC. Mars was the general coordinator of HITCON (Hacks in Taiwan Conference) PEACE 2022, HITCON 2021, and vice general coordinator of HITCON 2020.

Sheng-Hao Ma is currently working as a senior threat researcher at TXOne Networks, specializing in Windows reverse engineering analysis for over 10 years. In addition, he is currently a member of CHROOT, an information security community in Taiwan. He has also served as a speaker and instructor for various international conferences and organizations such as Black Hat USA, DEFCON, CODE BLUE, HITB, VXCON, HITCON, ROOTCON, Ministry of National Defense, and Ministry of Education. He is also the author of the popular security book "Windows APT Warfare: The Definitive Guide for Malware Researchers".

Industry 5.0: Looking into the Future

Authors: Sh. Alok Kumar Sinha, Sh. P.K Gupta, Sh. Sumit Kumar Haldar

1.0 Preamble:

Perhaps the greatest learning from the Industry 4.0 era was the understanding that technology alone does nothing. Machines depend on operators, programmers, and maintenance. Not everything can be automated. Additionally, it is to be noted that human cognitive power and analytical capabilities remain irreplaceable. Industries work by transforming resources into goods, but the most valuable and irreplaceable resource in any industry is the people that work in it and uses its products. Industry 5.0's focus is on creating value beyond financial results. Industry 5.0 seeks to improve the quality of life, not only of people involved in industrial processes but of society as a whole.

2.0 Introduction:

Industry 5.0 is already an emerging trend and the future. It stands for the interaction and collaboration between man and machine. This cyber-physical systems revolution that was summarized in Industry 4.0 has evolved into Industry 5.0 and is fundamentally changing the way we live, work, and relate to one another. Industry 5.0 recognizes the power of industry to achieve societal goals beyond jobs and growth, to become a resilient provider of prosperity by making production respect the boundaries of this planet and placing the well-being of the industry worker at the center of the production process. Industry 5.0 complements the existing Industry 4.0 paradigm by having research and innovation drive the transition to a sustainable, human-centric and resilient industry. This next wave of industrial revolution is slated to define how we collaborate and how we define the rules between human and machine interaction. The levels of collaboration between people and machines will change given that most automation, machine intelligence, and even robots are working in the background, to support the workforce or taking on large portions of production and manufacturing tasks and processes.

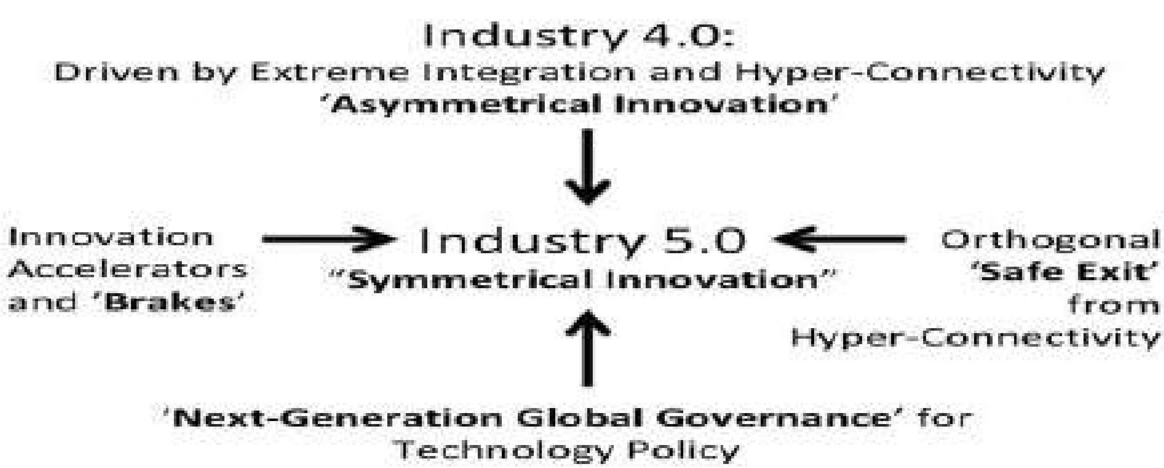


Figure-1 Industry 5.0 Symmetrical Innovation (from Open source)

Business leaders can no longer focus on developments and trends in their sectors alone but will need to understand potential transformations and disruptions in the entire world of suppliers, customers and global markets. The rapid pace of change is challenging the entire workforce, governments, legislators and regulators to an unprecedented degree. The world of the "work-life merge", the term coined by Facebook executive Emily White in 2012 describes a life in which work and free time are no longer neatly compartmentalized but seamlessly jumbled up together. This aspect which actually got accelerated due to COVID-19 is in most probability going to be the new norm in the near future. At the same time, there is a risk that parts of society might feel left out due to the perception that jobs are being taken away by automation and immigration, or because they lack the skills required for the newly created jobs. In fact Industry 5.0 has not kept people from getting jobs, but Industry 5.0 brought about the importance of including human beings in the process. The infographic below illustrates this paradigm shift:

Figure-2 Industry 4.0 vis-à-vis Industry 5.0 (from Open source)

3.0 Industry 5.0 Constituents:

Industry 5.0 centers around three interconnected core values: human-centricity, sustainability and resilience. The human-centric approach puts core human needs and interests at the heart of the production process, shifting from technology-driven progress to a thoroughly human-centric and society-centric approach. As a result, industry workers will develop new roles as a shift of value from considering workers as "cost" to "investment". Technology is to serve people and societies, meaning that technology used in manufacturing is adaptive to the needs and diversity of industry workers. A safe and inclusive work environment is to be created to prioritize physical health, mental health and wellbeing, and ultimately safeguard worker’s fundamental rights, i.e., autonomy, human dignity and privacy. Industrial workers need to keep up-skilling and re-skilling themselves for better career opportunities and work-life balance.

Figure-3 Three facets of Industry 5.0 (from Open Source)

For industry to respect planetary boundaries, it is required to be sustainable. It needs to develop circular processes that re-use, re-purpose and recycle natural resources, reduce waste and environmental impact, and ultimately lead to a circular economy with better resource efficiency and effectiveness. Resilience refers to the need to develop a higher degree of robustness in industrial production, arming it better against disruptions and ensuring it can provide and support critical infrastructure in times of crisis. The future industry needs to be resilient enough to swiftly navigate the political / geopolitical shifts and natural emergencies. Industry 5.0 identified the following six enabling technologies:

1 Individualized human-machine interaction technologies that interconnect and combine the strengths of humans and machines.

2 Bio-inspired technologies and smart materials that allow materials with embedded sensors and enhanced features while being recyclable.

3 Digital Twins and simulation to model entire systems.

4 Data transmission, storage, and analysis technologies that are able to handle data and system interoperability.

5 Artificial Intelligence to detect, for example, causalities in complex, dynamic systems, leading to actionable intelligence.

6 Technologies for energy efficiency, renewables, storage and autonomy

4.0 Challenges & Responses:

Industry 5.0 present some unique challenges that are not seen in the past such as

• Social heterogeneity in terms of values and acceptance

• Measurement of environmental and social value generation

• Integration from customers across entire value chains to SMEs

• Inter-disciplinarity of research disciplines and system complexity

• Ecosystem-oriented innovation policy with agile, outcome-orientation

• Productivity is required, while large investments are needed

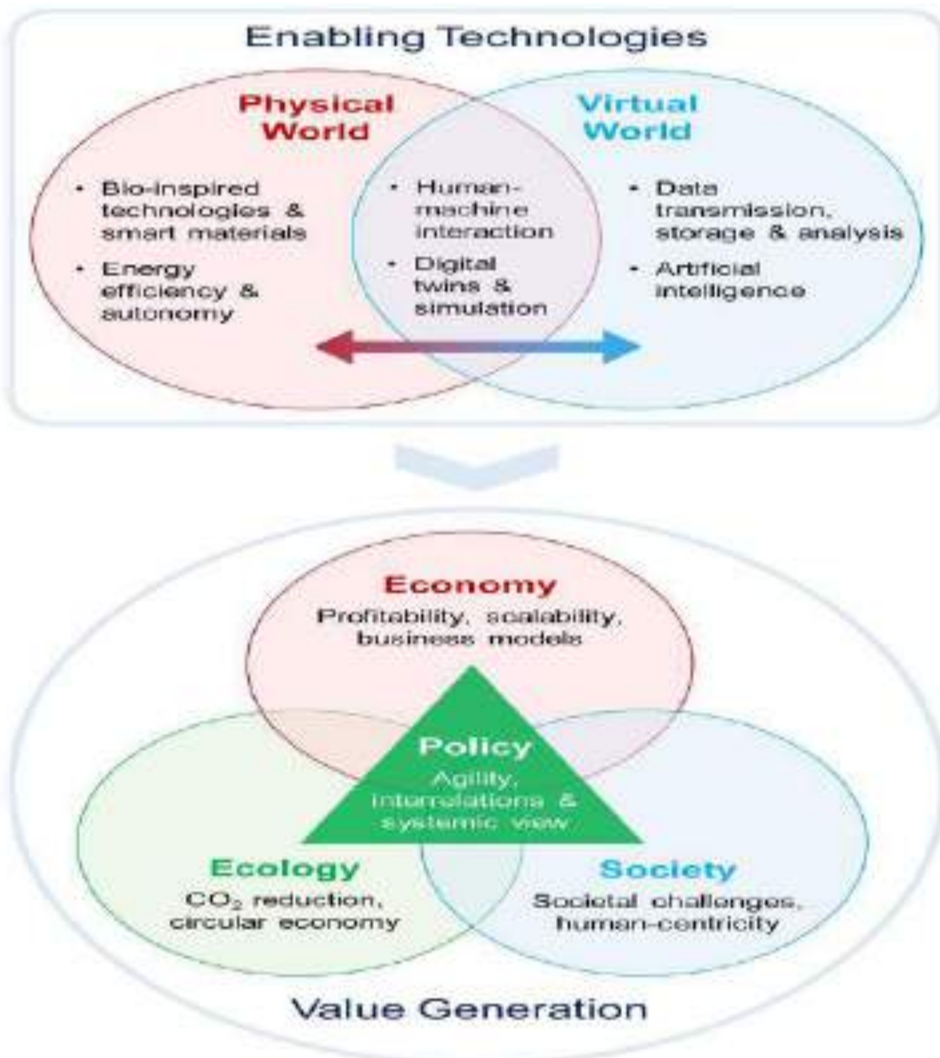


Figure-4 Enabling Technologies & Value Generation (from Open Source)

5.0 Technologies forming the foundation of Industry 5.0

Boston Consulting Group identified nine key enabling technologies of Industry 4.0, whereas the EU identified six enabling technologies of Industry 5.0. These technologies can be identified as

1. Artificial Intelligence and Machine Learning
2. Robotic Process Automation (RPA)
3. Edge Computing
4. Quantum Computing
5. Virtual Reality and Augmented Reality
6. Blockchain
7. Internet of Things (IoT)
8. 5G
9. Cyber Security

The terminologies used for these technologies may differ, but there is a clear cross-over. It is believed that many enabling technologies of Industry 4.0 can help, and will undoubtedly be used to, achieve the societal goals of Industry 5.0. There are, however, some more targeted technologies of Industry 5.0 that require attention, such as bio-inspired technologies and technologies for energy efficiency, storage, and renewable energy.

Unlike Industry 4.0, Industry 5.0 makes a bold focus shift from individual technologies to a systematic approach. This approach empowers the industry to achieve societal goals beyond jobs and growth and places the wellbeing of the industry worker at the center of the production process. This may help explain why Industry 5.0 is considered a different type of Industrial Revolution from the other Industrial Revolutions. Industry 5.0 is not a chronological continuation of, or an alternative to, the existing Industry 4.0 paradigm. Industry 5.0 is the result of a forward-looking exercise, a way of framing how industry and emerging societal trends and needs will co-exist. As such, Industry 5.0 complements and extends the hallmark features of Industry 4.0.

Top technological advancements to be considered for Industry 5.0:

1. **AI Powered Cybersecurity**: The steep increase in cyberattacks, email phishing scams, and ransomware is forcing cybersecurity firms to search for tech solutions to address the vulnerabilities. Criminals are hacking individuals' accounts, countries' critical infrastructure, and businesses of all sizes, causing millions of dollars in losses. Workplace digitization and remote working in response to the COVID-19 virus made it a priority to retrain employees on online safety to reduce data breaches and losses. Businesses are also adopting new cybersecurity technologies, such as

artificial intelligence (AI), to monitor and guard networks against hackers in real-time rather than responding to the threat after the damage is already done. Moreover, cloud storage companies are offering end-to-end encryption for online data storage and data transfers.

2. **5G Technology Adoption**: 5G will boost the Internet of Things (IoT), which involves internet-powered smart devices linking and operating together. Unlike with 4G, many devices can connect to the 5G network without a significant drop in speed, latency, and reliability. That's because of the network-slicing feature that creates independent networks offering different services for each device.
3. **Internet of Behaviors (IoB):** Businesses are using analytics and big data techniques to determine the data's value in what is now known as the Internet of Behaviors (IoB). By reviewing this customer information, businesses can personalize their services, market their products, and improve a customer's experience with the company. Website hacking and other cybersecurity challenges also make customers uncomfortable about risking their privacy in return for valuable services. A different approach to data collection will be vital for businesses' data analysis needs.
4. **Artificial Intelligence and Machine Learning of Things:** Artificial intelligence is one of the most consistently evolving technologies in the world. Its widespread use symbolizes its potential to provide solutions in multiple industries, from health, security, and education to logistics and information technology. Applications of AI include automation in manufacturing, guiding self-driving cars, operating as smart online assistants such as Siri or Google. Cognitive Manufacturing is usually reffered to as a combination of IoT and analytics (or artificial Intelligence) meant to make full use of the enterprise data and information, from the design to shop-floor and maintenance, in order to
    a. Intelligently use assets and equipments
    b. Develop cognitive processes by analyzing information from workflows and context/ environment, in order to enhance decision-making
    c. Optimization of resource use (with a special insight on knowledge management)

    Cognitive technical systems should have the ability of perceiving situations, identify them and decide either to apply an existing procedure or to try a set of actions that may address parts of the identified situation, allowing the fulfillment of the system's goals. However, perhaps the most potent power of AI is in analyzing large chunks of data and providing reports that can be used by organizations to develop strategies and solutions.

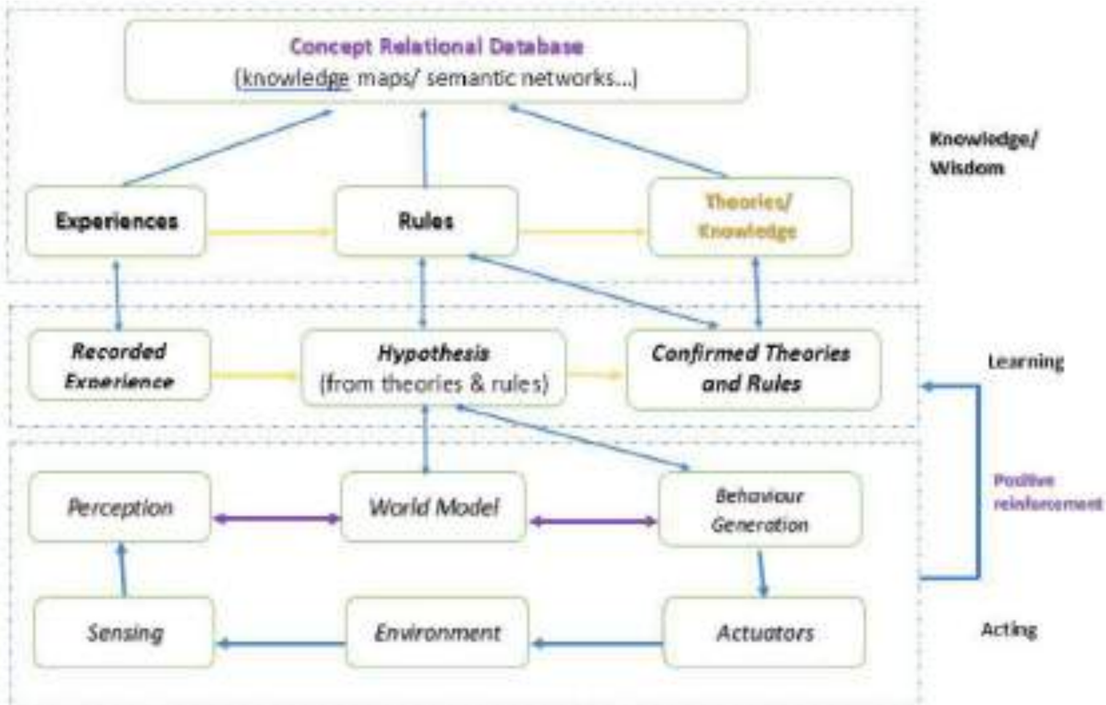


Figure 5 – Perception-oriented Architectural approach for Cognitive Enterprise (from Open Source)

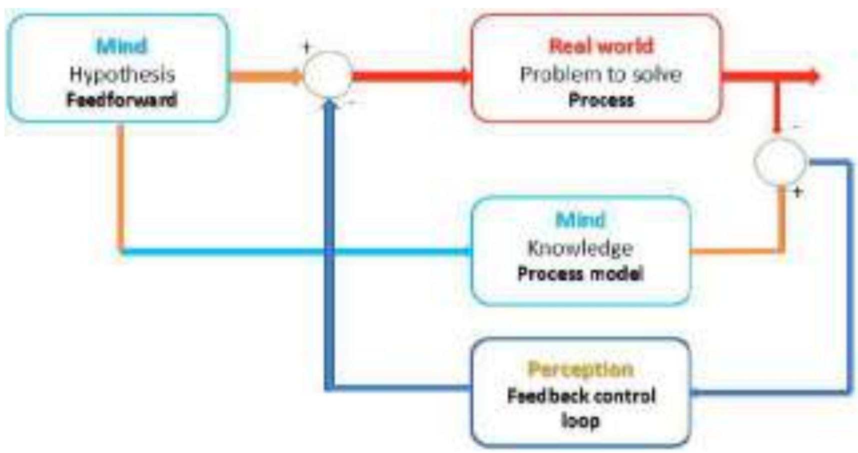


Figure 6 – Feedback and Feed-forward loop for the perception oriented architectural approach. (from Open Source)

5. **Metaverse:** The metaverse is a virtual, three-dimensional space that people can log into as avatars to socialize, work, shop, collaborate, or play games together. Companies are investing in novel technologies to bring the metaverse to life, such as virtual reality (VR) and augmented reality (AR). For example, VR headsets enable people to explore and immerse themselves in digital worlds and share experiences.
6. **Blockchain Technology:** After years of uncertainty, blockchain technology is now establishing itself as a viable solution to many tech challenges. Blockchain is a distributed ledger of decentralized data, and it underpins cryptocurrencies, digital payment technologies, encryption

technology, and blockchain gaming. A rising trend is for content creators to use non-fungible tokens (NFTs)—blockchain data units that are not interchangeable–to create digital work, sell it online, and earn cryptocurrencies. Blockchain's ledger feature is making the technology applicable for storing medical data and other personal records, protecting copyrights, listing title deed owners, tracking digital transactions, trading in NFT marketplaces, and supply chain monitoring.

7. **Clean Technology (cleantech):** The desire for sustainable living is influencing the development of new technologies known as clean technologies–or cleantech, in short. Cleantech reduces the environmental impact of products or services while optimizing the use of natural resources. Renewable energy has been the most notable attempt at developing sustainable technologies, with wind, hydroelectric, and solar power having a lower carbon footprint than fossil fuels. Currently, the top cleantech trends include rechargeable batteries, electric vehicles and motors, solar panel development, biofuel-powered turbo generators, and waste management technologies.
8. **Educational Technology:** Educational technology (edtech) companies have emerged to provide solutions by creating digital platforms for remote learning. Investments in the e-learning industry are increasing as startups form to innovate online education software and video conferencing technologies to give students access to teachers and courses. Online classes can be made fun and engaging by gamifying the experience. Integrating AI into the teaching platforms personalizes the coursework, tracks students' learning styles, provides reports on their progress, and automates grading. In addition, AI simplifies the curriculum-creation process by reviewing the educational content available and highlighting what should be included in the lessons.
9. **Collaborative robotics & related technologies:** Collaborative robots are a relatively new invention in the robotics industry, but already, there are several different kinds. Their instant success in a wide range of industries has spurred rapid product innovation, resulting in four major types of collaborative robots. The different types of collaborative robots are defined by their safety and programming features, or the way in which they avoid potentially dangerous encounters with human workers. Each type of collaborative robot deploys unique methods and technologies to maintain a safe operating space - this difference defines which environments they're best suited for.

   Major Types of Collaborative Robots:

   According to ISO 10218 part 1 and part 2, the four types of collaborative robots are defined as safety monitored stop, speed and separation, power and force limiting, and hand guiding.

a. *Safety Monitored Stop*: collaborative robots defined as safety monitored stop are intended for applications that have minimal interaction between the robot and human workers. Typically, these types of collaborative robots actually leverage an industrial robot with a series of sensors that stop robot operation when a human enters the work envelope.

b. *Speed and Separation*: these types of collaborative robots are similar to safety monitored stop collaborative robots in the fact that they leverage an industrial robot. However, speed and separation collaborative robots use more advanced vision systems to slow operations down when a human worker approaches and stop operation altogether when a worker is too close to the robot.

c. *Power and Force Limiting*: these types of collaborative robots are built with rounded corners and a series of intelligent collision sensors to quickly detect contact with a human worker and stop operation. These collaborative robots, which use collaborative robot arms, also feature force limitations to ensure any collisions are unlikely to result in injury.

d. *Hand Guiding*: these collaborative robots are equipped with a hand-guided device by which an operator directly controls the motion of the robot during automatic mode. While in automatic mode, the robot performing hand-guiding collaboration responds only to the operator's direct control input. This allows the robot, for example, to support the weight of a heavy workpiece while the operator manipulates it into position, thereby reducing the operator's risk of repetitive-stress injury. Similar capabilities can be used to "teach" or program a robot, but properly speaking, hand guiding as a collaborative operation occurs while the robot is in automatic mode, during normal production, whereas programming is not done in automatic mode nor used during production.

The four major types of collaborative robots defined above include every type of robot intended for some degree of human interaction during operation. Not all are built for constant collaboration, but each features a number of safety capabilities to prevent serious injury. Collaborative robots have been an important development in the robotics industry - the first automation technology that allows safe operation directly alongside human workers. The four types of collaborative robots have emerged in a relatively short time span and more are likely to emerge as the industry matures.

10. **Bionics & Synthetic Bionics:** Bionics is "the imitation or abstraction of the inventions of nature" (Sachsenmeier, 2016). According to European Commission (2012), bioeconomy is "The production of renewable biological resources and the conversion of these resources and waste streams into value added products, such as food, feed, biobased products and bioenergy. It includes agriculture, forestry, fisheries, food and pulp and paper production, as well as parts of chemical, biotechnological and energy industries. Its sectors have a strong innovation potential due to their use of a wide range of sciences (life sciences, agronomy, ecology, food science and social sciences), enabling and industrial technologies (biotechnology, nanotechnology, information and communication technologies (ICT), and engineering), and local and tacit knowledge". Bioeconomy

is crucial in achieving a sustainable economy (Schütte, 2017). Smart use of biological resources for industrial purposes will help to achieve a balance between ecology, industry, and economy.

Research on five emerging areas are being given priority. These are

- Securing global nutrition,
- Ensuring sustainable agricultural production,
- Producing healthy and safe foods,
- Using renewable resources for industry,
- Developing biomass-based energy carriers.

Another vision for Industry 5.0 is set forth by Michael Rada (Rada, 2015; Rada, 2017). Rada states that the priority of Industry 5.0 is “to utilize efficiently workforce of machines and people, in synergy with the environment. It goes back from a virtual environment to a real one.” He also provided a definition for industry 5.0 (Rada, 2017). The theme of this vision is Industrial Up-cycling. This vision focuses on waste prevention. Furthermore, Rada points out that we need to turn to human element in the manufacturing process. He criticizes the current digitization trend that is the effort to embed 1s and 0s into any living organism (Rada, 2015). According to Rada, Industry 5.0 includes 6R methodology and L.E.D. principles. The 6R are:

1. Recognize: First, we need to recognize the opportunities offered by Industrial Upcycling. An awareness is the first required step.
2. Reconsider: We need to evaluate and reconsider our business and manufacturing processes. A redesign of processes to realize the benefits of Industrial Upcycling is an essential step.
3. Realize: After recognition of the opportunities and reconsideration of business processes, we need to realize the business process improvement or innovation.
4. Reduce: Reducing the use of resources to achieve efficient outcomes is the essence of the methodology.
5. Reuse: Reusing the materials considered as useable prior to process improvement is also at the center of the methodology.
6. Recycle: Recycling as much as possible is one of main expected outcomes of the Industrial Up-cycling effort. Naturally, the ideal is the zero waste.

6R methodology actually defines a business improvement model. Depending on the specific case, it can be considered as a business process improvement or a business process innovation. Therefore, the 6R methodology is subject to the rules, assumptions, and dynamics of process improvement efforts. L.E.D. stands for Logistics Efficiency Design. It is designed for global supply chain efficiency improvements. Its goal is to eliminate the waste created by the current modern standard buyer-supplier business relations. L.E.D is the concurrent application of transparency, profit sharing, and efficiency in the supply chain (Rada, 2017). Four types of waste are identified in Industrial Up-cycling. These are physical waste, social waste, urban waste, and process waste.

Physical Waste: The actual physical waste introduced during and after the production. It is basically the trash.

Social Waste: It is the unused potential of the manpower. People unemployed is at the heart of social waste.

Urban Waste: This type of waste includes brownfields, empty spaces, and inadequate infrastructure.

Process Waste: Overproduction, overstocking, empty transport vehicles on the roads are among the process waste.

According to Rada, Industry 4.0 focus at best is on quantity and mass production. However, the focus of Industry 5.0 is a higher life standard and creativity with high quality custom made products. The theme of Industry 5.0 is simply sustainability. In recent years many companies started programs for green manufacturing and production. Furthermore, there is renewed focus on social responsibility projects. The awareness for environmental protection is increasing among people. Customers begin choosing products developed by companies promoting green production. A quick analysis of the comparison shows that industry 5.0 will have a wider and deep impact on society.

	Industry 4.0	**Industry 5.0**
Motto	Smart Factory	Bioeconomy
Motivation	Mass Production	Sustainability
Power Source	Electrical power - Fossil based fuel - Renewable power sources	Electrical power - Renewable power sources
Involved Technologies	- Internet of Things (IoT) - Cloud Computing - Big Data - Robotics and Artificial Intelligence (AI)	- Sustainable Agricultural Production - Bionics - Renewable Resources - Human Robot Coordination
Involved Research Areas	- Organizational Research - Process Innovation and Improvement - Business Administration	- Agriculture - Biology - Waste Prevention - Organizational Research - Process Innovation and Improvement - Business Administration

6.0 Discussions and Conclusion:

Industry 4.0 is still in its early stages. It was officially introduced in the beginning of 2010s. In only a few years, experts and academia started discussing Industry 5.0. Moreover, these experts also point out the inadequacies of Industry 4.0 and propose Industry 5.0 to overcome the shortcomings of Industry 4.0. One logical conclusion is that Industry 4.0 was introduced without adequate vision. Previous industrial revolutions occurred naturally unlike Industry 4.0, which is formally defined and forced upon the industry. It is possible to argue that this artificial revolution start is premature and proposed without adequate maturity. To call a concept an industrial revolution, we need to observe a widespread change both in industries, businesses, and society. Currently, with its current definition, Industry 4.0 should actually be a proposal. It is clear that Industry 4.0 is still under development.

Smart mass production seems to be the goal of Industry 4.0. Sustainability is main theme in Industry 5.0 proposals. Actually, they are both inadequate by themselves as sustainability and mass production are not mutually exclusive. Therefore, combining these two goals or themes and redefining the next industrial revolution may be a better approach. As a result, the motto of the next industrial should at least be "sustainable smart production". Furthermore, the next industrial revolution – regardless of its name, version, and definition – should encompass the following technologies and research areas:

- Internet of Things (IoT)
- Cloud Computing
- Big Data
- Robotics and Artificial Intelligence (AI)
- Sustainability and environmental protection
- Bioeconomy
- Waste Prevention
- Business Administration and Organizational Research

Analytical, Automation & Instrumentation Solution Offerings

AXIS

AXIS SOLUTIONS PVT. LTD.

Plot No. 324, Road No.5, G.I.D.C., Kathwada, Ahmedabad-382 430, Gujarat, India.
Tel. : +91792290 0860/61 | Fct. : 9925001633 / 9909906354
info@axisindia.in | www.axisindia.in

Session 3

Session 3

1. Reliability for effective safety Management - Forbes
2. Micro Modular Smart Sample Conditioning – Spirare
3. Molecular Technology for Health Monitoring of Critical Equipment – Protech
4. Enhancing reliability and resilience of generation thru Cyber Security - NTPC

Reliability for Effective Safety Management of Rotating Machines with Condition Monitoring

By

Mukesh Vyas
Forbes Marshall
mvyas@forbesmarshall.com

Agenda

Condition Monitoring of Rotating Asset

- Why Required & Global Trend
- Monitoring System : API670 & Non API670

Wireless Solutions

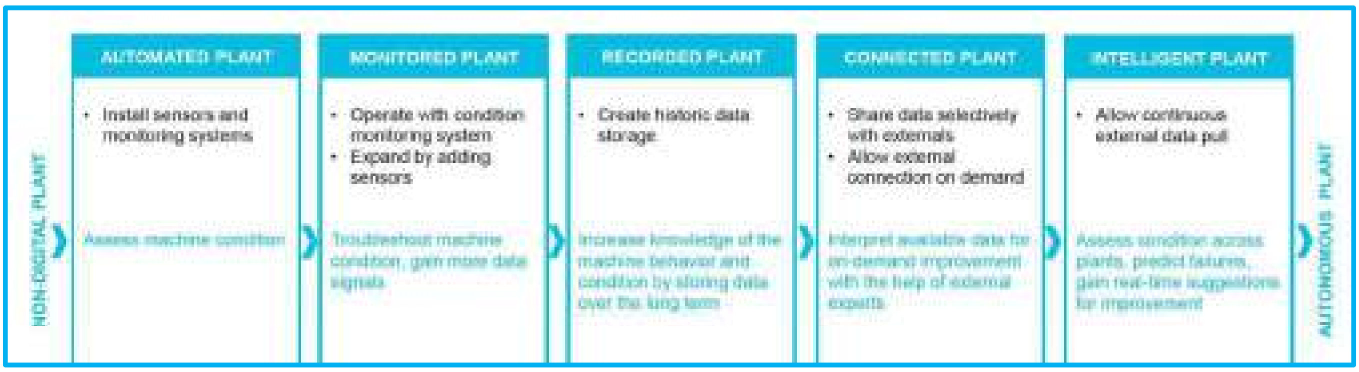
Cyber Secure Solutions

Cloud Based Solutions (Make in India)

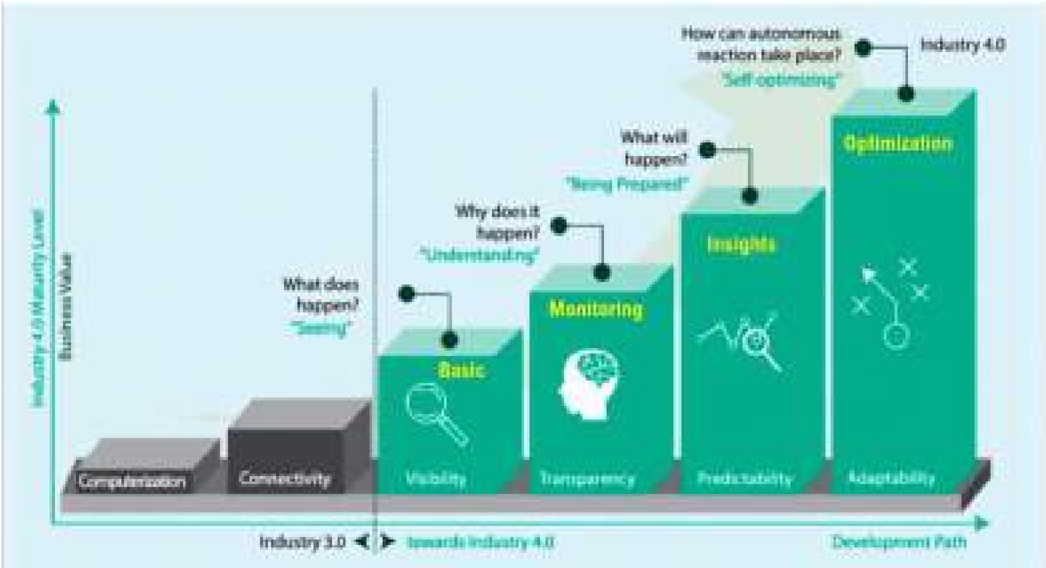
Conclusion

“Machinery Protection System”

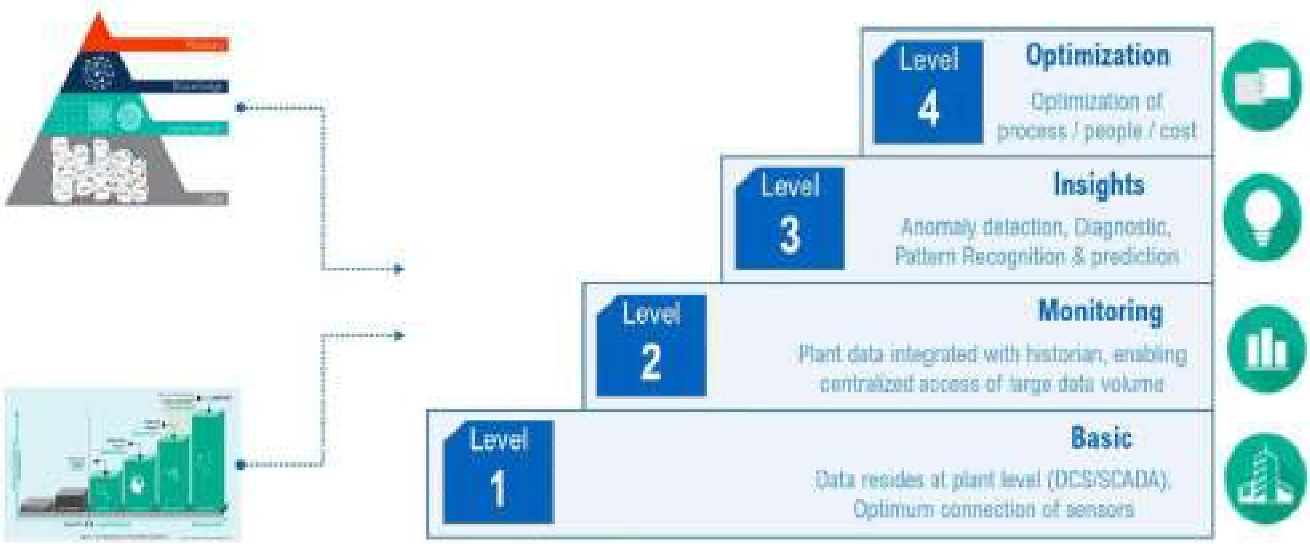
“The use of systems that shut a machine down or return it to safe or nondestructive mode of operation without human intervention”



Forbes Marshall Confidential
mvyas@forbesmarshall.com

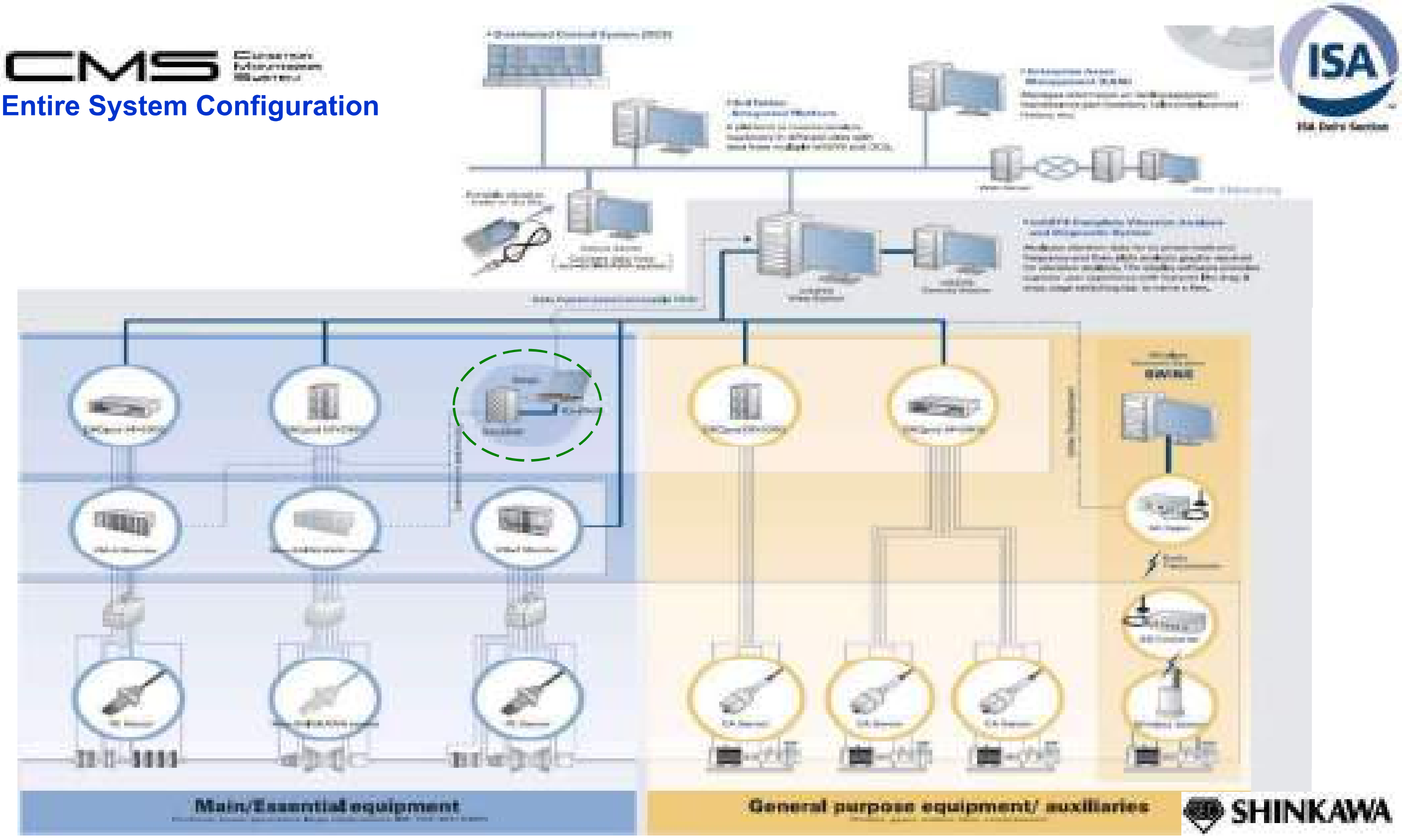


- Organizations are moving towards Industry 4.0
- There are 4 maturity levels identified in development towards Industry 4.0
- These building blocks can provide the platform in understanding assets or equipment performance
- Subsequently can present information for decision making by asset owners

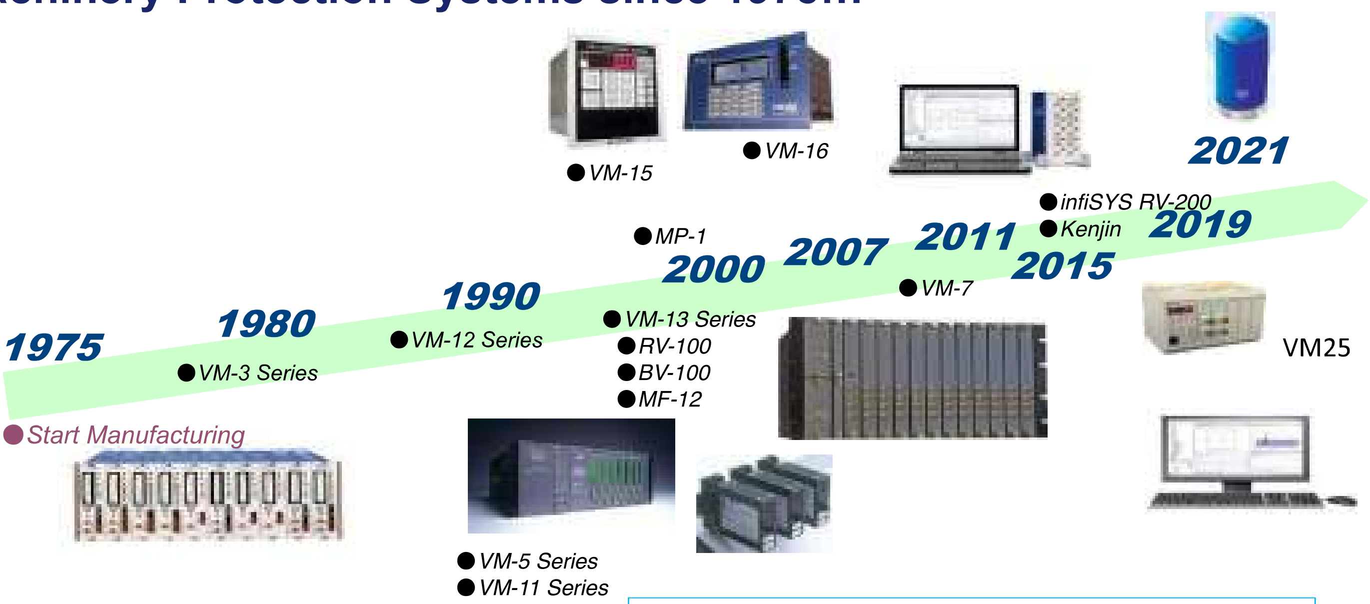


CMS

Entire System Configuration



Machinery Protection Systems since 1975…



Analog Solutions …….Digital Solutions

1) API 670 System for Critical Machines
2) Cloud Based Monitoring for

Unveiling ZARK Cloud Based MMS & CMS Solutions

SHINKAWA FORBES MARSHALL


ACCESS TO YOUR MACHINES
ANYTIME, ANYWHERE
WITH ZERO INFRASTRUCTURE COSTS


Wireless Condition Monitoring
IIoT Technology - Industry 4.0
Triaxial vibration and temperature sensor
Bluetooth 5.0 communication
Alerts via text message and email
Quick and easy to install
Low cost


Machine
Your business uses machines to make products. When the machines aren't fit to do the job, you're out of business.
ZANK
A true wireless device that monitors the fitness of your machine and lets you know when there is a problem.
Machine Dossier
Plant Reliability Ecosystem resides in the cloud and gives you access to machinery information from anywhere.
Reliability Collective
Machinery and Reliability Experts at the ready to collaborate with you to solve problems.
Mobile
We don't carry cell phones anymore, we carry Smart Devices. Receive email or SMS alerts when your machinery's conditions change.
Spark Process
A unique and powerful tool that allows all the key stakeholders to easily collaborate, share information and solve problems.

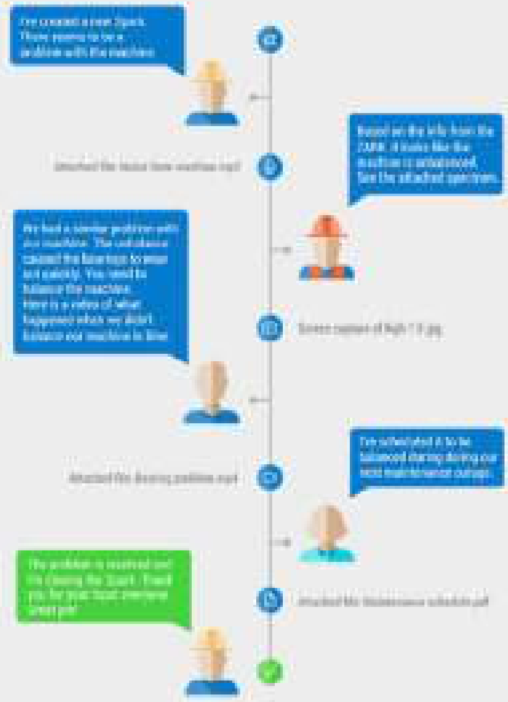

Machine Dossier
Plant Reliability Ecosystem
MACHINE
IMAGE LIBRARY
industry bundles
MACHINE
CONDITION
easy to interpret
vibration signals
SPARK
collaborative
problem solving
CONDITION CONTENT
along Timeline Navigation

SPARK PROCESS

COLLABORATIVE PROBLEM SOLVING

Although highly useful in diagnosing machinery faults, complex vibration signals can be confusing to interpret. Even though a ZARK is able to pinpoint a number of defects automatically, sometimes it would be nice to get an expert opinion before taking action to correct a problem.

Machine Dossier can connect you to a wide array of experts in various reliability disciplines. We call this group the Reliability Collective. Connecting them to your machines is as simple as starting a SPARK – our cloud-powered problem resolution tool.

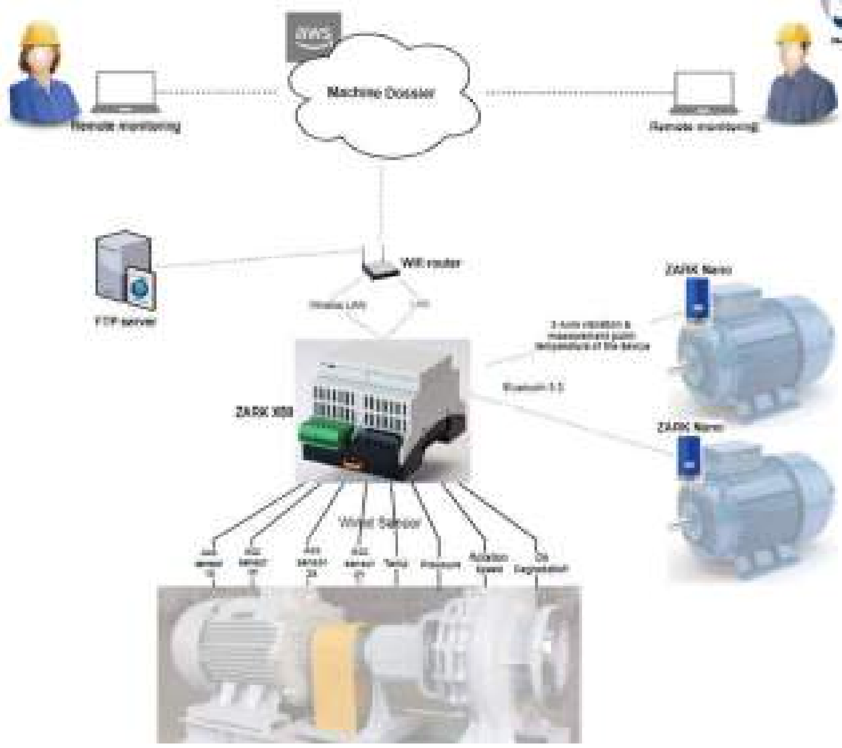


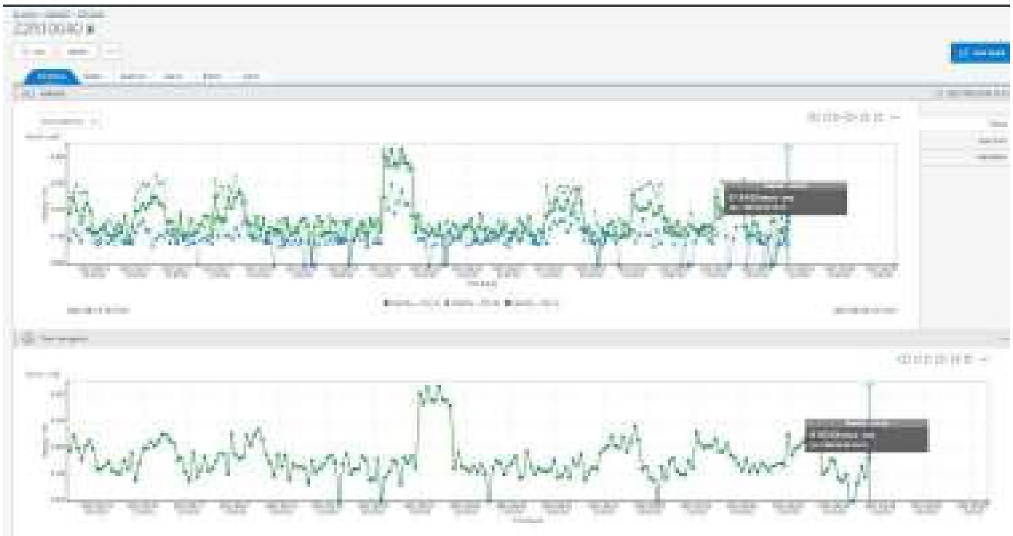
System architecture

AWS based

Data measurement device ZARK X8II

Wireless vibration sensor ZARK Nano





Measurement Point: Trend

- Trend
- Spectrum
- Waveform

Make in India

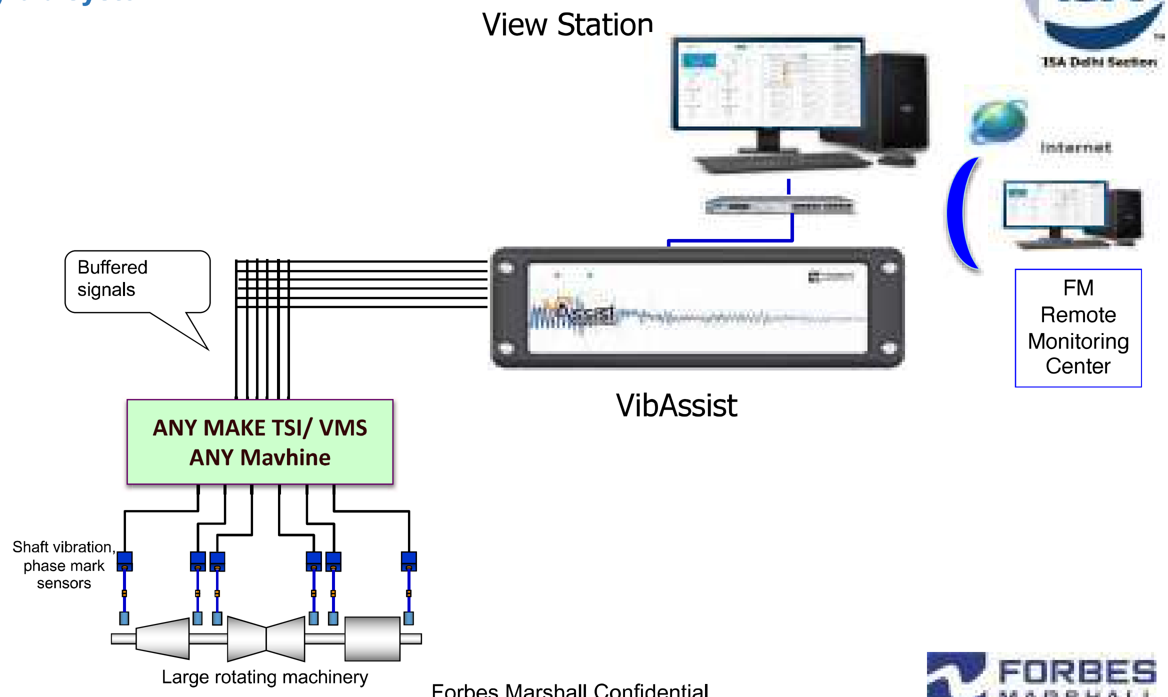
आत्मनिर्भर भारत.

AATMANIRBHAR BHARAT.

#VOCALFORLOCAL

VibAssist: Vibration Analysis & Diagnosis Software

- Plug and Play to any old system
- AI Based
- Remote Support



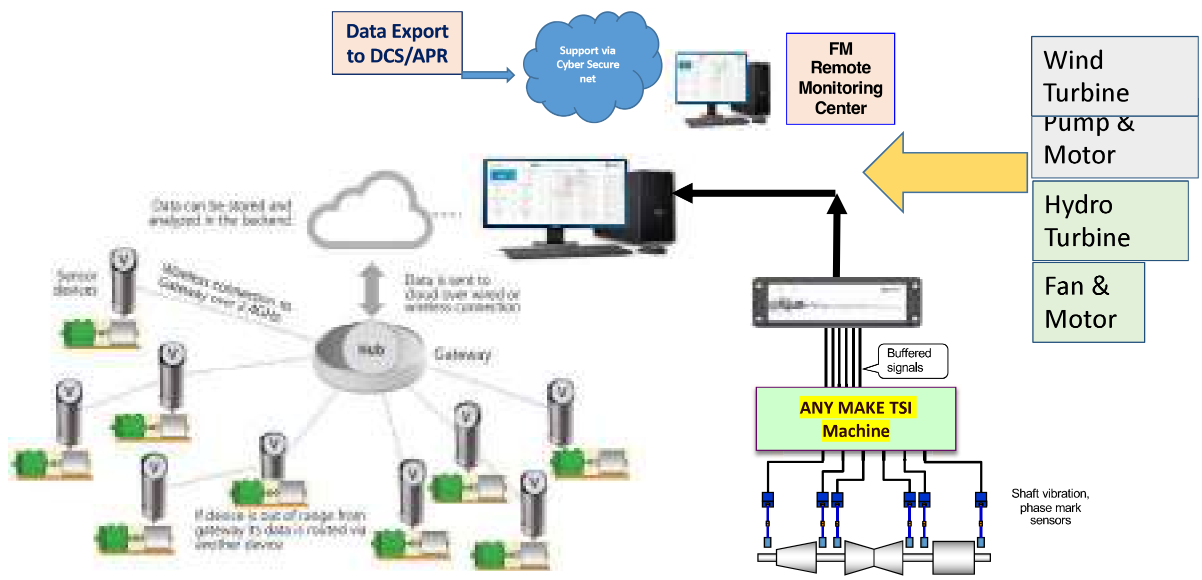
MAKE IN INDIA

Forbes Marshall Confidential
mvyas@forbesmarshall.com

FORBES MARSHALL

Plant wide Rotating Machines Monitoring , Analysis & Diagnostic

Critical Machines + Non Critical Machines



Forbes Marshall Confidential
mvyas@forbesmarshall.com

VibAssist™ Analysis Software

Remote Vibration analysis

Expert Work Force is Limited and costly	Data Collectors and Maintenance Cost	Globally Paradigm Shifted by having Internet available at all plants with higher speeds with firewall protection.
•- Limited people having expertise on machines and difficult to afford such people at every plant	•- Data Collectors and Software Cost is quite higher investments and need to maintain which calls for Manpower	

Achilles Communication Certification

Certificate Level	During attack Network function	After attack Network function
Level1	Does not have to work	Keep on work.
Level2	Keep on work.	Keep on work.

Security standard of control system

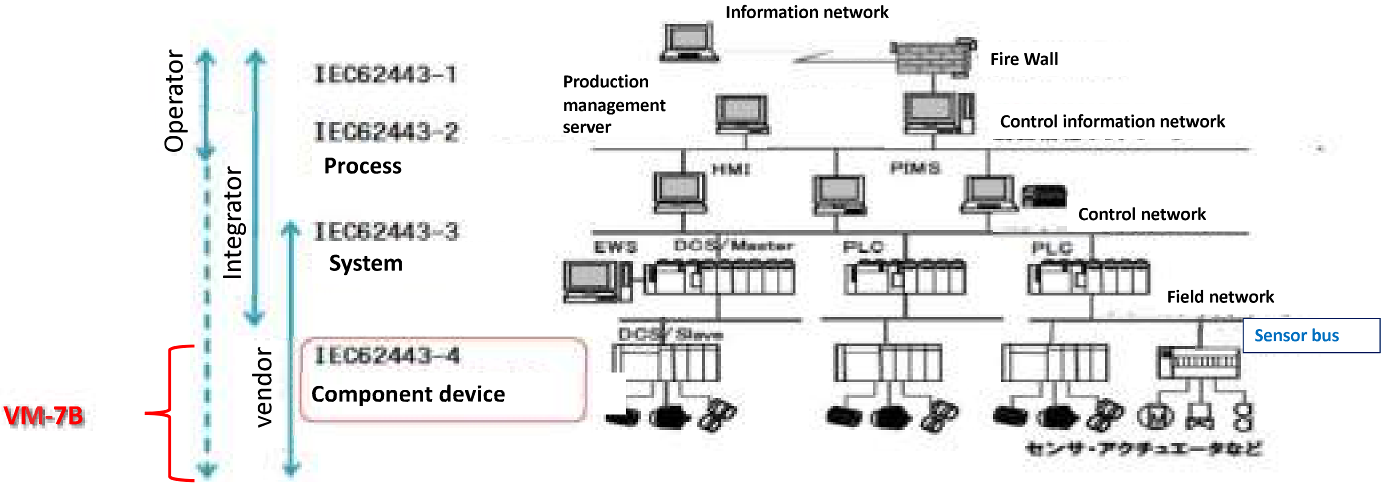
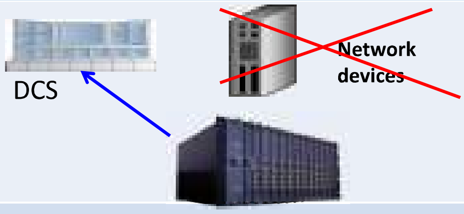
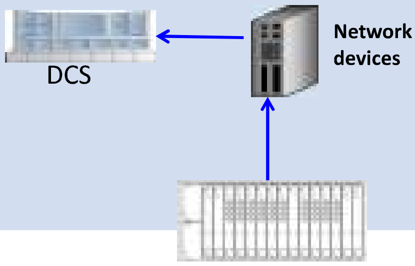


Figure 3： Configuration for IEC62443
(Reference source：IPA「Details of IEC62332 and CSMS/EDSA standard」)

Cyber Security of Monitoring System

Product	Certification	Implementation	
		Hardware (External network devices)	Network specialist
VM-7	The world's first TSI monitor that has Achilles certification Level 2		Not required Easy construction
Other company monitor	Achilles certification Level 1		Required

Conclusion

- Level 1 : Loop Powered Sensors : Only when overall vibration required
- Level 2 : BOP VMS : Sensors & Monitoring System (Non API , Wireless , Cloud Based)
- Level 3 : Critical & Secondary Critical Machines (API 670 System)
- Plant Wide Monitoring : Integrated Solutions VMS / MMS & CMS.
- Remote Support : Monthly Inputs to avoid failures by Expert & Collaborative Problem Solving

Forbes Marshall Confidential
mvyas@forbesmarshall.com

Setting the Standard for Automation™

ISA Delhi Section

µ MODULAR SMART SAMPLE CONDITIONING

Chandan Sanyal
Subarna Chakraborty

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

1

ISA Delhi Section

SPIRARE ENERGY

SPIRARE ENERGY

SMART SAMPLE CONDITIONING SYSTEM

12 & 13 May, 2023

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

2

Agenda

3

PROBLEMS IN CONVENTIONAL SCS

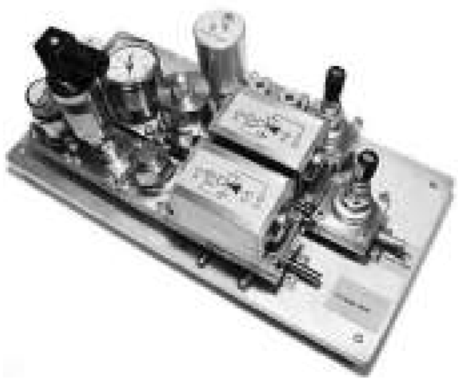
-Longer tubing run
-Multiple end connections creating more leakage points
-Multiple dead legs
-Valve Wear
-Takes up more space
-Slow Response Time
-Representative Sample
-Requires more Maintenance
-High engineering, drafting and assembly cost
-Multiple Cables (Fiber Optic Cables, IS Barriers etc.,)
-Difficult to remotely monitor, check or troubleshoot SCS
-High Total Cost of Ownership
-Requires Skilled Labours and Workers
-Requires more assembly time

"At least 80% of our analyzer problems are caused by the sample system"
Petrochemical Analyzer Specialist

4

OBJECTIVES OF A SMART SCS

-Facilitate the acceptance/implementation of... **modular, miniature** & **smart** process analytical technology
-Promote the concept of... **at the pipe/field-mounted ("by-line")** analytical
-Lay the groundwork for... **open connectivity** communication architecture
-Provide a technology bridge to the process for... "sensor/lab-on-a-chip" **microanalytical devices**



Features & Benefits:

- Minimum or no tube runs
- Stick design ensures zero dead legs
- Requires less time to assemble
- Compact Design
- Requires less maintenance time
- Single Modbus cable reduces cabling requirements
- Valves in modular system are designed for high cycle life. Hence, reduces wear and tear problems
- Continuous remote monitoring of Pressure, Temperature, Flow and Differential Pressure with a single device
- Less response time
- Ensures representative sample

5

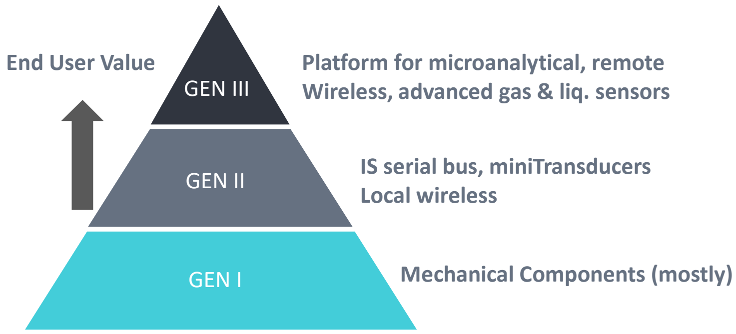
NeSSI (NEW SAMPLING AND SENSOR INITIATIVE

NeSSI is the **New Sampling and Sensors Initiative**, which was started within the **Center for Process Analytical Chemistry** (**CPAC**) as an ad-hoc group of about ~250 people from international companies and universities.

Companies integral to CPAC and NeSSI (i.e., sponsors, users, suppliers, participants), not including various universities are **ABB, CIRCOR, ExxonMobil, Chevron, Siemens, Emerson, Swagelok, Parker Hannifin, Dow, Air Products, Honeywell, UOP**.

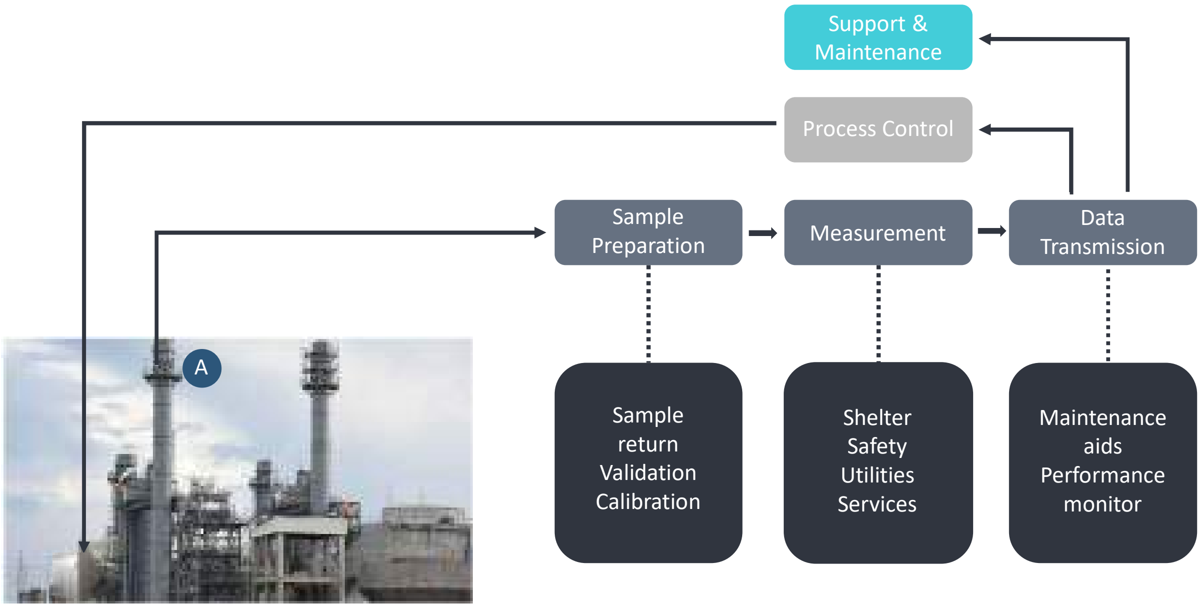
Their charter was to:

1. Improve Sample Conditioning System reliability and serviceability
2. Provide lowest cost of ownership by optimizing capital costs and operational costs
3. Use a standardized, non-proprietary platform for mechanical and communications technology



6

WHAT CONSTITUTES A PROCESS ANALYTICS SYSTEM?



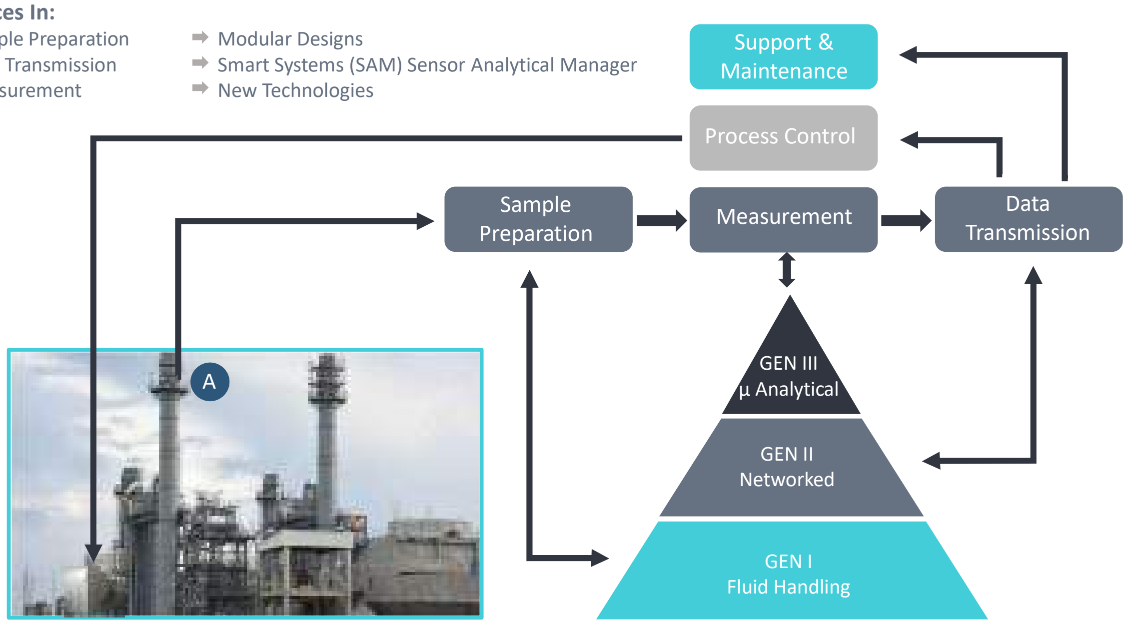
7

WHAT IS ON THE HORIZON FOR PROCESS ANALYTICS?

Advances In:

- Sample Preparation
- Data Transmission
- Measurement

➡ Modular Designs
➡ Smart Systems (SAM) Sensor Analytical Manager
➡ New Technologies



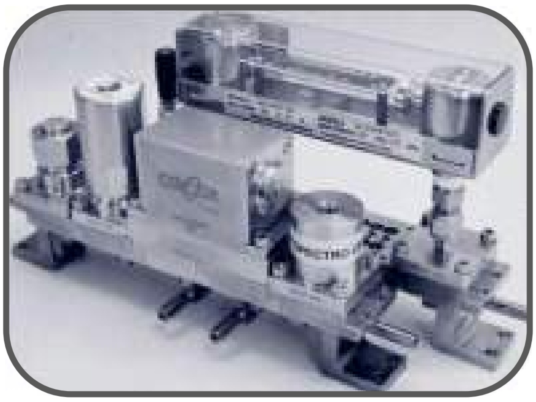
8

GENERATION I:
SMART SCS

9

OBJECTIVES OF GENERATION I: SCS

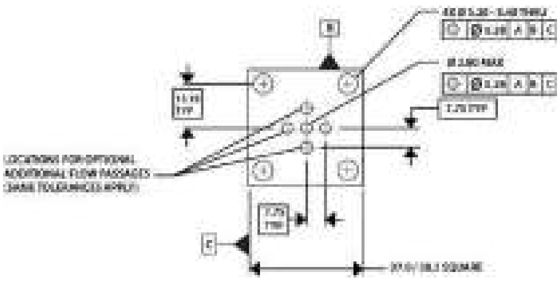
- Standardization of Design
- Compact footprint
- Foundation for next generation analyzers
- Fewer leaks
- Faster component replacement
- Greatest Flexibility and Expandability
- Visible Flow Traceability
- Complete set of mechanical and electronic components with a wide variety of functionality
- Comprehensive design support with CT76 Visio Design tool
- Improved Reliability
- Quality of Measurement
- Reducing total cost of operation/ ownership



10

NeSSI SUBSTRATE DESIGN

ANSI/ISA 76.00.02-2002, IEC 62339-1:2006(E)

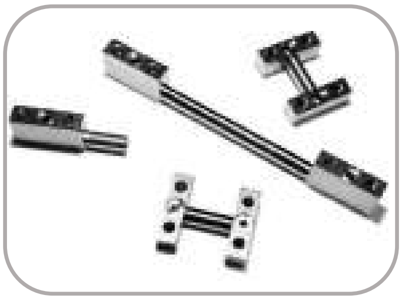


- The specification is very open
  - 4 bolt holes & 5 gas ports on a 1.5” plate
- Not all NeSSI is the same (by a long shot)
  - Pressure ratings vary tremendously
  - Process flow path design is different for all vendors
  - Flow is almost always constrained by the top-level components and not the substrate (i.e.: Valve C_v)
  - Stream selection valve technology varies widely by manufacturer
  - Completed system size can be very compact or very spread out (hybrid) based on customer preference

11

SMART SAMPLING BLOCK & TUBE ARCHITECTURE

Building Block



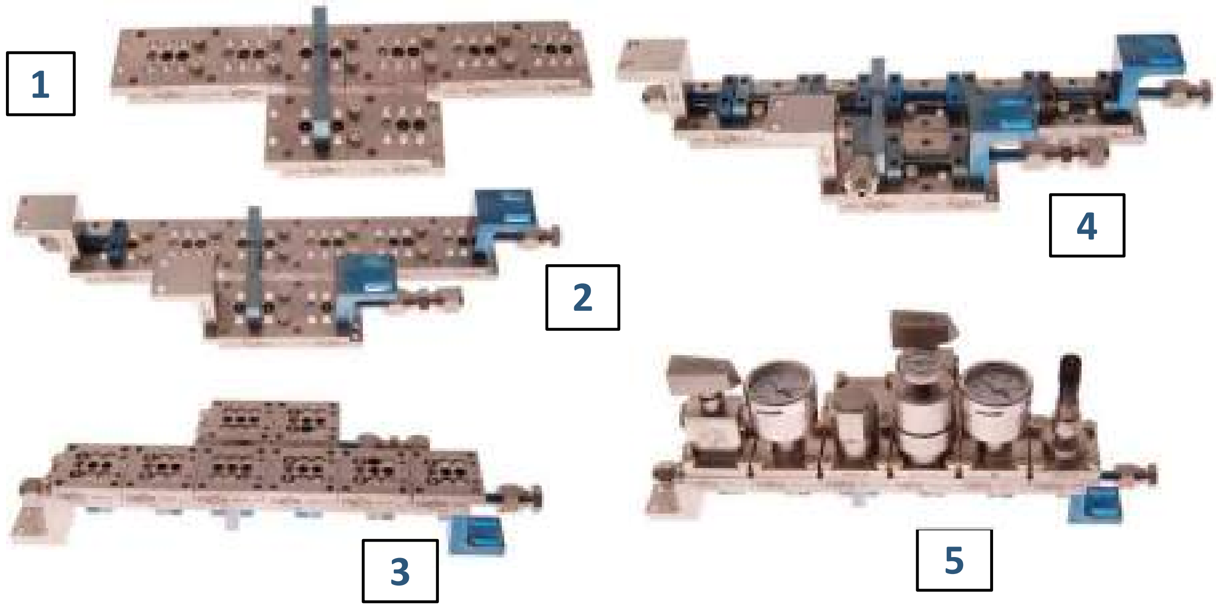
Standard Flow Tubesets

- **One Building Block**: creates all your system configurations.
- **Standard Flow Tube sets**: pre-welded, minimum in number, maximum in flexibility for your sample system designs.
- **Simple Building Block approach**: allows for initial assembly & field reassembly without Factory modifications of base.

12

ASSEMBLY ARCHITECTURE

FLO PRESSURE



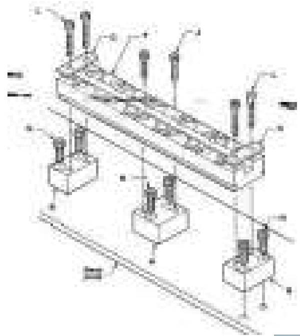
13

ASSEMBLED SYSTEM

FLO PRESSURE

14

ASSEMBLY TEST OF SMALLER SYSTEM (76 PIECES)



15

SURFACE MOUNT COMPONENTS

- 2-way Ball Valve
- 2-way Diaphragm Valve
  Needle Valve
- Pressure Gauge
  Rotameter
- Digital Temperature Meter
- Relief Valve
- Regulator
- Inline/ Tee
  Type Filter
- Coalescing Filter

- 3-way Ball Valve
  DBB valve
- Metering Valve
- Pressure transducer
- Digital Flowmeter
- Check Valve
- Backpressure Regulator
- Bypass Filter
- More………

16

DBB STREAM SELECT

Features & Benefits:

- Zero Leakage
  +
- Zero Maintenance
  +
- Zero Fugitive Emission
  +
- Zero Contamination

---------------------EQUALS--------------------

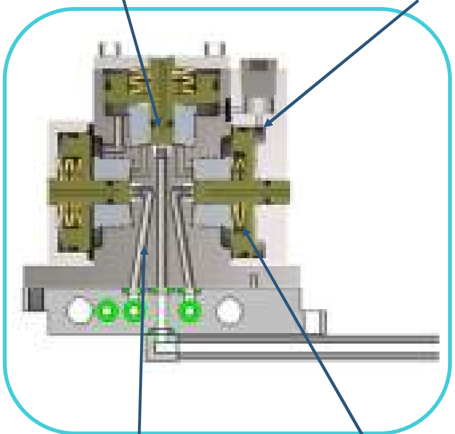
➢ Fastest Cleanup Performance & Lowest cost of Ownership

17

DBB STREAM SELECT

Hard polymeric, non-permeable valve seats, no moving elastomers
ZERO Leakage

Stroke limited actuation pistons allow for minimal fatigue on springs and actuation seals
ZERO Maintenance



Lowest internal volume and surface area inside and downstream of valve
ZERO Contamination

Triple redundant diaphragms with metal-to-metal seal to atmosphere
ZERO Fugitive Emissions

Design Features:

- Smallest Dead Volume / Fastest Response time of any valve in the market
- Independent sweep loop design
- Metal to Metal Seals to Atmosphere: No contamination
- Elgiloy fatigue resistant diaphragms / No Dynamic O-rings in Process stream
- Extended Valve life: 1,000,000 Cycles
- 0.23 Cv Flow Capacity: Suitable for liquid service
- 50 psig Actuation Pressure: Lowest on the market
- Diaphragm design holds integrity in vacuum
- Vapor or Liquid Process Pressure up to 500 psig: Highest on the market
- Small static O-rings: Cheap ($250) upgrade to Kalrez
- Activation Indicator for All Diaphragms

18

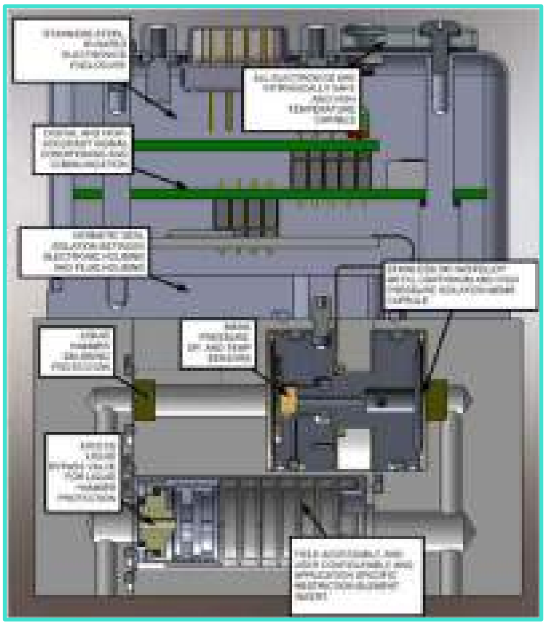
DMT (DIGITAL MULTIVARIABLE FLOWMETER)

Provides fluid upstream & differential pressures, volumetric & mass[1] flow rate and fluid temperature in a single compact unit.

- Innovative design provides ease of mount and maintenance.
- 50: 1 turndown ratio; 0.25% repeatability.
- 1/4" Female NPT and ANSI/ISA-76 compliant versions available.
- Digital protocols: » Modbus RTU intrinsically safe digital bus (Class 1, Division 1, and ATEX Zone 0)2. » CANbus intrinsically safe digital bus (Class 1, Division 1, and ATEX Zone 0)2.
- Robust industrial design, all stainless steel construction, IP65 (pending) for corrosive and high temperature environments.
- Cleanable flow elements clog resistant deign using Flow Configuration Modules (FCM). Extra FCM cartridges available for the rebuilding or re-ranging.
- Status indication LED's, field addressable and embedded electronic data sheet.
- Factory calibrated unit delivered, plug-and-play.

19

DMT (DIGITAL MULTIVARIABLE FLOWMETER)



Different connectors and status indicating LED's

Features designed exclusively for petrochemical sample systems

- Intrinsically Safe electronics
- Pressure, temperature, and flow
- Liquid or gas
- High pressure and pressure shock resistant
- Ingress/ environmental protection
- Corrosion resistant (internally and externally)
- High temperature capable
- Visual Indication
- Configurable flow module (CFM) for various applications and flow rate
- Anti-clogging flow restriction with integral relief valve

New multi-variable pressure, differential pressure, and temperature combo sensor (**co-developed with Ametek using their MEMS Technology**)

20

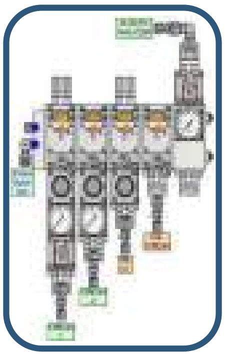
DVM (DIGITAL VALVE MANIFOLD)

Low power, digital bus enabled solenoid pilot valve manifold for hazardous area applications.

- Rugged, ultra-low power (~0.2W per valve, 1.2W total) minimizes energy consumption needed for hazardous areas
- Pilot solenoids rated for 10 million cycles
- Compatible with CANbus for Intrinsically–Safe Digital bus applications (Class 1 Div 1, or Zone 1) and Non-incendive Modbus RTU applications (Class 1 Div 2, Zone 2) applications
- All stainless-steel construction for IP65 and corrosive high-temperature environments
- Solenoids are PPS plastic encapsulated with integrated voltage and current surge protection.
- Integrated valve “lock-out” feature (patent pending) utilizes mechanical jumpers which can be installed to prevent actuation of valve combinations that could cause accidental system upsets or safety incidents.
- No valve relays or digital contact closures required: Plug and Play with any PLC or automation system that utilizes Modbus or CANbus communication.
- Status indicating LED’s and field digital ID addressable

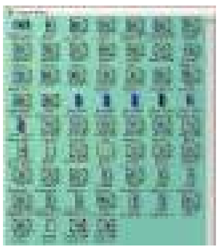
21

VISIO DESIGN TOOL

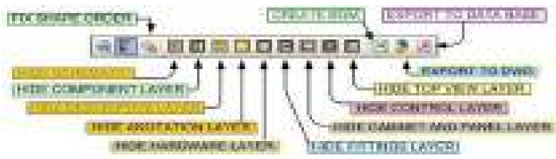


Features & Benefits:

- Drag and Drop Pick List
- Saves designing man-hour
- Improves productivity and quality of your submittals
- Reduce errors, omissions, & misunderstandings through clear and actual visual submittals
- Generate proposed design drawings in a fraction of the time it takes without automation
- Minimalize or eliminate re-work due to inconsistencies between drawings
- Better visuals in CT76 layouts than with CAD drawings
- A complete Bill of Material generated in MS Excel

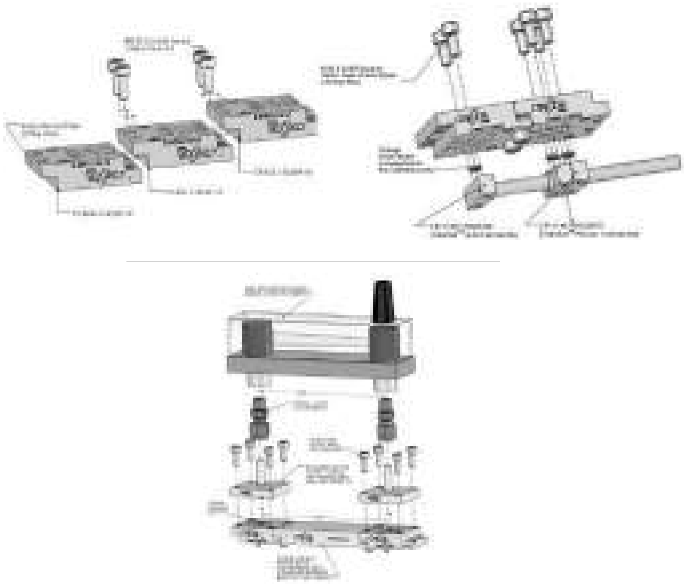


THE ADD-IN TOOL BAR



22

SMART SAMPLING ASSEMBLY



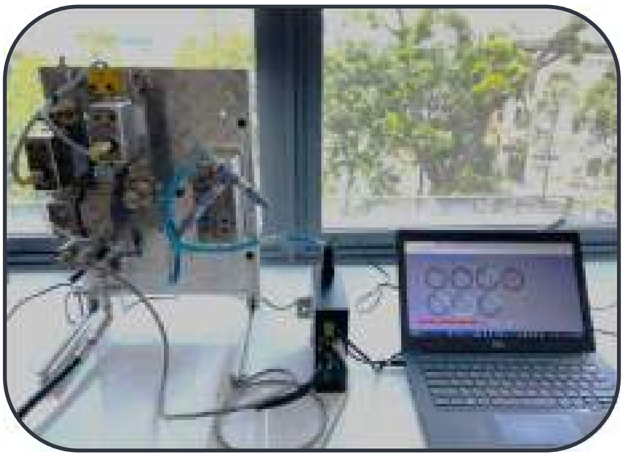
CT76 Scale Drawings

GENERATION II: SMART SCS

OBJECTIVES OF GENERATION II: SMART SAMPLING

FLO PRESSURE

- failsafe system for uninterrupted analysis
- real-time information
- verification of system health
- local visualization and control
- remote access and control
- verification of flow and temperature
- rapid response
- Non- proprietary
- To reduce manual checking (rounds)
- Adopting the use of a safe low energy-Intrinsic Safety for the NeSSI bus
- A move away from centralized control (automation) model to a local/field control model using a small computing device called the Sensor Actuator Manager (SAM).
- Introduction of a Graphical User Interface (GUI) for better visualization of physically compact sampling



25

SAM- SENSOR ANALYTICAL MANAGER

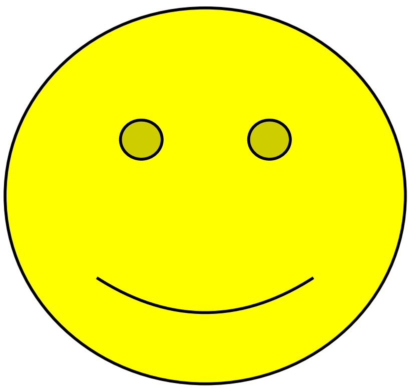
FLO PRESSURE

INTERFACE MANAGER

I AM "SAM", I DO 5 JOBS

Field Interface
- Graphical
- Wireless
- e.g. Bluetooth™, 802.11

Gateway to an Ethernet LAN
- OPC perhaps



Host to a Sensor/Actuator Bus

Software Applets for Sample System Repetitive Tasks (Industry Common)

"Open" Development Space for Custom Software

26

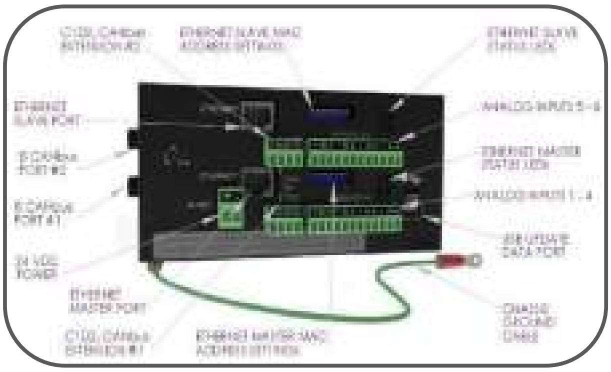
CIM 76- Communication Gateway

CIM has been developed to bridge a gap between hazardous area, Class 1, Div 1 and Class 1, Div 2 or non-rated areas for the implementation of a digital network operating inside a sample conditioning system cabinet and PLC analyzer network

- The CIM is available in two versions; the CIM76 (single board version) and CIM76+ (dual board version)
- Application layer used to handle the Data Objects employs the iCAN protocol, based on the CANopen protocol.
- Communication is accomplished through a 9.5V IS powered communication bus
- The interface between the CIM is adapted by various protocols; Ethernet/IP, Modbus TCP, and Profinet.
- 4 analog (4-20 mA) inputs available for non CANbus devices
- Performs the higher level CANbus functions of bus speed management and error arbitration
- Requires CIDI 9.5VDC power supply for IS CANbus and C1D2 24 VDC for processors

27

CIM 76- Communications Gateway

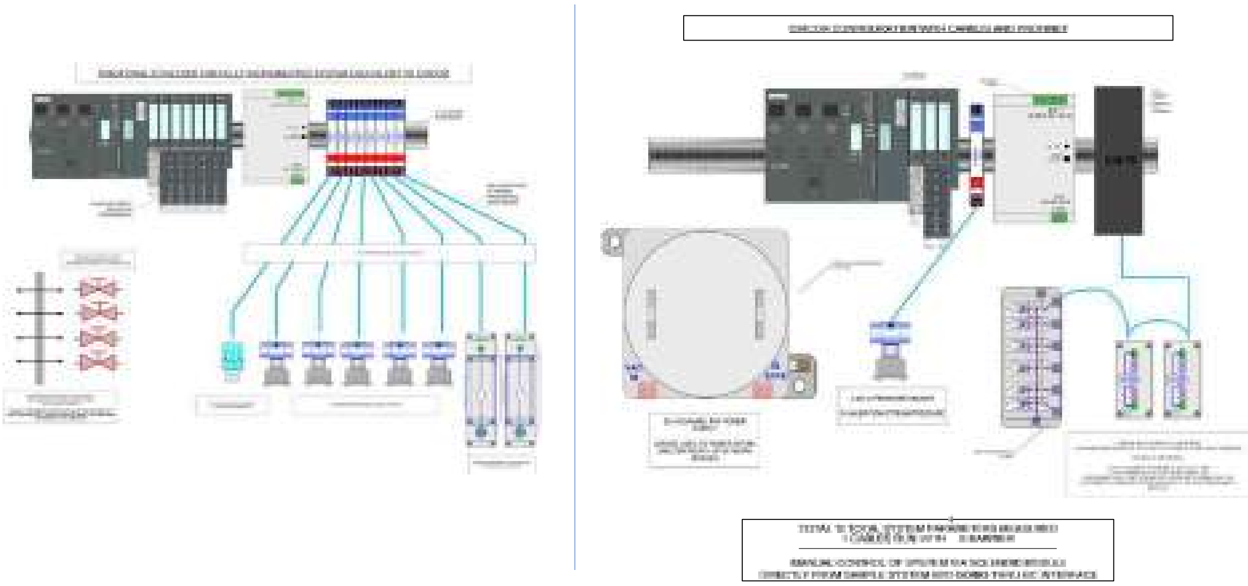


- Password protection, SMTP email server for alarms, embedded web server for dynamic data and configuration viewing via a web browser and ftp server for local information storage
- Error messages and alarms are handled via an email server
- A total of 20 error messages can be configured, 10 at a normal user level and 10 at an admin user level.
- The dynamic web server allows remote interface with the CIM via the Ethernet port.
- A maximum of 48 simultaneous users can view network configuration information via html.
- External EEPROM non-volatile mem ory for data and configuration storage

28

DIGITAL ARCHITECTURE- TRADITIONAL v/s SMART

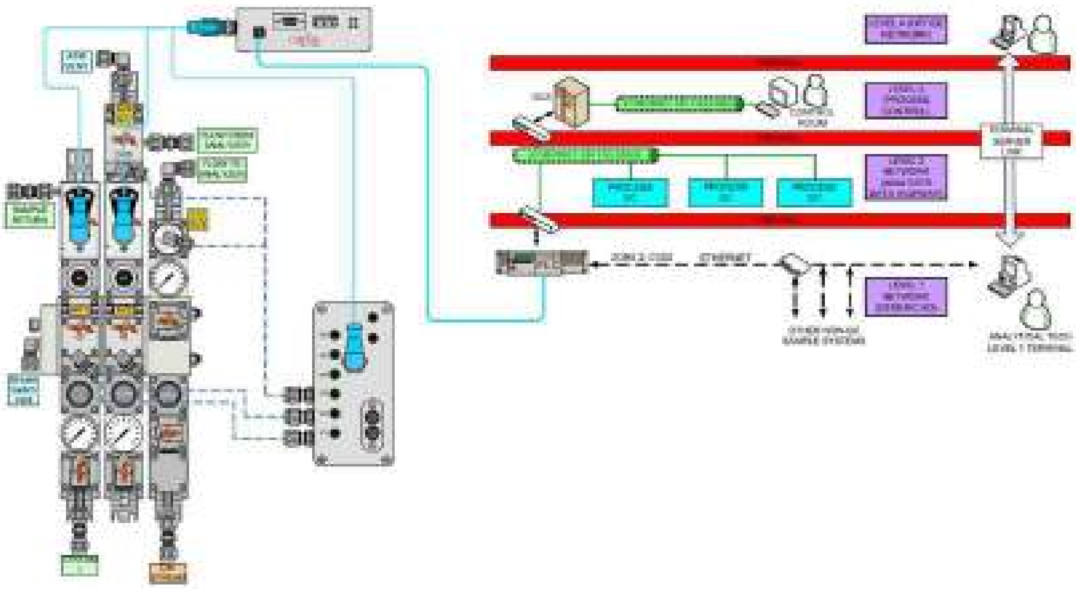
FLO PRESSURE



29

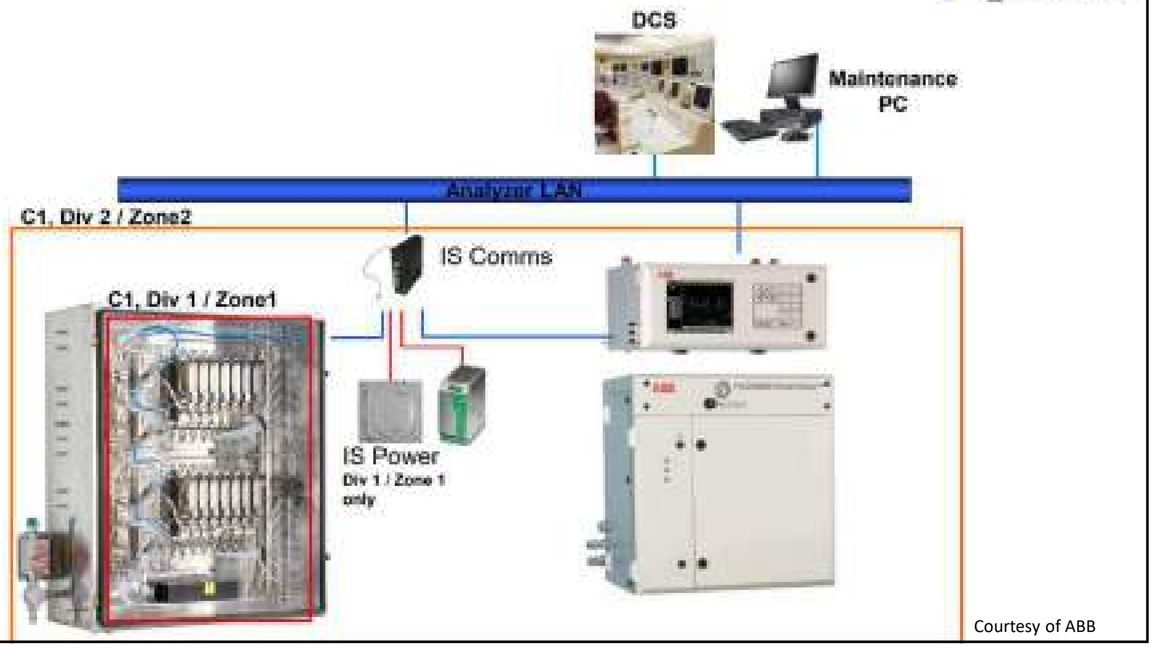
DIGITAL ARCHITECTURE

FLO PRESSURE



30

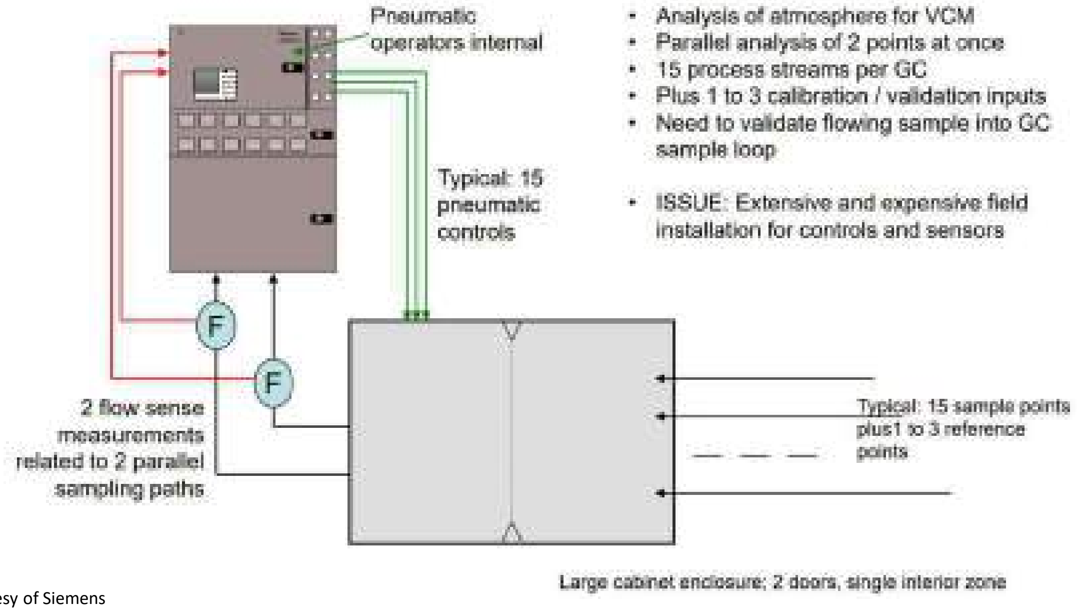
DIGITAL ARCHITECTURE WITH ABB PGC 5000



Courtesy of ABB

31

AIR MONITORING WITH SIEMENS MAXUM II



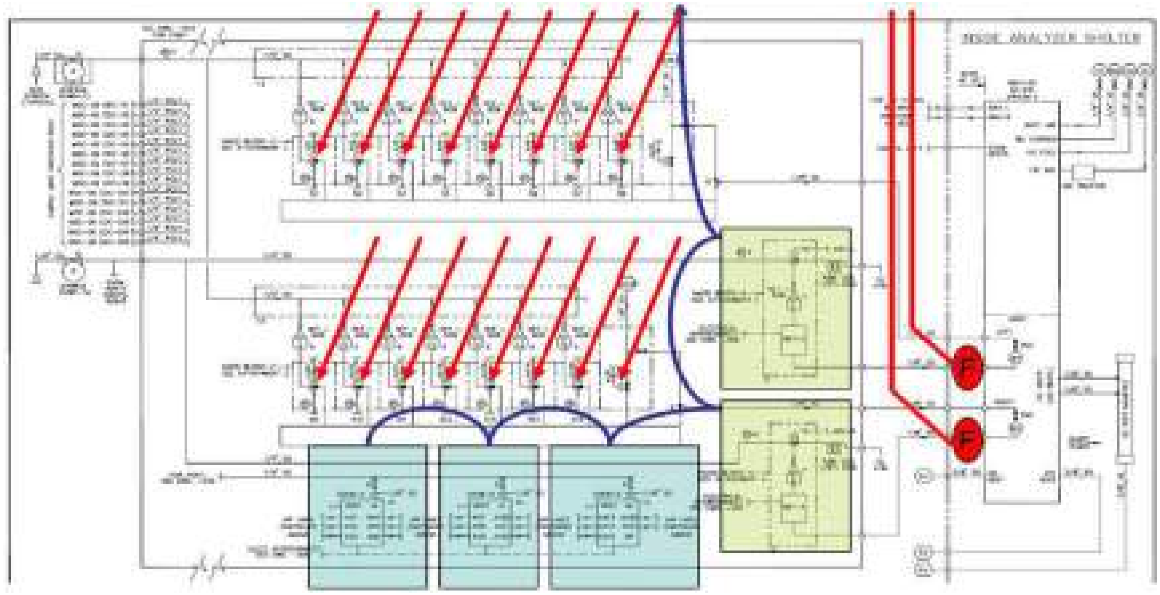
- Analysis of atmosphere for VCM
- Parallel analysis of 2 points at once
- 15 process streams per GC
- Plus 1 to 3 calibration / validation inputs
- Need to validate flowing sample into GC sample loop

- ISSUE: Extensive and expensive field installation for controls and sensors

Courtesy of Siemens

32

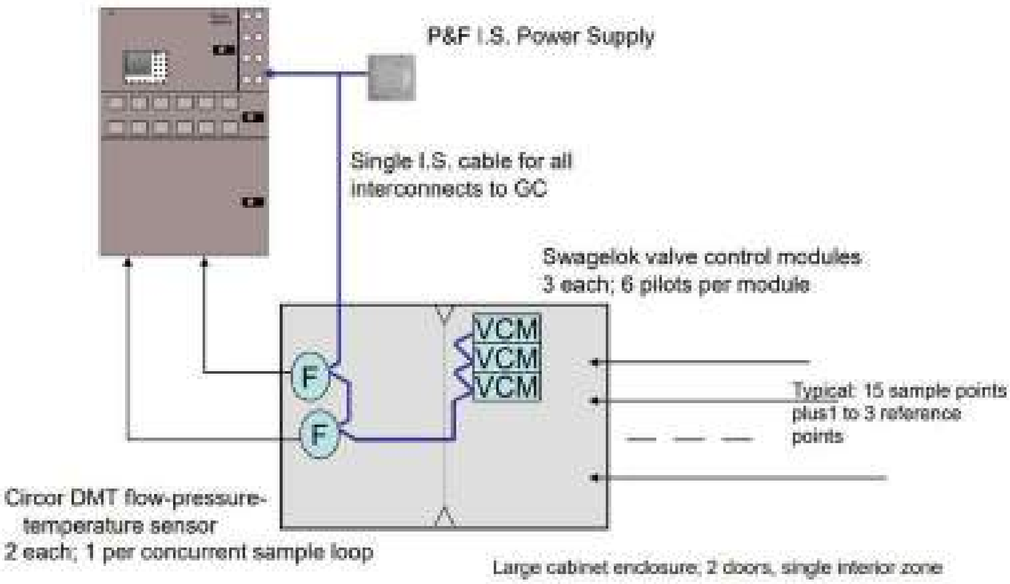
AIR MONITORING WITH SIEMENS MAXUM II



Courtesy of Siemens

33

AIR MONITORING IMPROVED USING SMART SCS



Courtesy of Siemens

34

DIGITAL ARCHITECTURE WITH SIEMENS MAXUM II

WHAT CHANGED?

- Rotameters eliminated; replaced with Flow-Pressure Temperature Sensors
- Thermometer eliminated; replaced with Temperature Sensor
- Pressure Sensors added to standard bottle inlet and inlet to analyzer
- Pilot Valve Module (DVM) in analyzer eliminated; replaced with Pilot Valve Module
- Cabinet window eliminated; all sensors can be read from outside and remote
- All new Sensors and Pilot Valve Module connected to analyzer by single I.S. bus cable

HOW DOES IT WORK?

- Any blockage of bypass loops diagnosed by in-line flow and pressure sense
- Heat tracing and speed loop temperature diagnosed by in-line temperature sense on each process gas
- Main-stream filters diagnosed by differential pressure across filter to selected stream
- Blockage of analyzer loop in SV or other valves diagnosed by in-line sample flow and inlet and outlet pressures
- Fluctuations of return point pressure diagnosed by in-line Pressure Sensor
- Calibration-Validation bottle checked by inline pressure sensor
- SSO, ARV and Stream Select valves switched inside cabinet
- Cabinet heater diagnosed by Temperature Sensor

35

SMART SAMPLING GENERATION:II VALUE PROPOSITION

- **Maintenance on demand vs scheduled maintenance and predictive vs reactive**
  - More efficient use of limited analyzer technician time
- **Remote access to critical process data**
  - Off specification product flaring
  - Environmental fines
  - Employee safety (priceless)
- **Remote diagnostics and control**
  - Valve switching and flow measurement
  - Flow control
- **Standard vs Custom designs**
  - Less time to engineer a system (no variability in design)
  - Less expensive to maintain
- **Cost Savings**
  - Ultra-low power consumption
  - Single I.S. bus cable to connect Pilot Valve Module and all Sensors
  - Extreme high cycle life of valves, pilot valves and other devices

36

GENERATION III:
SMART SCS

37

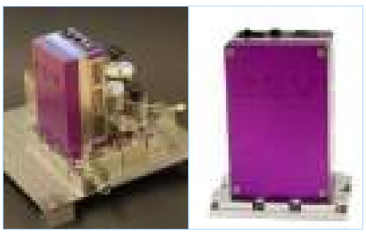
NeSSI GENERATION III: µANALYTICS

Generation III will allow tighter integration of the sample conditioning and analytical measurement devices.

Spectrophotometer
Cell UV / NIR
(fiberoptic) Corner-cube Reflectors
Applied Analytics Inc.
Analyzer-on-a-Block
UV/VIS/NDIR

Smallest ANSI/ISA-76 Mass Flow Controller/Meter

HORIBA STEC: SEC-G111/SEF-G111 Series



Thermoscientific
C2V-200 Micro GC

Agilent Die-electric Sensor

38

NeSSI GENERATION III: µANALYTICS

Vapochromic Oxygen Sensor

Teledyne Oxygen Sensor
Fuel Cell or Zirconium Oxide Sensors

- Offer an SP76 compliant oxygen sensor

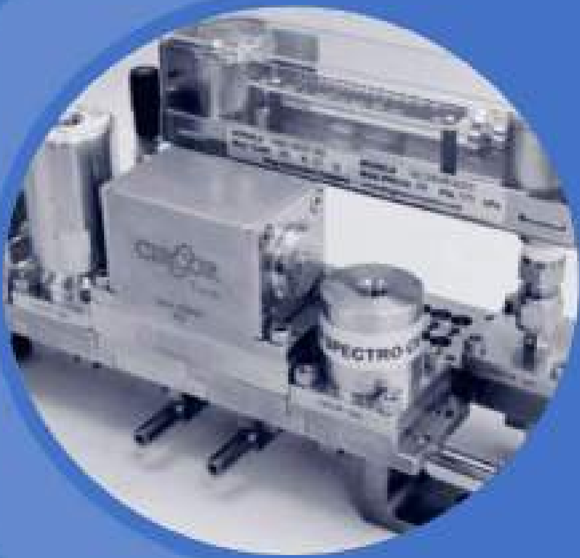
NeSSI RAMAN Probe

39

NeSSI GENERATION III: FUTURE

- NeSSI™ Generation 1 and 2 technology enablers for Generation
- 3 Integration of micro/mini analytical devices with digital SHS components on ANSI/ISA SP76.00.02-2002 standard substrate
- At-line and wireless
- Represents an opportunity to drastically reduce the infrastructure costs associated with traditional process analytical systems

40

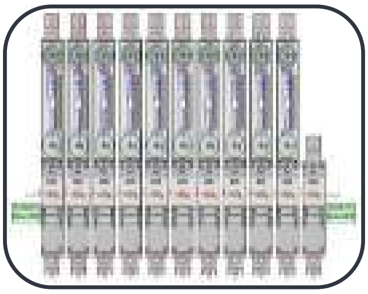


APPLICATIONS:
SMART SCS

41

SHELL HOUDINI YOKOGAWA: A COMPLETE WIFI PROJECT

FLO PRESSURE



42

SHELL HOUDINI YOKOGAWA: A COMPLETE WIFI PROJECT

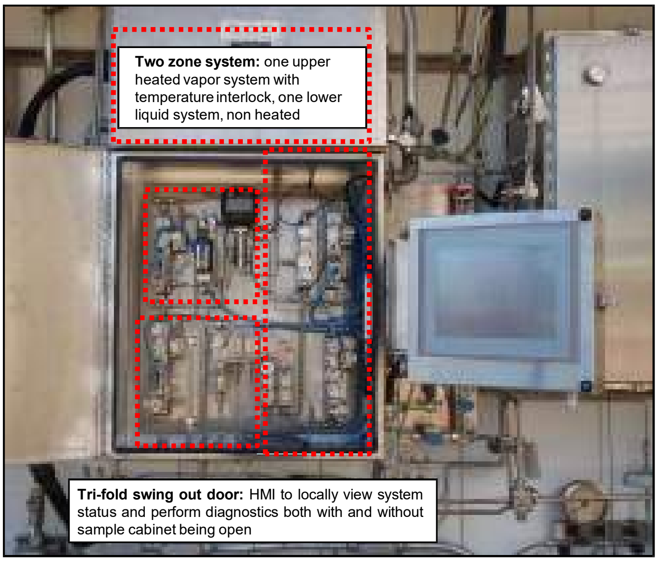
FLO PRESSURE SAMPLING SYSTEMS

43

INSTALLED EXAMPLES

FLO PRESSURE SAMPLING SYSTEMS

3-in-1 SHS, Isobutylene Application



Modular SP76 technology enables space savings to ***fit 3 independent sample systems into one system footprint*** on shelter

✓Common "stick" design methodology allows for easy visualization and troubleshooting

✓Both visual and electronic pressure and flow sensors

ProfiNET™ enabled PLC

Three Analyzers are supported with this SHS configuration:

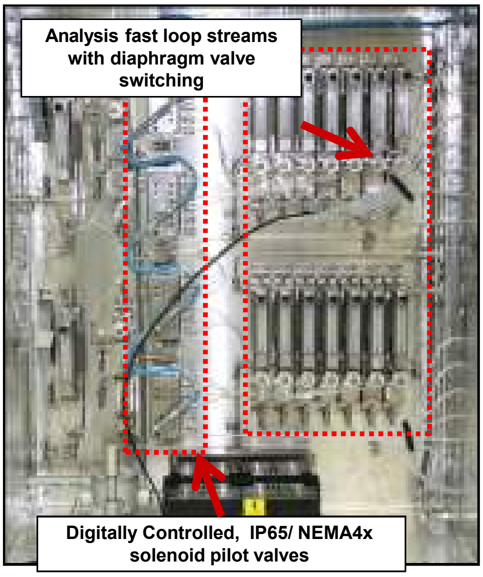
- **Siemens GC**
- **Ametek Moisture**
- **GE Panametrics Moisture**

✓Sensing digital relays from a **GC** and controlling system valves

✓**HMI commands/visualization and alarms/ data to DCS system**

44

AMBIENT AIR MONITORING



- ***Modular SP76 technology enables space savings to compact 88 air analysis streams*** into a single small shelter with no PLC control or external I/O equipment other than CANbus I/O extenders with fiber optic links to GC
  - Each system uses CANbus solenoid valves for actuation (up to five per system)
  - Only one communication line and one common air supply line thru cabinet is needed
  - Eliminates need for:
    - **Large pneumatic bulkhead manifolds thru cabinet insulation**
    - **Pneumatic tubing run installations, labeling, leak checking, troubleshooting**
    - **Solenoid valve relays, PLC DIO cards, IS barriers**
- Analytical method and all valve sequencing is directly controlled by ABB PGC-5000 GC via a fiber optic CANbus link

45

AMBIENT AIR MONITORING

46

AMBIENT AIR MONITORING

FLO PRESSURE

47

HYBRID SYSTEM

FLO PRESSURE

48

STAND ALONE UNITS



49

Q&A?

50

THANK YOU

PHOTONIC MOLECULAR TECHNOLOGY FOR HEALTH MONITORING OF CRITICAL EQUIPMENT USED IN REFINERY AND PIPELINE

Dr. VSN Rao Tatavarti & Biren Mahendra Shah

ABSTRACT

It is true that current sensors used for condition and vibration monitoring have certain limitations, such as being contact-based, application-specific, and expensive for broader deployment. These sensors also require frequent calibration and can be limited in their ability to manage frequency.

Developing a real-time remote condition and vibration monitoring system that is contactless, universal, and low-cost is valuable to the field. Such a system could significantly improve the efficiency and safety of various industrial processes and provide valuable data for predictive and preventative maintenance.

Nonetheless, with the growing demand for remote monitoring solutions, deploying a cost-effective, contactless system for condition and vibration monitoring would undoubtedly significantly impact various industries.

NEW SCIENCE - A PARADIGM SHIFT

Condition and vibration monitoring involves continuous evaluation of the health of plant equipment and structures throughout their service life. This approach enables the early recognition of faults and potential failures, which can prevent costly downtime and repairs. While closely related, condition monitoring and protection require different implementation approaches. Effective condition monitoring can provide primary protection, but its

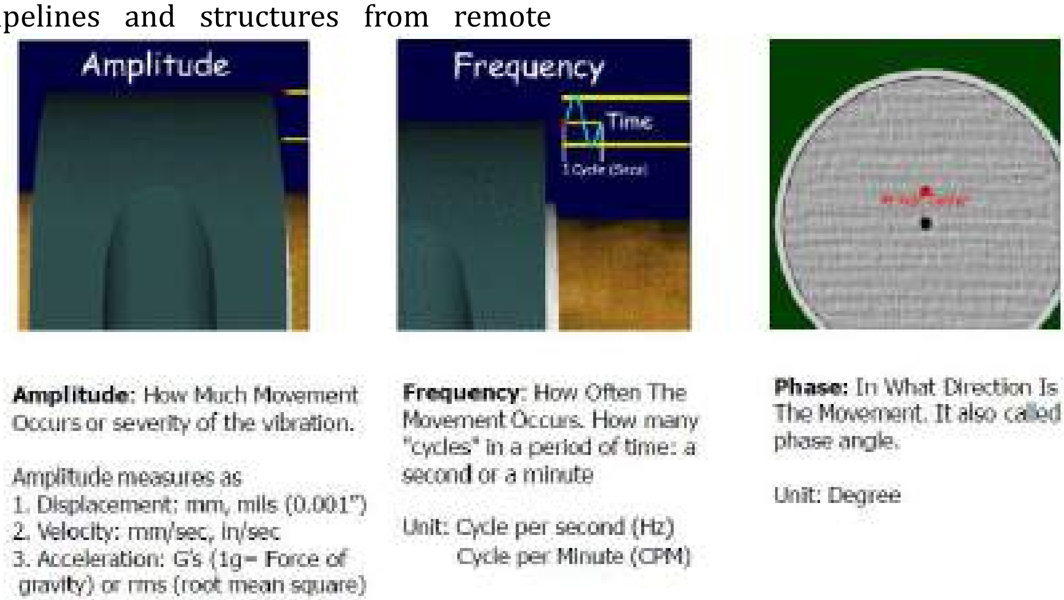
primary function is to detect faults early, reducing the risk of equipment failure and increasing overall operational efficiency. The vibrations produced in a machine are the best indication of the machine's health. Vibration analysis remains the best measure of machine health of all predictive maintenance (PdM) technologies. This is true because vibration monitoring can alert us to many conditions indicating potential machine failures.

Indigenous innovative photonic technologies and systems **VIDUR** (**V**ibration **I**ntelligence **D**ata **U**nravelling **R**emotely) and **VEDA** (**V**ibrational **E**ffects – **D**etection **A**nalysis) are Photonic Systems for Real-Time Vibration and Condition Monitoring. These systems can perform condition and vibration monitoring robustly from remote locations on a non-contact basis, *accurate* monitoring of vibrational displacements, velocities, and accelerations for various applications in the real world across all industries, the designed and developed innovative photonic systems capable of monitoring real-time vibrations on machines, pipelines and structures from remote locations. The systems are compact, portable and can easily be deployed at any location for real-time vibration and condition monitoring in a non-intrusive fashion, even at inaccessible locations.

The Technology

VIDUR is based on light scattering and can measure tiny particles and molecules' size, weight, and movement. With just one beam of light, this technology can monitor various parameters, including weigh-in-motion, record behaviour, movement, force, acceleration, position, static & dynamic load, leakages, corrosion, erosion, acoustic, flow, pressure etc.

VEDA is a non-acoustic non-imaging photonic system. VEDA can uniquely monitor seismic vibrations with extreme sensitivity to the nanometer level. In addition, it can listen to the sound at the location being monitored, all without physical contact. It can extract data on vibrational displacement, velocity, and acceleration parameters from remote locations in real time, both in time and frequency domains.



Photonic technology offers significantly improved sensitivity and efficacy for real-time remote monitoring of machines and structures compared to conventional monitoring systems.

Vision on Autonomous Maintenance

VIDUR and VEDA monitor and qualifies the following 5 important aspects:-

1) Detecting the existence of the damage
2) Locating the damage/porosity
3) Identifying the types of damage
4) Quantifying the severity of the damage
5) Resolution

This results in:

- Equipment restoration and proper management
- Prevent equipment deterioration.
- Establish basic conditions.

Inter-comparison of various Conventional technologies with novel photonic technologies

The present systems of VEDA and VIDUR can remotely monitor the vibrations and condition of machines and structures simultaneously in the time and frequency domains. The multifarious advantages of the new photonic systems (VEDA and VIDUR) are summarised IN TABLE 1&2.

Mechanism	Technology	Sensor	Advantages/Capabilities	Limitations
Remote / Non-contact	**Non-destructive**	Visual	*No sensor required.*	• *Suitable only for visible surfaces.* • *Generally, detects only larger defects* • *Misinterpretation of cracks and scratches.*
		Photonics (*VEDA / VIDUR*)	*Precise, Fast, Continuous, Remote Monitoring with High Sensitivity (nanometre resolution).* *Portable, Low Cost and Low power requirements.* *Damage detection, quantification and localisation feasible.* *Single system can scan large areas effectively.*	• *Line of sight to be free of obstructions when operated from a long-distance location.*
Contact		Fiber Optics (FBG)	*Precise, Sensitive, Fast* *Multiplexing capability* *No EMI issues*	• *Needs mounting on machine or structure or embedding into the structure.* • *Temperature sensitive* • *Affected by dynamics in the environment.*
		X-Ray / Radiography	*Fast results* *Detection of internal defects*	• *High Cost and Power* • *Low grade information* • *Difficult to apply to some part of the structure*
		Eddy Current	*Portable* *Moderate cost* *Immediate results* *Sensitive to displacement changes*	• *Essentially a surface inspection tool.* • *Sensitive to temperature.* • *Suitable for inspection of metals only* • *Affected by moisture and humidity* • *Time-consuming to scan large areas*
		Ultrasonic	*Good accuracy.* *Passive / Active Sensing mechanisms can be used.*	• *Have minimum sensing distance* • *Need to properly align the transducers.* • *Affected by ambient temperature, and humidity.*
		Strain, Displacement, Velocity, Acceleration	*Directly calibrated physical parameters for studying dynamic response of structures.*	• *Varying characteristics based on materials used for sensing* • *Limitations in time and frequency responses*
	Destructive	Core-cutter, *etc.*	*Easy to implement*	• *Limited accuracy* • *Destroys the structure.*

Table 1: Various methods of Machine and Structural Health Monitoring – their advantages and limitations

Methods of SHM based on different NDT methods and Vibration Sensors	*Sensitivity / Accuracy / Frequency Response Range*	*Usable for global inspection*	*Detection of internal defects*	*Detection of defects far away from Sensors*	*Defects in areas with one surface accessible*	*Estimation of size and location of defect*	*Contact required*	*Identification of defects in inaccessible locations*
Visual	Limited	Yes	Partially	No	Yes	Partially	No	No
Magnetic	Limited	No	No	No	Yes	Partially	Yes	No
Radiography	Limited	No	Yes	No	No	Yes	Yes	No
Eddy current	Limited	No	No	No	Yes	Partially	Yes	No
Acoustic emission	Limited	Yes	Yes	Partially	Yes	No	Yes	No
Ultrasonic	Limited	No	Yes	No	Yes	Yes	Yes	No
FBG	Limited	Yes	Yes	No	Partially	Yes	Yes	No
Vibration Displacement / Velocity / Acceleration	Limited	Yes	Yes	Partially	Yes	Partially	Yes	No
Photonics (VEDA / VIDUR)	**Good**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**No**	**Yes**

Table 2: Inter-comparison of various NDT technologies vis-à-vis the Photonic Systems of VEDA/VIDUR.

Table 2, in which with the state of art sensors and technologies for structural health monitoring and management that are currently available are compared with the new photonic technologies (VEDA and VIDUR).

Technologies for integrating various spatially separated systems using fundamental communication concepts of the Internet of Things are also incorporated for quick deployment. The ML/AI model learns the dynamics of each industrial asset and process from historical photonic sensor data, creating prescriptions by searching for the optimal values of critical control parameters and closing the loop by sending prescriptions back to assets and processes to be activated.

Conclusion

One thing that will ultimately shape the breadth and speed at which I**IOT** (Industry, Innovation, Operation & Transformation), **AOT** (Array of Things) and **AI** {**Artificial Intelligence**}) integrated with Big Data Platform take hold in the world are by using **Photonic Sensors**. With more than 20 years of diligent R&D, CATS has developed cutting-edge multipurpose sensors using laser (light) as a medium for multifunctional applications like Pipeline condition integrity, Real-time Vibration Monitoring (Turbines, highly critical machines, motors, conveyors, Transportation systems etc), Structural Stability, (Colling towers, Silos, Bridges, Tunnels, Mining, Stacks and Chimneys, Boilers, Offshore Oil fields, etc.).

PROF. DR. RAO TATAVARTI
Co-founder and Chairman (www.cats-global.com)
Over 30 years of R&D and Innovation in Aerospace Engineering, Biomedical Engineering, Biotechnology, Fluid Dynamics, Photonics, Signal Processing, Image Processing, Satellite Image Processing, Ocean Engineering and Technology.

BIREN SHAH
Co-founder and Managing Director (www.cats-global.com)
Over 25+ Years of Experience in Business Development and Strategy, Articulating the right solutions with low Opex and low Capex, Financial Engineering, Marketing and Sales, Security Solutions, Biocryptics, & BIG Data

ENHANCING RELIABILITY & RESILIENCE OF GENERATION THROUGH CYBER SECURITY

Alok Kumar Sinha[1]
Add General Manager, PE-C&I
CC-EOC, NTPC LIMITED

Some Nath Kundu[2]
Deputy General Manager, PE-C&I
CC-EOC, NTPC LIMITED

Kuldeep Singh Yadav[3]
Senior Manager, PE-C&I
CC-EOC, NTPC LIMITED

Abstract: *Being a progressively interconnected world today, gone are the days when OT system used to operate in isolation. Increased convergence of IT-OT has resulted in numerous benefits for the organisations on one hand while on the other hand rendering the system vulnerable to newer threats. With increased technological advancements, the line separating IT & OT will become thinner in days to come. With such scenario in sight, developing a secure OT architecture is a challenge, requiring a multi-pronged approach to identify and tackle both known & unknown potential security threats. This paper is an effort to highlight various steps necessary to develop a secure ecosystem for OT.*

Keywords*:* Cyber-Physical system, Defense in depth, IACS, HIDS, NIDS, DMZ, SIEM, Legacy system, Upgradation, Supply chain security, CCMP, CSMS, CII, PPT, MITRE ICS ATT&CK framework

A. Introduction

Till recently, ICS were considered very much different from IT systems in the sense that IT systems are connected to outside world while systems in an ICS were isolated or air-gapped from outside world and were using proprietary protocols over specially customized hardware and software. Now with changing business requirements, it has become imperative to connect the OT systems with business network i.e. IT network as well as most of the underlying network infrastructure in OT is now based on COTS (Commercial off the shelf) items used in IT. With such connectivity & system scenario, the threat landscape of OT systems has increased manifold introducing newer threat vectors & vulnerabilities with easy availability of services in the form of MaaS (Malware as service), HaaS (Hacking as a service), FaaS (Fraud as a service) and highly skilled, motivated hackers with targeted sophisticated resources. Air gapped control of OT, no connection to internet, and perception of limited knowledge of hackers in safety systems & OT are now a myth.

According to *Gartner*, security incidents in OT and other cyber-physical systems (CPS) have three main motivations: actual harm, commercial vandalism (reduced output) and reputational vandalism (making a manufacturer untrusted or unreliable). Gartner predicts that the financial impact of CPS attacks resulting in fatal casualties will reach over $50 billion by 2023[4]. Even without taking the value of human life into account, the costs for organizations in terms of compensation, litigation, insurance, regulatory fines, and reputation loss will be significant.

OT controls the physical systems & processes and hence have different kind of risks and priorities. Depending on the process under control, the risks can be related to human safety, environmental impacts, social impacts and impacts on organisation/national economy. Aligning the priorities of CIA triad with health, safety and environment will ensure conformance of scripting a true cyber secured architecture for OT vis-a-vis IT security. The CIA triad relevant to IT systems gives way to AIC triad wherein the availability of the OT takes the priority over integrity & confidentiality. Protection of Industrial control Cyber-Physical Systems' (CPS) hardware/software components, personnel, environment and organisation's business interest from unauthorized access or attack, leading to disclosure/compromise/destruction of financial, safety and physical indices of a system should be the ultimate aim of cybersecurity of OT (Operational technology).

B. Sketching strategy/roadmap for a cyber-resilient OT system

From the genesis, OT systems were built with a focus on performing the desired task within limited time ensuring availability. Each OT system has its own complexities, criticality. Securing plethora of mixture of different such OT systems which were never built with the idea of cyber security is the biggest challenge. Some potent challenges being faced are:

- Proprietary protocols with modified OSI model
- Replacement of Legacy systems
- Identifying and accounts assets
- Identifying critical information infrastructure
- Availability of cyber secured components - OT systems were designed with focus on availability
- Risk management
- Monitoring hosts & network
- Incident response and recovery
- Patch management (Compatibility, Outage schedule & Confidence Issues)
- Cybersecurity audit - VA/PT and compliance
- Dearth of Domain experts and lack of OT cyber security awareness
- Connectivity with business network securely

For a good OT cyber security architecture, these challenges are to be treated as opportunity. The design, engineering, implementation, operation & maintenance should consider a multi layered approach based on a defense in depth architecture to secure the system from external as well as internal threats. It should encompass aspects like physical security, laid down policies and procedures, segregating business processes & network, use malware prevention controls, access controls, advanced and intelligent monitoring & detection system and ensuring periodic patching.

1.1 **Physical security:** Protect people, process & technology from theft, tempering, fire, flood or any other natural calamities and targeted attack from disgruntled employees or terrorists. Minimum controls being use of physical access control, barriers, locks, video surveillance, alarm system & logbooks. For example, USB devices can be an easy source of infection. All the USB ports shall be kept disabled in all workstations & servers. USB locks can also be used.

1.2 **Policy, Procedures & guidelines:** Framing & strictly complying with organisations' strategic & tactical cyber security policies and procedures encompassing people & business process considering the technology at hand. These are live documents which are to be regularly visited and updated as per the regulatory, governance, risk & compliance (GRC) requirements. Adherence to security framework like NIST framework, standards like ISA/ IEC 62443 while framing the cybersecurity policy, baseline, guidelines and procedures with due care and due diligence w.r.t. business continuity plan and mandatory compliance to government regulations is essential.

1.3 **Security Zones:** The architecture of the control system network to be segregated in various zones like internal zone (where control system & HMI resides), DMZ or buffer zone & External zone. Communication protocol from internal zone to DMZ & from DMZ to external zone to be kept different. Cracking multiple protocols increases the difficulty of attack.

1.4 **Network protection:** Firewall with Intrusion prevention system shall be implemented at IACS (Industrial Automation & Control System) network perimeter and IDS (Intrusion Detection System) at Station LAN switch level. To enforce Defence in Depth, it should be ensured that these two systems are of two separate makes. For example, Network hardening can be implemented using measures like network storm control settings, ACLs, hardware MACsec etc. as per the communication required within and between identified zones.

1.5 **Electronic security perimeter isolation:** Identifying the different access points of IT/OT interface and remote access is critical. Ensuring data flow in only one direction i.e. from internal to external through use of Data diode or unidirectional gateway solution helps in creation of a near air gapped environment for internal OT network.

Interconnection with IT Systems for data acquisition: This functionality is an online (continuous), uni-directional communication of Process status to Corporate IT network for MIS purposes and this link is to be protected by using firewall with IPS at OT DMZ end. Only the services needed for this communication are to be permitted in the firewall and all other communication are to be blocked.

1.6 **Asset identification, visibility, monitoring & intrusion detection solution,** to monitor the whole OT network, can be implemented in a way ensuring no disturbance to OT. This kind of solution can help in creation of a live digital inventory of all OT assets and increase the visibility into the system. Any deviation from normal behaviour/dedicated task or intrusion of new assets will trigger alarm. This will also give a pretty good idea of existing threat repository of a given asset and the likelihood for any notable consequence. Signature, behavioural and anomaly-based host IPS/IDS & network IPS/IDS at strategic locations will help in monitoring host as well as network.

One important mode of documenting & verifying asset inventory is through rigorous site survey

1.7 **Backup and recovery:** Scheduling regular backups of all configurable systems' configurations, applications, installed media, licenses and database, prioritized by criticality, is essential. Duplication of backups and concept of tertiary backups (onsite and offsite storage of backup) is recommended to ensure smooth recovery in case of a ransomware attack or unexpected/accidental damage of backup media. Mapping of backup types' restoration time with business impact analysis for a given process and periodic testing of restore of these backups is necessary.

1.8 **Log monitoring, analysis & retention of logs:**
Such solution should be implemented for OT (including System logs, Security logs, Windows event logs, Error logs, Network logs, End points logs) having capacity of storage for a minimum period as per the regulatory or organisational requirement. Log based intrusion detection system (LIDS) or Security Information/ incident and Event Management (SIEM) functionality can be used for continuous aggregation, categorization and analysis of OT data like Alerts, alarms, events, and baselines (usually in the format of Syslog and Windows Events) for the purpose of alerts, response, and reports to be acted upon by the security team . This will help in identification of risks at an early stage and respond to these accordingly.

1.9 **Whitelisting & Malware Prevention:** Whitelisting of applications guard against execution of unwanted applications, unauthorized changes in memory (memory protection) and files. It has advantages of protection against zero-day vulnerabilities, requirement of no signature updates, being lightweight and more efficient than blacklisting. However, whitelisting is not capable of identifying malwares. Mixed deployment of Antivirus scanning for OT system and DMZ helps in identifying **malicious behaviour/signatures. Antivirus** should be kept updated with latest OT validated signatures.

1.10 **Access Control:** Establishing Controls, be it technical or through policy & procedures, to ensure use of system resources by authenticated and authorized users or systems. Enforcement of this control and documenting change management is of highest priority. Whenever possible, centralized identity and access management (IAM) tools like Active Directory (AD) with Role based Access control (RBAC), TACACS+ or RADIUS must be used with multi factor authentication (MFA) method. Organisational data with high sensitivity or business consequences should be restricted with separate access control. Concept of zero trust in IAM for east-west as well as north-south traffic within the ESP and its external interface will help in enhancing trust within and outside the perimeter.

Remote access to OEM for diagnostics: In case of diagnostic support required from Vendor, remote access may be provided (through VPN IPSec with MFA or using zero trust) to DMZ, for accessing logs, or an identified jump server, for accessing OT system. However, priority should be only for one way read only access of logs from internal to external. In general, the OT system diagnostics and necessary changes should be carried out by the trusted internal personnel as per communication from vendor over hotline. Separate authentication mechanism should be used for internal & external users and common TCP ports used should be changed from default. All sessions should be continuously monitored and logged with mechanism for termination of session by internal entity. Since, this is not a regular requirement, this connectivity is to be established only when such requirement of remote support occur else the same shall be kept isolated and most of the time vendor shall be asked to provide onsite support.

1.11 **Patch management & periodic updates**: A stratified procedure for patch management and installation of updates shall be established. It is strictly not advisable to have a direct internet connection into the OT network for patch downloads. OEM validated patches should be downloaded at a designated, sanitized, standalone station authenticated by OEM over VPN IPSec tunnel. This standalone station must not be connected in any way to the OT network. These patches are to be transferred on a sanitized and dedicated storage media after checking for vulnerabilities over a sandbox environment. Based on the evaluation of the applicability of the patches w.r.t. the concerned assets, the patches should be further tested in a Test environment to understand installation procedures and rollback procedures in case of non-satisfactory operation. On successful testing, the patches should be deployed in the target OT system and change management documented.

1.12 **System Hardening**

To reduce the attack surface, all systems which are configurable are to be hardened. Patching & update of OS, disabling unnecessary services, unused/unnecessary user accounts, applications, network protocols, introducing authentication, access control and security control are necessary measures. Center for internet security (CIS) benchmarks can be used for this purpose. Use of security compliance tool kit and Windows defender exploit guard are highly recommended. For examples, while installing firmware updates, update file Hash should be compared with as manufactured update hash.

C. Upgradation of legacy systems

The evolution and system development lifecycle of OT system is longer compared to IT. Most of the devices (hardware & software) being used in OT environment are based on certain OS platform. When the OS platform is declared obsolete, no further security updates/patches are available. This renders the OS platform vulnerable to various kinds of security threats. Hackers try to exploit these vulnerabilities. Also, the system remains vulnerable to old malwares and zero days. Hence, as an organisation, the best practice is to go ahead with upgradation of obsolete system. The challenge of upgradation of obsolete system is the opportunity of securing the system by design (as stated above in *Sketching strategy/roadmap for a cyber-resilient OT system*), implementation of best cyber practices and ensuring the cyber posture during engineering, operation & maintenance.

Till the time, equipments/systems nearing end of life or left without support from OEM are not replaced, various hardening measures along with countermeasures should be adopted for the time being to mitigate risk arising out of unsupported legacy and obsolete system.

D. Risk management

The basic life cycle comprises of identifying individual OT assets, allocating them into zones and conduits, performing risk assessment, applying countermeasures based on target security level to be achieved and maintaining with change management and incident response and recovery. Drawing parallel from ISMS (Information security management system), a CSMS (cyber security management system) is to be formulated with periodic audits and compliances. Once the OT system has been designed and implemented, based upon the threat information, intelligence, threat historical data, threats for the target system are to be identified and listed. Complying to the regulatory and organisational vulnerability assessment, penetration testing requirements, scheduled audits are to be performed to obtain list of vulnerabilities. Threats & vulnerability database obtained from LIDS/SIEM/HIDS/NIDS are to be matched with audit findings and a comprehensive list of threat and vulnerabilities are to be prepared. This will clearly lead to identifying cyber security risks for a given business process, considering the consequences and impact on the likelihood of listed threat vectors exploiting any of the listed vulnerability. **Critical information infrastructure** (CII) of an organisation are those business processes where likelihood of impact & consequences w.r.t. safety, environment, financial and reputation are critical and high.

It is very important for an organisation to know the tolerable risks and based on the method of 4 Ts (Tolerate, Transfer, Terminate and Treat), the unmitigated risk is be mitigated by introducing, installing and commissioning validated countermeasures. In this way, the risk can be managed.

There is no denying the fact that implementing a good cyber security infrastructure is a costly affair, it is important to balance the benefits of risk reduction against the cost of security measures to mitigate the risk while achieving a desired security level.

Using tools like operational security (OPSEC) and Open source intelligence (OSINT), organisations can identify what kind of company information, IP addresses, ports, services, applications & technologies and employee information are exposed externally. Adversarial risks can be evaluated using MITRE ICS ATT&CK framework to gain insight into the exact nature of threats in terms of combinations of tactics & techniques and prepare the defence plan accordingly.

E. Supply chain security

The OT supply chain is a complex and interconnected system with a variety of hardware, software, and managed services and a wide range of entities like OEMs, third-party vendors, suppliers, service providers, and system integrators etc. Like any other chain, a supply chain is only as strong as its weakest link.

Different adversaries can target OT supply chain at various stages like design, development and production, distribution, deployment, maintenance, and disposal. Various kind of vulnerabilities can be introduced in the supply chain like malicious software, hardware, and counterfeit components; flawed product designs; and poor manufacturing processes and maintenance procedures.

At the time of cyber factory acceptance test (CFAT)/ cyber site acceptance test (CSAT) of the system, it is essential to ensure sanctity of the application software & firmware before the same is dispatched to site or handed over for operation. The same should also be carried out during every software & firmware upgrade, update, and patching. The intent is to have a mechanism to verify that the application software & firmware does not contain any malicious code or is not operating contrary to its stated purpose.

Cryptography, blockchain technology, use of digital verification and taking blanket compliance against backdoor are key measures to prevent malware/trojan intrusion in supply chain management (SCM). Concept of hardware security to obfuscate IC layout, countermeasures against side channel attacks is to be introduced. Labs capable of fuzz testing, VA/PT and embedded device component security testing are to be encouraged in large numbers to enhance cybersecurity testing capabilities of Indian government.

Third party governance in the form of service level agreement (SLA) and SOPs are to be integrated in the cyber posture through policy, procedure and guidelines. These should also be made essential component of contractual requirement. Asset owner's supply chain security management should consider security requirement in specification, security by design, secure implementation and security testing with requirement for secure product life cycle and security development life cycle.

F. Incident response and recovery

Every organisation should have a well-documented Cyber crisis management plan (CCMP) clearly covering the important aspects of incident response life cycle comprising of response planning, incident prevention, detection, containment, remediation, recovery & restoration and most importantly post incident analysis & forensics. For this, the organisation should have an identified cyber security incident response team (CSIRT) – a cross functional team comprising of specialists from different departments including legal & HR. Enforcing techniques mentioned above in *Sketching strategy/roadmap for a cyber-resilient OT system,* will help in incident prevention, detection, recovery and restoration. Containment plan is very critical and should be clearly documented to stop the spread of any kind of attack. Preservation of forensic data is of utmost importance as evidence for further analysis and reporting. Immediate intimation about an incident to concerned government nodal agencies and statutory bodies is to be strictly complied subsequently followed by sharing of relevant forensic evidences. Remediation in the form of fixing the root cause of the problem, will prevent the recurrence of such problems.

G. Training & awareness

PPT (People, process, technology) framework is a widely recognised framework which defines these three elements as three important pillars of building organisational capability. A balance between these elements is must for holistic improvement. Any weakness in one, can negatively impact other two and hence degrade the overall performance of the organisation.

Talking about cyber security posture and its awareness in OT, people are the ultimate user of technology and shall manage the process. However, people are considered the weakest pillar in this framework. It is vital to build the competencies of the personnel having authorized cyber or authorized physical access (unescorted or escorted) to the Critical Systems. Considering this as an organisation, maximum impetus should be given in upskilling, training and awareness of the people component.

Training programmes like awareness, staff training and continual dedicated technology updation training etc. shall be designed for all people having any direct or indirect role in OT cyber security with a practical approach to help all stakeholders understand the risks and best practices for keeping OT systems secure. This will ensure uniform cyber readiness across the organisation irrespective of different geographical locations and complexity of the OT environment.

Conclusion

OT processes being very much varied based upon type of OEM, implementation philosophy, criticality of process is overall a complex portfolio to monitor for threats. Vast threat landscape with varying threat vectors, actors and vulnerabilities at hand calls upon staying one step ahead in the game. Intelligent and techno-economical choice of techniques will not only reduce the cost of security countermeasures but also increase the security level by decreasing the probable cost of security breaches. Increasing the visibility of assets, decrease in response time and quick recovery will help in better controls and measures for secured and reliable business continuity.

Acknowledgement & References:

[1] ISA/IEC 62443 series of standards
[2] NERC CIP Reliability Standards
[3] NIST Cybersecurity Framework
[4] https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber attackers-will-have-we

Author Profile

Alok Kumar Sinha, HOD-Project Engineering C&I and AGM at NTPC Limited, with nearly 30 years of experience in various facets of power plants Design, Engineering & maintenance with special expertise in Protection system of boiler, turbine, Flexible operation of power plant, Digitalization, Project management, RGMO/FGMO, FGD, Control system etc.

Some Nath Kundu, Alternate CISO & DGM at NTPC Limited with nearly 19 years of experience in OT, Cyber Security, Risk Management, ZTNA, SASE, Enterprises Architect, Incident handling and analysis, Digital Transformation, handling legacy systems in a safe and protected posture, Infrastructure, Policy making, Techno-commercial dealings, Team Building & Leadership domains, imparting training and awareness. Technocrat with specialization in end-to-end Cyber Security and Infrastructure Consulting solution, Management, Enterprise Integration Strategy, Digital & Enterprise Architecture and Consultancy Projects on OT systems including Critical Information Infrastructure (CII); directed the business operations through executive level planning and analysed delivery issues in a timely fashion. Liaised with several ministry committees for Cyber Security related regulation framing, identifying Cyber Security testing requirements, Audit criteria, training and awareness. Acted as an Enterprise Architect to provide high-level designs across the Engineering and Technology domain; Subject Matter Expert for driving technology discussions and analysing the existing architecture for gaps in addressing business needs. Gained expertise in Human Machine Interface, Control System Networking, Network Security, Third Party Interfacing & OPC, Display Systems, Control Room Design, Interoperability of one make OT through the application of another make OT, upgradation of OT legacy system to a more secured latest OT architecture.

3. Kuldeep Singh Yadav, Senior manager at Engineering division, NTPC Limited with nearly 13 years of experience in various facets of power plants including networking, cyber security, Digital transformation, human machine interface, Consultancy Projects on OT systems including Critical Information Infrastructure (CII), Display Systems, Control Room Design, Interoperability of different OT systems, upgradation of OT legacy system to a latest & secured architecture, power plant engineering and maintenance. CEH certification, Certification in Foundation course in management from IIM Indore, Harvard ManageMentor & GPiLearn.

BARTEC

AUTOMATION & ENTERPRISE MOBILITY

Bus Technology
Mobile Computer
Panel PC
Touch panel with LED Technology

Industrialized Tablet PC
Smartphone Impact X
Wireless X
Camera Gravity X & Orbit X

CONTROL & CONNECTION EQUIPMENT

Control & Indicating Equipment
Ex d & Ex p Solutions in Aluminium, Polyester
& Stainless Steel versions
Installation Technology
Switches
Line Bushings & Cable Glands
Lighting & Signalling devices
Motors

HEATING TECHNOLOGY

Heating Cables
Connection systems
Plexo Kits
Control Systems
Heaters / Radiators
Turnkey Projects

ANALYZERS & MEASUREMENT TECHNOLOGY

Cloud Point Process Analyzer
Distillation Process Analyzer
Flash Point Process Analyzer
Freezing Point Process Analyzer
Pour Point Process Analyzer
RVP Process Analyzer
Capillary Viscosity Process Analyzer
NIR Process Analyzer
Moisture Analyzer

Bartec India Pvt. Ltd., *C-56/45, 1st Floor, Priska Tower, Sector-62, Noida – 201309, Uttar Pradesh, India*
Phone: +91 120 4523200/201 email: info.bartecindia@bartec.in

Session 4

Session 4

1. Application of Digitization in Automation of Process Industry - HMEL
2. Securing Operational Technology - Schneider

APPLICATION OF DIGITIZATION IN AUTOMATION OF PROCESS INDUSTRY & CYBER SECURITY CHALLENGES

KAILASH KUMAR, SHRISH MISHRA

HMEL REFINERY BATHINDA

ABSTRACT

Process industries have substantial benefits in achieving operational excellence by integrating the complex automation systems with data analytics tools outside the operation technology, however this integration has potential to compromise the OT with severe implications due to cybersecurity challenges as well. New enabling technologies such as IIoT, asset management system, Alarm rationalization systems pushes manufacturing enterprises to implement IT/OT integration to benefit in terms of cost optimization, business process improvement, decision-support, etc. In this paper the benefits & vigilance in OT integration are discussed to have secured and optimized digital transformation.

KEYWORDS

Industry 4.0, IT-OT-Integration, Digitalization, Automation

INTRODUCTION

Most process industries deal with high-value products and raw materials, for example – in the Oil and Gas industry, the infrastructure required for oil extraction, refining and processing involves considerable effort and cost. Hence, the primary goal is to optimize infrastructure and resource utilization with minimum downtime. The ultimate objective of all activities at different layers of the plant is to maximize production by achieving the best possible uptime. Organizations must have proper plans to embrace new technologies backed by reliable data and secured infrastructure. Such preparedness and deliberate efforts ensure that technology and process transition happen in a phased manner, resulting in minimum plant downtime.

A majority of process Industry require integrating shop floor systems, so called OT systems, with an enterprise's office floor systems (IT systems). The integration of IT and OT also becomes a main component for collaborative networks, enabling to harvest their full potential. In addition, suitable methods for approaching a structured IT-OT-Integration process and understanding of associated hidden hazards are missing. Thus, combining a company's digitalization goals with the as is assessment of its infrastructure and introduction into IT-OT-Integration and utility potentials, this paper presents an application of digitization in automation of process industry & cyber security challenges.

NECESSITY OF DIGITAL TRANSFORMATION & AUTOMATION

Today's technology offers process industries unprecedented ability to leverage data to develop intelligence for decision support, both in real time and over time. Process Industries that adopt a technology strategy to align core operations with overall objectives can generate data-driven information at hand to be more agile, resilient and innovative – ultimately reducing cost and mitigating risk. External factors driving such automation tool and further OT-IT strategies include:

A. **VOLATILITY**- Looking back at pandemic 2019-time transformation of data played significant role in changing our strategies and adapting new business opportunity. Industries globalization, economic instability and aging infrastructures require industries to be more agile. Connecting OT to business tools enables them to develop predictive information to reduce operational variability, and base workflows and capital planning on actual operational history and data.

B. **OPERATING COST**- IoT Reduced costs of sensors and connectivity has made it more feasible to create a comprehensive digital footprint of operations, including mobile assets and workforce. As the data volume and variety continue to expand, integrated OT environments and interoperability with IT systems will become necessary.

C. **COLLABORATIVE ECONOMIES/BUSINESS PROCESS IMPROVEMENT**- For enterprise initiatives such as product genealogy, supply chain management and emissions reporting, operational accountability stretches beyond traditional boundaries and across extended value chains. Moreover, connected product and services are introducing the need for collaborative data ecosystems that connect industries with suppliers and customers.

AUTOMATION METHODOLOGY IN PROCESS INDUSTRY WITH THEIR FUTURE POTENTIAL

A. IDENTIFYING GAPS BETWEEN EXISTING AND NEW DIGITALIZED WORLD

This paper presents the thought process for selection of digitization methods and their benefits to organization and further future risk and challenges involved while implementing the same.

Fig.1

Fig.1 gives an overview of this process. In the beginning, potential digitalization measures, the so-called utility potentials, are selected. In this paper, the term utility potential is used to describe business benefits (utility) in combination with their digitalization measure (potential).

The identified utility potentials were each analyzed to determine the required functionalities and architecture within the construct of IT components, OT components and their corresponding connectivity. This analysis was supported by modelling the expected data flow, to demonstrate the individually required system in a network of general IT and OT components, as shown in Fig. 2. The model allowed an intuitive translation of the utility potentials into the proposed IT-OT-Integration Profile.

B. AUTOMATION AND DIGITAL TRANSFORMATION METHODOLOGIES

Available methodologies can be classified as per related area of improvement. These areas of improvements are referred as Utility potentials and are mapped to general benefits to be achieved in production, consisting of cost reduction, optimization of process time, enhancement of the product’s quality and flexibility of production.

Utility potentials can be classifiable into the categories as promotion of transparency, decision support and active production adaption (Table 1).

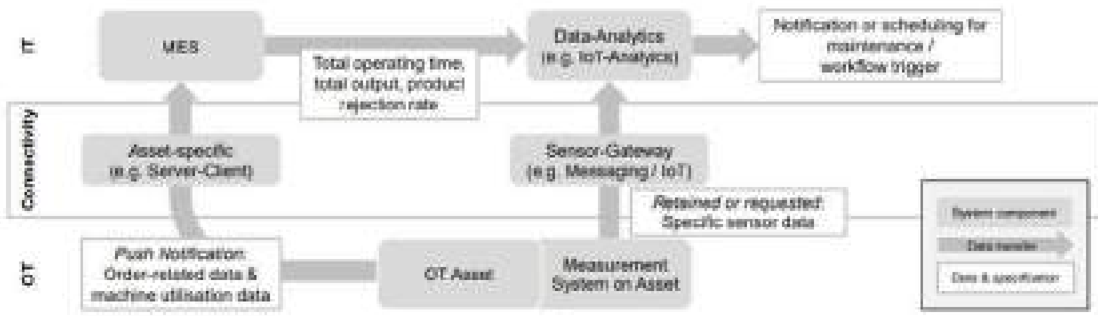


Fig.2

Table 1: List of Utility Potentials	
Transparency	Digital Order Tracking
	Digital Worker Guidance
	Realization of digital work-flow
	Realization of Condition Monitoring
	Automatic Process Quality Documentation
	Automatic Collection of Production KPI
	Databased derivation of actual Process Cost
	Order Status Transparency in Production
Decision Support	Predictive Maintenance
	Dynamic Pricing in Production
	Realization of Production's Digital Show
	Automatic Quality Evaluation with Data Analytics/Machine learning
Active Production Adaption	Reduction of Machine Downtime
	Production Process Optimization with Data Analytics/Machine Learning
	Optimization of Process Duration
	Active Energy Management using data analytics
	Adaptive Production Adjustment for errors and downtimes
	Automatic Machine Configuration based on the order

Table.1

The category promotion of transparency includes measures, in which data is collected to visualize operational conditions and further allow the analysis of simple causalities between process parameters and the product.

The support of decision-making builds on top of the enhanced transparency, by utilizing further data sources and active analysis to generate insights into production, forecasts and detect necessary actions.

The final category, active production adaption, usually adds onto the previous decision-making, by actively reacting to available information. The adaption takes the form of automatic decision-making and regulation of the process or system. In contrast to the perceived complexity, the measures implementing active adaption can also represent a simple functionality such as the automatic configuration of machines in response to an order command.

Table.2 provides the list of automation methodologies implemented in our process control ecosystem.

Fig.3 demonstrate the model of APM where IT/OT Integration introduced.

DIRECT IT/OT INTEGRATION	**INDIRECT IT/OT INTEGRATION**
Advance Process Control	MES
Alarm Rationalization	Turnaround Management
IIOT	Material Management
Asset Performance Management	SAP Automation
Cyber Security Implementation	

Table.2

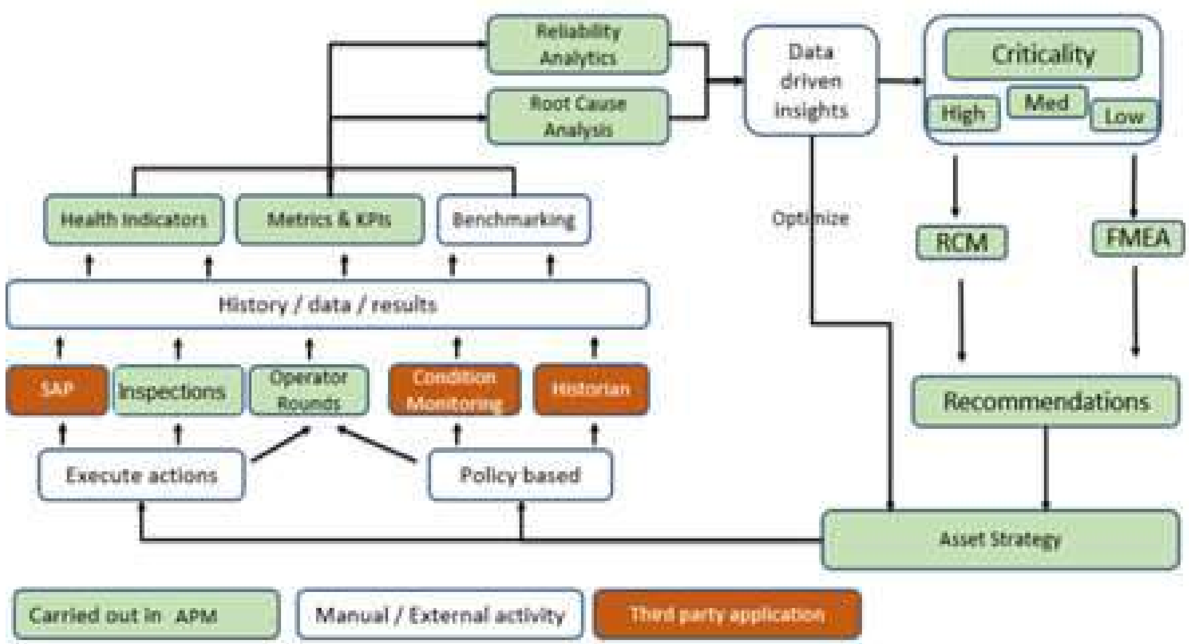


Fig.3

CHALLENGES

Since information technology (IT) was introduced into all walks of life, the threat from hackers and virus attacks have never been got rid of. However, it does not prevent industrial enterprises from adopting the commercial-off-the-shelf software and hardware and the general network connectivity into operational technology (OT) networks, such as industrial control networks. IT/OT convergence provides attackers more opportunities to launch targeted attacks whose consequences can be disastrous against the real physical world. Industrial control security incidents in the past decade are the best proof that cyberattacks are gradually infiltrating from the IT networks to the OT networks. Apart from the cyberattacks migrated from IT networks, some inherent issues exist in the OT networks, such as design defects in industrial control network protocols and vulnerabilities of proprietary devices .

On account of frequent interactions between IT devices and OT components, there are no clear boundaries between IT and OT partitions in the current industrial environment. In other words, any compromise that occurred on the devices or networks in either IT or OT side has an undesirable impact on the overall safety and security. Therefore, both IT and OT aspects should be taken into consideration simultaneously for cybersecurity analysis in a comprehensive assessment. In general, the security assessment mostly relies on a standalone vulnerability scanning for services or devices in the IT and OT networks.

To tackle the challenges of IT-OT-Integration, both the potential digitalization use cases that are of relevance for a company's digital transformation as well as the existing IT-OT-Landscape need to be considered. This ensures the alignment of a company's strategic goals with its current situation.

SECURING AND OPTIMIZING DIGITAL TRANSFORMATION

Vigilant approach and precautions while implementing digital transformation is required to have secured and robust system.

Architecture of ICS at our process industry is designed in line with IEC-62443.

The following solutions are implemented in OT environment –

- **Centralized User/System Management (Active Directory)**
- **Centralized Anti-Virus and OS Patch Management**
- **Backup and Recovery System**
- **Firewall / Secure Architecture and Secure Remote Access.**
- **Application Whitelisting**

Operational data often remains landlocked for many reasons. An article in the New York Times in 2014 said that companies estimated that data scientists spend 50 to 80 percent of their time on the mundane work of data preparation. Resistance to change, fear of security breaches, different organizational priorities and risk to process integrity also weigh heavily against efforts to align architectures across functional departments. Growing volumes of IoT will only amplify the need for governance, context and automated connections.

Corporate Organization OT often lives in a parallel, but separate, universe from IT and business groups. Even as technical barriers to OT-IT convergence fall, traditional cultural and functional boundaries remain.

Safety and Security Many organizations create a demilitarized zone around OT systems that includes firewalls, data diodes and one-way networking systems as well as razor wire and personnel access control. Even when a company wants additional stakeholders to have access, clearance has to be obtained.

CONCLUSION

Bridging the OT-IT gap is a critical step to enabling digital transformation. By automating data integration and eliminating information silos, everybody inside an organization – from an operator to the C-suite – can begin to understand how their actions affect profitability or productivity in real time. Live, active insight from operational data will play an instrumental role in cutting costs, energy and emissions, improving the return on capital and accelerating the development of new products. It’s no exaggeration to say that data will be the most valuable resource for most companies in the future.

For over 30 years, industries have been leveraging sensor-based data to gain visibility into operations, support continuous improvement and generate information to optimize overall enterprise performance. As the global business climate grows more unpredictable and competitive, enterprises that can create a unified view of operational data and merge it with business information will be poised to respond to disruption and differentiate themselves. As IoT, Big Data and advanced analytics play a more prominent role in industrial settings, we need to be more vigilant in IT-OT convergence.

Mastering the IT-OT-Integration process is a challenge for many companies, especially process industries. Therefore, this paper presents a set of utility potentials as well as an IT-OT Integration profile to structure and assist the integration process. In the beginning, thought process for identifying automation gaps in industry is presented. Afterwards a set of utility potentials to select in the beginning of an IT-OT-Integration project is shown. Subsequently, an Integration profile with the categories IT, OT and Interface to assist the structured as is assessment of an IT-OT-Landscape is introduced. Finally, the challenges and cautions in this digital transformation is discussed.

ACRONYMS

IT- Information Technology

OT- Operational Technology

BIOGRAPHIES

Sh. Kailash Kumar is from Bareilly, Uttar Pradesh. He graduated in Electronics and communication engineering from HBTI, Kanpur in 1998. He has 25 years’ experience in various process industries and joined HMEL in 2013. At present, he is AGM-Instrumentation and working as Instrument Maintenance Head in HMEL refinery at Bathinda, Punjab.

Sh. Shrish Mishra was born in Kanpur, India in the year 1991. He graduated in Instrumentation and Control engineering from NIT JALANDHAR. He joined HMEL in 2013. At present he is working as Deputy Manager at HMEL refinery at Bathinda, Punjab.

Securing Operational Technology (OT): Addressing digital risks in business-critical infrastructures

by Schneider Electric

Executive summary

Digital transformation enables industry to improve operational and business performance in ways never imagined before. To take advantage of the Industrial Internet of Things (IIoT), companies must expand connectivity across their people, assets, and systems, and make full use of extracted data to improve their operations and processes. All this connectivity closes the gap between IT and OT, meaning a company's operations are in sync with their business, enabling greater performance. However, it also widens the attack surface for would-be cybercriminals.

This white paper examines risks to Operational Technology (OT) as industrial facilities implement IoT devices across the environment. In the age of the IIoT, cybersecurity can no longer be an afterthought. There is too much at stake, financially and operationally.

Global industry faces a new reality: today's bad actors frequently have unlimited time, resources, and funding to carry out their cyberattacks. In the face of new, ever more dangerous threats, forward-thinking companies will quickly implement best practices for securing their mission- and business-critical environments. By making security part of the operations lifecycle, companies are more likely to succeed in the digital economy.

Contents

Thriving in the digital economy

"Any skilled engineer can take control remotely of any connected 'thing'. Society has not yet realized the incredible scenarios this capability creates."

André Kudelski, Chairman and CEO of Kudelski Group[2]

Without question, the hyper-connected economy is here. About 20 billion objects are connected to the internet at present,[1] with objects and machines becoming increasingly interconnected to each other. As global industry integrates technology at the heart of its facilities and operations, the question everyone should have in mind is: how can we secure this fast-proliferating digital landscape in industrial environments?

Indeed, while having hundreds of devices connected to the same network eases processes and improves efficiency, it also opens a wider window to security threats.

An attack in the Information Technology (IT) world can result in significant theft, loss, or misuse of data, which can be a blow to a company's reputation. In many cases, industrial stakeholders can look to IT security as good practice. IT security at large is widespread across markets. By contrast, the practice of securing the Operational Technology (OT) environment is in its infancy, and it is even more critical. That is because an attack in the OT space can have direct repercussions on physical surroundings, such as a full grid outage or, in the most extreme cases, the loss of human life.

Revealing the impact

"Popular movies have frequently exploited the idea that the infrastructure of modern life is vulnerable to well- staged cyberattacks. But the real-world Stuxnet virus succeeded better than anything out of Hollywood in proving that power plants and other nuclear assets can indeed be sabotaged."

McKinsey & Company[4]

Industry's first wake-up call was the Stuxnet case, which surfaced in 2010. This malicious computer code wormed its way into the middle of an Iranian nuclear plant, ultimately affecting about 100,000 computers worldwide (mostly in Iran), including uranium centrifuges.[3] More recently, an industrial facility in the Middle East was the target of a highly sophisticated and prolonged cyberattack, dubbed Trisis or Triton. When attackers attempted to infiltrate the facility's safety integrated system, the system detected an anomaly and took the plant to a safe state via a shutdown. Unfortunately, such cybercrimes are no longer relegated to the world of science fiction.

Similarly, everyone remembers WannaCry, the ransomware attack that affected more than 200,000 computers across more than 150 countries.[5] WannaCry caused damage to many users, from individuals to huge companies and industrial facilities. By encrypting computers and machines in factories and asking for payment, the ransomware was able to cause huge damage to the IT and OT organizations.

This last mass attack was eye-opening well beyond the incident, as it ultimately revealed that all industrial players needed to work together to ensure a path to safety in the OT world across the entire digital ecosystem.

Accelerating OT security

In the past, before the proliferation of the Industrial Internet of Things (IIoT), OT infrastructure was fairly safe from cyberattacks. This is because proprietary standards and hard-wired connectivity protected devices in a unique way. The widespread integration of embedded devices and OT networks with corporate or IT infrastructure has created a much greater attack surface over an increasing number of open networks. Every endpoint in a factory or facility is a possible path for hackers, and the impact on maliciously accessing industrial controls could be disastrous.

When it comes to cybersecurity, IT stakeholders typically look to secure data and protect data privacy. Industrial companies, by contrast, seek to protect safety, efficiency, and reliability as they race to seize the many benefits created by converging their IT and OT. These advantages include just-in-time inventory, faster production, improved energy use, and better safety, but the real benefit is a new-found ability to manage and control business performance.

What are common OT risks?

As industrial companies implement cybersecurity strategies as an inherent aspect of their digital transformations, it is important to recognize the differences between securing the IT and the OT environments. Companies can garner lessons learned from IT over decades and, in turn, create a holistic approach to ensure that cybersecurity in a hyper-connected world adopts strategies concerning known and emerging risks and threats. According to the State of Industrial Cybersecurity 2019 survey, about “70% of companies surveyed consider an attack on their OT/ICS infrastructure likely. Despite this, many have yet to define their own approach to implementing OT/ICS cybersecurity.” [6]

So, what are the inherent risks in OT?

A wide attack surface

Today’s cyberattacks are numerous, frequent, and more threatening than ever before. Attackers aim to infiltrate and manipulate not just an individual company, but the entire ecosystem to which it belongs. Needless to say, 20 billion connected objects create many endpoints. Each device can be an entry point for hackers to access the broader industrial ecosystem. Consider, for example, that in today’s digital factory, there are hundreds —and even thousands — of connected sensors across the industrial environment. Each is a potential target for hackers.

Legacy infrastructure with aging assets

Many of the systems that control the world's most critical operations were installed and developed decades ago, before the advent of the IIoT and back when cybersecurity was not even a consideration. Additionally, these systems are built for the long haul: they have decades-long lifespans and, in many cases, will continue to operate until the plant is decommissioned. Securing these systems in the age of the IIoT is doubly challenging due to the technical limitations of the devices and the need to maintain compatibility with other legacy infrastructure. Here, as new integrations of current technology proliferate
at lightning speed, digital risk increases if an end-to-end cybersecurity plan to address both current and legacy systems is not in place. According to an Accenture survey, 79% of CEOs questioned indicated that their organization is "adopting new and emerging technologies faster than they can address related security issues." [7]

Targeted attacks on unique weaknesses

In addition to managing aging assets, industrial companies are wrestling with the fact that OT cyberattacks often target unique weaknesses for a very precise impact. Instead of targeting a weakness that will affect the biggest number of users, as often seen in the IT space, recorded cases show that, industrial hackers generally focus more resources on attacking a specific weakness in a rare device to aim at a single target.

This particular type of modus operandi requires specific paths of protection.
Typical defensive measures, such as antiviruses, are not commonly applicable due to the limitations of the devices; regular antiviruses would unacceptably slow or incapacitate them. What's more, it is expensive, complex, and inefficient to design specific protection programs for each device. To stop an attack once it is detected, the devices should be quickly disconnected from the system. Such a disconnection is very challenging in many factories. Though the installation of patches is a common remediation for IT systems, it
is often more complicated to implement in industrial environments as patches should be installed during the limited maintenance periods and may require device recertifications, leaving the devices exposed during the gap.

Regular exposure to third-party access

In addition, the OT environment is particularly exposed to third-party risks. Compared to IT, OT environments are more likely to rely on vendors for ongoing support but less likely to formally manage the associated external risks. These vendors are often granted privileged access through their own laptops and USB devices, the internet, or fully
hosted environments with little control. Even with no malicious intent, this broader access poses a huge risk in terms of cybersecurity despite the dangers of infection. Several heavy industrials have reported that third parties frequently connect laptops and external storage devices directly into OT networks without any prior cybersecurity checks.

Addressing these OT risks

As the IIoT promises to advance the world with significantly more cost-effective deployments, advanced analytics, and immense scalability, it also introduces cybersecurity threats previously relegated to the IT department. Now, many devices can connect to the internet, share information, and receive control signals or configuration updates. These new devices present security risks that historically have been unfamiliar to operational teams. Connecting these devices exposes them to the outside world, which means malevolent actors with high skills can intercept, modify, or disable these devices. Their motivational interests can range anywhere from criminal to national security or societal change.

With such complex OT risks, it is essential to protect industrial assets and processes and move from reaction to proactive prevention. Some practices that might seem simple are essential. For example, having stricter password policies, giving basic training to employees, or including cybersecurity terms within suppliers' contracts are fundamental steps that can have a big impact on securing an ecosystem. Here are some recommended steps for securing the OT environment:

Network segmentation

Intelligence is migrating upward through the automation hierarchy and into the IT architecture. The data from the factory devices is fed upward into the control layer, and onward so business and operations managers have real-time insight into the performance of the plant. With that data, they can make better real-time decisions on what actions to take for better business outcomes.

For the factories producing more advanced technologies with higher risks, high-level security solutions can be implemented, the most secure of which is the networking segmentation (conduits and zones systems).

In this case, the factory is divided into zones, with each being isolated from one another. In order to allow the information to circulate, channels (conduits) are created between the different zones. These conduits allow only specific information to circulate, enabling the user to monitor it while blocking the rest of the incoming or outgoing information. Attackers or malware that have breached one zone will find it difficult to pivot to another zone if controls such as a properly configured data diode, firewall, IPS, or IDS are in place.

These ensure that only authorized traffic is allowed to traverse zone boundaries.

Figure 1: Network segmentation to separate IT and OT environments

People and operating models

Though most of the risk management solutions and mitigations involve technological methods, the human factor in cybersecurity should not be neglected. It is a huge part of the risk landscape. In the realm of industrial control systems, human error and unintentional actions are responsible for more than a fourth (27%) of network incidents.[8] That is why it Is essential to implement mandatory, ongoing training that is consistently and continually adapted depending on the expected cybersecurity involvement of the worker. Policies should be created and enforced to help formalize standards and guidelines. These policies might focus on numerous aspects of the network management and facility organization, and can include measures such as password regulations, incident management actions, and user access controls. In addition, in case of a crisis, playbooks should be available to help the worker to focus on essential specific actions while being possibly overwhelmed by a stressful situation.

Avoiding the cascading effect

Recent malware attacks show that an OT infection can spread to the IT domain and vice versa, in a cascading effect. This was the case with the infamous ransomware WannaCry. Though it was initially aimed at PCs, it soon propagated to the OT environment, where devices were a lot harder to protect and to patch. For that specific pattern to happen, the ransomware was exploiting a weakness in the Server Message Block protocol, through four unprotected ports. By blocking the access to these ports, the zone was able to remain WannaCry-free. Thus, the network segmentation method discussed previously has proven an efficient way to avoid cascading the effect.

Securing legacy infrastructure

One of the major challenges for securing both IT and OT equipment is how to address the cybersecurity hurdles of legacy systems, especially infrastructure with a capital expenditure whose lifespan is 30 years or longer. Although the new generation of physical infrastructure products and solutions are far more cybersecure, it can be practical and economically feasible to apply a range of basic but effective security controls to legacy systems to improve their security posture.

Continually securing legacy operations and systems against new threats is a challenge, but it is not impossible. It is critical to strive to adhere to industry-recognized practices to further reduce threats to aging installations. Taking these precautions and speaking with security consultants and cybersecurity providers can significantly increase the layers of protection. These precautions, which may be more critical for legacy infrastructure lacking advanced cybersecurity controls due to their age, can include:

- Keeping all programming software locked in cabinets and not connecting them to any network other than the network that the devices are intended for.
- Locking all controllers in cabinets and not leave them in “program” mode.
- Implementing physical controls such that no unauthorized person has access to the ICS and safety controllers, peripheral equipment, or the ICS and safety networks.
- Locating control and safety system networks and remote devices behind firewalls and physically and logically segmenting them from the business network.
- Banning laptops that have been or are connected to any other network, besides the intended network, from connecting to the safety or control networks without proper sanitization.
- Scanning all methods of mobile data exchange such as CDs or USB drives with an isolated endpoint running the latest antivirus signatures before allowing these media into the OT environment.
- Minimizing network exposure for all control system devices and systems, and ensuring that they are not accessible from the internet unless a risk assessment has been performed and the risk is within acceptable thresholds.
- Using secure methods, such as Virtual Private Networks (VPNs), when remote access is required. At the same time, it should be recognized that VPNs may have vulnerabilities and should be updated to the most current version available.
- Recognizing that a VPN is only as secure as the connected devices themselves.

Adopting shared responsibility

Cybersecurity is everyone’s responsibility, and each party has a role to play. Manufacturers and Original Equipment Manufacturers (OEMs) should endeavor to provide the safest, most up-to-date devices at the moment of production. Manufacturers and OEMs must also design safe protocols and interfaces for these devices, offer basic security training, and develop patches when needed. In parallel, end-users of the systems are obligated to train their workforce on safe practices and provide them with guidelines on what to do in the event of a cyber incident. Furthermore, end users must be responsible for keeping their devices up-to-date, as per the given instructions. By uniting manufacturers, OEMs, and utilities practices, the OT world will become inherently more secure.

What is Schneider Electric doing to secure its supply chain?

Schneider Electric's digital risk strategy recognizes that cybersecurity is not just a feature of hardware or software components. Since Schneider Electric's Smart Factory program was launched, there has been a greater focus on cybersecurity. This program is based on Schneider Electric's IoT-enabled EcoStruxure™ platform, which comprises connected products; edge control; and apps, analytics, and services. These solutions can greatly contribute to an increase in productivity and to more accurate and easier process controls. To be able to use the features of this new platform safely, cybersecurity must be included in risk management discussions.

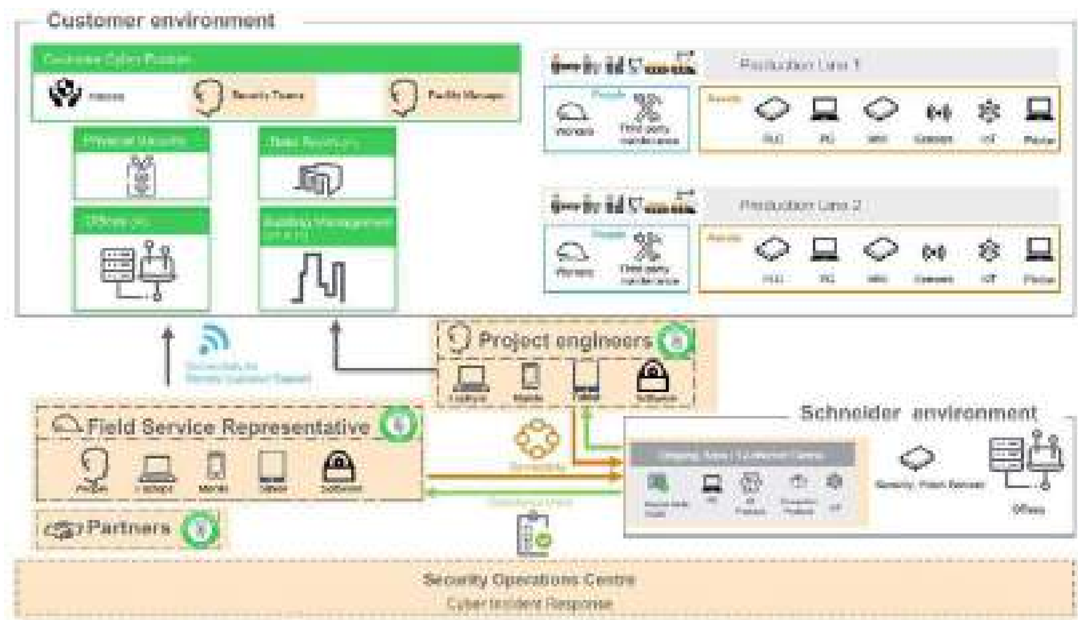


Figure 2: Securing the end-to-end digital ecosystem from supply chain factories and customer-facing activities beyond field services

Cybersecurity is a fundamental, ongoing business practice that strives to identify, mitigate, and reduce risks by applying standards and good practices to people, processes, and technology across the end-to-end digital landscape. Relevant challenges are identified for high-value assets, the at-risk population, and IT/OT segmentation. Then, the cybersecurity framework is designed with a mix of policies and best-in-class solutions. This strategy is communicated with providers and suppliers to ensure their understanding and compliance with Schneider Electric's security policy, which creates a holistic strategy from the supply chain to deploying solutions to customer sites.

To secure its own factories across the global supply chain, Schneider Electric adopts a cybersecurity strategy that uses the ISA/IEC 62443 set of cybersecurity standards as a baseline. The ISA/IEC 62443 approach comprises four levels that Schneider Electric has condensed into basic, intermediate, and advanced. The basic level has been mandated for all Schneider Electric factories. One of the requirements to reach this level is the designation of a Cybersecurity Site Leader. Skilled and trained accordingly, this person must be appointed in each plant to ensure that these actions are properly implemented and that 100% of shopfloor employees have completed a cybersecurity training.

According to the required level of security, intermediate and advanced levels are also deployed in Schneider Electric plants. For instance, at OT factories producing advanced technologies, remote access controls must be implemented for subcontractors, and firewalls must be installed to separate the networks. The plant is divided into several zones that are isolated from each other by conduits and zones. By doing so, Schneider Electric takes care that if an installation is compromised by a virus, access to this installation can be controlled to protect each zone.

Figure 3: Scalability of the deployment strategy for cybersecurity on industrial sites

In order to ensure optimal protection and reaction in case of alerts, Schneider Electric cybersecurity stakeholders often organize penetration tests and incident response simulations. This testing means that some facilities are assessed on their reaction to a possible cyberattack. Through these operations, new measures and trainings are implemented to confirm up-to-date safety.

Raising the bar of OT security via collaboration and partnerships

In isolation, it is possible for a company to have good cyber posture. However, unity around cybersecurity is essential to ensure security for all. In order to contribute to global efforts, Schneider Electric gives precedence in contributing to organizations such as the following:

ISA Global Cybersecurity Alliance

"As industry confronts escalating, innovative, and dangerous cyberattacks, every organization interested in securing our global infrastructure should collaborate to improve how end users defend themselves"

Mary Ramsey, executive director of ISA[10]

Led by its members, including Schneider Electric as a founding member, the International Society of Automation (ISA) Global Cybersecurity Alliance advances the development of new standard-based defensive strategies that contribute to improving cybers the OT space.[9]

To do so, cybersecurity knowledge and information must be shared in an open environment. This knowledge and information sharing helps facilitate the awareness and response to threats. Also, as no initiative can be complete without collaboration of governments and regulatory agencies, the ISA Global Alliance takes the initiative to encourage the advocacy of new measures and accelerate the development and adoption of standards in accordance with the prevailing, globally recognized ISA/IEC 62443 set of cybersecurity standards.

Cybersecurity Coalition

"Joining the Cybersecurity Coalition demonstrates that Schneider Electric takes cybersecurity challenges seriously and that we are committed to playing a foremost role in developing solutions. Our membership ensures we have a focused seat at the table to initiate open, transparent, and collaborative conversations that advance the adoption of cybersecurity policies and laws for the benefit of our customers, partners, and all stakeholders across our extended enterprise, including the communities and environments we mutually serve"

Hervé Coureil,
Chief Digital Officer,
Schneider Electric.[11]

Schneider Electric affirms its role in strengthening digital trust as a member of the Cybersecurity Coalition. The Coalition addresses the intersection between governments, researchers, and vendors. Here, the Coalition is focused on several critical policy issues that require close alignment and coordination to protect the vital interests of cybersecurity products and services industry, including:

- Promoting responsible vulnerability research and disclosure
- Promoting effective privacy processes within cybersecurity policy
- Establishing cybersecurity procurement requirements for government systems
- Increasing information sharing and threat intelligence
- Promoting sound cybersecurity practices in government at all levels

A cybersecurity partner ecosystem

Schneider Electric places a high priority on strengthening cybersecure digital innovation through an extended enterprise approach that includes strategic partnerships with best-in-breed technology providers, customers, startups, universities, and developers. The resulting ecosystem advances co-innovation and the development of more secure EcoStruxure solutions while also providing an open community to developers.

Examples of this digital ecosystem approach include collaborative development and management of a Security Operations Center (SOC) with IBM. This has led to the creation of incident response teams that strengthen resilience and responsiveness capabilities.
Another example of a partnership is the one between Schneider Electric and Partners, a specialist in providing visibility and greater security to OT networks.

Realtime Threat Monitoring

To secure the network and assets inside the 300 factories and facilities across Schneider Electric's global supply chain, a partnership was leveraged with real time threat monitoring partners, an OT security specialist firm. Real time threat monitoring partners smart solution monitors network flows transiting between devices, in turn informing the SOC as soon as any abnormality is detected. It also knows in real time which device is connected to the intranet or internet, as well as the specifications of each of these devices. This real-time monitoring allows live tracking of devices from initial deployment to when to patch, to obsolescence.

Public partnerships

Schneider Electric also engages in numerous public partnerships to help make both legacy and new products more cybersecure. For example, Schneider Electric is an active member of the Cybersecurity at MIT Sloan (CAMS, formerly IC^3), an interdisciplinary forum that brings together MIT faculty / researchers and C-level cybersecurity experts on cyberspace, cybercrime, and cybersecurity as applied to critical infrastructure.

Improving the security of industry with cybersecurity training and services

Schneider Electric also leads its own initiatives and collaborative resources for customers and partners. For example, Schneider Electric offers a Cybersecurity Virtual Academy which provides a thought leadership platform for the company and cybersecurity services for partners and customers who would like to reinforce their cybersecurity posture.

Cybersecurity Virtual Academy

Investing in awareness and training is much less expensive than the cost of remediation, a damaged reputation, or downtime. At Schneider Electric, sharing information with customers and partners is essential. That is why Schneider Electric created the Cybersecurity Virtual Academy to provide value-added content and engage customers, prospects, and other interested groups in an ongoing dialogue about cybersecurity topics.

Cybersecurity Services

Cybersecurity defenses are only as strong as the weakest link – if they are implemented improperly or left accessible, the system is not secure. Cybersecurity is a journey, not a destination.

Schneider Electric's cybersecurity solutions are applied from the operations perspective while integrating the appropriate policies and requirements. Schneider Electric has deep knowledge and experience in cybersecurity, allowing it to provide customized and flexible experiences to customers independent of system vendors.

For the customers who would like to go even further, their maturity can be assessed, such as in the diagram below. With comprehensive services, Schneider Electric can help to progress from the initial stages with the potential to reach the optimizing level depending on the requirements.

Initial 1.0	Developing 2.0	Defining 3.0	Managing 4.0	Optimizing 5.0
People: No dedicated staff for security activities but risks broadly accepted.	**People**: Leadership structure formalized & management roles assigned.	**People**: Roles & Responsibilities established and formalized.	**People**: All RACI roles filled with dedicated resources and/ or responsibilities assigned.	**People**: Ongoing development & training, continuous improvement.
Process: No governance or management system in place.	**Process**: Basic governance framework and policy created.	**Process**: Comprehensive Cyber management system established.	**Process**: Formalized governance group, reviewing performance & metrics.	**Process**: Cybersecurity management system fully implemented.
Technology: No emphasis on formalized security controls.	**Technology**: Some technology implemented in an ad-hoc fashion.	**Technology**: Formalized technical controls.	**Technology**: Control measures in place & monitored for compliance.	**Technology**: High level of automation for monitoring, compliance & performance.

Figure 4: A cybersecurity assessment can determine an organization's level of maturing in protecting the digital ecosystem

One of the main focuses at Schneider Electric is to enhance safety and security at every stage of a component's life. To do so, a global team with strong IT experience and deep knowledge of the OT world can help customers assess their needs and detect gaps in their cybersecurity management. This means secure, tailored solutions can be recommended and implemented. More importantly, Schneider Electric has the skills and experience to monitor and maintain existing and deployed installations more securely and independent of system vendors. Furthermore, it is essential to share knowledge and experience to develop the cybersecurity mindset that is critical today and in the future.

Schneider Electric solutions revolve around four essential factors:

- **Permit**: The access to the network is subject to safety measures such as authentication, authorization, and physical identification.
- **Protect**: The network is protected from malware and viruses and can have some advanced protection tools installed.
- **Detect**: Issues in performance, anomalies, and intrusions should be detected as soon as possible to allow an adequate response.
- **Respond**: Once a cyberattack is found, incident response is activated, and forensic investigations conducted. If needed, recovery can be made from a backup.

A regulatory snapshot and perspective

With Schneider Electric's cybersecurity services, for every decision taken and each action made, there is always a fundamental link to people, processes and technology.

In general, global cybersecurity policies and regulations are focused on the requirements of Internet of Things (IoT) devices. These regulations typically do not target OT specifically, instead, they combine OT into the broader definition of IoT devices. In other words, policy and regulation that Schneider Electric tracks targets any "connected devices" or "IoT device" regardless of the intended use or customer base. Below is a high-level overview of the key regulations that have a direct impact on the OT environment. Note that that these are the laws currently in place/effective today; many more are pending in various jurisdictions and the regulatory landscape is constantly evolving.

European Union (EU) Cybersecurity Act[12]: On March 12, 2019, the EU Parliament voted to adopt the EU Cybersecurity Act, a sweeping regulation that will establish certification schemes to apply to a range of online services and connected devices. The strategies are currently being contemplated by DG-Connect and ENISA and will be established over the next several years.

- The product certification strategies are organized into three categories: 1) Basic, 2) Substantial, and 3) High, which correspond to the perceived risk associated with the product function, data, and environment.
- Assurance level "High" is reserved for products used in critical infrastructure applications, where many Schneider Electric OT products could be impacted.
- There are also EU member state IoT requirements and certification programs. In general, the EU Cybersecurity Act aims to harmonize and standardize these programs into a European-wide cybersecurity certification program.

Chinese Cybersecurity Law[13]: This sweeping law governs industry, citizen, and government roles and expectations in cybersecurity and privacy. The law effectuates the implementation of several policies and regulations that have a direct impact on OT. Below are the selected highlights:

- ***Cybersecurity Classified Protection Scheme or Multi-Level Protection Scheme (MLPS) 2.0***[14]: MLPS is part of the Chinese Ministry of Public Security's critical infrastructure protection scheme, and it places requirements upon networks and devices depending on the sensitivity of their application.
- ***Critical Network Equipment Security Testing Implementing Procedures***[15]: Requires certain products (e.g. PLCs) to undergo security testing and certification prior to sale within China. In many cases, however, the underlying standards by which testing is to take place are still in progress.
- ***Cybersecurity Review Measures***[16]: Requires a "national security review" when products (including OT) and services may impact national security and authorizes the exclusion of products and companies that pose a supply chain risk to the Chinese market.
- ***Cybersecurity Vulnerabilities Administrative Regulation***[17]: Specifies procedures and responsibilities for vendors and network operators who discover cybersecurity vulnerabilities (to include OT manufacturers). It also discusses patching, countermeasures, and reporting requirements to relevant government agencies.

U.S. NIST IoT Security Minimum Baseline[18]: This is a U.S. effort to harmonize international IoT security requirements into a voluntary minimum baseline. Once finalized, the baseline will likely be incorporated into federal and state procurement requirements for IT and OT devices. Below are two related legislative efforts that place new requirements on OT device manufacturers:

- ***IoT Cybersecurity Improvement Act of 2019***[19] – Legislation in the U.S. Senate that will, if passed, establish new security requirements (based on the NIST IoT security baseline) for most IoT devices sold to the federal government.
- ***CA Connected Device Law***[20] – This is a new California state law that places requirements on manufacturers of "connected devices" to ensure devices sold in California after January 1, 2020, are equipped with "reasonable security features".

These country-specific requirements for IoT device manufacturers present several limitations. Instead of promoting widespread, open innovation, economic prosperity for the global digital economy, or consistent security protocols, disparate requirements will likely lead to regulatory fragmentation. As a result, only large players might be able to meet this myriad of requirements and consumers will be left to determine how secure a device is based upon where it is manufactured.

At Schneider Electric, there is hope for an alternative path — one that fosters both innovation and security for industry players, governments, and global citizens. It is a path where governments, vendors, and industrial companies work collaboratively, through open dialogue, to find a common regulatory ground. Ideally, this path would lead to harmonization and interoperability between IoT security requirements and corresponding certification schemes, enabling more secure devices to more quickly reach the users who need them.

Conclusion: Strengthening digital trust

Governments and industry have an opportunity to come together to work collaboratively on common solutions that will benefit all citizens. Doing so allows industry stakeholders to facilitate the tectonic shift in industrial revolution can be catalyzed by accelerated digitization in a safer, more productive, and more efficient way in our hyper-connected world.

At Schneider Electric, we strive to do our part. We are highly focused on safety and the legendary reliability and cybersecurity of our solutions to ensure business continuity in protecting people, assets, and data. As members of both the Cybersecurity Coalition and the Global Cybersecurity Alliance, we will work across industry, governments, and our customers to secure the global digital economy. Only together can we raise the bar on protecting the industry at large and strengthening digital trust and confidence as global industry pursues the benefits of the IIoT.

References

1 Gartner. (2017). Leading the IoT: Gartner insights on how to lead in a connected world. Retrieved from https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

2 Hutt, R. (January 23, 2016). 9 quotes that sum up the Fourth Industrial Revolution, World Economic Forum Agenda. Retrieved from https://www.weforum.org/agenda/2016/01/9-quotes-that-sum-up-the-fourth-industrial-revolution/

3 Zetter, K. (November 29, 2010). Iran: Computer malware sabotaged uranium centrifuges. Wired. Retrieved from https://www.wired.com/2010/11/stuxnet-sabotage-centrifuges/

4 Heiligtag, S., Maurenbrecher, S., and Niemann, N. McKinsey. (February 2017). From scenario planning to stress testing: the next step for energy companies. Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/from-scenario- planning-to-stress-testing-the-next-step-for-energy-companies

5 Reuters. (May 14, 2017). Cyber attack hits 200,000 in at least 150 countries: Europol. Retrieved from https://www.reuters.com/ article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries- europol-idUSKCN18A0FX

6 Menze, T. ARC Group and Kapersky. (July 2019). The state of industrial cybersecurity report 2019. Retrieved from https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf

7 Abbosh, O., and Bissell, K. Accenture. (2019) Reinventing the Internet to secure the digital economy. Retrieved from https://www.accenture.com/us-en/insights/cybersecurity/reinventing-the-internet-digital-economy

8 Schwab, W. and Poujol, M. CXP Group and Kapersky. (July 2018). The state of industrial cybersecurity report 2018. Retrieved from https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf

9 Schneider Electric. (July 29, 2010). Schneider Electric is Founding Member of ISA Global Cybersecurity Alliance. Retrieved from https://www.se.com/ww/en/about-us/press/news/corporate-2019/founding-member-of-isa-global-cybersecurity- alliance.jsp

10 Opiah, A. (August 14, 2019). ISA Global Cybersecurity Alliance Welcomes Schneider Electric As Founding Member. Retrieved from https://data-economy.com/isa-global-cybersecurity-alliance-welcomes-schneider-electric-as-founding- member/

11 Schneider Electric. (March 4, 2019). Schneider Electric Affirms Role in Strengthening Digital Trust by Joining the Cybersecurity Coalition. Retrieved from https://www.se.com/ww/en/documents/Press/2019/03/04-release-cybersecurity- coalition-tcm50-463982.pdf

12 The EU Cybersecurity Act. Retrieved from https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

13 Creemers, R., Triolo, P., and Webster, G. (June 29, 2018). Chinese Cybersecurity Law Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). Retrieved from https://www.newamerica.org/cybersecurity-initiative/ digichina/blog/translation-cybersecurity-law-peoples-republic-china/

14 Lu, X., Triolo, P., Sacks, S., Creemers, R., and Webster, G. (July 18, 2018). Progress, Pauses, and Power Shifts in China's Cybersecurity Law Regime. Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/progress- pauses-power-shifts-chinas-cybersecurity-law-regime/

15 L, C., Neville, K., and Webster, G. (June 12, 2010). Translation: New Draft Rules for 'Critical Network Equipment Security Testing' in China. Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-critical- network-equipment-testing-implementing-measures-draft-comment

16 Sacks, S., Creemers, R., Laskai, L., Triolo, P., and Webster, G. (May 24, 2019). China's Cybersecurity Reviews for 'Critical' Systems Add Focus on Supply Chain, Foreign Control (Translation). Retrieved from https://www.newamerica.org/ cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-critical-systems-add-focus-supply-chain-foreign- control- translation/

17 Peterson, D., Zhong, R., (June 19, 2019).Translation: Chinese Rules for Managing Cybersecurity Vulnerabilities Published in Draft Form. Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-rules- managing-cybersecurity-vulnerabilities-published-draft-form/

18 NISTIR 8259(Draft). (July 2019). Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers. Retrieved from https://csrc.nist.gov/publications/detail/nistir/8259/draft

19 S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017115th Congress (2017-2018). Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

20 CA Connected Device Law. SB-327 Information privacy: connected devices.(2017-2018). Retrieved from https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

Schneider Electric USA
800 Federal Street, Andover, MA 01810 Telephone: 978-794-0800 www.schneider-electric.us

Session 5

Session 5

Demo on Digital Twins, Digital Worker enablement & Optimization – Rockwell Automation India

Session 6

Session 6

1. An introduction to Ethernet – P & F
2. Earthquake Early Warning System - EIL

Setting the Standard for Automation™

ISA Delhi Section

Digital Transformation of Process Plants

An introduction to Ethernet – APL

Binoy Kamath
Pepperl+Fuchs Group

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

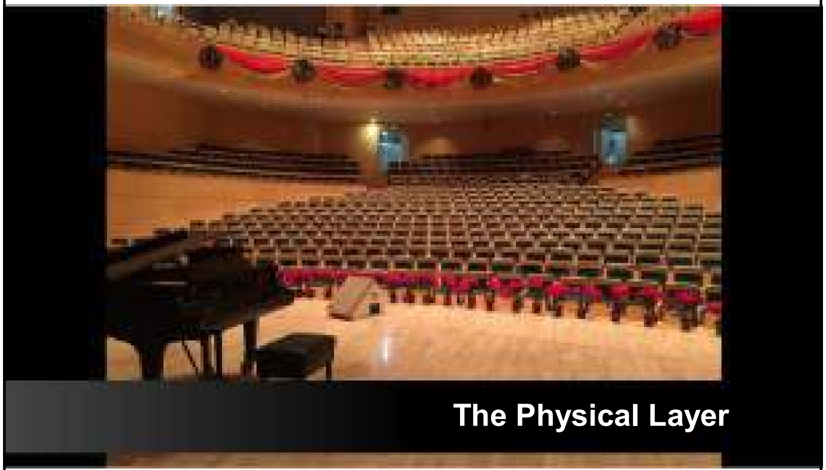
1

Instruments

2

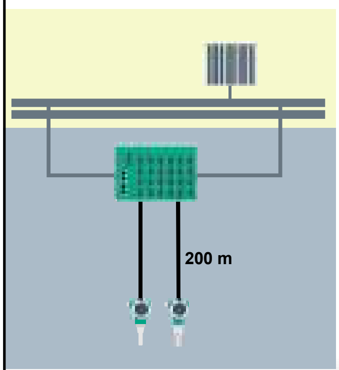
3

4

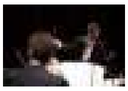


5

Elements of an Automation System

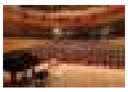


Control

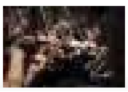


Protocols

Physical Layer



Instrumentation



6

OSI Model

Data Models, Protocols and the Physical Layer

Control and Plant Asset Management (PAM) and Engineering Station

Device Description: FDI | EDDL | FDT/DTM | GSDML | DD | …

7	Application	PROFINET, EtherNet I/P, HART-IP, Modbus TCP, OPC-UA	PROFIBUS PA / Foundation Fieldbus H1	HART
6	Presentation			
5	Session			
4	Transport	TCP / UDP / Direct Layer 2 Access		
3	Network	IP		
2	Data Link	Ethernet + TSN	Adressing	
1	Physical Layer	ethernet-apl™	Manchester Bus Powered	4-20 mA with Frequency Shift Keying

7

HA249

Ethernet-APL is the technology that enables transparent, … network communication between controller and instrument

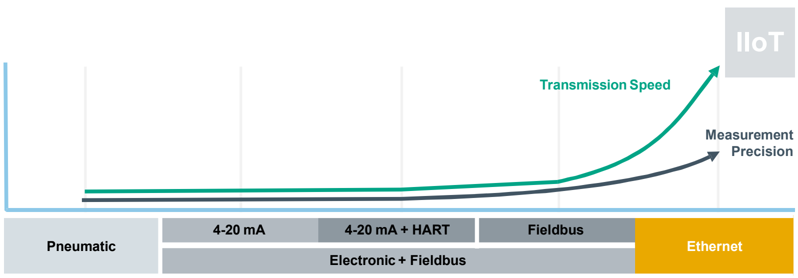
8

Slide 8

HA249 Diese Seite aufschönen und schärfen.
Hennecke Andreas, 26-10-2022

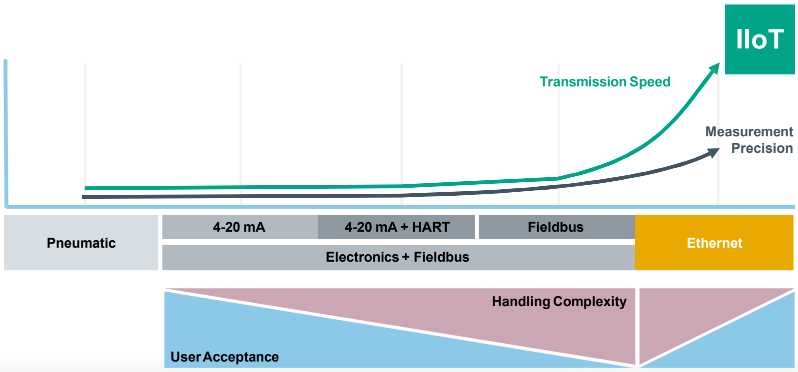
9

Evolution of Communication Technologies



10

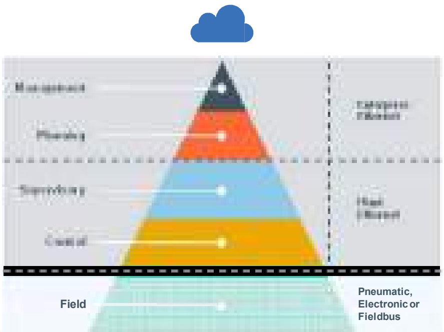
Evolution of Communication Technologies



11

Connecting to the Field Level Today

Reasons why Ethernet could not previously be extended from the Plant to the Field



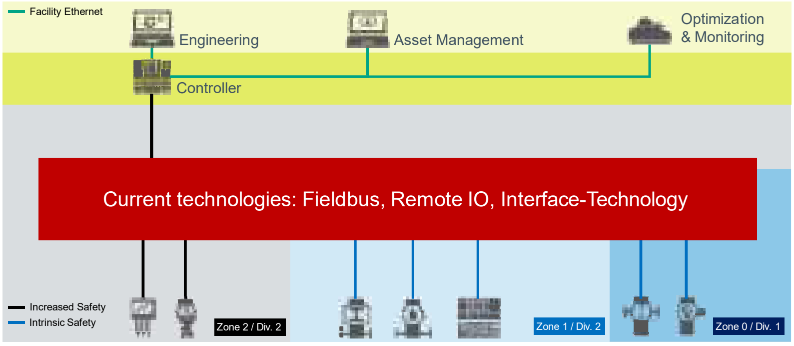
Requirements of process industries

- Twisted pair cabling
- Loop-powered devices
- Reaching long distances
- For explosion hazardous areas
- Easy to handle technology
- Connectors for harsh conditions

Serial bus and analog connectivity only

12

The Field of Process Plants Today



13

Ethernet-APL is A Single Pair Ethernet

Definition in the context of many Ethernet variations on single-pair wires

SPE = Single Pair Ethernet: Definitions for various Ethernet physical layers for single balanced or twisted pair cables. Examples are: 10BASE-T1 (new), 100BASE-T1, 1000BASE-T1 with optional power over data line (PoDL).

Ethernet-APL: A single-pair Ethernet based on 10BASE-T1L as defined in IEEE 802.3cg, with additional provisions specific to process industries. Additional standardization for interoperability includes:

- Intrinsic safety as new chapter IEC 60079-47 ED1: 2WISE
- Port profiles for optional power supply and hazardous area protection.

14

Technical Specifications for the Advanced Physical Layer

Parameter	Specification
Standards	IEEE 802.3 (10BASE-T1L), IEC TS 60079-47 ED1 (2WISE)
Power supply output (Ethernet APL power switch)	Up to 60 W, On APL Trunk
Switched network	Yes
Reference cable type	IEC 61158-2, Type A
Maximum trunk length	1000 m / into Zone 1 / Div. 2
Maximum spur length	200 m / into Zone 0 / Div. 1
Speed	10 Mbps, full-duplex
Hazardous area protection: Inspired by fieldbus	For all zones and divisions. With optional intrinsic safety at the device

15

The Work Packages

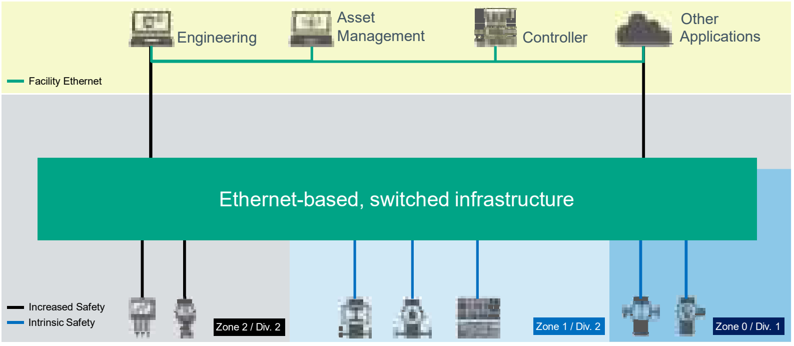
Standards, guidelines, and specifications for immediate usability

Communication	Standard	IEEE 802.3	✔
Power and Cabling	Standard	IEC 61158	✔
Intrinsic Safety	Standard	IEC 60079	✔
Conformance Testing	Specification	User Organizations	✔
Engineering Guidance	Guideline	User Organizations	✔

2022-06-21 Page 15
Ethernet-APL - Grundlagen - DSM

16

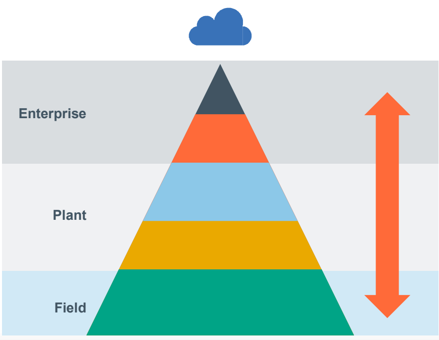
The Field of Process Plants Future



17

Connecting to Field Level with Ethernet-APL

Enabling seamless Ethernet connectivity throughout all levels from Enterprise to the Field

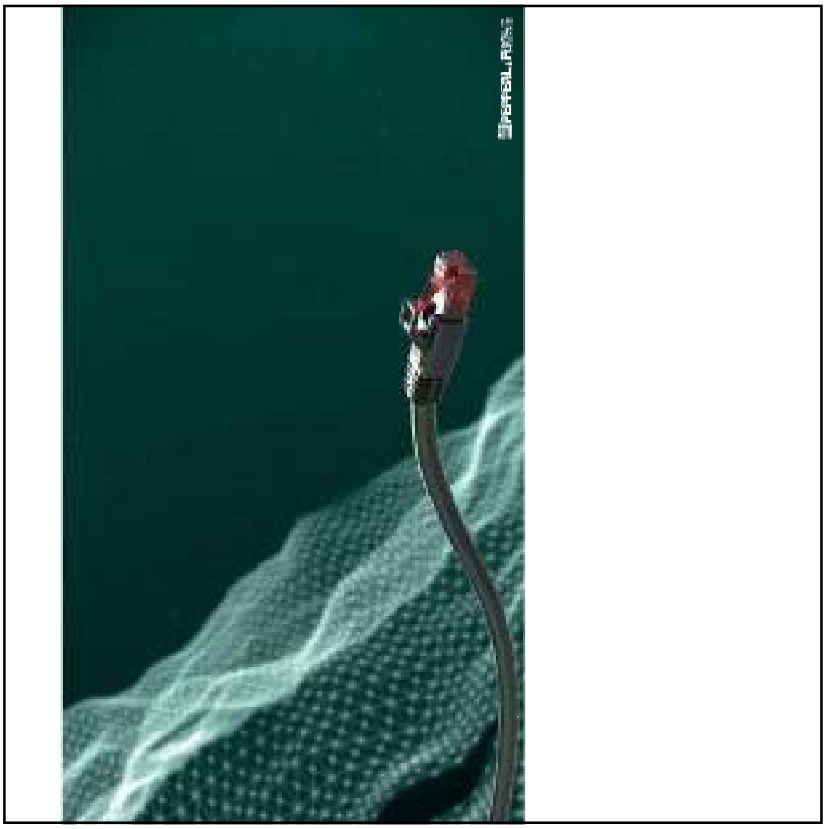


For process industries with

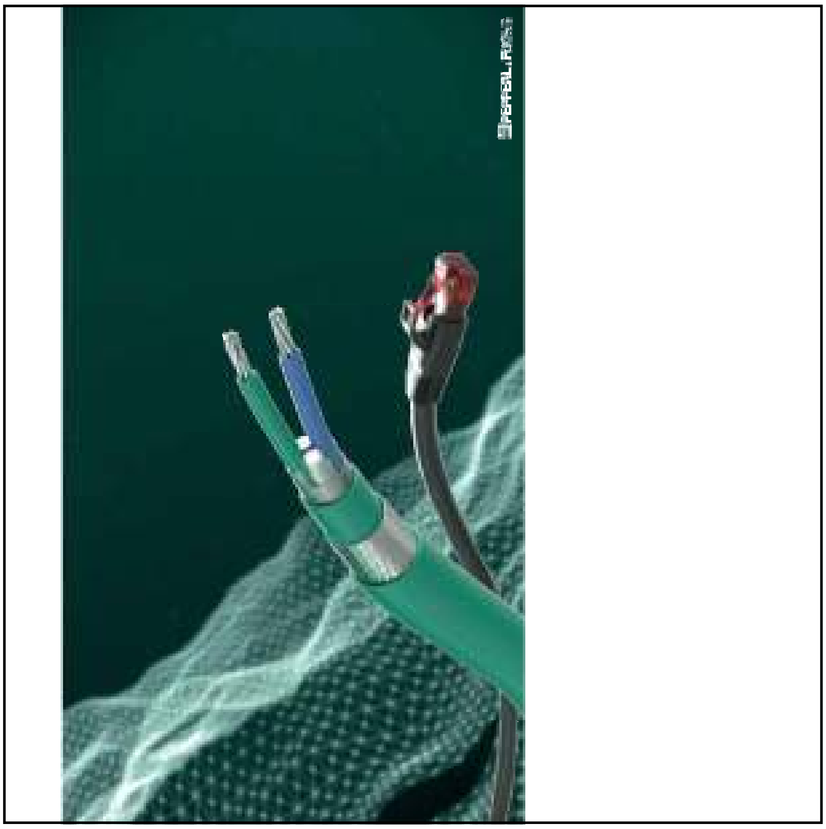
- Open and concurrent access
- Future-proof for enhancements

Field connectivity with Ethernet-APL

18



19



20

21

Explosion Protection

Interoperability and handling simplicity defined

IEC TS 60079-47, 2021-03 (2-WISE)
2-WISE = 2-Wire Intrinsically Safe Ethernet

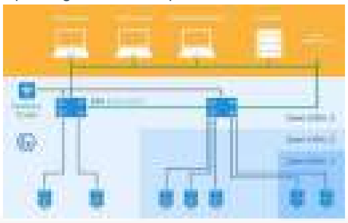
- Device interoperability defined
- Simple planning and installation rules
- Simple validation without intrinsic safety calculations

For hazardous areas: Divisions and Zones
Derived from FISCO

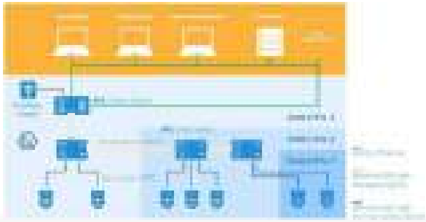
22

Free and Flexible Topology Design for any Plant Layout

Star Topology
Spur segment cable up to 200 m

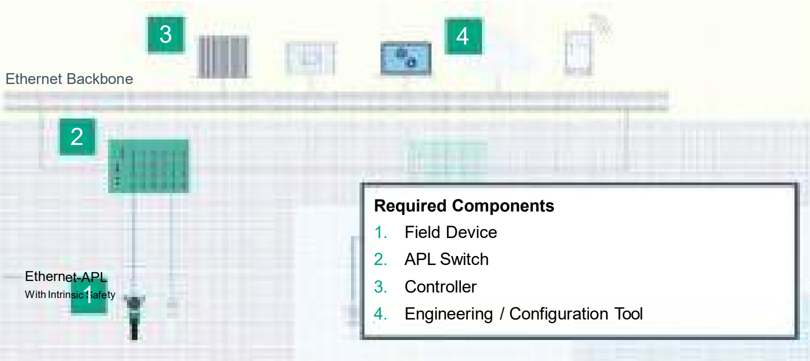


Trunk-and-Spur Topology
Trunk segment cable up to 1000 m



23

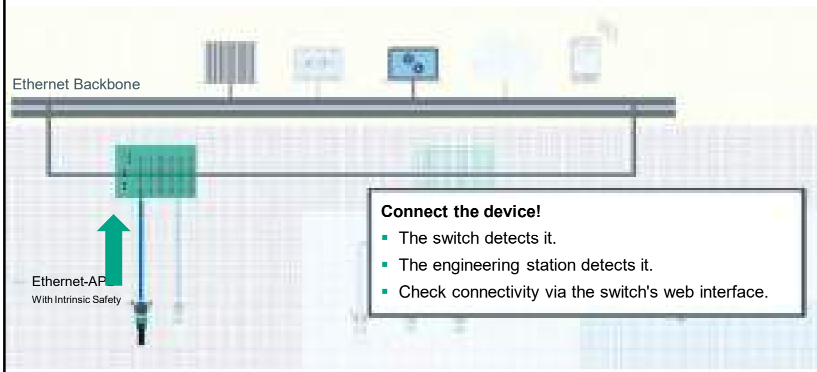
Required Components



Required Components
1. Field Device
2. APL Switch
3. Controller
4. Engineering / Configuration Tool

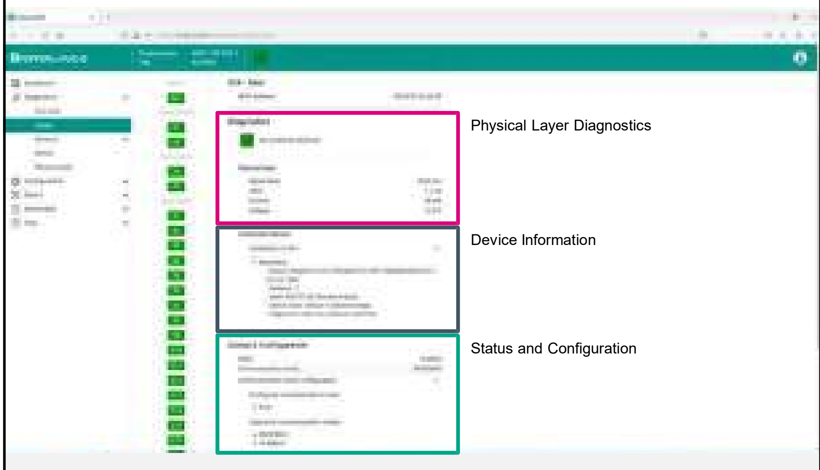
24

Connect the Device



2022-11-07 | Page 24
Ethernet-APL Engineering - Webinar UK - Andreas Hennecke - Public

25



26

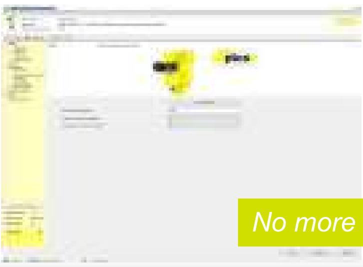
27

Fast & Efficient Process Comissioning

…fast device handling leads to **MUCH** lower commisioning time

Example: Verification of tank volume on Vegapuls 64 HART vs. Vegapuls 64 APL (Profinet)

HART: 2 min/update



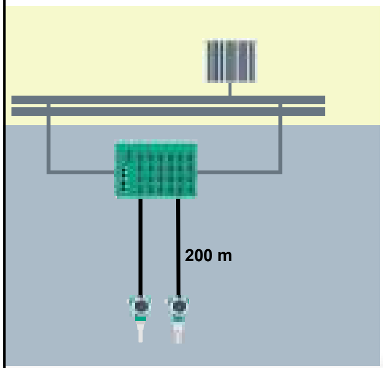
APL: 2 sec/update

No more time for coffee!

PEPPERL+FUCHS

28

Integration of Ethernet over APL



- Ethernet traffic passes through
- Media redundancy protocol (MRP)

DCP, DHCP, MRP, VLAN, IGMP,
SNTP, HTTP, HTTPS, LLDP, SNMP

29

Standards for Ethernet-APL

Extending Single Pair Ethernet for the Field Within Process Plants

Standard	Purpose and Content
IEEE 802.3cg-2019	2-wire Ethernet, 10BASE-T1L for cable lengths up to 1000 m
IEC 61158-2, Type A	Cables: Overview of supported cable types and impacts on cable lengths
IEC 61158-2, Port Profiles	Interoperability: Functional and electrical requirements for power concept between ports on source side (switch) and load side (field device)
	Application fit: Usage in hazardous and non-hazardous areas
	Connection technology: Focus on simple installation
	Surge protection: Protection from voltage spikes
	EMC: Resilience to electro-magnetic interference
Relevant Chapters of IEC 60079 for explosion protection	
IEC 60079-47:2021 (TS)	2-wire intrinsically safe Ethernet concept (2-WISE)
IEC 60079-0 IEC 60079-11 IEC 60079-25	Support of all explosion protection techniques incl. intrinsic safety
IEC 60079-14	Electrical installations design, selection and erection

30

Technologies to the Field Today

Main Attributes Used in the Field within Process Plants Today

	Pneumatic	Analog	Low-speed Digital	High-Speed Digital	Ethernet
Technology	Pneumatic	4-20 mA	4-20 mA + HART	Fieldbus	Ethernet
Communication Type	Air	Analog	Analog + serial	Serial digital	Digital network
Measurement	1 value	1 value	1+N values	N values	N values
Local access to data	-	-	Gateway required	Integrated	Integrated
Remote access to data	-	-	Gateway required	Gateway required	Integrated

Past — Present

31

Users' Voices

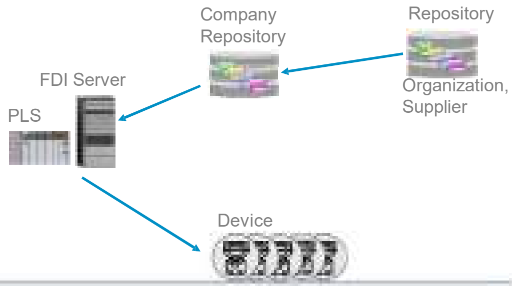
32

Gaining Acceptance

Device exchange and commissioning

Device integration from repository

- One central source for all device integration
- Overview of all devices in use, operation, suppliers
- Simple maintenance and update



33

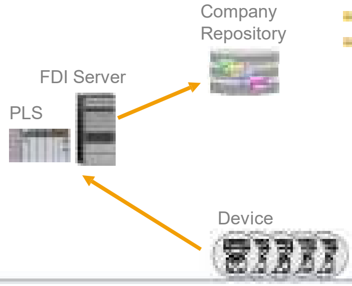
Gaining Acceptance

Device exchange and commissioning

Device integration in the device

- Clear mapping of device and description files
- No search for correct data
- Without online connection

- Device data:
  - FDI Package
  - Operating instructions
  - Certificates



34

Fast & Efficient Device Handling

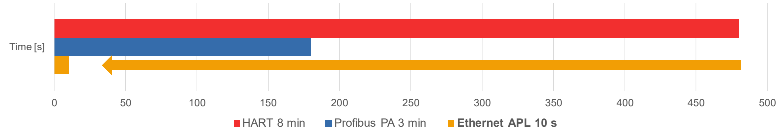
10 MBit bandwidth down to the field device

No more waiting

Interface speeds

HART	Profibus PA	Ethernet-APL
1,2 kBit	31,25 kBit	10000 kBit

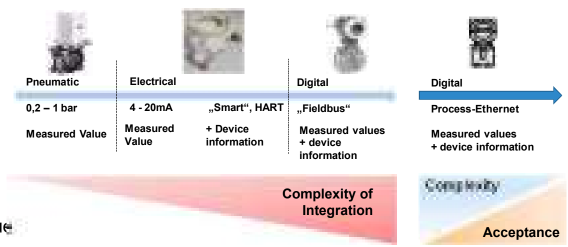
Comparison: Up-/download time for a coriolis massflow meter (shorter is better)



Reducing Complexity

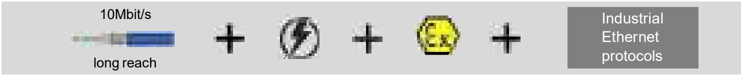
As described in NE 168: Requirements for a field-level Ethernet communication system

- Commissioning
- Device replacement
- Configuration
- Accessible added value



https://www.namur.net/fileadmin/media_www/Dokumente/AK_Position_2.6_APL-network_topologies_2021-07-08_EN.pdf
https://www.namur.net/fileadmin/media_www/Dokumente/AK_Position_2.6_Ethernet_APL_2021-07-09_EN.pdf

Advantages over all Life Cycle Phases



- → Homogeneous network with seamless data access
- → Consistency and reusable designs
- → Simplified DCS integration
- → Time savings in commissioning
- → Efficiency in error finding
- → 2nd - Insights for process optimization, digital transformation …

Ethernet-APL Virtual Workshop | Customer Panel | Public
2021-10-05
Slide 36

37

38

Customers Already Showing Interest

Potentials showing interest and opportunites

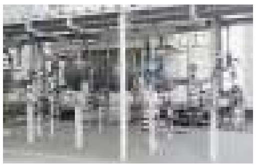
39

Your next Steps towards Ethernet-APL

Contact your Ethernet-APL subject matter experts

DEMO AVAILABLE AT B5 Pepperl+Fuchs Stall

Develop a pilot or proof-of-concept testbed at your Plant



40

In Summary

Ethernet-APL, is a simple & rugged technology for Ethernet, which fulfills the requirements of process industries today and tomorrow.

41

42

43

44

Thank you!

Ethernet-APL - Seamless Communication in Practice

45

Questions and Answers

Overview:	www.pepperl-fuchs.com/apl	Technology:	www.pepperl-fuchs.com/apl-tec
The Project:	www.ethernet-apl.org	Products:	www.pepperl-fuchs.com/fieldconnex

Your automation, our passion.

2022-06-21 | Page 45
Ethernet-APL - Seamless Communication in Practice

PEPPERL+FUCHS

46

Pepperl+Fuchs SE

Contact
Binoy Kamath

+91 9980122391

47

EARTHQUAKE EARLY WARNING SYSTEM

ABSTRACT

Scope/Objective:

This paper gives an overall view ofEarthquake Early warning System (EqWS)that detects earthquakes so quickly that alerts can reach many people and plant operators before the actual shaking arrives. Earthquake Warning System is a technological intervention to avert colossal loss of human life and infrastructure. It is the solution provided to activate appropriate actions for safety during impending earthquake.

Till now there is no proven method to forecast precise occurrence time of an earthquake nor its location or size.Yet, utilizing state of the art scientific methodologies, as done in this Earthquake Early warning System,it is now possible to quite accurately assess Ground Acceleration values as soon as an earthquake emerges using its primary waves. Thus, warnings about a potential strong shaking can be generated almost instantaneously, until destructive secondary and surface waves arrive.

Based on fast and reliable communication channels, the system provides crucial lead time to take measures which may help reduce catastrophic impacts of seismic events.

Methods/ Procedure/ Process:

The system is devised for regional notification of a substantial earthquake based on voting system of Seismic Sensing Nodes (SSN). The multiplicity of such nodes ensure elimination of false alarm due to man-made activities at local level. SSNs are strategically located to gather information about seismic activity and communicate to a Central Control Unit (CCU) regarding potential earthquake incidence. Central Control Unit provides final decision based on signals of the individual Nodes and generates an audio-visual alarm for impending earthquake with estimated severity level.CCU also sends message to the Emergency Alert Delivery System for generating various alarms and activating emergency departments and plant operating systems to take measures based on pre-defined SoPs.

Components/ Features:

1) Seismic Sensing Node (SSN): SSN is equipped with accelerometer sensor, GPS, Processor and communication modules.
2) Central Control Unit (CCU): CCU is provided with Graphical User Interface (GUI). GUI is the main user interface and provides information regarding latest event details, event log of all seismic activities and health status of all connected seismic sensing nodes.
3) Event Information: It displays the latest true seismic event which is sensed by pre-defined number of SSNs along with Peak Ground Acceleration (PGA) sensed by the nodes.

4) Report: A report is generated for all the true events and programmable levels have been defined for severity based warning.

Conclusion:

Earthquake early warning system have been proved to be useful tools to mitigate the industrial, social and economic impact on communities and businesses.

It helps to take additional safety measures based on deploying necessary SoPs once earthquake early warning alert is received. It can also prevent cascading failures in the aftermath of a seismic event.

This system can be utilized for Refineries,Petrochemical Plants, Fertilizers, Chemical Plants,Power Plants, Nuclear Power Plants, Mines, Caverns, Metros, Airports, High Speed Train Network, Smart Cities and Infrastructure and Public Emergency services etc.

The technological solutions to handle each situation or industry are site and application specific. There is no single solution. The EIL powered Earthquake Early Warning System described here can be customized based on need of application or industry.

It can be concluded that the value propositions of Earthquake Warning System ensuring early warning to deploy necessary actions and maintaining the overall plant/operational safety are too great.

Keywords: Earthquake Early Warning System(EqWS), Seismic Sensing Node(SSN),Central Control Unit(CCU),Engineers India Limited(EIL)

By: Mr. SaikatBhowal and Mr. Javed Akhtar

एनटीपीसी
NTPC

Azadi Ka Amrit Mahotsav

Transforming into a "Sustainable Integrated Energy Company"

India's largest Power Company, NTPC is venturing into new business areas like e-mobility, Waste to Energy, Power Distribution and Green Hydrogen.

"Excellence in Corporate Social Responsibility"

atd
Association for Talent Development

NTPC ATD BEST Award Winner 2022

Follow us on: /ntpc1 /ntpclimited /ntpcltd1 /ntpclimited /company/ntpc ntpc_limited

Session 7

Session 7

1. Automation Stripper Tracking calculations – GAIL
2. Emerging Trends and Developments in Industrial Automation - Rittal
3. Operational transformation of 690 MW power plant – NHPC
4. O-PAS – Reliance
5. Automation & Calibration in IIoT platform - Fluke

AUTOMATION OF STRIPPER TRACKING CALCULATIONS IN SCLAIRTECH BASED LLDPE PLANT AT GAIL PATA

Manupati Sravan Kumar, Md. Shahid Jamal, Aritra Bhattacharya, Priyanshu Raj

GAIL (India) Ltd., Pata

ABSTRACT

GAIL's LLDPE-1 plant based on Nova's SCLAIRTECH technology manufactures a wide variety of polyethylene resins. The polyethylene pellets formed after extrusion are accumulated in a stripper which is essentially a 22.5 m tall cylindrical vessel. The polymer pellets spend about 5-7 hours in the stripper while they are steam stripped to remove residual solvent (cyclohexane). The contents of the stripper are divided into imaginary lots based on their entry time into the stripper. The contents of the lot are tracked by a plant engineer on a two-hour basis to ensure that contents of one lot may not contaminate the contents of another in the blender. This is especially helpful when the plant has undergone a shutdown or a reaction upset has occurred. The calculations are elementary unsteady state material balance calculations based on FIFO principle. Until now this entirely mechanical operation was performed manually by a plant engineer. This calculation process has since been automated and integrated into the DCS system (Yokogawa Centum VP). The only manual intervention required since is the decision on when to start and stop lot. This has improved operation significantly.

INTRODUCTION

LLDPE-1 plant at GAIL's Pata plant is a 210 KTA swing polyethylene unit based on Nova Chemicals, Canada's SCLAIRTECH solution polymerization technology. The plant is capable of producing grades ranging from 0.918- 0.962 g/cc in density and 0.5- 23 dg/min in melt flow index. The typical combinations of the reactors can confer a wide range of end use properties to the polymer. The polymerization reaction of ethylene to polyethylene takes place in the solution phase- where cyclohexane acts as a solvent. The solvent is inert and is flashed off after the completion of the reaction in a series of flash vessels where the pressure is lowered step by step. The molten polymer (with about 2 % cyclohexane) is extruded to form 3 mm PE pellets. The pellets are conveyed using water to a stripper where the residual cyclohexane is steam stripped and recovered. The pellets at the outlet have < 500 ppmw of cyclohexane.

Since the plant is in continuous operation it becomes necessary to separate the different grades and properties into different lots. This is done in blenders. However, during grade change overs or plant upsets it becomes critical to ensure that the off spec material does not contaminate the on spec material. To ensure this polymer is separated into 'imaginary' lots in the stripper. This tracking process is required to be done esp. during plant upsets and grade changeovers to compute when these pellets will reach the bottom of the stripper so the material of the same can be taken in a separate blender.

A 'lot' in the stripper is defined as a finite, non-zero quantity of polymer that has a definite start and end time, defined by the panel engineer, for the purpose of separation in the blenders. Under most circumstances, this nomenclature has no bearing on the final lot number that is assigned serially. Suppose, at time $t = t_0$

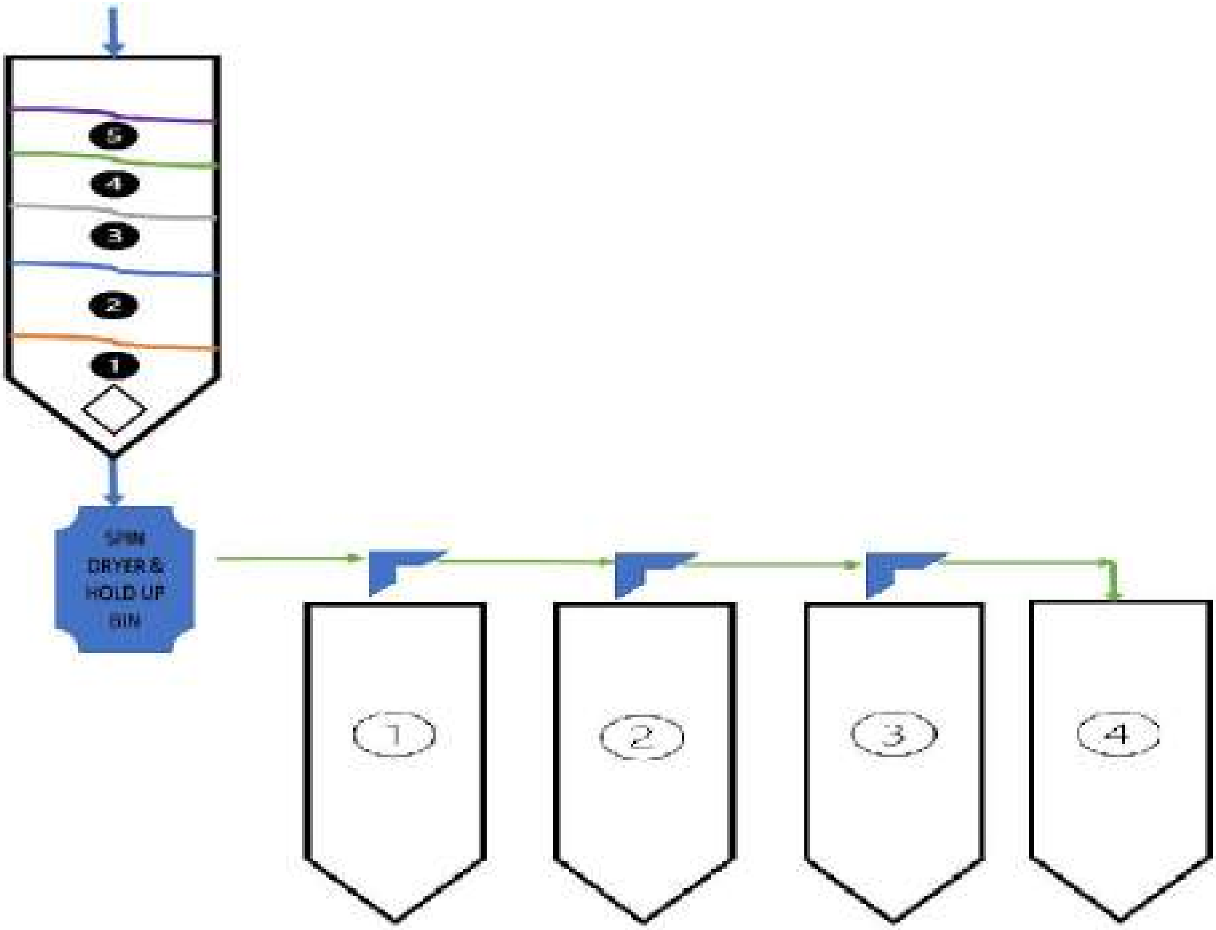
A reaction dip occurs which has potential to deviate from on-spec properties then the production from t= $t = t_0 - 15$ min upto the normalization of reaction conditions is assigned to a separate 'imaginary' lot. This lot will begin at the top and as material is emptied out from the bottom the interface will descend along the stripper. When the interface reaches the stripper bottom, the finishing area panel engineer switches over into a fresh blender, so that this product might not contaminate the final on-spec material.

Until recently these calculations were done by hand every two hours throughout the day. Computers excel at repetitive computational tasks and hence this was a prime candidate for automation.

METHODOLOGY

The purpose of the sheet is two-fold: firstly, to calculate the two-hourly production rate and secondly to track the position of different lots in the stripper

There are four blenders equipped with strain gauge type load cells capable of weighing upto 110 MT which are used to hold & blend the contents out of the stripper.



Assume that

$mout = \sum_{i=1}^{4}\{\text{BlenderWt}_{i}(t + \Delta t) - \text{BlenderWt}_{\text{i}}(t)\}$

Where Δt>0 and

Let $\{\text{BlenderWt}_{\text{i}}(t + \Delta t) - \text{BlenderWt}_{\text{i}}(t)\} = f_i$

If $f_i>=0$, $f_i=f_i$

Else $f_i=0$

i.e. **only the increase in blender weights** is considered for the computation of stripper outlet rate.

The above diagram represents a schematic of the stripper under normal circumstances. The lots are numbered such that 1 is the bottom most lot while 5 is the top most lot. The stripper may contain as many as five different lots depending on circumstances such as adsorber changeover, adsorber backflush, grade changeover, reaction dips, reaction terminations, colour shots.

The lot numbers are to be imagined as empty vessels on a carousel or Ferris wheel. Once it empties its contents at the bottom of the stripper the empty lot returns to the top of the stripper such that it is ready to receive polymer again. The polymer is filled into the lots sequentially i.e. 2 follows 1, 3 follows 2 and so on. However, after lot 5 is completed polymer enters into lot 1 again.

In every time period one lot is unloading while another is loading. In the case depicted in the schematic, lot 1 is unloading while lot 5 is loading. Hence, the stripper inlet mass flow rate is to be incremented into the lot 5 whereas the mass out computed by rise in blender weights is to be deducted from lot 1.

The lot interface will move by the same amount as the volume of polymer taken out of the stripper. Some mixing may occur at the interfaces so it becomes essential to accurately track them and determine when an interface of concern reaches the stripper bottom.

The stripper calculations are done on the basis of the feedbacks from two sets of instruments: the blender load cells and the stripper level transmitter. The blender load cell is used to determine the stripper outlet rate while the level is used to determine the accumulation/depletion term thus allowing computation of the stripper inlet rate.

$$\rho * Ac * \frac{dh}{dt} = min - mout$$

Since the bulk densities of all polymers manufactured in the plant are known this can be easily computed. This calculation is repeated every minute on the DCS and the results are recorded every two hours to determine the amount of polymer produced. The polymer is assumed to be removed from the bottom most lot and the polymer always comes into the topmost lot unless a new lot is initiated. The stripper inlet rate is set to zero if the extruder is stopped.

Under circumstances when the polymer entering the stripper is of a different bulk density than the polymer exiting the stripper, a volume balance can be relied on to determine the value of production,

$$Ac * \frac{dh}{dt} = Vin - (\frac{m_{out}}{\rho_{out}})$$

$$\mathrm{m_{in}} = \mathrm{V_{in}} * \rho_{in}$$

Although the basic assumption in the stripper is that the material that enters first exits first i.e. FIFO (first in first out) since counter current stripping of the pellets is done with steam it is possible that there is mixing of pellets at the interface. Hence whenever a lot of special interest (i.e. color shot, reaction dip, reaction startup) is separated a buffer time is taken (say 10-15 minutes production on either side). By ensuring that accurate tracking of polymer interfaces takes place it is desired that the buffer time will be reduced and the effective on-spec production can be increased.

CONCLUSION

The project is undergoing rigorous in plant trials and every corner case is being ironed out. Simplifying the process of tracking and making it more accurate result in better plant operation and higher prime grade production.

Image 1: Polymer Inventory Sheet

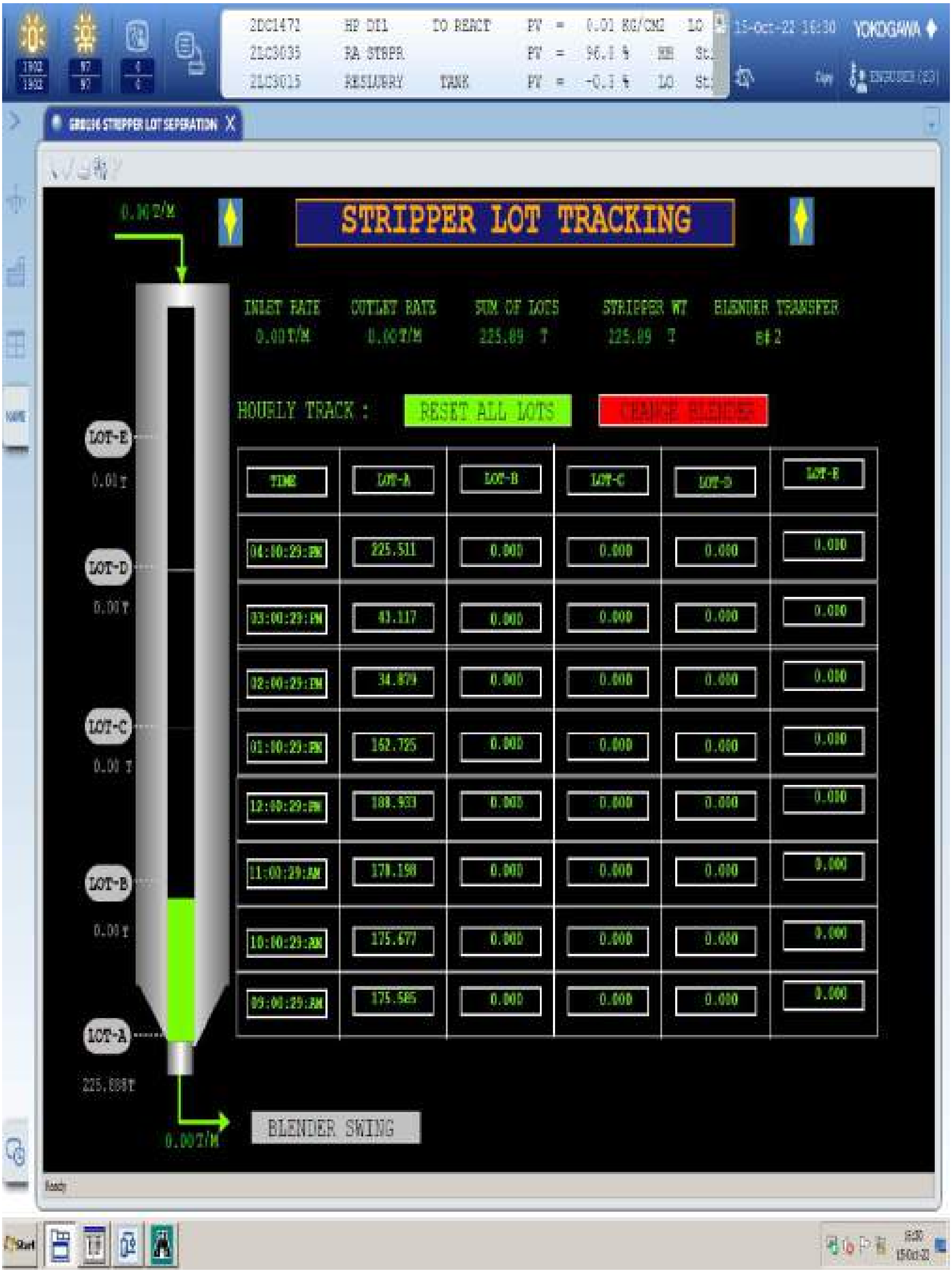


Image 2: Lot Separation Sheet

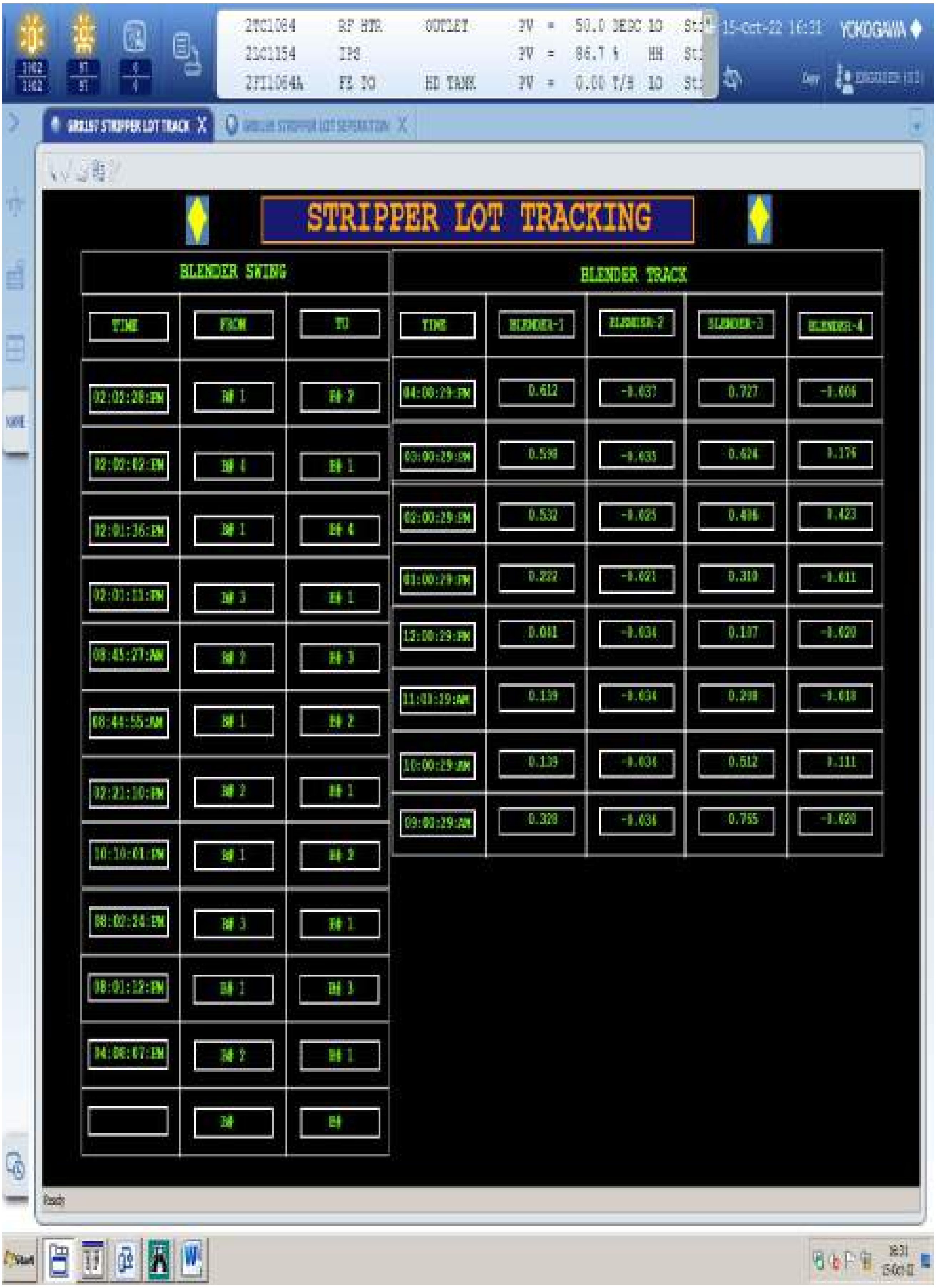


Image 3: Blender Swing Entries/ Production

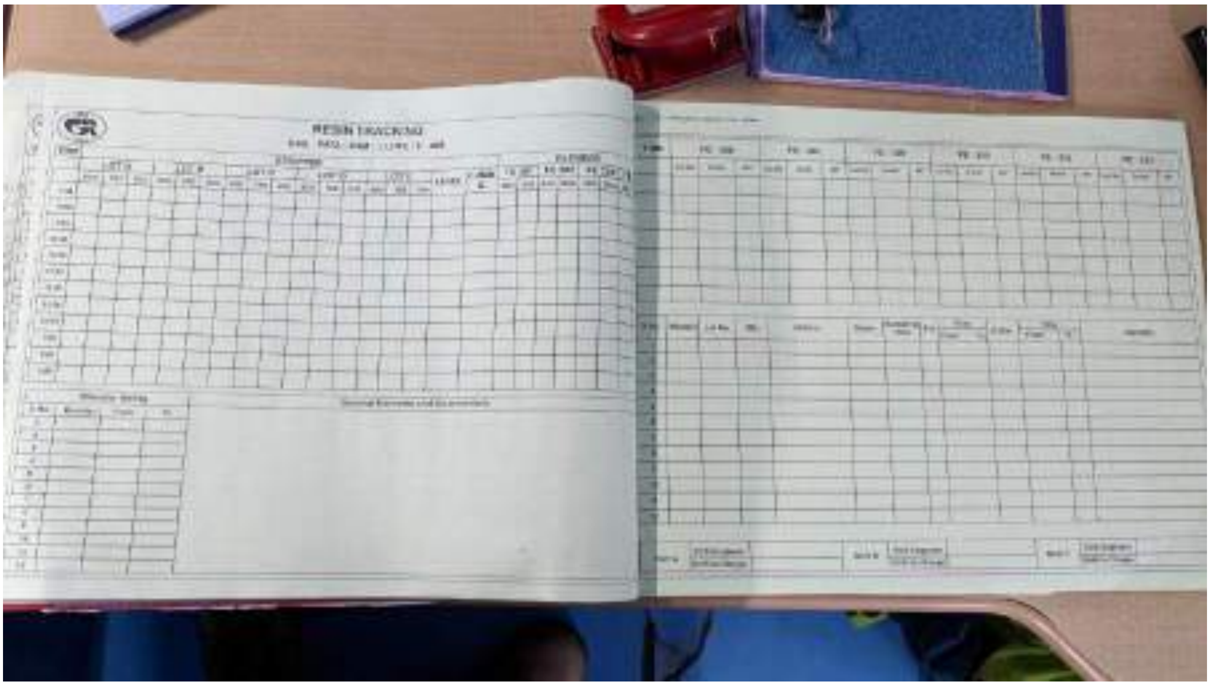


Image 4: Manual Calc Sheet

ACKNOWLEDGEMTS

The authors would like to acknowledge the help of Operations and Instrumentation department personnel at LLDPE-1, Pata site and HODs of the respective departments.

BIOGRAPHIES

Sh. Manupati Sravan Kumar is a graduate from NIT Trichy and is currently serving as Senior Engineer (Instrumentation) at GAIL's LLDPE-1 facility

Md. Shahid Jamal is a graduate from BIT Sindri and is currently serving as Chief Manager (Petrochemical Operations) at GAIL's LLDPE-1 facility

Sh. Aritra Bhattacharya is a graduate from NIT Warangal and is currently serving as Manager (Petrochemical Operations) at GAIL's LLDPE-1 facility

Sh. Priyanshu Raj is a graduate from ISM Dhanbad and is currently serving as Manager (Petrochemical Operations) at GAIL's LLDPE-1 facility

Setting the Standard for Automation™

ISA Delhi Section

Transformation

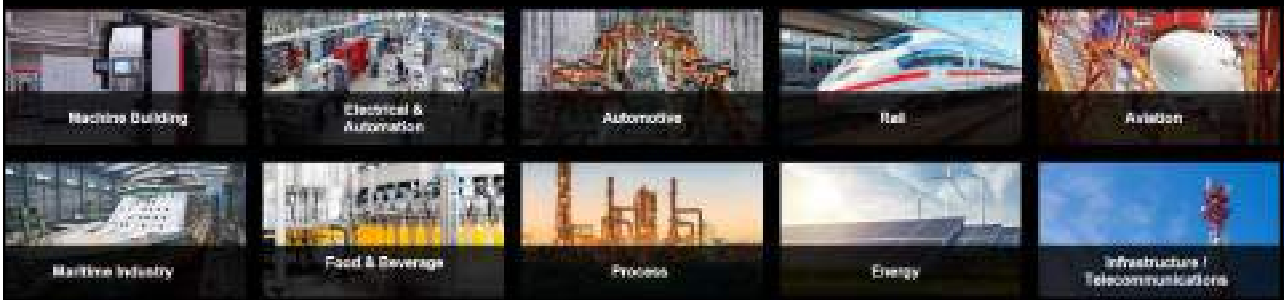
Emerging Trends and Developments in Industrial Automation

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

1

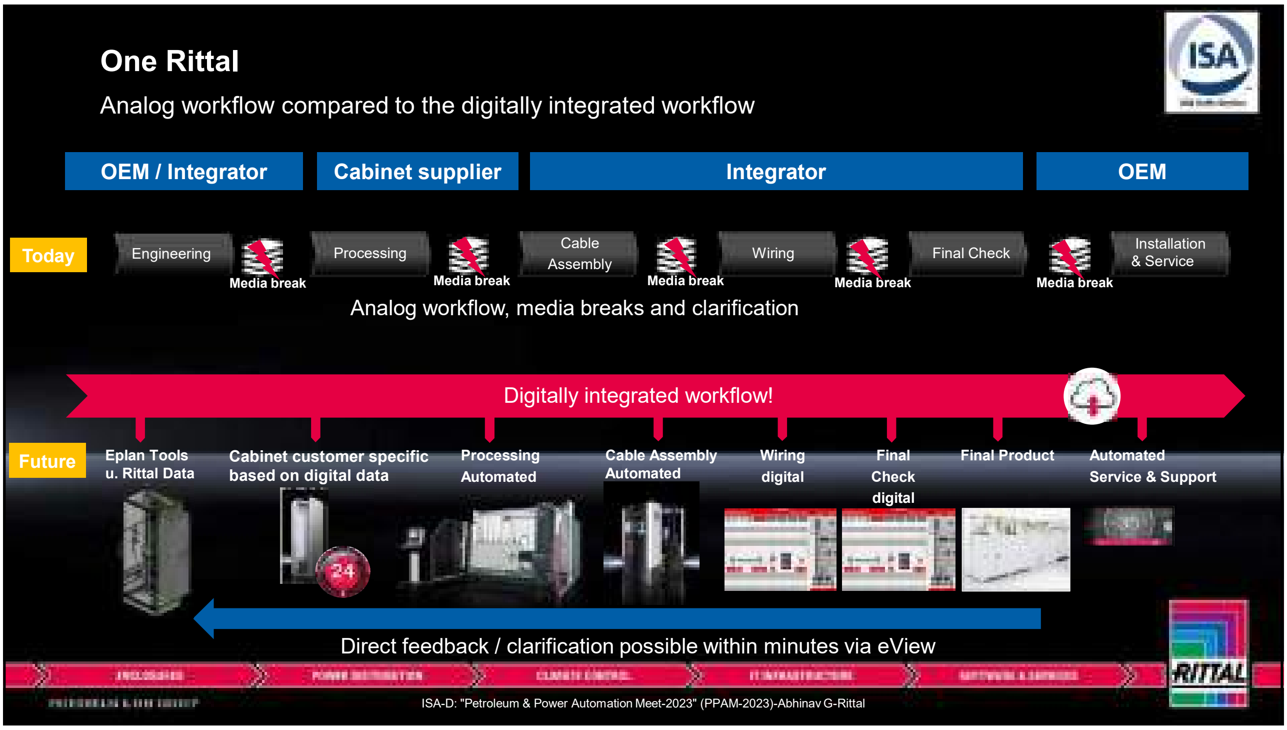
We understand your business

Solutions that suit the digital value chain in industry



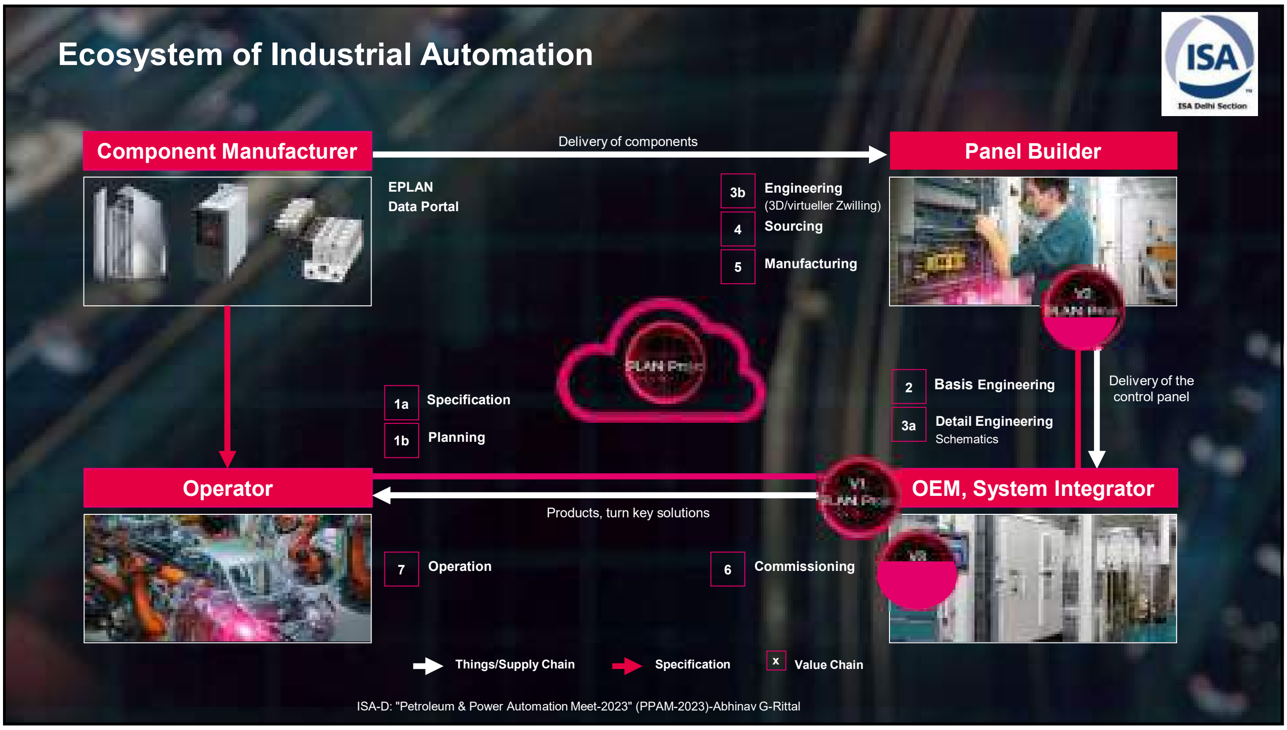
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

2



One Rittal
Analog workflow compared to the digitally integrated workflow
OEM / Integrator
Cabinet supplier
Integrator
OEM
Today
Engineering
Media break
Processing
Media break
Cable Assembly
Media break
Wiring
Media break
Final Check
Media break
Installation & Service
Analog workflow, media breaks and clarification
Digitally integrated workflow!
Future
Eplan Tools u. Rittal Data
Cabinet customer specific based on digital data
Processing Automated
Cable Assembly Automated
Wiring digital
Final Check digital
Final Product
Automated Service & Support
Direct feedback / clarification possible within minutes via eView
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal
RITTAL

3



Ecosystem of Industrial Automation
ISA Delhi Section
Component Manufacturer
Delivery of components
Panel Builder
EPLAN Data Portal
3b Engineering (3D/virtueller Zwilling)
4 Sourcing
5 Manufacturing
1a Specification
1b Planning
2 Basis Engineering
3a Detail Engineering Schematics
Delivery of the control panel
Operator
OEM, System Integrator
Products, turn key solutions
7 Operation
6 Commissioning
Things/Supply Chain
Specification
x Value Chain
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

4

Big Picture – "Connecting ecosystems. Smarter."

1. Genuine values for the customer:
Beyond products and solutions

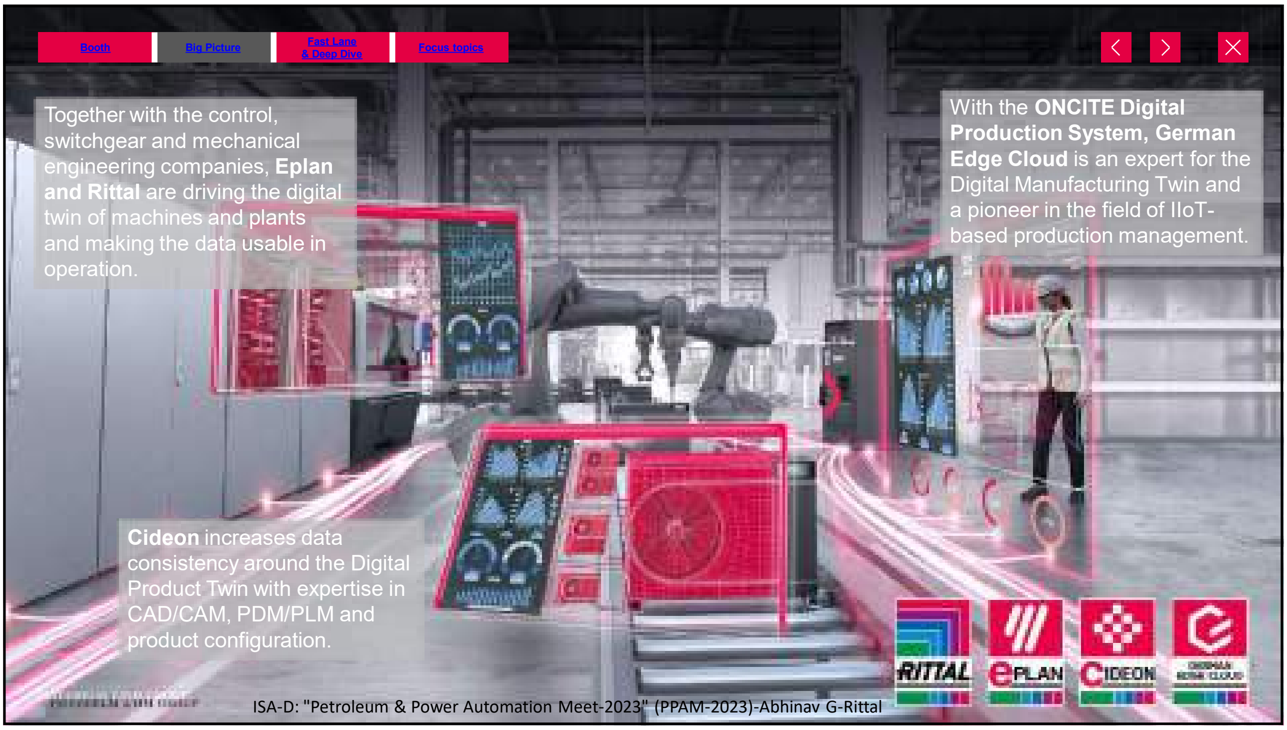
- The industry is feeling pressure to change. The question is how can the manufacturing industry deal with the pressure on efficiency and productivity, with the shortage of skilled workers and at the same time, or precisely because of this, with the digital transformation?
- In addition, how can it make the transition from crisis management to long-term transformation in terms of energy supply, product carbon footprint and sustainability? Alongside digital transformation, energy has become a business-critical factor.
- Rittal, Eplan, Cideon and German Edge Cloud will discuss these questions with visitors to the Hannover Messe, and they are convinced that these issues cannot be considered separately, just as these challenges cannot be solved by one-off solutions or specific companies. To this end, Hannover Messe is the ideal forum where people can discuss solutions and make connections. Networking the overarching ecosystems and developing standardised platforms for the future are the goals.

- Products and one-off solutions are no longer enough the reach them. Understanding the challenges that emerge in the big picture means having a good understanding of customer processes and streamlining them from end to end. That can only be achieved by a combination of hardware and software. Therefore, we no longer think of ourselves as a supplier or a provider of solutions. We think of partnership.

Big Picture

2. Genuine values for the customer:
Streamlining the value chain as a driving principle

- Specifically, the four FLG companies show how the processes in automation engineering, product manufacturing and production processes can be optimised and how the new ecosystems can be connected by way of a digital twin.
- Having this goal in mind is more relevant than ever because economic production with highly automated and efficient processes has been the ideal of the manufacturing industry not just since yesterday. The new imperatives of energy monitoring and management make this even more urgent. Only with the data from plants, product manufacturing and the production process is it possible to determine and reduce the product's carbon footprint and monitor energy flows in production, avoid or manage peak loads and, in the long term, control production according to energy availability or energy costs.
- Here is where Rittal, Eplan, Cideon and German Edge Cloud come in: They provide **support on the path to smart production** by drawing on their domain knowledge in control and switchgear manufacturing, PLM/PDM system integration, and IIoT.
- We know from experience and feedback from our customers reflects this: The decisive potential lies in the streamlining and industrialisation of process chains.



7

Booth | Big Picture | Fast Lane & Deep Dive | Focus topics

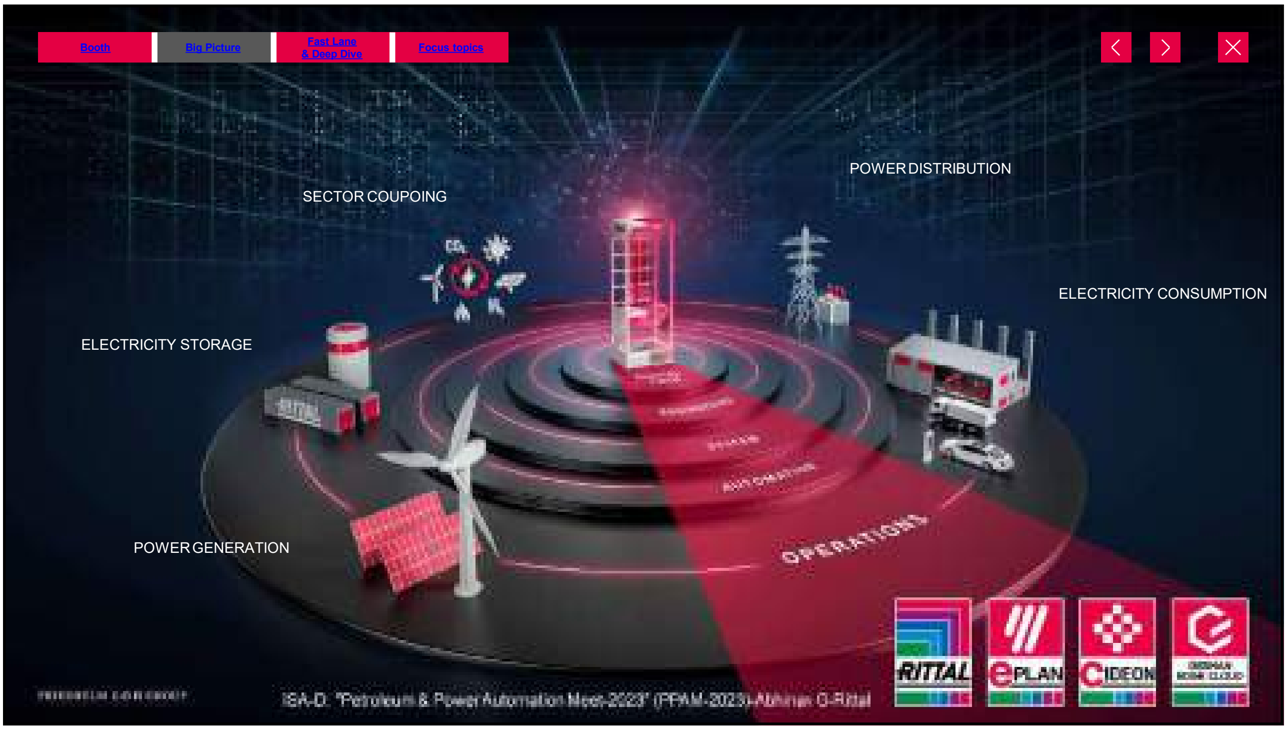
Big Picture

3. Genuine values for the customer:
Expertise for new ecosystems

- Further **opportunities** are opening up if we consistently pursue this path, for example in the **transformation of the energy sectors**. The upscale of energy infrastructure must pick up speed and precisely needs that: infrastructure. The critical factor for this is the industrialisation of the process chains – including digital twins that extend into operations.
- Our driving principle is
  - Streamline the value chain with
  - modularity and standardisation and
  - achieving data consistency through to operation
- We use our experience in control and switchgear manufacturing and support the upscale of infrastructure – from energy generation and storage to grid expansion and sector coupling to charging facilities for electric vehicles with end-to-end hardware and software solutions. The efficiency gain reduces costs, while the data, as the automation twin, opens up further possibilities for use in operation.

RITTAL EPLAN CIDEON

8

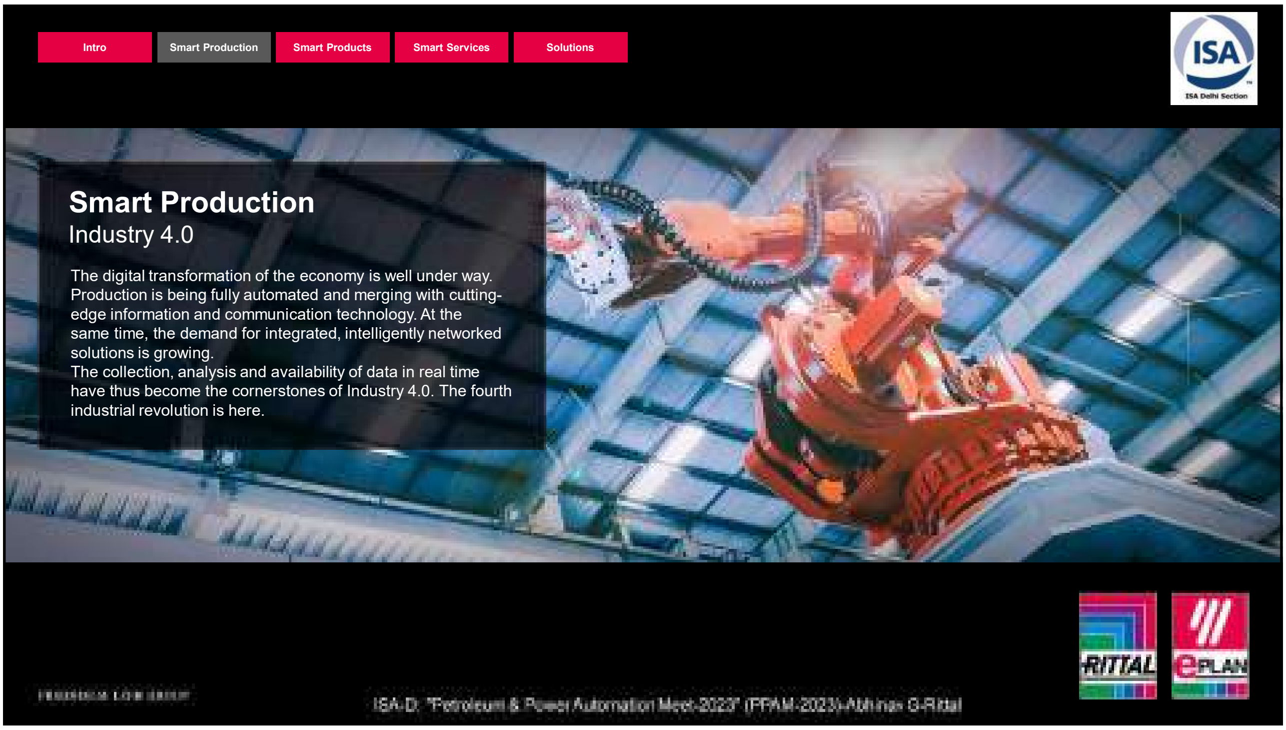

Booth
Big Picture
Fast Lane & Deep Dive
Focus topics
SECTOR COUPOING
POWER DISTRIBUTION
ELECTRICITY CONSUMPTION
ELECTRICITY STORAGE
POWER GENERATION
OPERATIONS
RITTAL
EPLAN
CIDEON
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

9

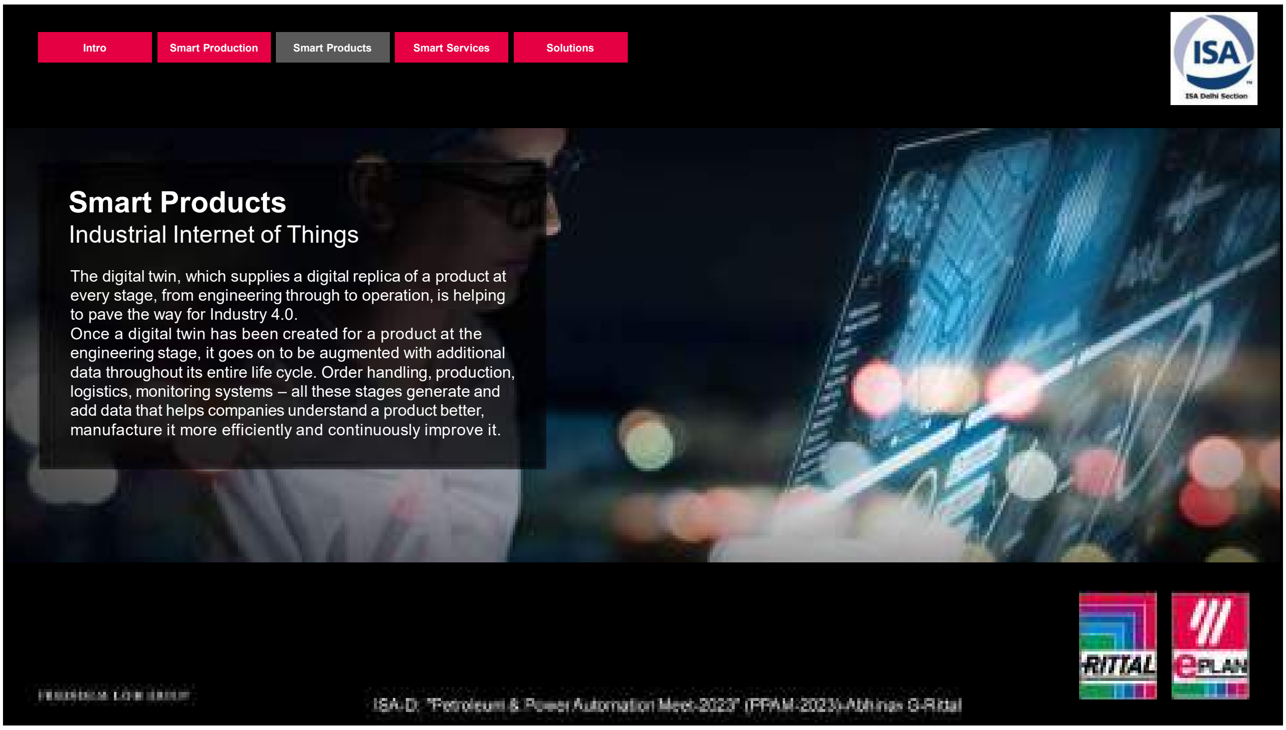

Rittal and Eplan:
Your strong partners for sustainable panel building and switchgear manufacturing.
RITTAL
EPLAN

10

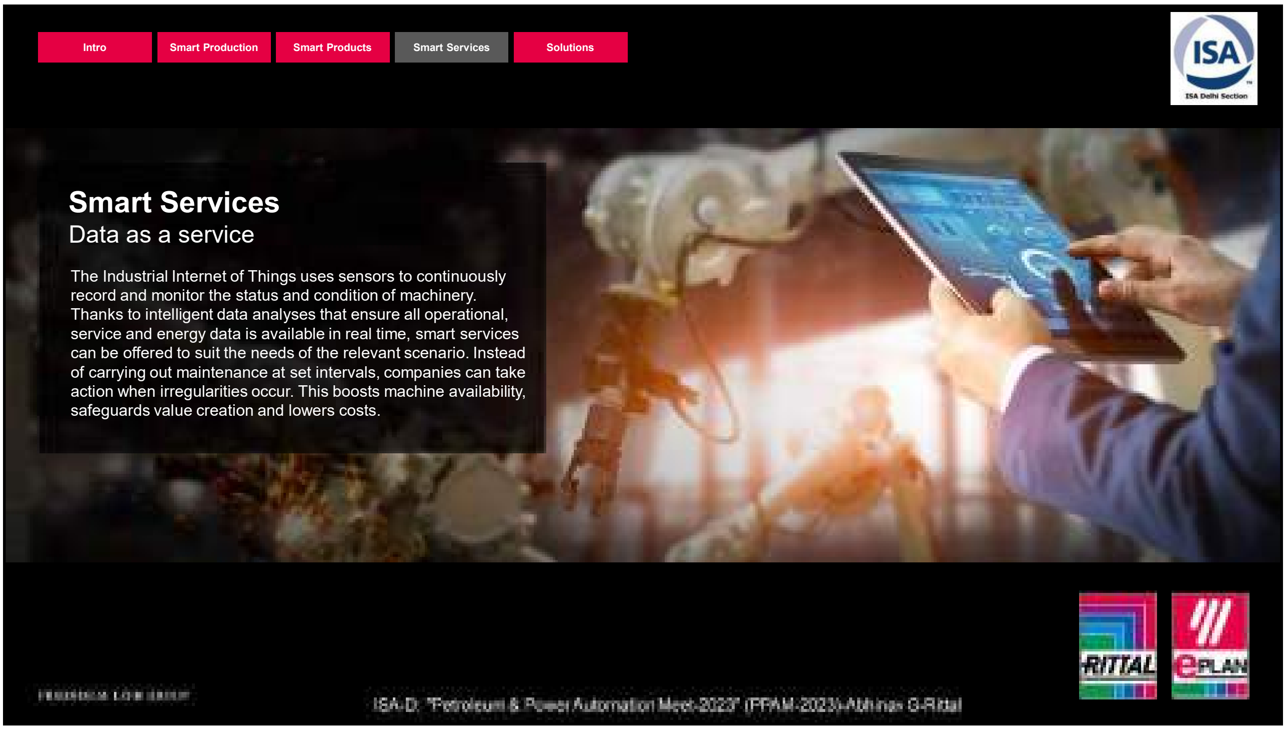
11


Intro
Smart Production
Smart Products
Smart Services
Solutions
ISA
ISA Delhi Section
Smart Production
Industry 4.0
The digital transformation of the economy is well under way. Production is being fully automated and merging with cutting-edge information and communication technology. At the same time, the demand for integrated, intelligently networked solutions is growing.
The collection, analysis and availability of data in real time have thus become the cornerstones of Industry 4.0. The fourth industrial revolution is here.
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

12


Intro
Smart Production
Smart Products
Smart Services
Solutions
ISA
Smart Products
Industrial Internet of Things
The digital twin, which supplies a digital replica of a product at every stage, from engineering through to operation, is helping to pave the way for Industry 4.0.
Once a digital twin has been created for a product at the engineering stage, it goes on to be augmented with additional data throughout its entire life cycle. Order handling, production, logistics, monitoring systems – all these stages generate and add data that helps companies understand a product better, manufacture it more efficiently and continuously improve it.
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

13


Intro
Smart Production
Smart Products
Smart Services
Solutions
ISA
Smart Services
Data as a service
The Industrial Internet of Things uses sensors to continuously record and monitor the status and condition of machinery.
Thanks to intelligent data analyses that ensure all operational, service and energy data is available in real time, smart services can be offered to suit the needs of the relevant scenario. Instead of carrying out maintenance at set intervals, companies can take action when irregularities occur. This boosts machine availability, safeguards value creation and lowers costs.
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

14

Intro | Smart Production | Smart Products | Smart Services | Solutions

Solutions
Digital Twin

By combining engineering solutions from Eplan with system and automation expertise from Rittal, you can optimise and industrialise your panel building and switchgear manufacturing processes.

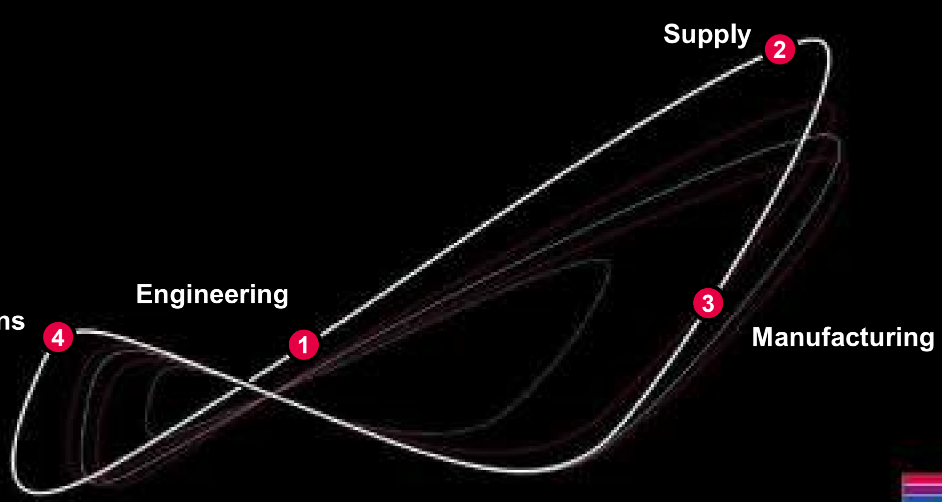
95% of companies have **boosted productivity,** while also **improving their products and services,** thanks to digitalisation.*

* According to the Digital Value 2018 survey of 200 decision-makers from a variety of sectors in Germany, Austria and Switzerland.

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

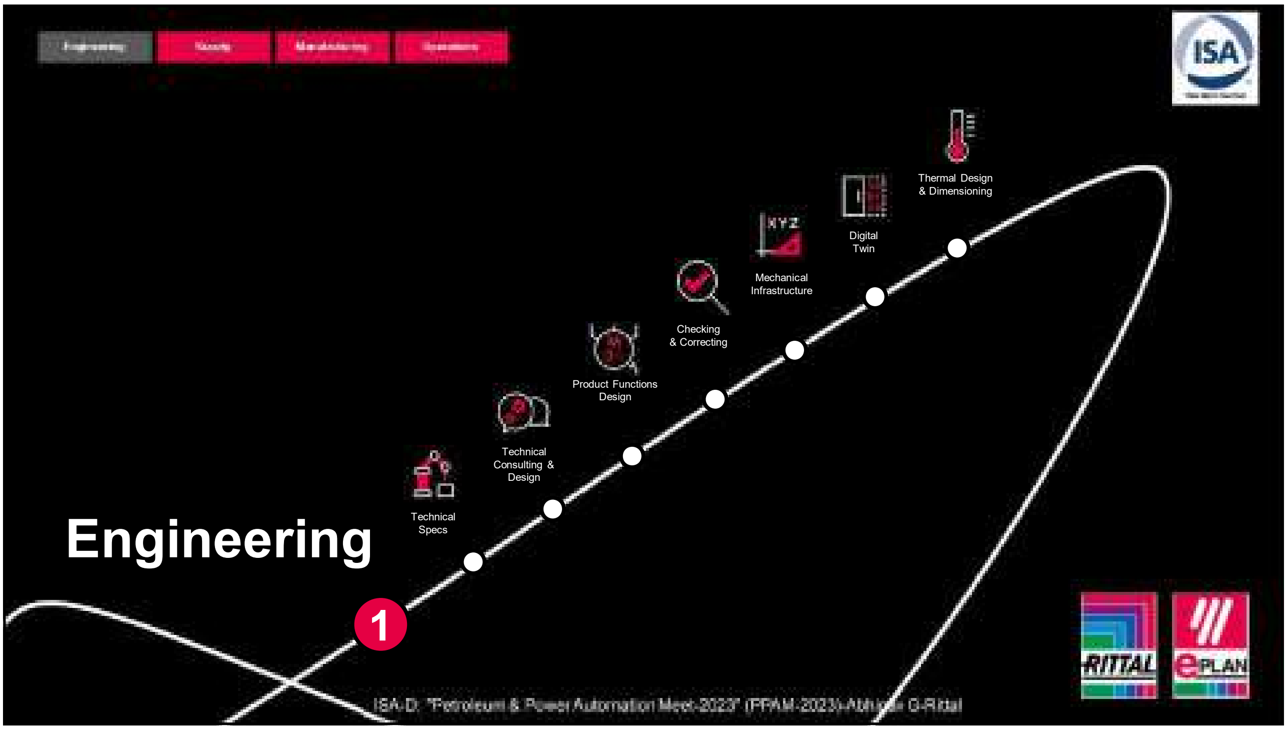
15

Rittal and Eplan: Your strong partners for sustainable panel building and switchgear manufacturing.

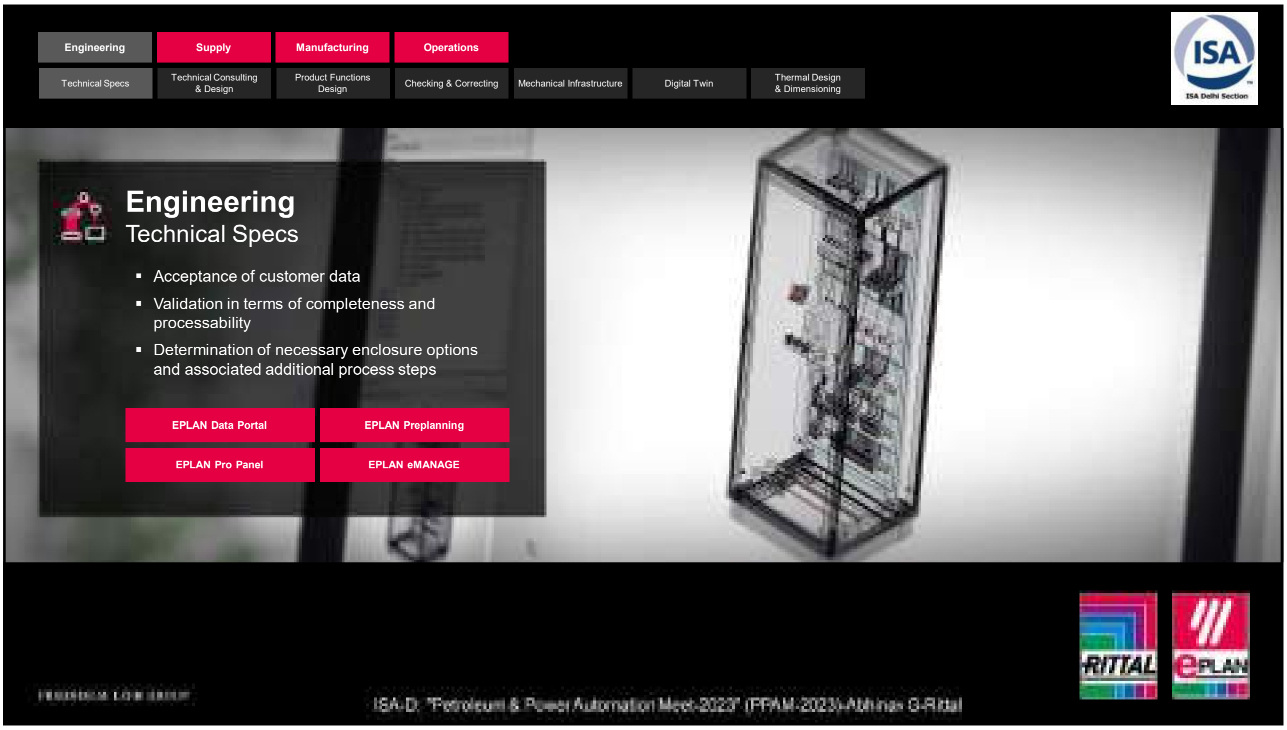


ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

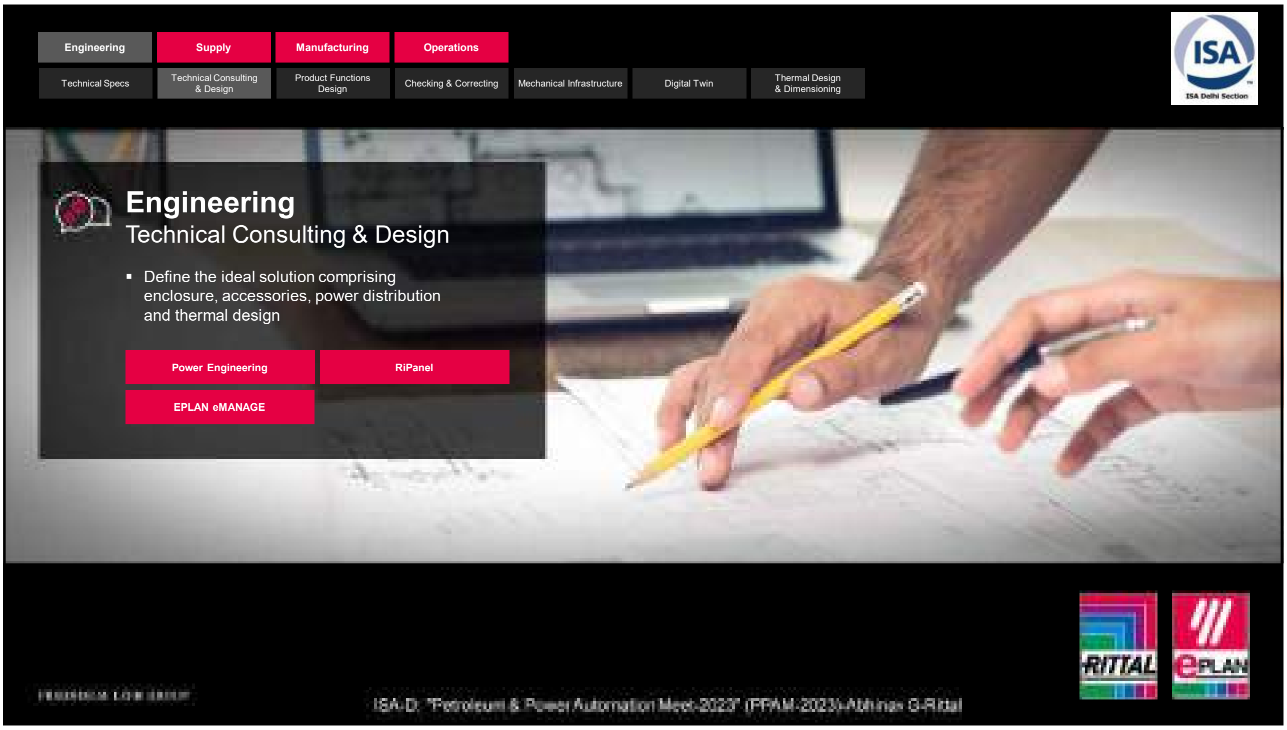
16


Thermal Design
& Dimensioning
Digital
Twin
Mechanical
Infrastructure
Checking
& Correcting
Product Functions
Design
Technical
Consulting &
Design
Technical
Specs
Engineering
1
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal
RITTAL
EPLAN

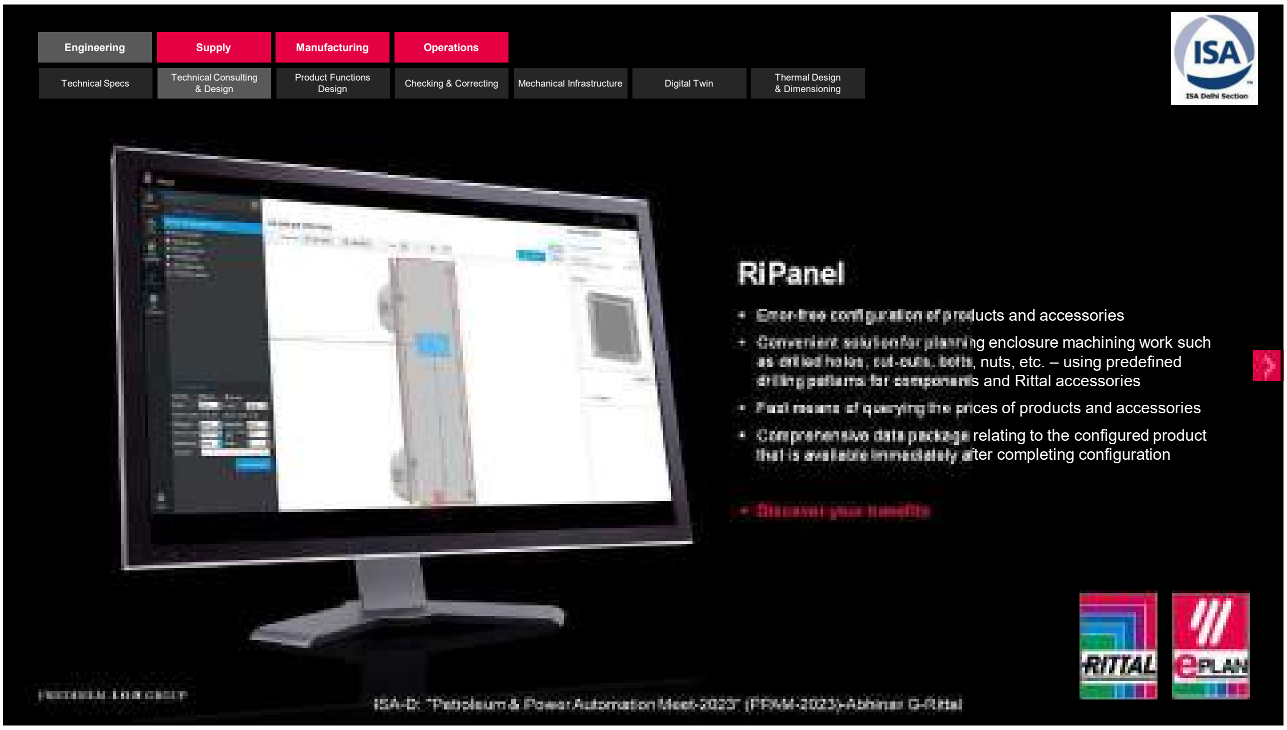
17


Engineering
Supply
Manufacturing
Operations
Technical Specs
Technical Consulting
& Design
Product Functions
Design
Checking & Correcting
Mechanical Infrastructure
Digital Twin
Thermal Design
& Dimensioning
ISA
ISA Delhi Section
Engineering
Technical Specs
Acceptance of customer data
Validation in terms of completeness and processability
Determination of necessary enclosure options and associated additional process steps
EPLAN Data Portal
EPLAN Preplanning
EPLAN Pro Panel
EPLAN eMANAGE
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal
RITTAL
EPLAN

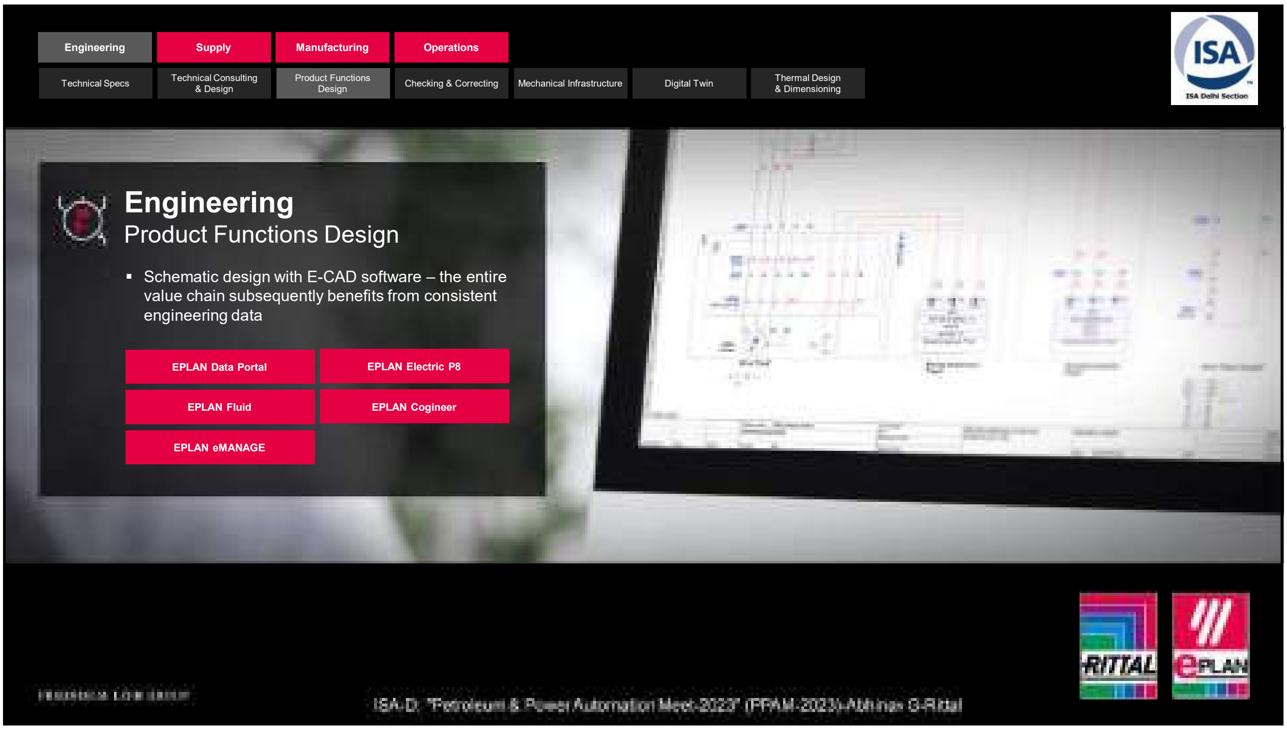
18


Engineering
Supply
Manufacturing
Operations
Technical Specs
Technical Consulting & Design
Product Functions Design
Checking & Correcting
Mechanical Infrastructure
Digital Twin
Thermal Design & Dimensioning
ISA
ISA Delhi Section
Engineering
Technical Consulting & Design
Define the ideal solution comprising enclosure, accessories, power distribution and thermal design
Power Engineering
RiPanel
EPLAN eMANAGE
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

19

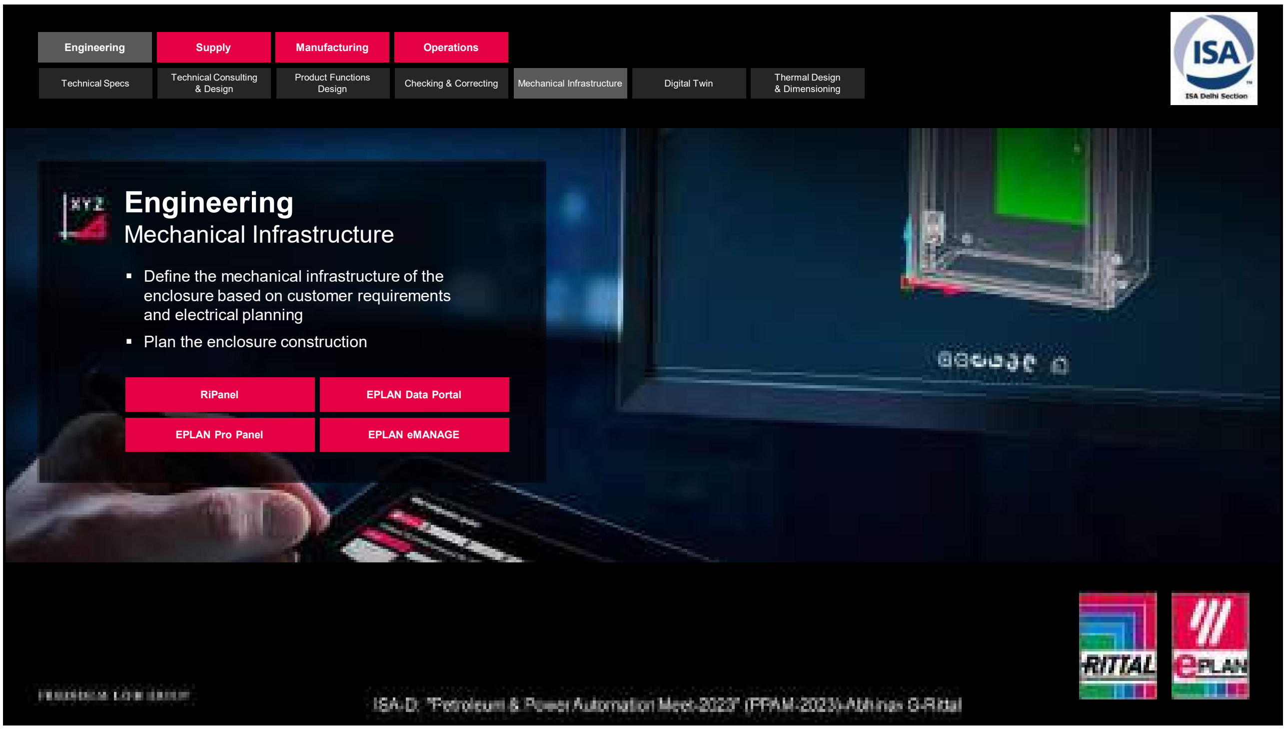

Engineering
Supply
Manufacturing
Operations
Technical Specs
Technical Consulting & Design
Product Functions Design
Checking & Correcting
Mechanical Infrastructure
Digital Twin
Thermal Design & Dimensioning
ISA
ISA Delhi Section
RiPanel
Error-free configuration of products and accessories
Convenient solution for planning enclosure machining work such as drilled holes, cut-outs, bolts, nuts, etc. – using predefined drilling patterns for components and Rittal accessories
Fast means of querying the prices of products and accessories
Comprehensive data package relating to the configured product that is available immediately after completing configuration
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

20



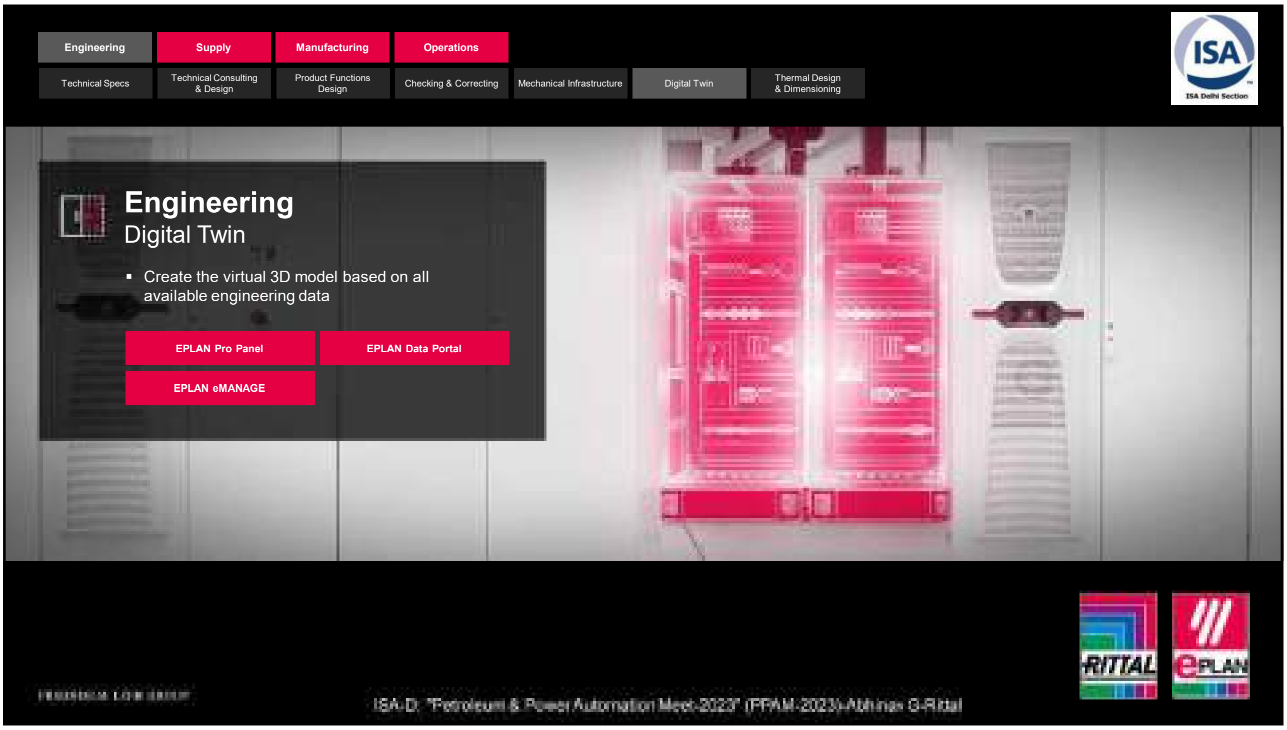
Engineering
Supply
Manufacturing
Operations
Technical Specs
Technical Consulting & Design
Product Functions Design
Checking & Correcting
Mechanical Infrastructure
Digital Twin
Thermal Design & Dimensioning
ISA
ISA Delhi Section
Engineering
Product Functions Design
▪ Schematic design with E-CAD software – the entire value chain subsequently benefits from consistent engineering data
EPLAN Data Portal
EPLAN Electric P8
EPLAN Fluid
EPLAN Cogineer
EPLAN eMANAGE
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

21

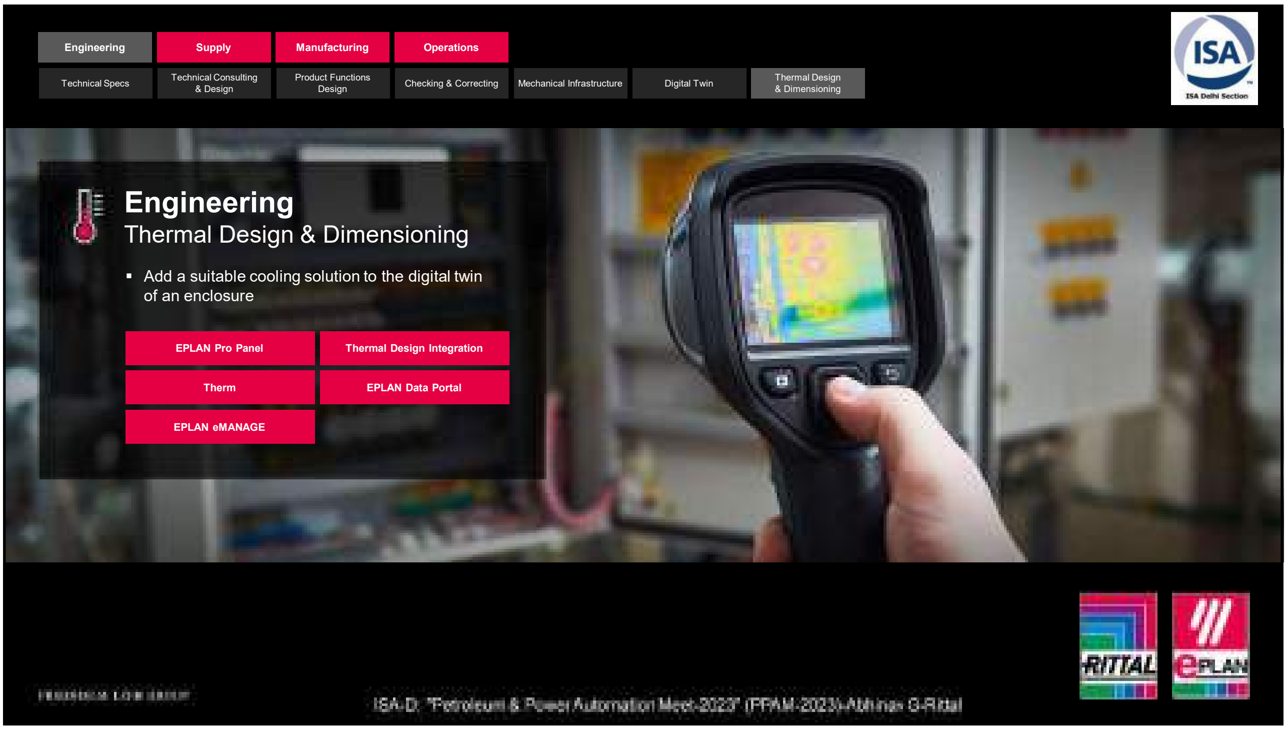


Engineering
Supply
Manufacturing
Operations
Technical Specs
Technical Consulting & Design
Product Functions Design
Checking & Correcting
Mechanical Infrastructure
Digital Twin
Thermal Design & Dimensioning
ISA
ISA Delhi Section
XYZ
Engineering
Mechanical Infrastructure
▪ Define the mechanical infrastructure of the enclosure based on customer requirements and electrical planning
▪ Plan the enclosure construction
RiPanel
EPLAN Data Portal
EPLAN Pro Panel
EPLAN eMANAGE
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

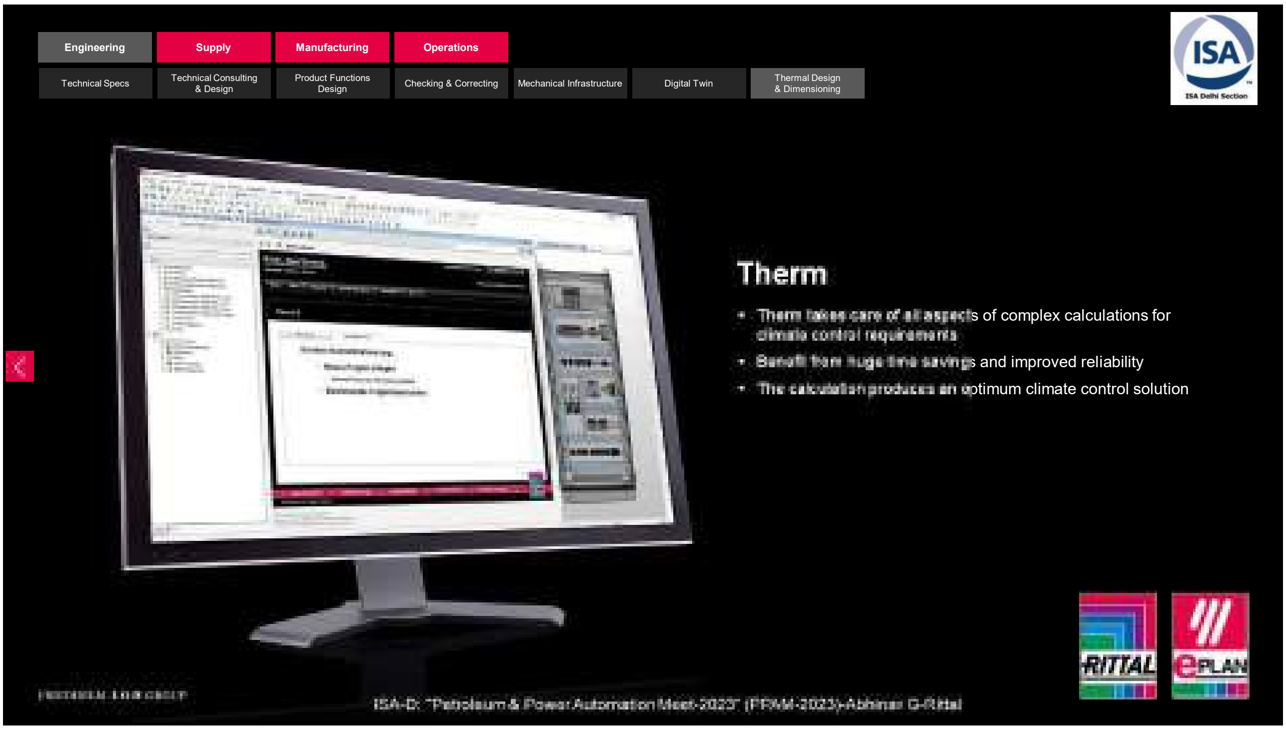
22


Engineering
Supply
Manufacturing
Operations
Technical Specs
Technical Consulting & Design
Product Functions Design
Checking & Correcting
Mechanical Infrastructure
Digital Twin
Thermal Design & Dimensioning
ISA
ISA Delhi Section
Engineering
Digital Twin
Create the virtual 3D model based on all available engineering data
EPLAN Pro Panel
EPLAN Data Portal
EPLAN eMANAGE
RITTAL
EPLAN

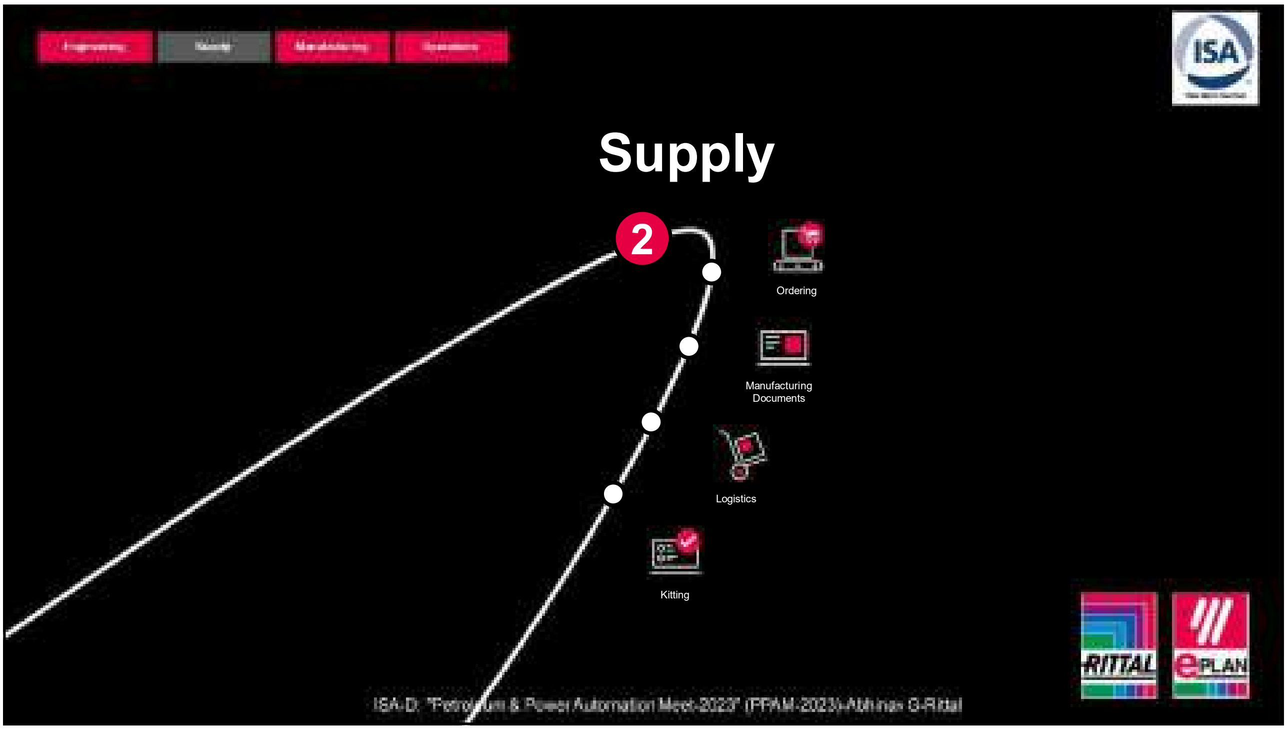
23


Engineering
Supply
Manufacturing
Operations
Technical Specs
Technical Consulting & Design
Product Functions Design
Checking & Correcting
Mechanical Infrastructure
Digital Twin
Thermal Design & Dimensioning
ISA
ISA Delhi Section
Engineering
Thermal Design & Dimensioning
Add a suitable cooling solution to the digital twin of an enclosure
EPLAN Pro Panel
Thermal Design Integration
Therm
EPLAN Data Portal
EPLAN eMANAGE
RITTAL
EPLAN

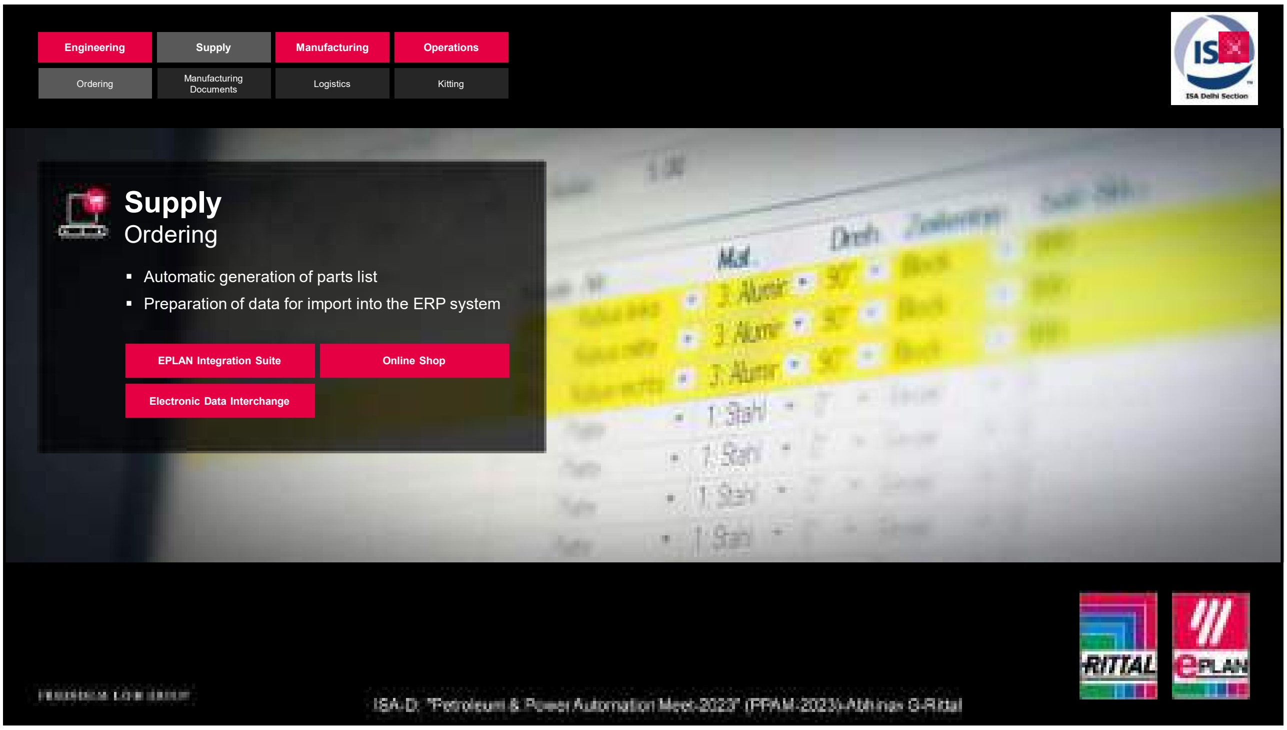
24


Engineering
Supply
Manufacturing
Operations
Technical Specs
Technical Consulting & Design
Product Functions Design
Checking & Correcting
Mechanical Infrastructure
Digital Twin
Thermal Design & Dimensioning
ISA
ISA Delhi Section
Therm
• Therm takes care of all aspects of complex calculations for climate control requirements
• Benefit from huge time savings and improved reliability
• The calculation produces an optimum climate control solution
RITTAL
ePLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

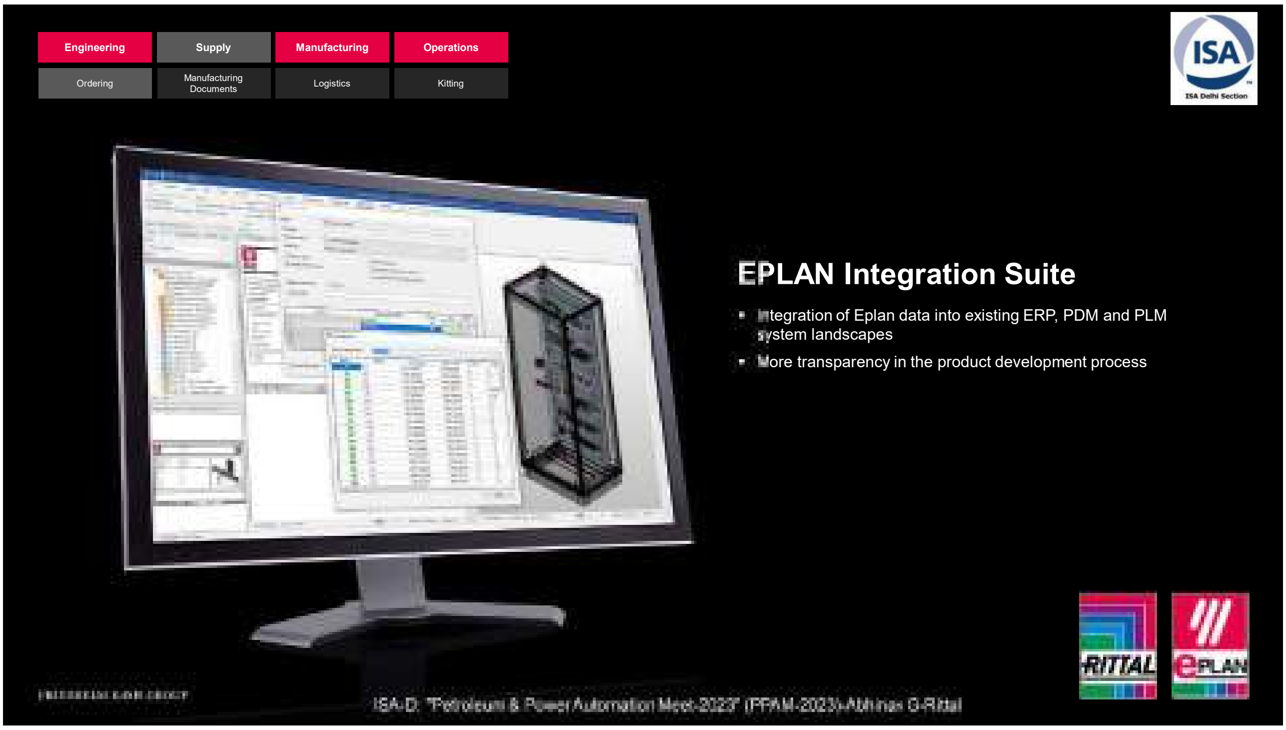
25


ISA
Supply
2
Ordering
Manufacturing Documents
Logistics
Kitting
RITTAL
ePLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

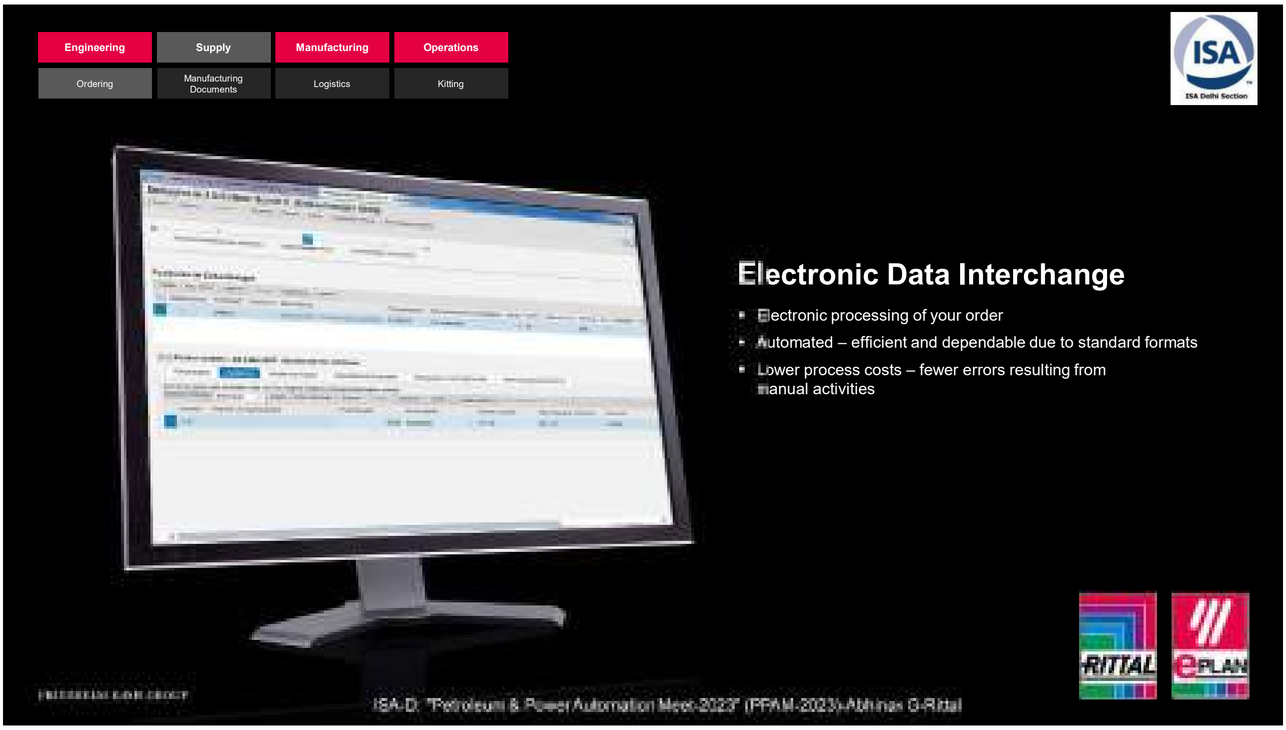
26


Engineering
Supply
Manufacturing
Operations
Ordering
Manufacturing Documents
Logistics
Kitting
ISA Delhi Section
Supply
Ordering
▪ Automatic generation of parts list
▪ Preparation of data for import into the ERP system
EPLAN Integration Suite
Online Shop
Electronic Data Interchange
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

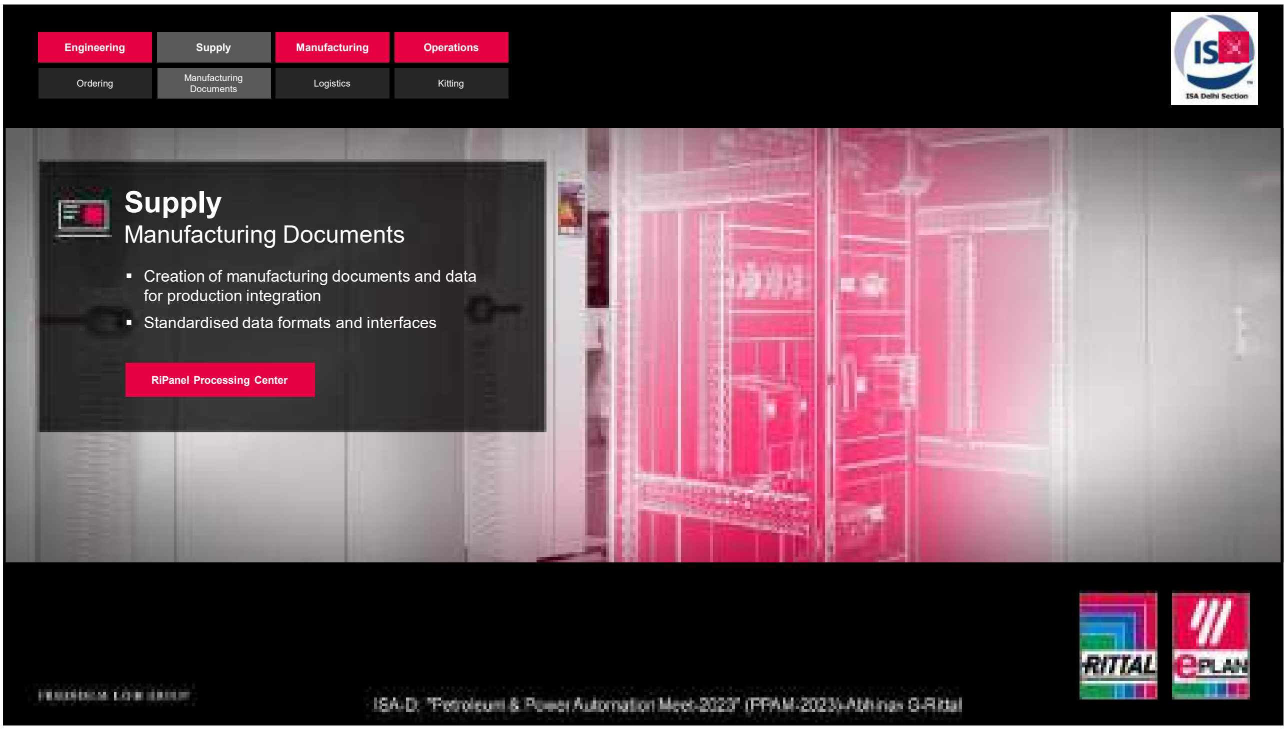
27


Engineering
Supply
Manufacturing
Operations
Ordering
Manufacturing Documents
Logistics
Kitting
ISA
ISA Delhi Section
EPLAN Integration Suite
▪ Integration of Eplan data into existing ERP, PDM and PLM system landscapes
▪ More transparency in the product development process
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

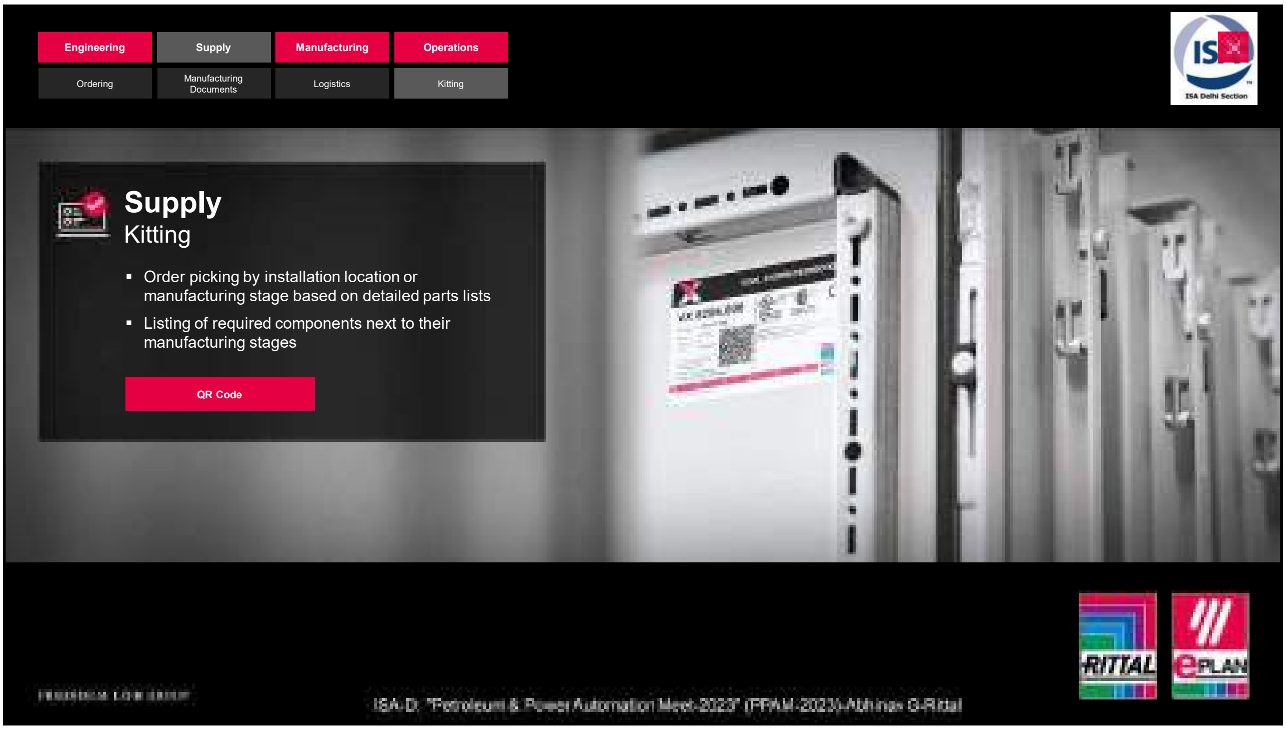
28


Engineering
Supply
Manufacturing
Operations
Ordering
Manufacturing Documents
Logistics
Kitting
ISA
ISA Delhi Section
Electronic Data Interchange
Electronic processing of your order
Automated – efficient and dependable due to standard formats
Lower process costs – fewer errors resulting from manual activities
RITTAL
ePLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

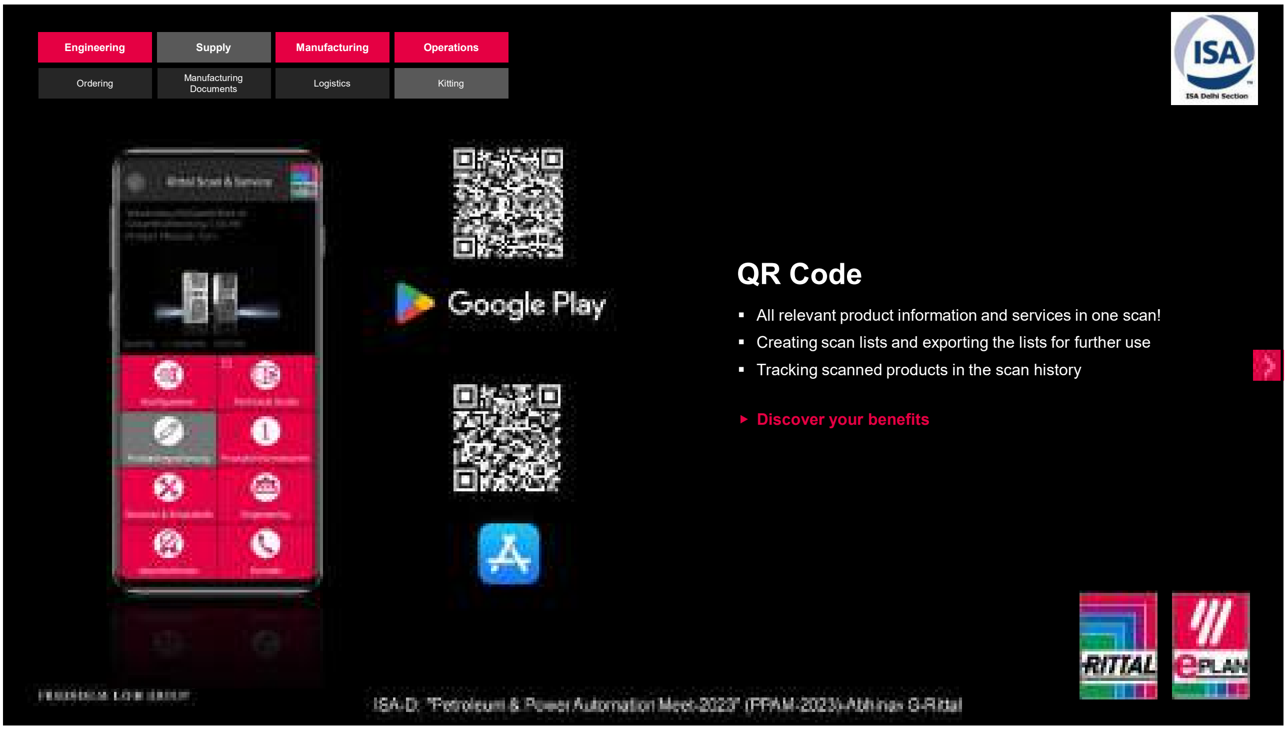
29


Engineering
Supply
Manufacturing
Operations
Ordering
Manufacturing Documents
Logistics
Kitting
ISA Delhi Section
Supply
Manufacturing Documents
Creation of manufacturing documents and data for production integration
Standardised data formats and interfaces
RiPanel Processing Center
RITTAL
ePLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

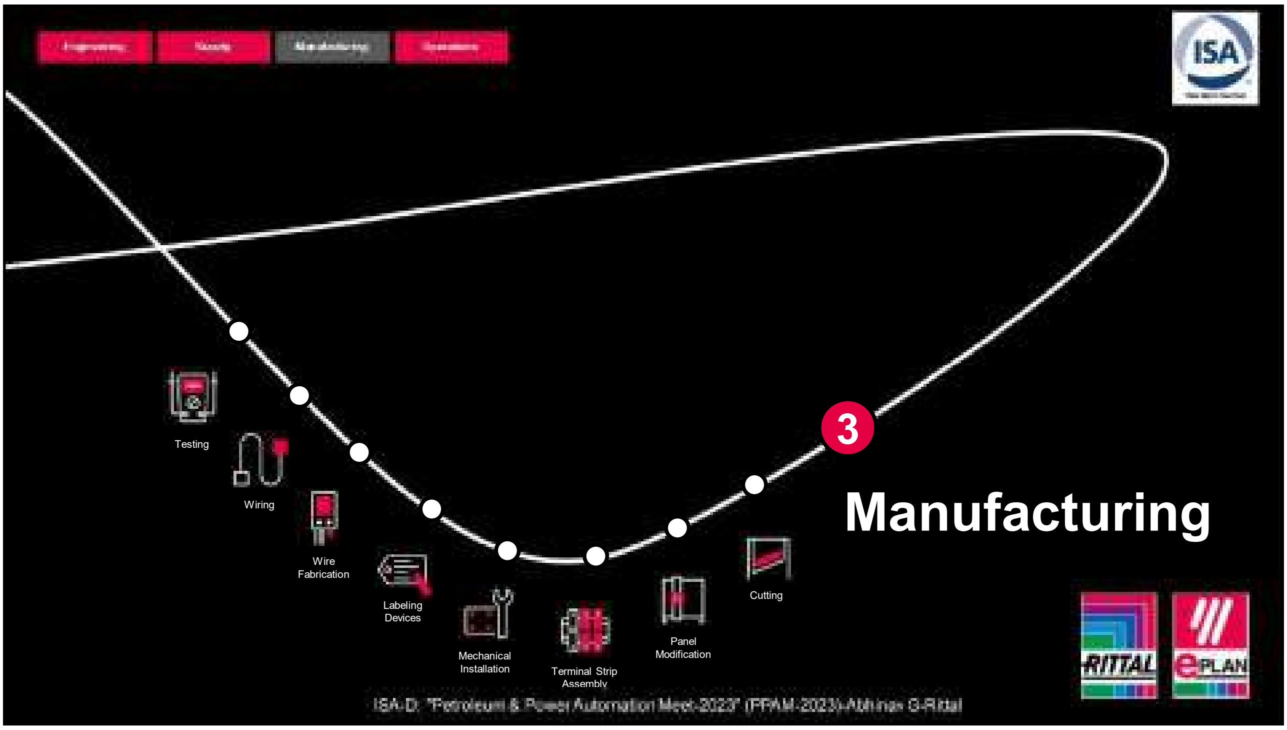
30


Engineering
Supply
Manufacturing
Operations
Ordering
Manufacturing Documents
Logistics
Kitting
Supply
Kitting
▪ Order picking by installation location or manufacturing stage based on detailed parts lists
▪ Listing of required components next to their manufacturing stages
QR Code
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

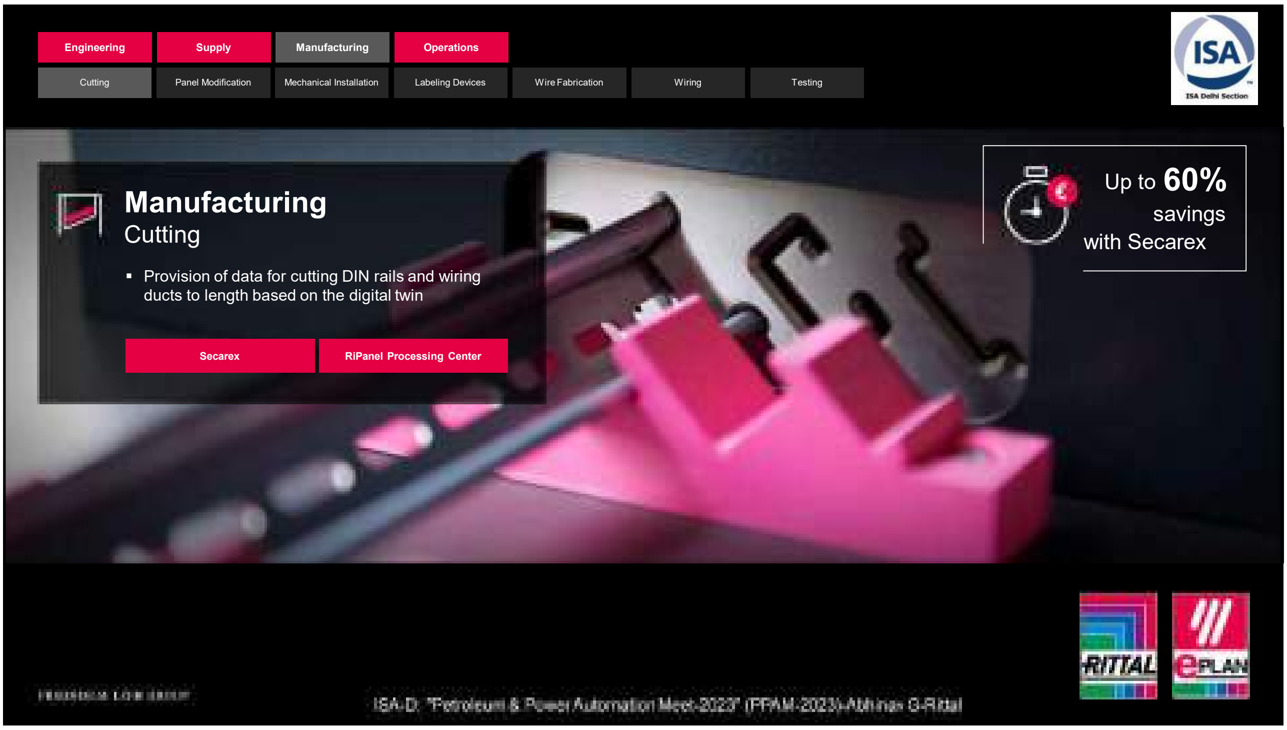
31


Engineering
Supply
Manufacturing
Operations
Ordering
Manufacturing Documents
Logistics
Kitting
ISA
ISA Delhi Section
Google Play
QR Code
▪ All relevant product information and services in one scan!
▪ Creating scan lists and exporting the lists for further use
▪ Tracking scanned products in the scan history
▸ Discover your benefits
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

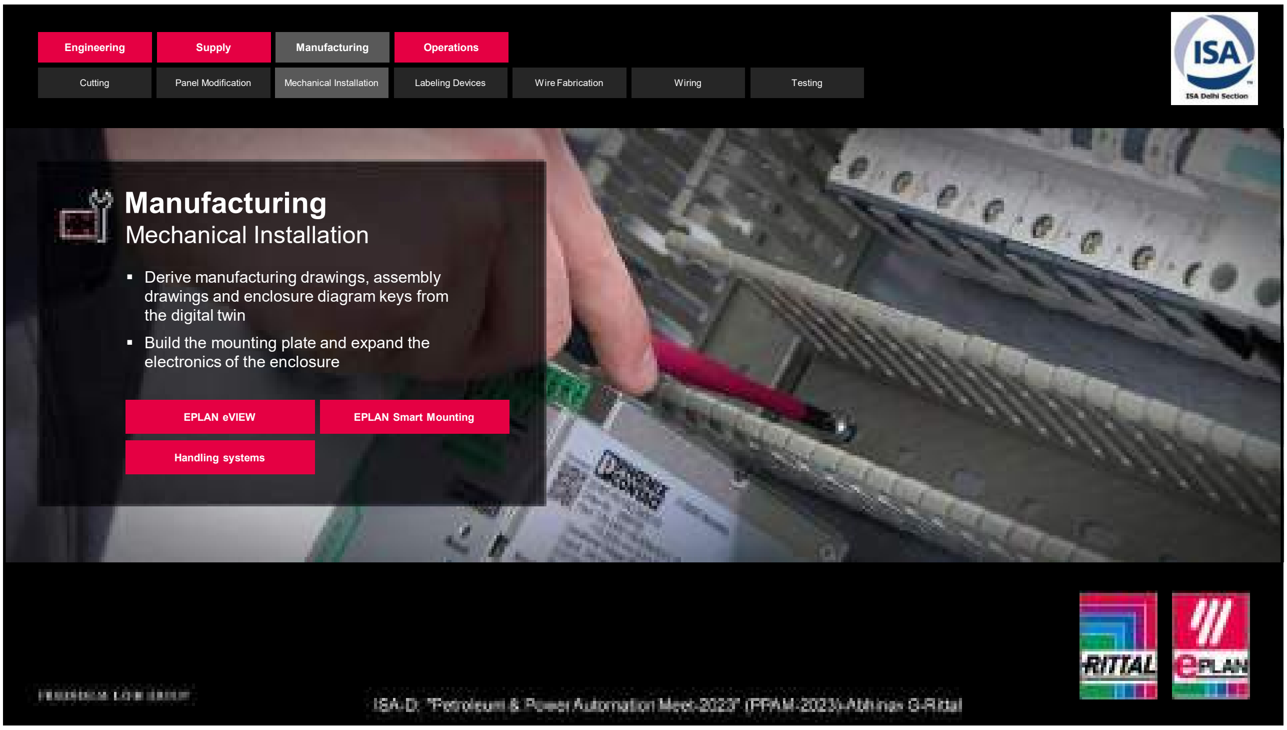
32


Testing
Wiring
Wire Fabrication
Labeling Devices
Mechanical Installation
Terminal Strip Assembly
Panel Modification
Cutting
3
Manufacturing
RITTAL
ePLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

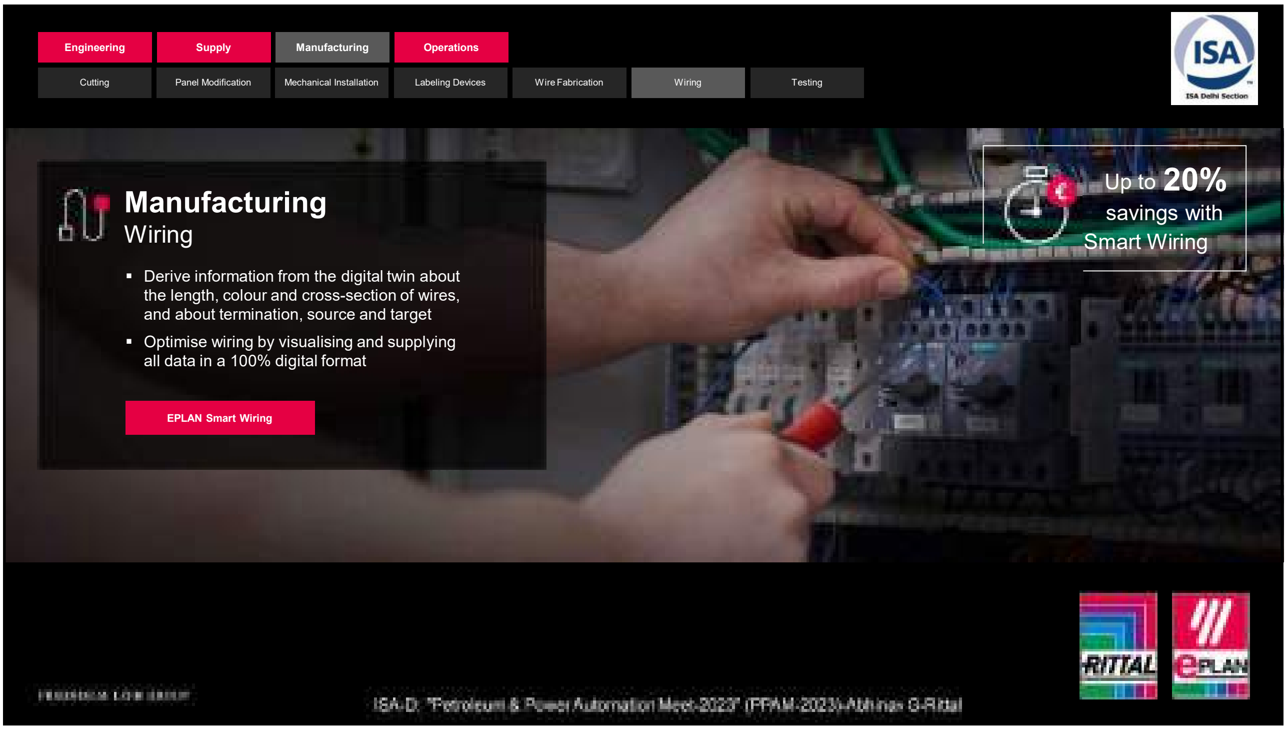
33


Engineering
Supply
Manufacturing
Operations
Cutting
Panel Modification
Mechanical Installation
Labeling Devices
Wire Fabrication
Wiring
Testing
ISA
ISA Delhi Section
Manufacturing
Cutting
Provision of data for cutting DIN rails and wiring ducts to length based on the digital twin
Secarex
RiPanel Processing Center
Up to 60% savings with Secarex
RITTAL
ePLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

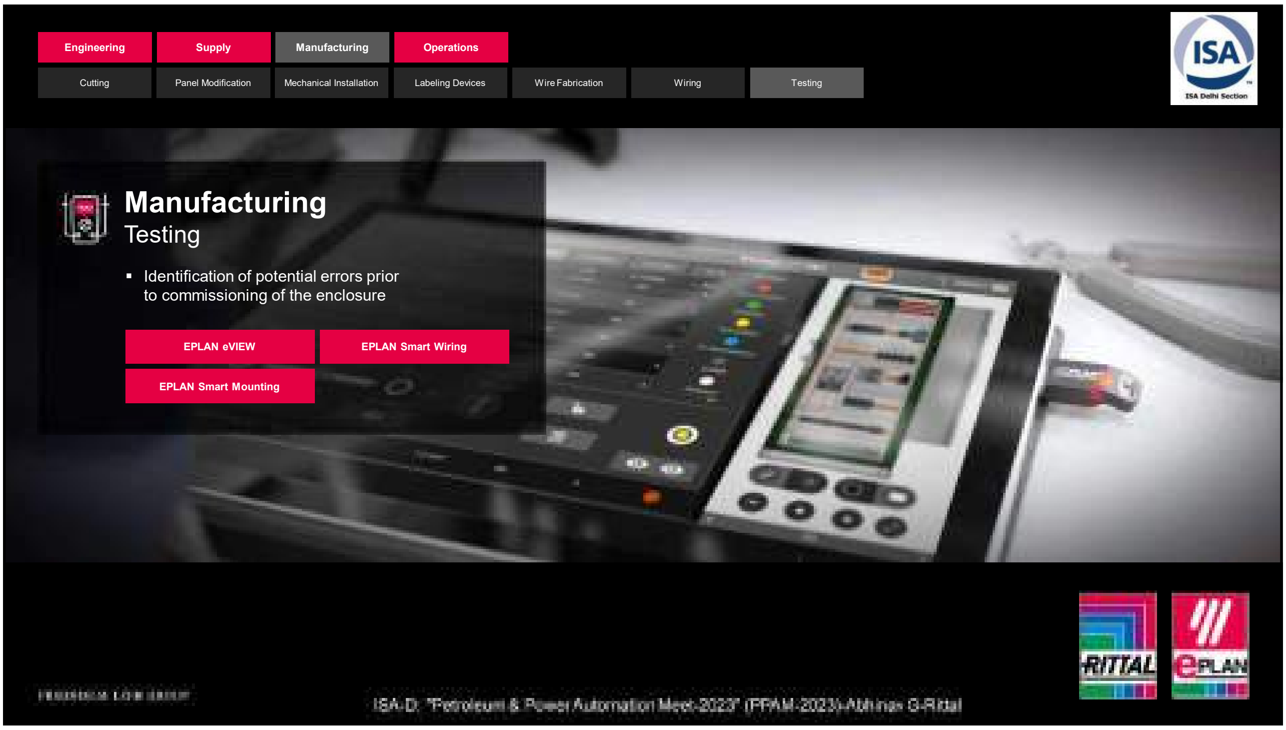
34


Engineering
Supply
Manufacturing
Operations
Cutting
Panel Modification
Mechanical Installation
Labeling Devices
Wire Fabrication
Wiring
Testing
ISA
ISA Delhi Section
Manufacturing
Mechanical Installation
▪ Derive manufacturing drawings, assembly drawings and enclosure diagram keys from the digital twin
▪ Build the mounting plate and expand the electronics of the enclosure
EPLAN eVIEW
EPLAN Smart Mounting
Handling systems
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

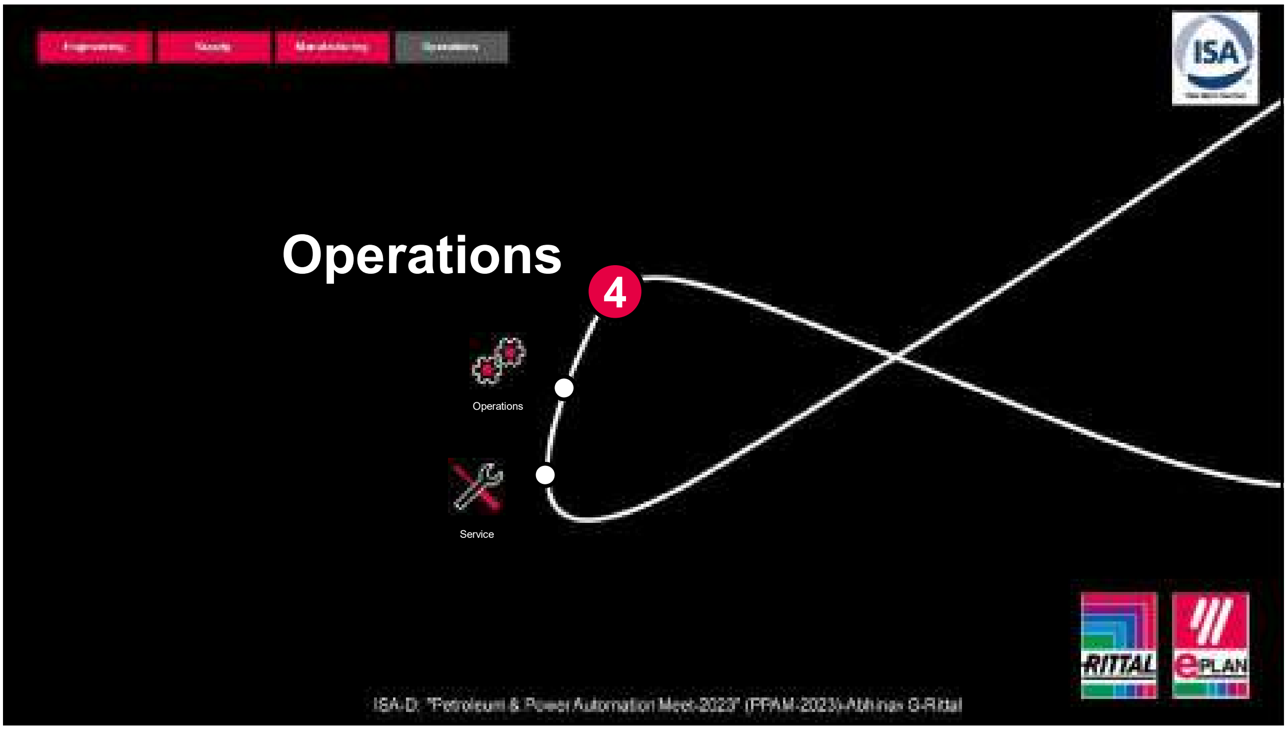
35


Engineering
Supply
Manufacturing
Operations
Cutting
Panel Modification
Mechanical Installation
Labeling Devices
Wire Fabrication
Wiring
Testing
ISA
ISA Delhi Section
Manufacturing
Wiring
▪ Derive information from the digital twin about the length, colour and cross-section of wires, and about termination, source and target
▪ Optimise wiring by visualising and supplying all data in a 100% digital format
EPLAN Smart Wiring
Up to 20% savings with Smart Wiring
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

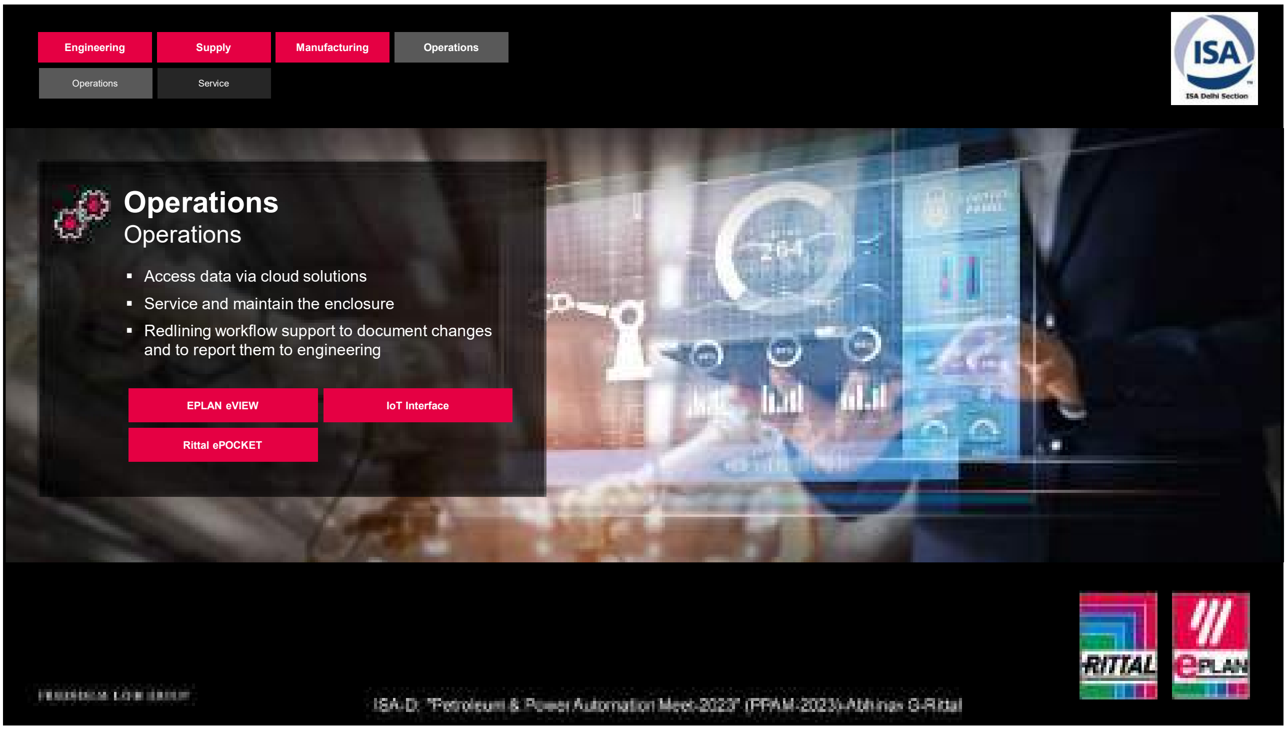
36


Engineering
Supply
Manufacturing
Operations
Cutting
Panel Modification
Mechanical Installation
Labeling Devices
Wire Fabrication
Wiring
Testing
ISA
ISA Delhi Section
Manufacturing
Testing
▪ Identification of potential errors prior to commissioning of the enclosure
EPLAN eVIEW
EPLAN Smart Wiring
EPLAN Smart Mounting
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

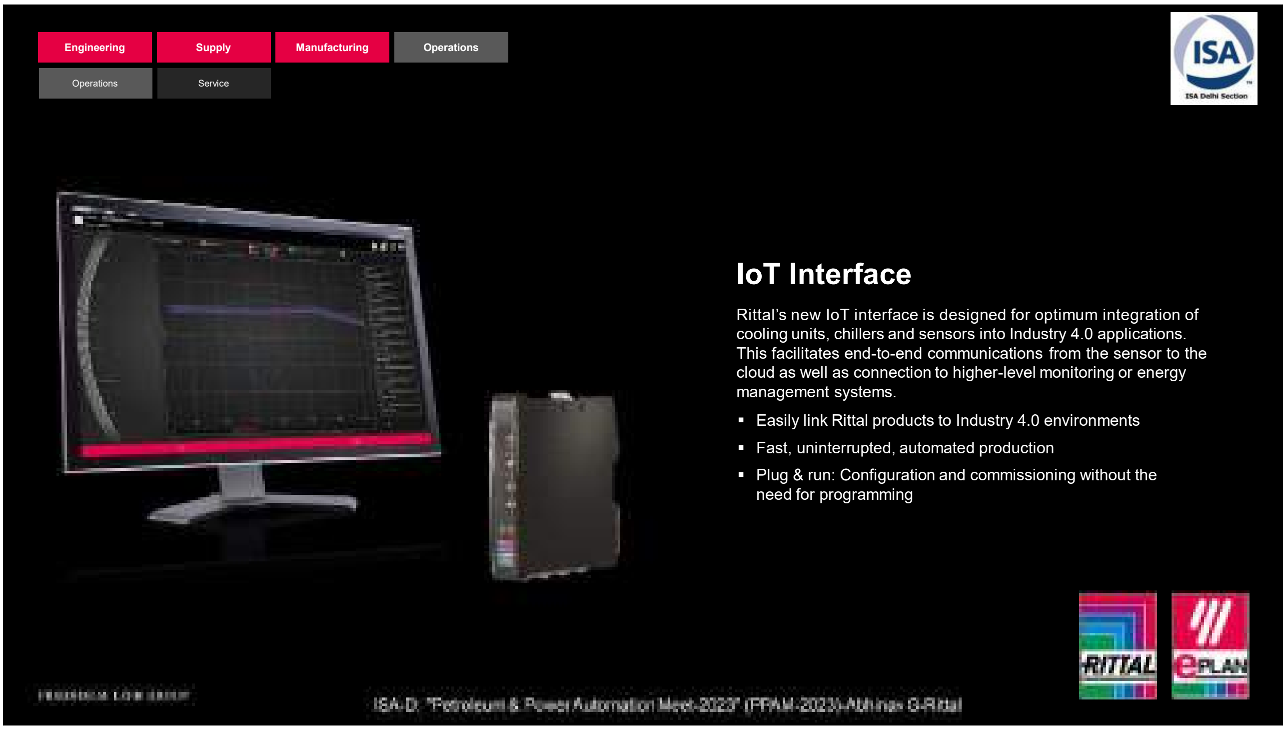
37


ISA
Operations
4
Operations
Service
RITTAL
EPLAN
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

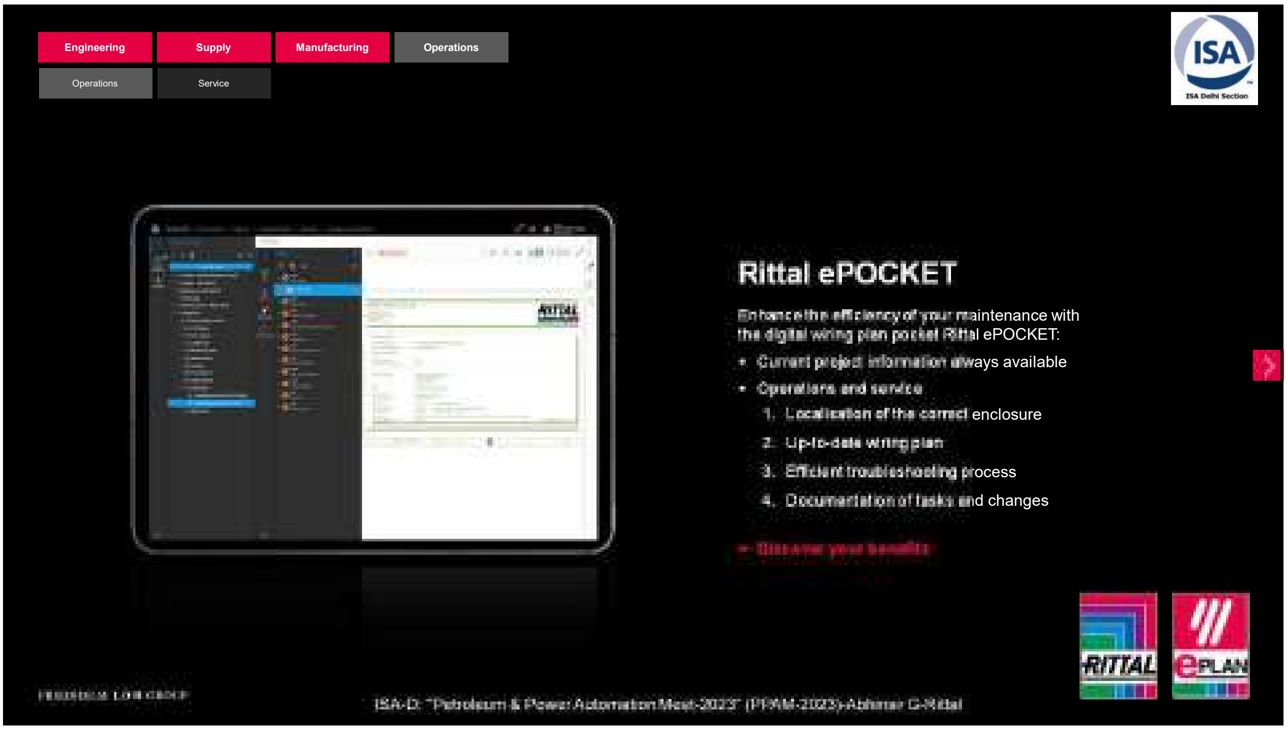
38


Engineering
Supply
Manufacturing
Operations
Operations
Service
Operations
Operations
Access data via cloud solutions
Service and maintain the enclosure
Redlining workflow support to document changes and to report them to engineering
EPLAN eVIEW
IoT Interface
Rittal ePOCKET
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

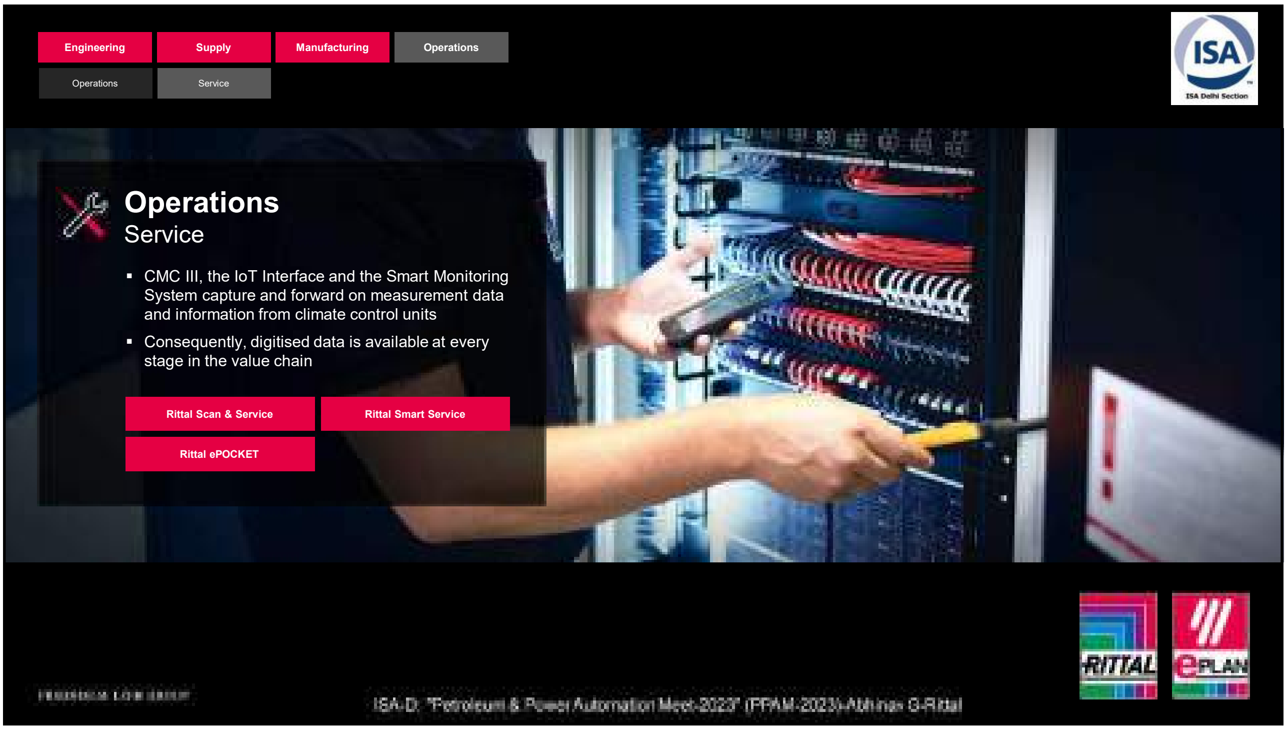
39


Engineering
Supply
Manufacturing
Operations
Operations
Service
IoT Interface
Rittal's new IoT interface is designed for optimum integration of cooling units, chillers and sensors into Industry 4.0 applications. This facilitates end-to-end communications from the sensor to the cloud as well as connection to higher-level monitoring or energy management systems.
Easily link Rittal products to Industry 4.0 environments
Fast, uninterrupted, automated production
Plug & run: Configuration and commissioning without the need for programming
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

40


Engineering
Supply
Manufacturing
Operations
Operations
Service
ISA
ISA Delhi Section
Rittal ePOCKET
Enhance the efficiency of your maintenance with the digital wiring plan pocket Rittal ePOCKET:
Current project information always available
Operations and service
1. Localisation of the correct enclosure
2. Up-to-date wiring plan
3. Efficient troubleshooting process
4. Documentation of tasks and changes
Discover your benefits
RITTAL
ePLAN
FRIEDHELM LOH GROUP
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

41


Engineering
Supply
Manufacturing
Operations
Operations
Service
ISA
ISA Delhi Section
Operations
Service
CMC III, the IoT Interface and the Smart Monitoring System capture and forward on measurement data and information from climate control units
Consequently, digitised data is available at every stage in the value chain
Rittal Scan & Service
Rittal Smart Service
Rittal ePOCKET
RITTAL
ePLAN
FRIEDHELM LOH GROUP
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

42

Engineering | Supply | Manufacturing | Operations

Operations | Service

Google Play

Rittal Scan & Service

- The configuration of a device can be transferred to other devices with just a few clicks
- Errors are read out via scan
- Product-specific spare parts and technical documentation are displayed in the app and can be conveniently ordered

RITTAL EPLAN

FRIEDHELM LOH GROUP

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

43

Engineering | Supply | Manufacturing | Operations

Benefit from the worldwide unique, modular Rittal system platform, consisting of the enclosure, power distribution, climate control, automation and IT infrastructure, as well as the software and service.

Ripploh Elektrotechnik & Engineering | ELPEX AG | Van Meer Industrial Services

Rittal – The System

Faster – better – everywhere.

- Thanks to their modular system architecture, Rittal solutions can be customised to meet your requirements.
- Enclosure construction is faster, more precise and reproducible with the automation solutions from Rittal Automation Systems.
- High-quality 2D and 3D data on every Rittal component is available in the EPLAN Data Portal, and it forms the perfect basis for the digital twin.
- The worldwide availability of our products and services ensures that your systems run smoothly at any time and at any location.
- We guarantee that standard products are rapidly delivered from stock.
- Our products' certified quality and international approvals guarantee that they can be used worldwide in every industry.

RITTAL EPLAN

FRIEDHELM LOH GROUP

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

44

Engineering | Supply | Manufacturing | Operations

Eplan helps you to develop a cross-disciplinary approach to your engineering. The EPLAN Platform provides the basis for this, by linking our software solutions together. EPLAN cloud additionally provides access to an innovative cloud system, and adds genuine value to your projects.

Ingela GmbH | Alexander Bürkle GmbH & Co. KG | The Weikl Group

EPLAN
Efficient engineering.

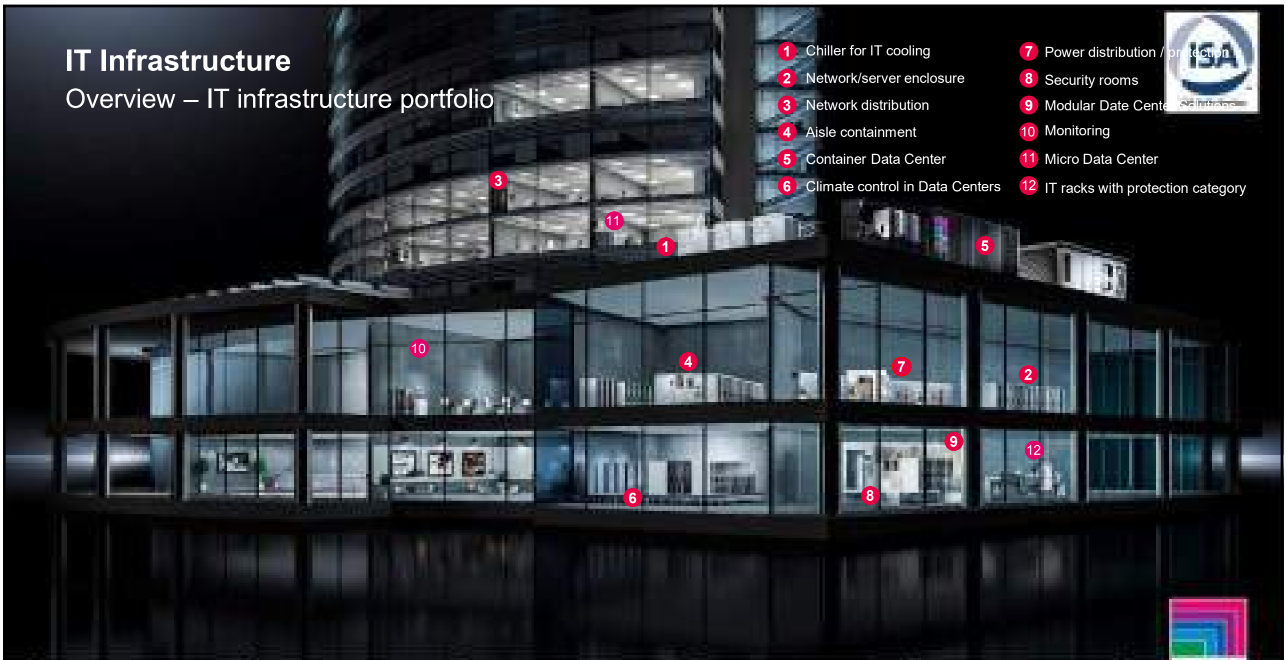
- The EPLAN Data Portal gives you access to product data from hundreds of device and component manufacturers.
- Create a virtual enclosure prototype in 3D with EPLAN Pro Panel.
- EPLAN Smart Wiring guides wirers through the wiring process one step at a time.
- Keep track of the current status of your project data across every location with the cloud-based EPLAN eVIEW solution.
- Data from the EPLAN Engineering software can be transferred directly to Rittal machines.

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

45

IT Infrastructure
Overview – IT infrastructure portfolio

1 Chiller for IT cooling
2 Network/server enclosure
3 Network distribution
4 Aisle containment
5 Container Data Center
6 Climate control in Data Centers
7 Power distribution / protection
8 Security rooms
9 Modular Date Center
10 Monitoring
11 Micro Data Center
12 IT racks with protection category



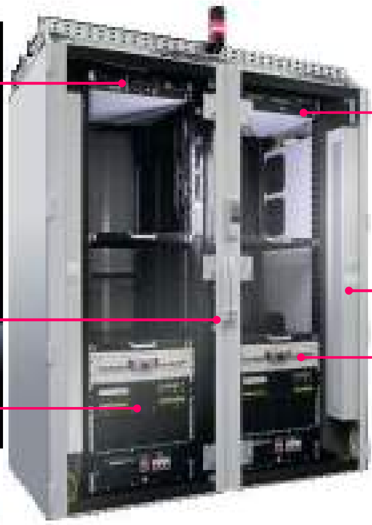
ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

46

EDGE Solution at a glance for Network/ IT Rack Solution

Monitoring & Alerts

Fire Suppression



Access Control

Cooling Unit

Power Distribution

UPS with Battery

RITTAL

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

47

Pre-configured package

Solution = Rittal Offering

Rittal Edge Data Center –2 Racks

- 2 IT Racks
- Refrigerant-based cooling solution for 1.5-3 kW, 7kW per rack
- Main power distribution for Single infeed by customer
- N+1 redundant 482,6 mm (19") UPS systems
- 4 redundant PDUs (2 per rack)

- Monitoring system Access control ,Alert by SMS & Email
- Fire extinguishing system
- Acoustic and visual alarm system
- Prepared for installation in any existing location
- Temperature range -20°C bis +45°C

Standardized components off-the-shelf! Faster Delivery

RITTAL

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

48

Pre-configured package
Example Solution

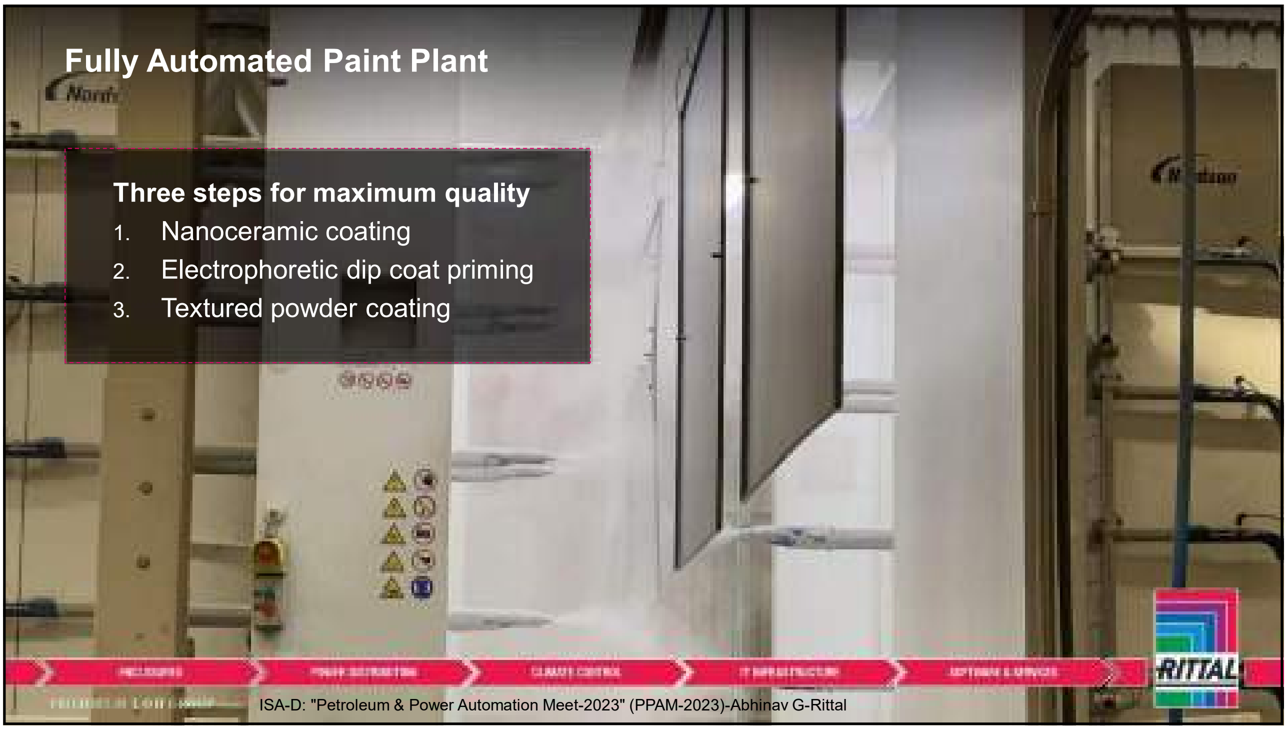
- No Raised Floor required
- 800Wx1200Dx2100H (mm) Racks
- Electrical Input panel
- UPS system
- Close coupled Indoor unit for air-conditioning
- Outdoor unit for air-conditioning
- Fire detection & Novec based suppression
- Central monitoring system
- Surveillance & automated recording of video
- Access control options for Rack door
- 100mm plinth for racks
- IT equipments, Servers, Storage, networking, etc

RITTAL

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

49

Fully Automated Paint Plant

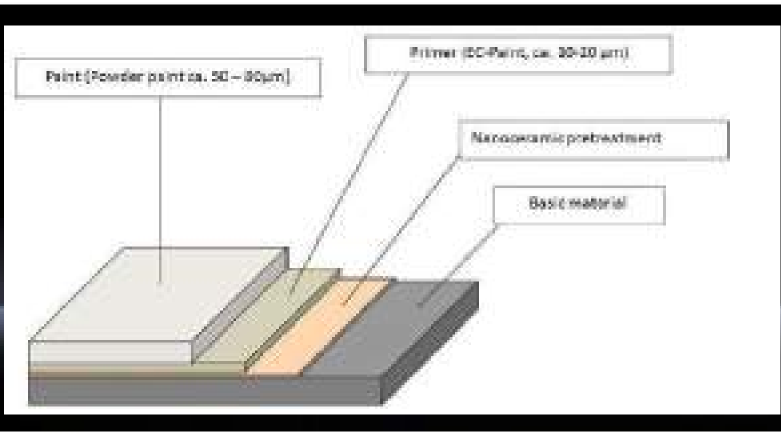


Three steps for maximum quality
1. Nanoceramic coating
2. Electrophoretic dip coat priming
3. Textured powder coating

RITTAL

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

50



51

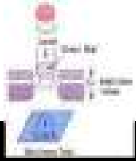
Testing of Technical Characteristics

Test procedures for the coating

- Mechanical resistance
- Corrosion resistance
- Capable of being over-painted
- Resistance in various media ,ease of cleaning
- UV resistance
- Aesthetic characteristics

52

Testing of Technical Characteristics



•Mechanical resistance
- Erichsen cupping test
- Mandrel bending test
- Cross-hatching
- Punch test
- Flying-stone damage

53

Testing of Technical Characteristics

Corrosion resistance

Splash water loading
- in constant climate
- in changing climate

Salt spray test-tested for 168 Hrs.

Over-painting

Compatibility of the paint systems
Adhesion to the paint undercoat
Cross cutting

54

Testing of Technical Characteristics

UV resistance
- Fast weathering
- Continuous test in outdoor use

Aesthetic characteristics
- Structure form
- Level of gloss
- Colour consistency

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

RITTAL

55

Rittal – The System.

Faster – better – everywhere.

Thank You !!!

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)-Abhinav G-Rittal

RITTAL

56

OPERANTIONAL TRANSFORMATION OF 690MW SALAL POWER STATION – NHPC LTD

Dharmesh Kumar Singh
Group Sr. Manager (Elect.)
NHPC Limited, Faridabad, Haryana

***Abstract*—**The hydro power stations contribute in the grid stability with the meeting of base load demand. The grid network is the link between the supplies from the generating stations with the demand network to be fulfilled in the distribution network. Today the reliability of the power system is important with the parameters to be maintained in grid reliability as required for the voltage and frequency to set for the quality power to consumer. Hydro Power stations is having the unique features to provide the stability in grid network.

In the recent past, various developments have been taken place for performance enhancement and an innovative approach developed in the industry. Due to the such enhancement and system stability, the extra control cable were removed from the old stations and new improved setup has been made by using the optical fibers and various automation used to enhance the functional performance of the hydro stations. This paper is one of the examples as the power output has been enhanced in Salal Power Station from the 650 MW to the 744 MW with enhanced capacity by way of various up-gradations as detailed in this paper.

Keywords**-**Human Machine Interface (HMI), SCADA (Supervisory control and data acquisition system), IT(Information Technology), OT(operational technology). SAB (Station Auxiliary Board), UAB (Unit Auxiliary Board),

BACKGROUND

Renovation & Modernization, Uprating and Life Extension (RMU & LE) of the existing old hydro electric power projects is considered a cost effective option to ensure optimization of resources, efficient operations, and better availability and also to augment (uprating) capacity addition in the country.

Recognizing the benefits of R&M of hydroelectric power projects, the Govt. of India set up a National Committee in 1987 and a Standing Committee in 1998 and thereafter had identified the projects/ schemes to be taken up for implementation under R&M. The National Perspective Plan document for R&M of hydroelectric power projects in the country was also prepared in CEA during the year 2000.

I. INTRODUCTION –SALAL POWER STATION

Salal Dam सलाल बाँध (Salāl Bāndh), also known as Salal Hydroelectric Power Station, is a run-of-the-river hydropower project on the Chenab River in the Reasi district of the Jammu and Kashmir UT. It was the first hydropower project built by India in Jammu and Kashmir under the Indus Water Treaty regime.

The project is located on the Chenab River near the Salal village in the Reasi District, a few kilometers south of Matlot where the river turns to a southerly course. The Salal project was conceived in 1920. Feasibility studies on the project commenced in 1961 by the Government of Jammu and Kashmir and a project design was readied by 1968. Construction was started in 1970 by the Central Hydroelectric Project Control Board (under the Government of

India's Ministry of Irrigation and Power). The design of the project contained a two stage powerhouse generating 690 MW power making use of the head created by the dam. The original Indian design provided for a 130 meter-high dam up to an elevation of 1627 ft above sea level, a 40 ft gated spillway at the top (between elevations 1560–1600 ft) and six under-sluices at elevation 1365 ft.] The under-sluices would have enabled the 'drawdown flushing' of sediments. However, at Pakistan's insistence, the under-sluices were permanently plugged with concrete, and the gates were reduced from 40 ft to 30 ft. This meant that the only live storage is between elevations 1570–1600 ft, and the storage below that level has got silted up, forming an elevated river bed. The level of the bed now varies between 477 M (1,565 ft) and 484 M (1,588 ft).

Salal Power Station is run-of-the-river scheme with an installed capacity of 690 MW (Stage-I of 3 x115 MW & Stage-II 3 X 115 MW) to harness the Hydropower potential of river Chenab. It is located in Reasi district of Union Territory of Jammu & Kashmir. The project comprises a 118 m high & 630 m long rock fill dam and 113 m high & 486.75 m long concrete dam with 6 penstocks of 265 m length and 5.23 m diameter each. The surface power house with installed capacity of 690 MW houses 6 units of 115 MW capacity each designed to operate under the rated head of 94.5 m and designed to generate 3082 million units in a 90% dependable year with 95% machine availability.

Units I, II & III of stage-I were commissioned in the month of November 1987 and Unit IV, V & VI of Stage-II in the month of June 1993, March 1994 & February 1995 respectively. The beneficiary states/UTs of this power station are Chandigarh, Delhi, Himachal Pradesh, Haryana, Jammu & Kashmir, Punjab, Rajasthan, Uttrakhand & Uttar Pradesh.

Location	Distt. Reasi, Union Territory of J&K
Approach	Nearest rail head: Katra; Nearest Airport: Jammu
Capacity	690 MW (6X 115 MW)
Design Energy	3082 MU (90 % dependable year with 95% machine availability)
Beneficiary States/UTs	Chandigarh, Delhi, Himachal Pradesh, Haryana, Jammu & Kashmir, Punjab, Rajasthan, Uttrakhand & Uttar Pradesh
Date of Commercial Operation (COD)	Unit#1 - 20/11/1987, Unit#2 - 20/11/1987, Unit#3-20/11/1987 , Unit#4-01/07/1993, Unit#5-23/05/1994, Unit#6-01/04/1995

Dam	Rockfill dam: 118 m high, 630 m long Concrete dam: 113 m high, 486.75 m long
FRL	487.70 m
MDDL Max TWL	487.70 m 397 m
HRT	NA
Penstock	Diameter: 5.23 m, Length : 265 m
TRT/Tail pool length	Dia 11 m, Length (Stage-I: 2.463 Km , Stage-II: 2.527 Km) Type: Horse shoe shape
Power House	Surface (6 generating units of 115 MW each)
Type of Turbine	Francis
Rated head	94.5 m
Design discharge	824 cumecs (for all 06 units)
Number of guide vanes	24
Generator	
Rated Continuous output	127.8 MVA
Rated Voltage	11 ± 5 % kV
No of Poles	32
Rated speed	187.5 RPM
Direction of Rotation (From Top)	Clockwise
Run away Speed	375 RPM
Generator Step up Transformer (GSU)	
Type	Single phase, step up transformer
LV Rating	11 kV
HV Rating	220/√3 kV
MVA Rating	43.33 MVA
Type of cooling	OFWF
Switchyard/Pot head yard	220 kV Outdoor (Size: 65 m X 240 m)
Evacuation of Power	Through 220 kV transmission lines
	06 Lines: -Salal - Jammu (I &II) and Salal - Kishenpur (I, II, III & IV)

MONTH WISE DESIGN ENERGY OF SALAL POWER STATION

Sr. No.	*Month*	*Design Energy (GwH)*
1	*April*	*189.52*
2	*May*	*324.94*
3	*June*	*471.90*
4	*July*	*487.70*
5	*August*	*487.70*
6	*September*	*424.30*
7	*October*	*229.61*
8	*November*	*128.63*
9	*December*	*94.57*
10	*January*	*60.69*
11	*February*	*68.97*
12	*March*	*113.47*
	Total	***3082.00***

Generation year wise before the Renovation and Modernization work:-

Sr No.	Year	Target In Mu	Achieved in Mu	Target PAF	Achieved PAF
1	2007-08	3285.9	3231.64	97.54	98.19
2	2008-09	3236.1	3009.05	97.08	98.50
3	2009-10	3180	3024	62	59.50
4	2010-11	3176	3230	62	63.1
5	2011-12	3135	3219	60.5	63.7
6	2012-13	3112	3277	64	65.8
7	2013-14	3090	3235	60	67.6
8	2014-15	3182	3492	60	67.4
9	2015-16	3180	3591	60	70.9
10	2016-17	3280	3423	64.3	70.4
11	2017-18	3379	3247	65	76.2
12	2018-19	3300	3412	78	84
13	2019-20	3550	4010	81	97.4

Generation and PAF after the completion of the renovation and modernization work in 2019-20 in phased manner:-

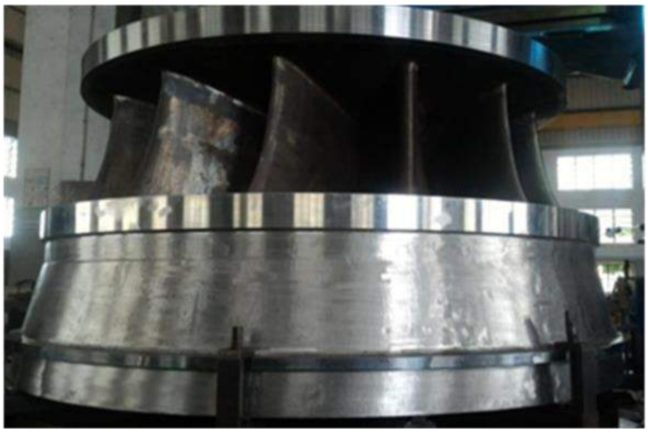
Sr No.	Year	Target in Mu	Achieved in Mu	Target PAF	Achieved PAF
1	2020-21	3850	3632	81	94
2	2021-22	3722	3485	81	89.8
3	2022-23	3718	3235	81	90

During the year, it was felt that the detailed improvements in the system with the modifications were needed for the enhancing the performance of 690 MW Salal Power Station as detailed below:-

a) Improved /modified runner for all the units.
b) New Digital Governor with modern features of automation
c) MOCB replaced with the SF_6 Breakers
d) Charging of 10 MVA 220/11 kV Power Transformer captive bay
e) Two no's of 1010 KVA DG SET installed at site.
f) SCADA arrangement for operation of all units and auxiliary supply set up.
g) Three layer pumping arrangement developed with flood dewatering pumps.
h) Gravity drain developed in the protection gallery to reduce the pumping load.
i) Choked interconnection of drainage sumps made through at Power House stage 1&2.
j) Brake arrangement modified with self double acting arrangement.

k) H.S. Lube system doubled arrangement to increase the reliability.
l) Fire fighting and CO2 system automated.
m) Modified L.P. Compressor.
n) Unmanned setup for the electrical network at Bidda and Dhyangarh.
o) Motorized valve for operating of cooling water flow to the units.
p) 42 No's of CT (Current Transformer) replaced with higher accuracy and class.
q) Flap gate arrangement at the Dam Site.
r) Modification in the supply arrangement for Jyotipuram colony via SCADA.

The details of the additional work as carried out:-



a) **Improved /modified runner for all the units: -** As per the model test carried out in USA with the higher capacity the modified runner were placed in all the six no's of turbine in phase manner for the enhancing the generation capability of all the existing units at Salal.

- ➢ Six Units of Salal Power Stations were designed for a rated head of 94.5 m.
- ➢ Due to reduction in head, Units were operating on off design conditions resulting in loss of energy and performance of units.
- ➢ Till 2016-17 during the peak season maximum Generation achieved was in the range 660-680 MW.
- ➢ To improve the performance of turbine units the Runner of all six units were replaced.

Modifications

- ➢ After installation of all 06 modified runners, the output of 115 MW can be achieved at 85 Meter Head with 90% Guide vane opening also the output has increased 5% additional Megawatt at 90 meter Head.
- ➢ The units are being operated with 5% additional MW during Monsoon period.
- ➢ Weight of New modified Runner is 27.5 Ton whereas weight of old Runner (BHEL) was 32.5 Ton.
- ➢ No. of Blades in new Runner is 13 whereas no. of blades in old Runner was 14.
- ➢ Discharge dia. for new Runner is 4175 mm where as discharge dia. for old Runner was 4092 mm.
- ➢ The height of new Runner is 2150 mm where as in old Runner was 1952 mm.

b) **New Digital Governor with modern features:-** All the existing old G 40 Governors were replaced by new digital governors in phase manner for the improvement in the performance of all the units with SCADA. During the modernization the reliability of the modified digital governors have increased overall performance of all the units with quick and easy synchronization.

c) **MOCB replaced with the SF6 Breakers:** - The old 1987 model MOCB were replaced with the SF6 quick acting breakers with the automated operating system of operation leading to significant contribution in the system improvement with reduction of downtime of outages.

d) **Charging of 10 MVA 220/11 kV Power Transformer captive bay:-** The captive bay at the Salal Power Station has made significant contributions to the readymade grid supply for the auxiliary system of the power station. This system enables the quick start/stop of the units with the reliable source of the power to the auxiliary demand of station load.

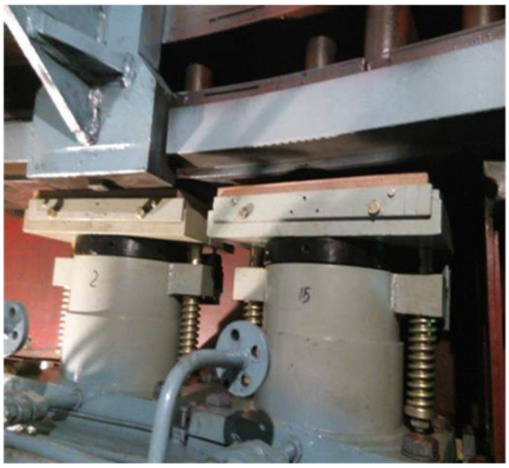
e) **Two no's of 1010 KVA DG Set installed at site: -** The two new 1010 KVA DG set were installed in the switchyard for the readiness of station auxiliary load demand. This has made the station trouble free in case of any crisis of power.

f) **SCADA arrangement for operation of all units and auxiliary supply set up:** The new Supervisory control and data acquisition system was installed for the operation of all units from the control room with the state-of-the-art facility of setting the load demand of units with the control and protection system. The SCADA system also sinks with the fire fighting system so that the fire system shall be activated in case of any eventuality. The all protection system checked with the wiring etc for the placement of SCADA Setup for all the units. The operation of the auxiliary load of the station is also set with the SCADA terminal operation window. This implementation leads to reduction of the control wiring inside the power house and also from the switchyard to the respective units.

g) **Three layer pumping arrangement developed with flood dewatering pumps:** - The three layers was developed to tackle any eventuality of flood circumstances in the power house. This setup is made with the ring main supply to the pumps for the operational requirement.

h) **Gravity drain developed in the protection gallery to reduce the pumping load**:- The gravity drain was made in the protection gallery so that the seepage water coming in this area shall directly fall in the tail pool area. Thus, the additional arrangement has made a significant contribution in the reduction of the pump load with the reduction in the auxiliary load of the station.

i) **Choked interconnection of drainage sumps made through at Power House stage 1&2.** The stage 1& stage 2 interconnecting drainage sumps were choked for several years, thus the efforts made to operationalized the interconnection line so that both the stages of the pumps may be used to clear the excess water from inside the power house.

j) 

Brake arrangement modified with self double acting arrangement:-The brake arrangement of the units has been modified with the self double acting arrangement for additional features for the quick stopping of the units.

k) **H.S. Lube system doubled arrangement to increase the reliability:**-The H.S lubricating system has been doubled with the taking care of reliable operation of the same. In case one of the pumps fails, the other gets operationalized as per the need of the system.

l) **Fire fighting and CO_2 system automated:** The firefighting and CO_2 system of power station has been automated with the SCADA Network. This setup has added advantage in case of any fire incident at generator, generator transformer or at critical items. The existing CO_2 fire fighting system installed at Stage I was more than 25 year old and obsolete. Considering the potential fire hazards & safety of the personnel, it was proposed to renovate the complete fire fighting system with modern features.

m) **Modified L.P. Compressor:** The low pressure (LP) compressor has been modified with automation of installation of lesser kW compressor, to reduce the energy consumption with more backup time. The setup has been made with the utilization of unused pressure vessels. The asset installed at the power house is more than 25 years old and thus has become obsolete and unreliable for operation. Therefore, proposed to replace the old LP compressors with a new 250 CFM capacity compressor.

n) **Unmanned setup for the electrical network at Bidda and Dhyangarh:** Due to technical advancement the network has been modified with shifting of transformers to one location at Jyotipuram and development of 11kV system with unmanned arrangement at Bidda and Dhyangarh with the additional network of CCTV.

o) Motorized valve for operating of cooling water flow to the units: The old manual valves for cooling water systems of stator and bearing coolers has been replaced with motorized valves with actuators and the command may be given directly from the Control room, this has added advantage in case of requirement of reverse cooling for the stator and bearing coolers.

p) CT replaced with higher accuracy and class: As per CEA Guidelines the "Energy accounting and Audit meters shall be of accuracy class of 0.2 and the accuracy Class of CT & VT shall not be inferior to that of associated meters". The associated meters (SEM) installed at Generator and Feeder of the generating station is of accuracy class of 0.2. Hence C.T of 0.2 Class is required to adhere to the guidelines of CEA. Accuracy class of existing CT was 1. Therefore, purchase of 42 nos. CT with better accuracy Class resulted in improved energy accounting.

q) Flap gate arrangement at the Dam Site. Loss of generation is occurring for cleaning of trash deposited during peak season. It was proposed that the design of radial gate no. 11 was modified to flap gate type so that trash can be flushed out from the reservoir easily by operating this gate and generation loss on account of trash choking is minimized.

r) **Modification in the supply arrangement for Jyotipuram colony:** Colony electrical network has been modified with standby arrangement with utilization of old non-performing assets and centralized power distribution arrangement with shifting of transformers from different locations to one location at Jyotipuram. The modification of the ring main system helps in restoration of power in case of any failure/tripping in the network.

REASON FOR THE UPGRADATION AND EASE OF OPERATION:

At the Salal Hydroelectric Plant, located on the river Chenab in Northern India having high silt prone area. The refurbishment of the runners, originally installed between 1987 and 1995, became necessary due to erosion damages that have been caused by the silty waters of the Himalayan Rivers. The six runners were manufactured and delivered gradually to reconnect the units to the grid step by step.

BENEFITS OF UPGRADATION:

In view of the details submitted and facts, the modifications at Salal Power Station at various stages contributed the overall improvement in the performance of the plant load factor with the enhancement of generation and reduction in the outages. This also helps in the reduction of outages and in efficient manner the operations is carried out with the implementation of SCADA in all units. The Total MW capacity of the Salal (6x115MW) stations has been improved by way of technical up-gradations as stated for the overall improvement in the performance of the station.

- The units are being operated with 5% additional MW during Monsoon period.
- The Total MW capacity of the Salal (6X115MW) stations has been improved from 660 MW to 744 MW and achieving high reliability of the station.
- The replacement of AVR with the DVR has also contributed in smooth functioning of the excitation system with access control to each thyristor bridge, fault detection and trouble shoot as per the operational aspect.
- Installation of new brake dust collector made the inside the generator barrel clean that leads to easy dissipation of heat inside the stator windings.
- The old DCDB- I &II for Stage 1&2 were commissioned with mother plant were more than 20 years old. DCDB-I was used for control and protection of Generating Units & All Lines DCDB -II was in use for control and protection of Generating Units only. During few past years modernisation and upgradation work carried out in the Powerhouse, Dam, Switchyard.
- Further SCADA system is being implemented in the Powerhouse.
- The old DCDBs were having malfunction problem and insufficient to meet the requirement of new schemes, i.e., extra supply lines, redundancy of independent source of DC supply, availing feedback from modules. New DCDBs having sufficient number of outgoing feeders along with few spare feeders of desired ratings is required with features for providing arrangement of auto change over & parallel operation of both incoming feeders along with potential free auxiliary contact in MCBs/ MCCBs.
- In view of the modifications and up gradation for various parts and equipment at Salal Power Station, contributed the overall improvement in the performance of the power plant load factor with the enhancement of station output.

BIOGRAPHIES

Sh. Dharmesh Kumar Singh was born in Fathepur, Uttar Pradesh in the Aug 1973 having master degree in Control and Instrumentation Engineering from Motilal Nehru Regional Engineering College(MNREC), and BE(Elect & Electronics). He joined NHPC Limited in the Nov 1998 at Salal Power Station as a Trainee Engineer and worked mainly in the field of Operation & Maintenance at the Salal (690MW) J&K, Chamera-I(540MW) HP, Nimmo Bazgo (45 MW) Leh and Parbati-III(520MW) HP Power Stations with the technical audits of NHPC operating stations. At present working as Group Senior Manager IT&C Division for the cyber security of NHPC Power Stations and also associated for the cyber security activity for the CERT Hydro for 35 No's of hydro Power utilities as per the guidelines of CEA.

Setting the Standard for Automation™

ISA Delhi Section

O-PAS™ and Reliance Industries Limited

Vaibhav Yagnik

ISA-D: "Petroleum & Power Automation Meet-2023" (PPAM-2023)

1

Agenda

ISA Delhi Section

1. Introduction to RIL
2. RIL pain points to join OPAF
3. OPAS Introduction
4. Adaption Scenarios
5. OPAS for existing facilities
6. RIL participation updates
7. Wrap Up

2

2

Disclaimer

Any statement, opinion, prediction, comment, or observation made in this presentation/publication are those of the presenter/author only and in no condition should be construed necessarily representing the policy and intent of Reliance Industries Ltd. (RIL).

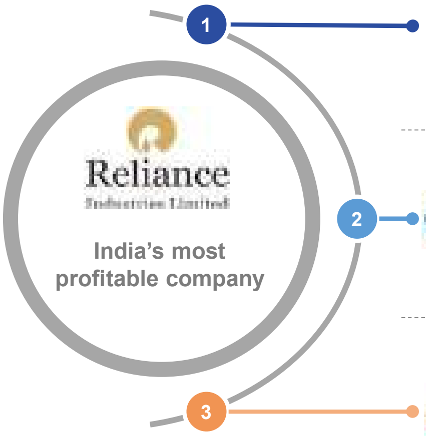
The information presented herein are of the presenter/author's own and in no way RIL attracts any liability for any inconsistency or irregularity in terms of the accuracy completeness, veracity, or truth of the content of the presentation/publication. In addition, RIL shall not be liable for any copyright infringement and misrepresentation for the presented content as the content is presumed in good faith to be a creation of presenter's/author's own mind.

The scope of this presentation/publication is strictly for knowledge sharing purposes and not necessarily to provide any advice or recommendation to the audience/readers. Any endorsement, recommendation, suggestion, or advice made by the presenter/author shall be in his personal capacity and not in professional capacity as an employee of RIL. Any person acting on such endorsement, recommendation, suggestion, or advice will himself/herself be responsible for any injury/damage.

3

3

New Reliance for a New India



O2C

Largest and most complex single site refinery at Jamnagar with 1.4 MMBPD crude refining capacity; **vertically integrated** portfolio across O2C value chain, among **lowest cost positions** and **global top 10 rankings in key products**

Jio-bp 51:49 fuel retail JV

A **global leader** and one of the **long-term winners**

Largest digital services provider in **India – 419.9 mn subscribers** (Jun'22)

1st operator[1] to **cross** 400mn subscribers in a **single country market**

Strategic investment by **Facebook & Google** and investments by **marquee financial investors** totaling to **$20bn for ~33% stake** in Jio Platforms Limited

Largest Organized Retailer in India

208 mn registered customer base with **a diversified product portfolio** of groceries, fashion & lifestyle, consumer electronics and connectivity across **15,866 stores across 45.5 mm sq. feet** (Jun'22)

Investments from Silver Lake Partners, KKR, GA, TPG, Mubadala, GIC, PIF and ADIA totaling **~$6bn for ~10% stake** in Reliance Retail Ventures Limited

Three mega growth engines and a strong liquid balance sheet

- Note: Exchange rate used: US$1 – INR 78.9725; [1] Outside China; [2]

 4

4

Phenomenal Growth Journey – Now A Top 100 Global Company

Reliance Industries Limited

Fortune Global 500 – 155th

Market Cap CAGR – 31% | Earnings CAGR – 25%

1977-80 — $ 0.01 Bn
- IPO

1981-90 — $ 0.1 Bn
- Patalganga Complex
  - PFY
  - PSF
  - PTA
  - PX

1991-2000 — $ 4 Bn
- Cracker and Polymers @ Hazira
- Fiber Intermediates @ Hazira
- Jamnagar supersite - Integrated refinery & petrochem complex
- GDR Issue
- 50/100 Years Yankee Bond
- Upstream – PMT

2001-2010 — $ 50 Bn
- Jamnagar refinery & petrochem complex – 2
- Fortune Global 500
- IPCL acquisition
- Acquired broadband spectrum
- Launch of Reliance Retail
- KG-D6 discovery & commencement of production
- Recron Malaysia

2011-20 — $ 93 Bn
- Ethane project, ROGC, Gasifiers commissioned
- Innovative financing – perpetual bond, EXIM facilities
- Launched Jio, all-IP digital network
- India's largest Rights Issue
- Largest capital raise through asset monetization across Jio, Retail and fuel retailing
- KG D6 new production system

2021-22 — $ 230 Bn
- Retail crosses 15,000+ stores, 193 million customers
- Jio crossed 400+ Mn subscribers
- JV with ADNOC
- Launch of New Energy & New Materials
- Acquired REC Solar
- First ever jumbo US$ Notes issuance from India

Note: CAGR since IPO

5

Reliance's Vision to be Net Carbon Zero by 2035

Reliance Industries Limited

Opportunity to accelerate New Energy and New Materials businesses based on RIL's vision of clean and green development

- **Integrated Solar Photovoltaic module factory**
  - Establish and enable at least 100GW of solar energy by 2030
- **Advanced Energy Storage Battery factory**
  - Collaborate with global leaders in battery technology to achieve the highest reliability round-the-clock power availability
- **Electrolyser factory**
  - Manufacture modular electrolysers of highest efficiency and lowest capital cost
- **Fuel Cell factory**
  - Fuel cell uses oxygen from the air and hydrogen to generate electricity, emitting non-polluting water vapour

Deploy next-gen technologies to combat climate change

6

Growth Engines for Sustainable Value Creation

- **Best-in-class** digital services with pan-India all-IP mobile and FTTH connectivity
- Focus on **subscriber ramp-up**, **enterprise solutions**, **narrow-band IoT** and scaling-up of digital platforms

- Reliance is well-placed to leverage its online ecosystem and offline network to **maximize the reach across India's consumption strata**
- **JioMart** to create value for entire retail ecosystem by **partnering with** small merchants, kiranas and farmers

Reliance O2C

- **World-class, integrated O2C platform to sustain growth and profitability** through demand and commodity cycles
- O2C to maximize downstream, reduce transportation fuels and **create clean and green energy platforms**

New Energy

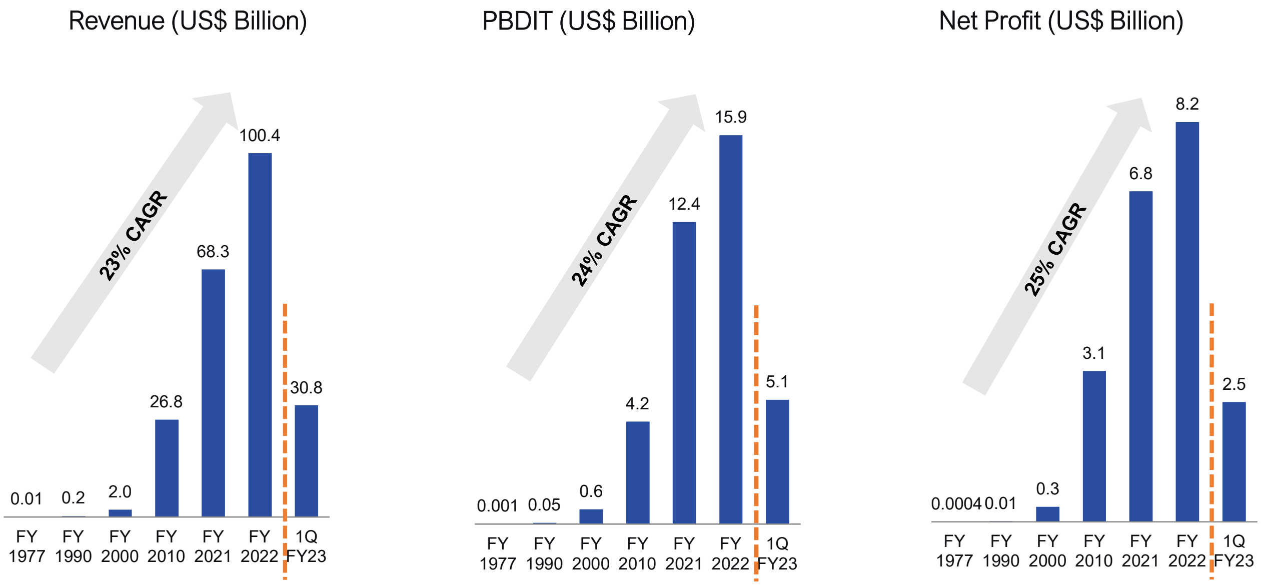
- Next big value creation engine – **New Energy and New Materials business**
- Technology and innovation focused partnerships in New Energy to achieve **Net Carbon Zero** by 2035

Multiple engines of growth with focus on consumers and technology

 7

7

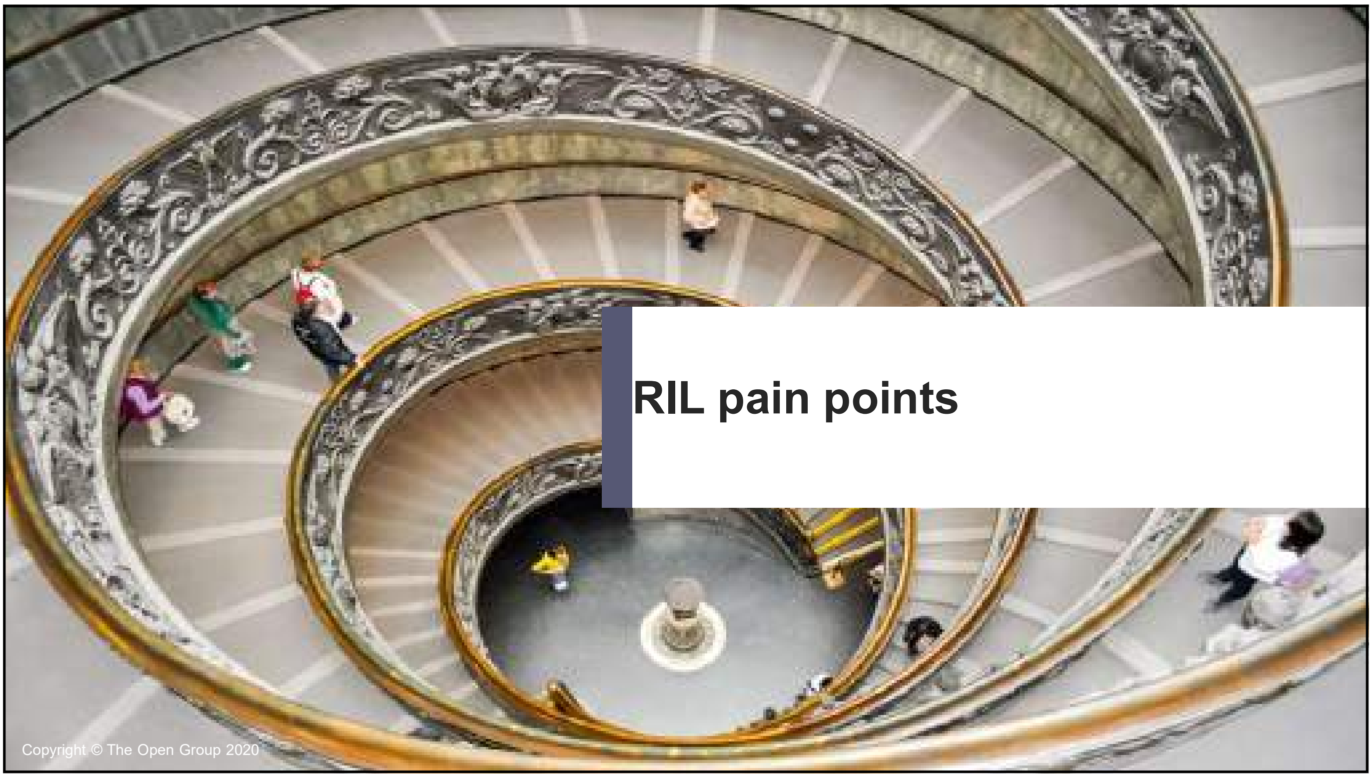
Robust and Consistent Earnings



Note: US$1= INR 78.9725, CAGR since IPO in 1977

 8

8



9

RIL pain points

Reliance
Industries Limited

RIL owns multiple Refinery, Petrochemical and Polyesters sites with 5000+ control systems running.

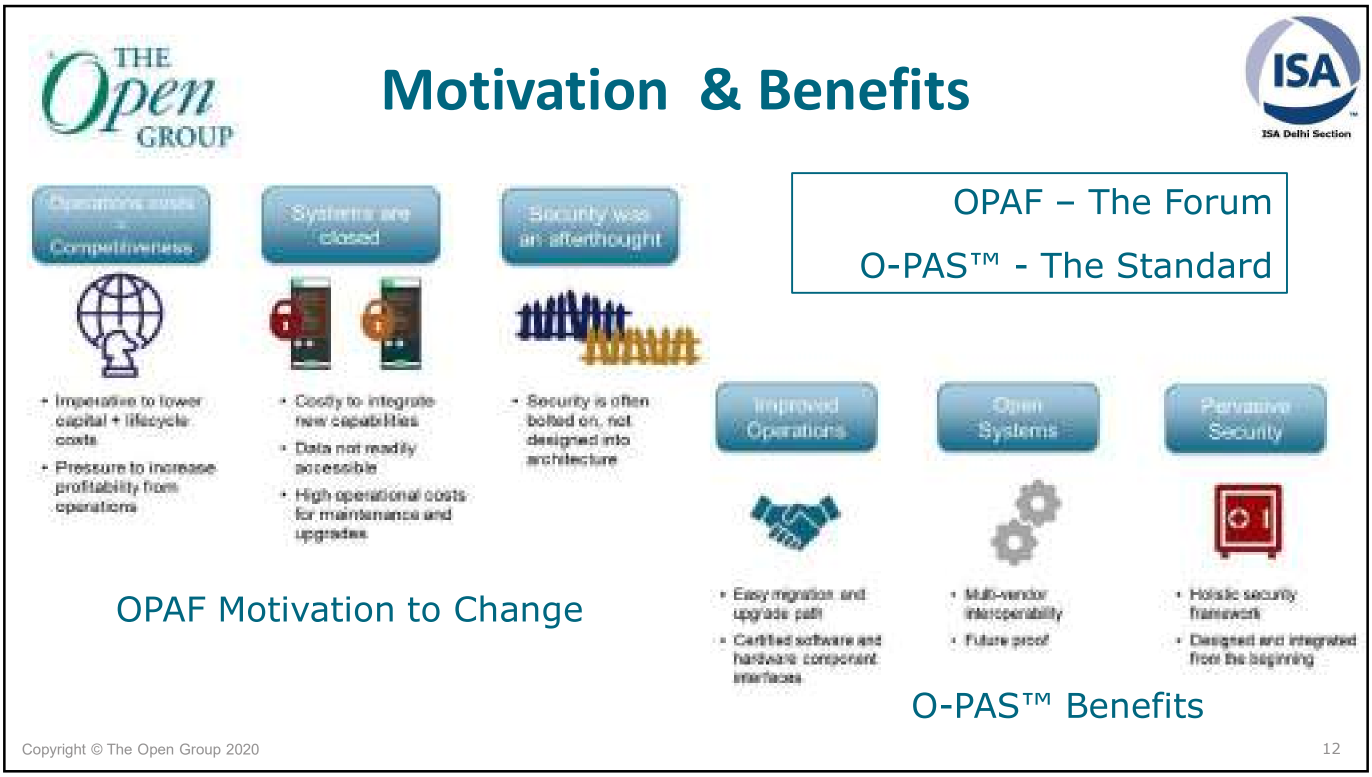
- Digital transformation needs more and better data – Constrained with legacy systems.
- New features can't be introduced in legacy systems w/o upgrade.
- Frequent obsolescence of Microsoft OS → No patches available for OS after obsolescence and security vulnerabilities remains unaddressed → Upgrade requires Front end upgrade leading to firmware upgrade in Backend leading to shutdown requirement (Min requirement)
- Shutdown frequency - ranging from 3 to 7 years → Upgrade requirement comes up every 5 ~ 6 years considering OS obsolescence.
- Cross platform upgrade → Protection of Intellectual Property (IP).
- Very high cost of upgrade → Reduced profit margins.
- Competency building up for new systems.
- Bolt on Cyber Security.

 10

10


OPAS Introduction
Copyright © The Open Group 2020

11


THE Open GROUP
Motivation & Benefits
ISA
ISA Delhi Section
OPAF – The Forum
O-PAS™ - The Standard
Operations costs = Competitiveness
Systems are closed
Security was an afterthought
• Imperative to lower capital + lifecycle costs
• Pressure to increase profitability from operations
• Costly to integrate new capabilities
• Data not readily accessible
• High operational costs for maintenance and upgrades
• Security is often bolted on, not designed into architecture
OPAF Motivation to Change
Improved Operations
Open Systems
Pervasive Security
• Easy migration and upgrade path
• Certified software and hardware component interfaces
• Multi-vendor interoperability
• Future proof
• Holistic security framework
• Designed and integrated from the beginning
O-PAS™ Benefits
Copyright © The Open Group 2020
12

12

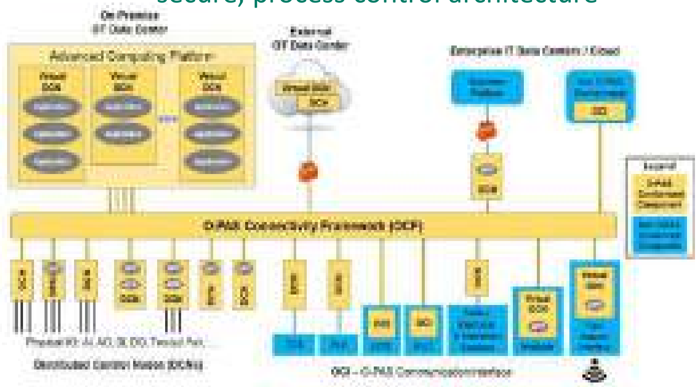
Transforming Process Automation

- Reduce cost of control system upgrade or replacement
- Increase value generation by removing barriers to technology insertion
- Design for adaptable cybersecurity

~~Proprietary Interfaces~~

Use Standards; e.g.
IEC 61131
IEC 61499
IEC 61850
IEC 62443
IEC 62541
IEC 63131
MTP
NOA
...

OPA Vision: Open, standards-based, interoperable, secure, process control architecture



13

13

Industry Engagement is the Key to Success

100+ Members in Open Process Automation Forum

20+ Hardware / Software Suppliers

5 Major DCS Suppliers

10 End-User Collaboration Partners

7 Announced Development Test Systems

Collaboration Partners

14

O-PAS™ Versions

Version	Year	Theme – Open, multi-vendor control system
V1	2019	Interoperability
V2	2020	Configuration Portability
V2.1	2022	Control Functionality
V3	**2023+**	**App Portability, Orchestration & Physical Platform**

Application Portability

Ensures **end users** have the ability to move their apps, whether custom developed or vendor provided, from platform to platform, as well as to use any process automation software, regardless of vendor.

System Orchestration

Ensures the ability to select and implement O-PAS certified products from multiple suppliers and to be assured those products will coexist seamlessly in a unified open process automation system.

Physical Platform

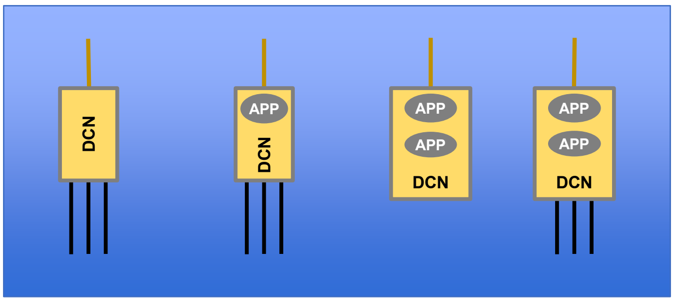
Ensures **end users** have the required degree of openness, interchangeability, interoperability and security across platforms within the system.

15

The O-PAS™ Standard V2.1 enable Products

- Development of software products triggered by V2.1
- Interoperability workshops allows for testing of supplier’s technologies in a safe environment
- End User test beds help establish product demand
- Certification provide confidence and supports commercial adoption

OPAF Certification Program supports a multivendor marketplace of O-PAS Products



16

16

O-PAS™ Certification

Overview

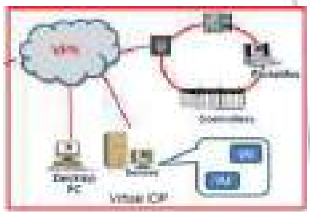
- Formal validation process managed by The Open Group
- Voluntary, paid service offering which enables Suppliers to have their products tested for conformance to O-PAS Standard
- Tests are executed at 3rd party labs accredited by The Open Group
- Products that demonstrate conformance to 100% of the O-PAS requirements receive Certification & are listed in the OPAF Certified Product Registry (Only Certified Products Listed)
- Certification Releases via Waves; Wave 1a in-progress!

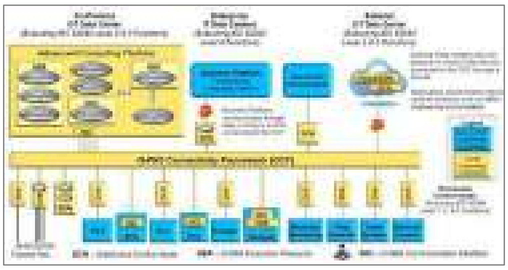
17

17

Interoperability Event (IOP)

- What is an IOP?
  - Vendor testing against each other
  - Usually physical connection
  - Virtual network configuration
- When did we have one?
  - June 2019 for O-PAS V1.0
  - January 2022, for O-PAS V2.1





18

18

Interoperability Event (IOP)

- Results:
  - 14 Organizations
  - Many profiles tested
  - Vendor found and fixed issue in product
  - Minor specification issue also identified
  - Feedback more IOPs needed

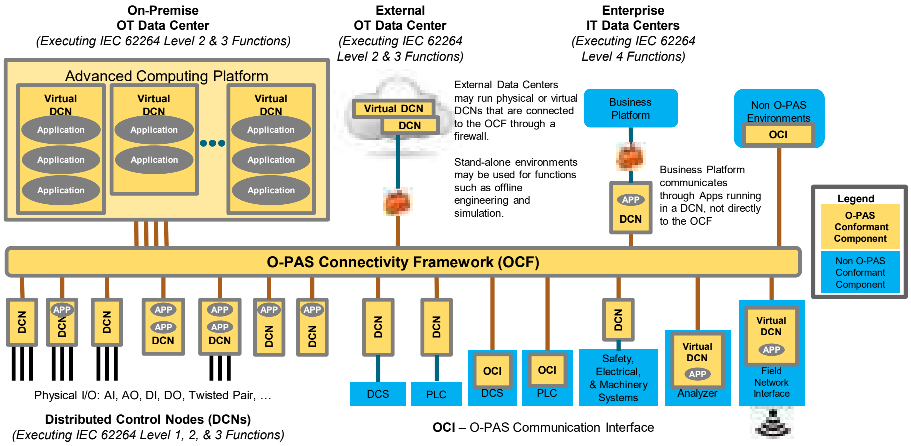
19

19

20

Concept Diagram of Process Automation System of O-PAS Components

ISA Delhi Section

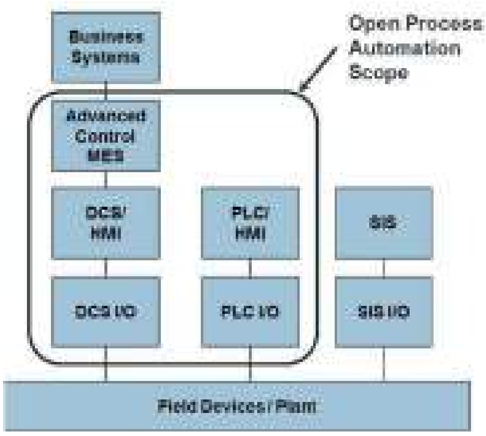


21

21

OPAF Scope: Core Automation System

ISA Delhi Section

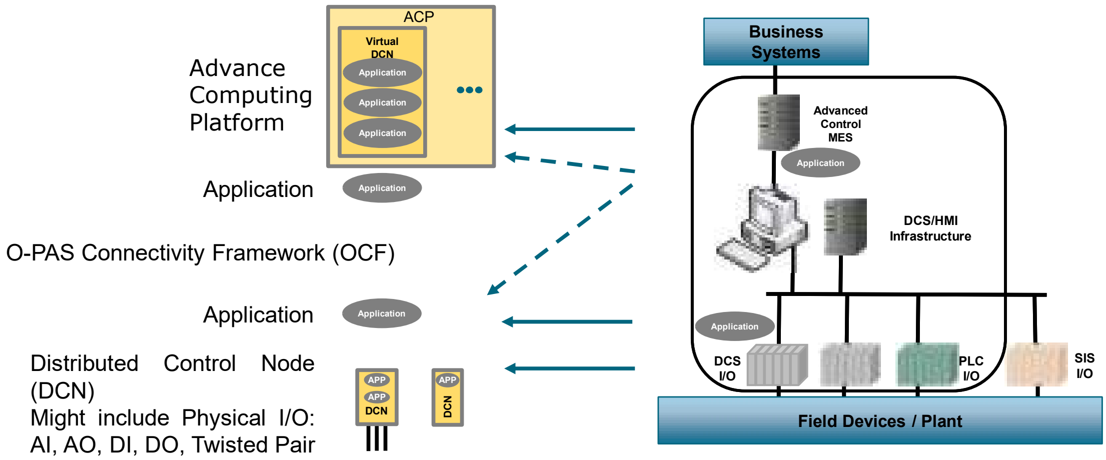


Term	Description
MES	Manufacturing execution system
DCS	Distributed control system
HMI	Human-machine interface
PLC	Programmable logic controller
SIS	Safety instrumented system
I/O	Input / Output point

22

22

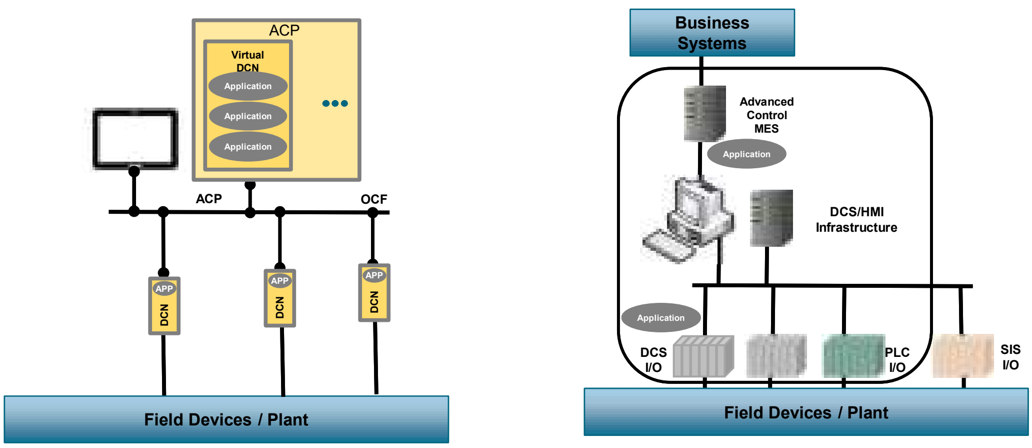
Traditional Automation System



 23

23

Gaining experience with O-PAS



OCF: O-PAS Connectivity Framework

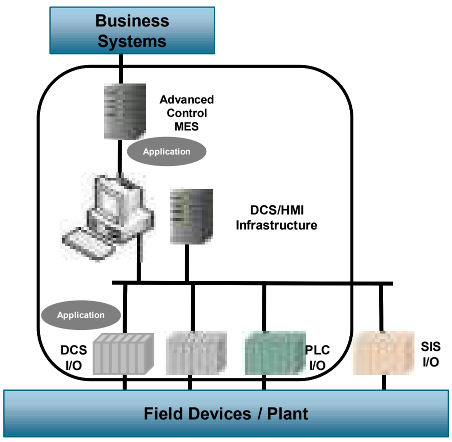
 24

24

O-PAS for existing facilities

25

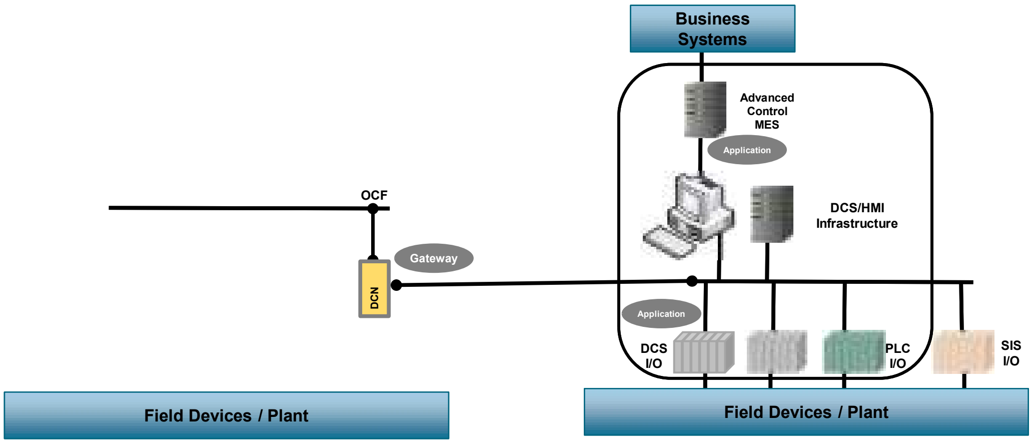
Getting Started



26

26

Getting Started

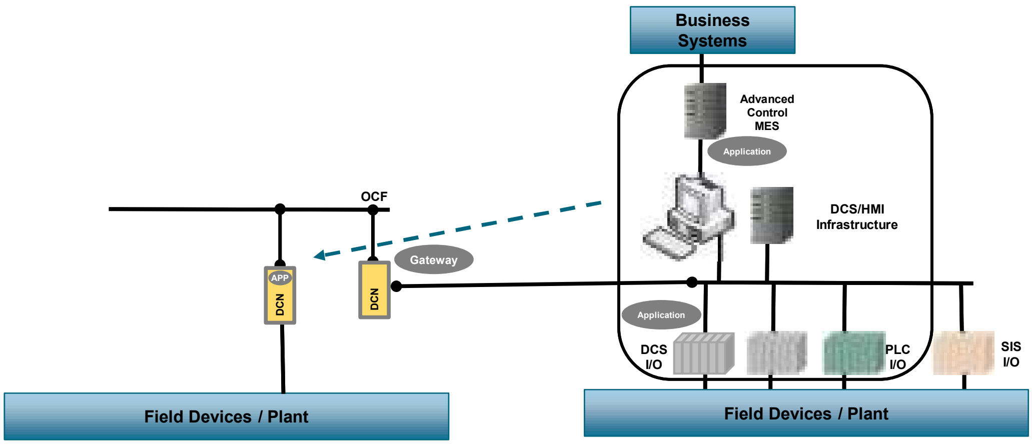


OCF: O-PAS Connectivity Framework

 27

27

Getting Started

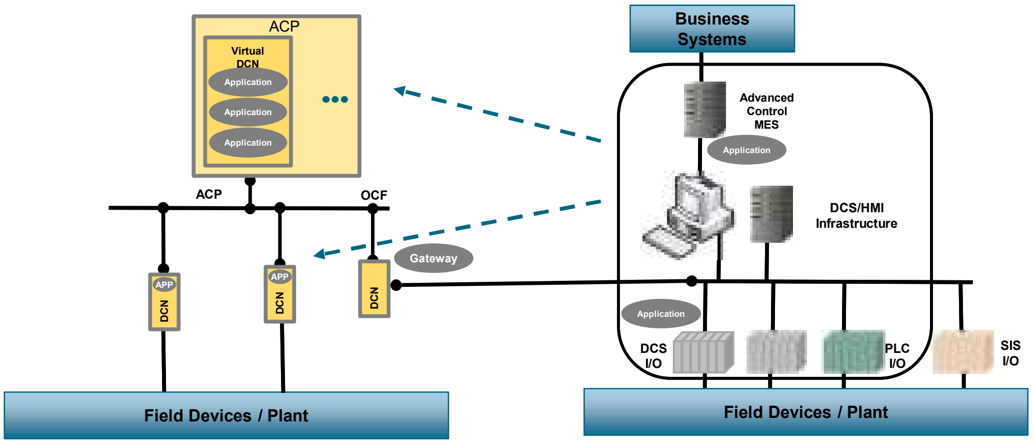


OCF: O-PAS Connectivity Framework

 28

28

Getting Started

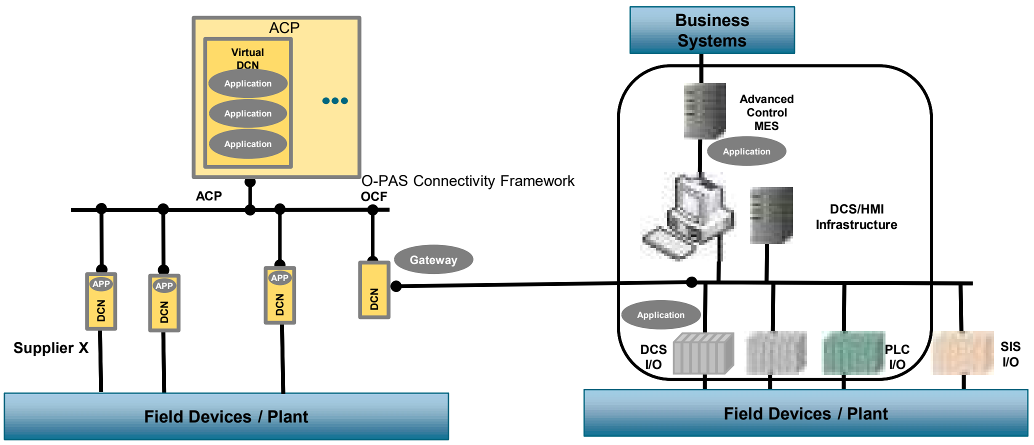


OCF: O-PAS Connectivity Framework

29

29

O-PAS system lifecycle benefits

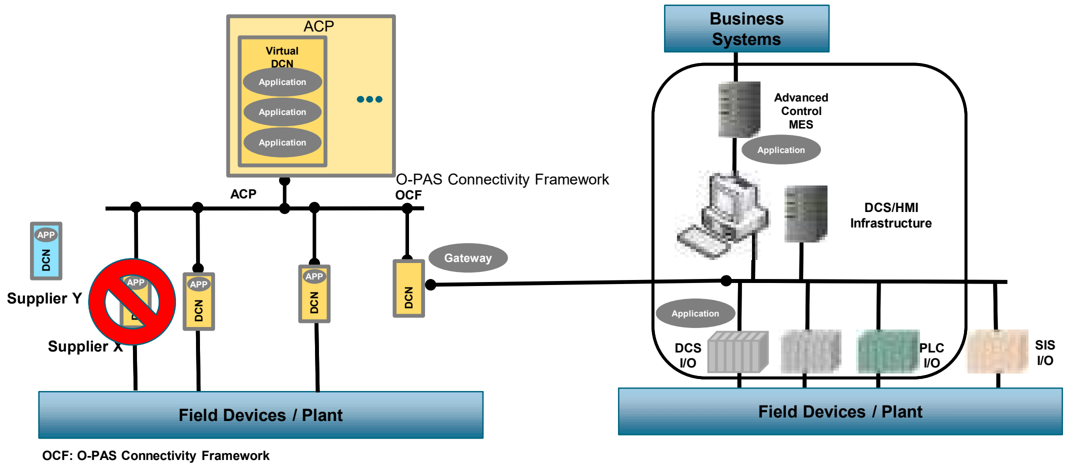


OCF: O-PAS Connectivity Framework

30

30

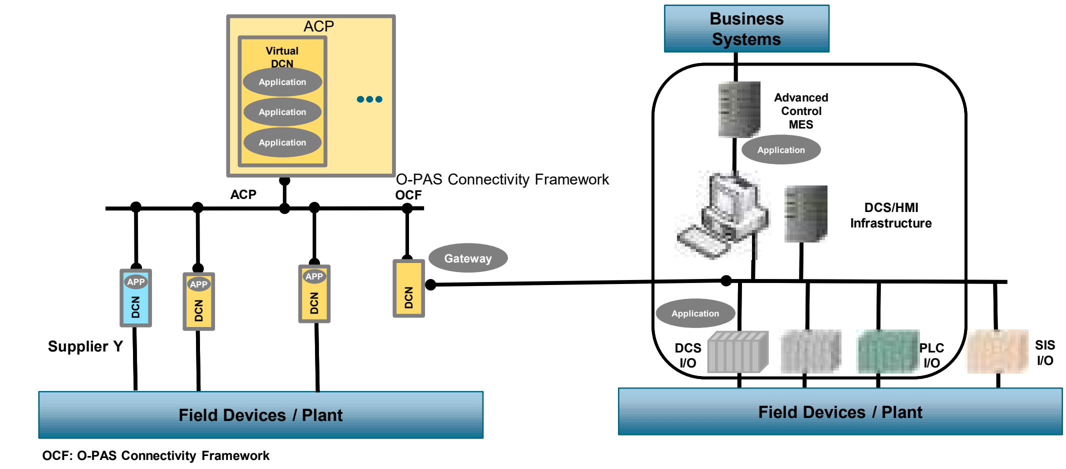
O-PAS system lifecycle benefits



 31

31

O-PAS system lifecycle benefits



 32

32

33

RIL Participation in OPA

Reliance
Industries Limited

- Dedicated RIL OPA Team – 13 members
- OPAF participation
  - Participated in Function Block subcommittee
  - Participates in Security subcommittee
- Periodic meetings –
  - Review and discuss OPA forum meetings' MOM and recordings
  - Review and Discuss OPA standards
  - Review and discuss Use cases for Test bed
- Participated in End user caucus and provided excellent inputs for HMI portability and Orchestration.
- Participated in outreach activities – ARC Forum, Automation Expo South
- Planning to participate in ISA activities

 34

34

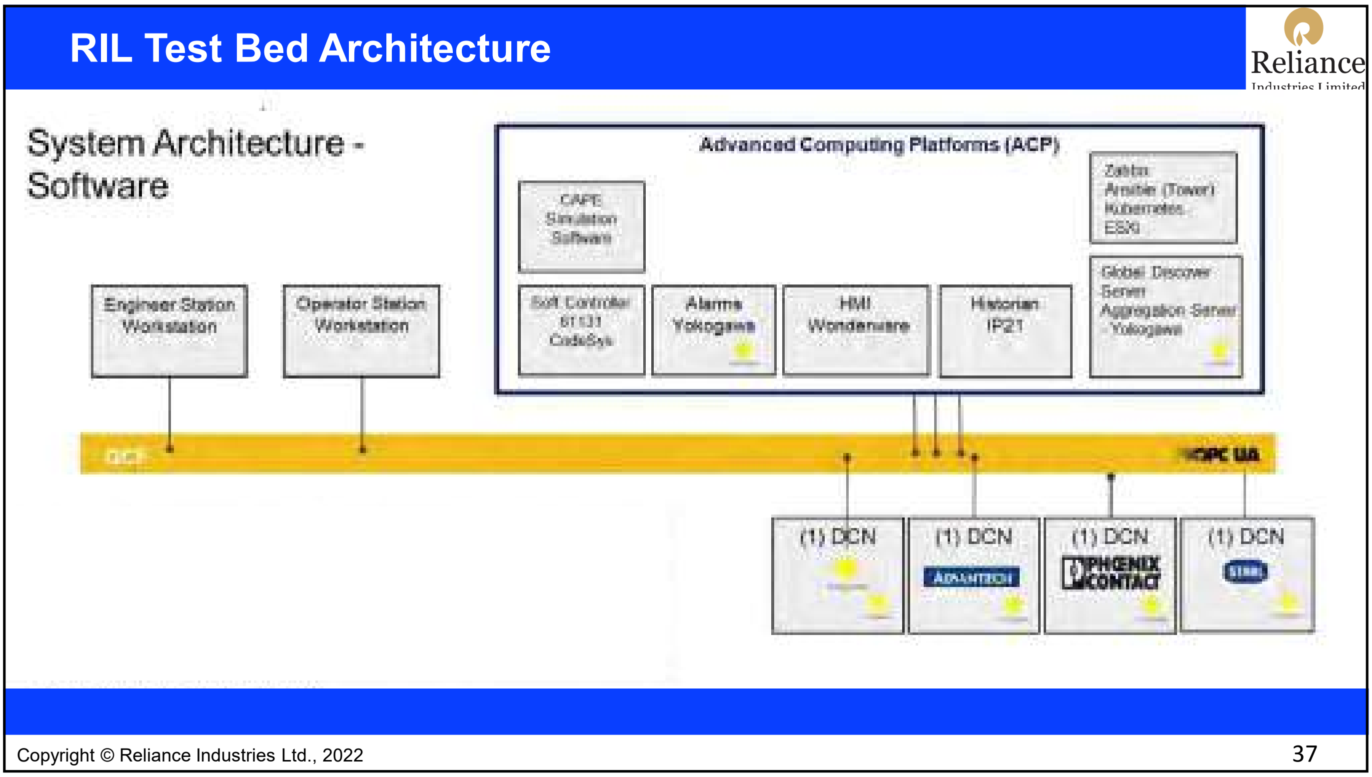
RIL & Collaboration Partners

- Collaboration partners – ExxonMobil, Aramco, BASF, Dow, Shell, Georgia Pacific, ConocoPhillips, Linde – Meeting every month
  - Partners providing updates on Test Bed
  - Integrating products of more and more vendors in Test Bed and sharing critical findings
  - Discussion on common topics of Interest
  - Discussing on future topics – HMI portability, Integration requirement of PLCs/ESDs, Fast MPC
  - Collaboration partners are working together to develop use cases of interest, and drive user requirements so that the standards are fit for purpose.

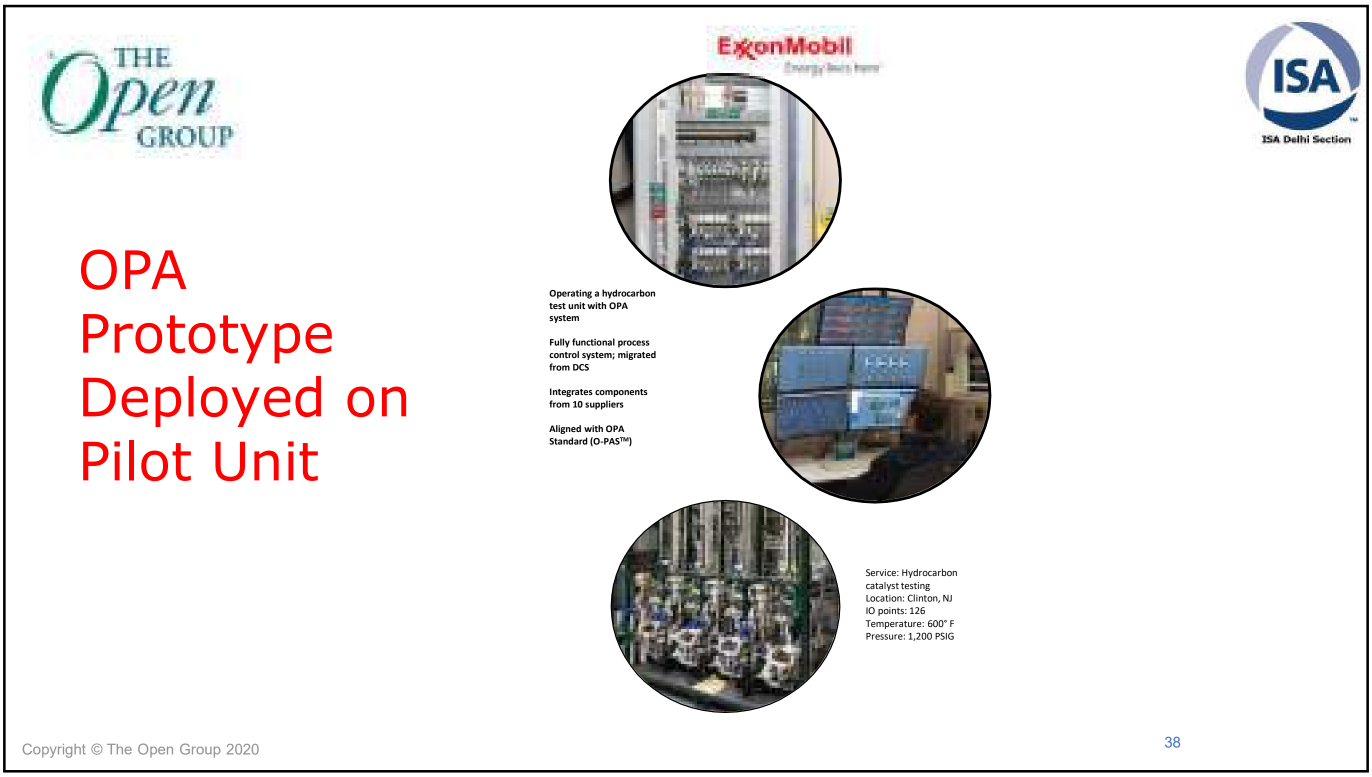
RIL Test Bed Updates

Planned to put Test Bed at Jamnagar Refinery site

- Selected Hardware and Software for Test Bed
- Yokogawa selected as System integrator for Test Bed.
- Test Bed – phase 1 implementation by Q3 2023
- Use cases and RIL requirements prepared to be tested with Test Bed
- On successfully meeting criteria, test bed will be expanded
- Final aim to put test bed for Field Trial in non-critical process application


RIL Test Bed Architecture
Reliance
System Architecture - Software
Advanced Computing Platforms (ACP)
CAPE Simulation Software
Zabbix
Ansible (Tower)
Kubernetes
ESXi
Soft Controller 61131 CodeSys
Alarms Yokogawa
HMI Wonderware
Historian IP21
Global Discover Server
Aggregation Server - Yokogawa
Engineer Station Workstation
Operator Station Workstation
OCF
OPC UA
(1) DCN
(1) DCN
ADVANTECH
(1) DCN
PHOENIX CONTACT
(1) DCN
Copyright © Reliance Industries Ltd., 2022
37

37


THE Open GROUP
ExxonMobil
ISA
ISA Delhi Section
OPA Prototype Deployed on Pilot Unit
Operating a hydrocarbon test unit with OPA system
Fully functional process control system; migrated from DCS
Integrates components from 10 suppliers
Aligned with OPA Standard (O-PAS™)
Service: Hydrocarbon catalyst testing
Location: Clinton, NJ
IO points: 126
Temperature: 600° F
Pressure: 1,200 PSIG
Copyright © The Open Group 2020
38

38

BASF “Clear Water“ Demo at 2019 NAMUR conference

ISA Delhi Section

BASF goals:

Agile proof of concept with real components and an uncritical process

“Success of OPAF initiative becomes more and more likely”

Open Automation Demonstrator for Chemical Industry
Nov 7, 2019

Courtesy: BASF

39

ExxonMobil open system prototype deployed on pilot unit

Operated hydrocarbon test unit with Open system

Fully functional process control system; migrated from DCS

Integrates components from 10 suppliers

Aligned with Standard (O-PAS™)

Service: Hydrocarbon catalyst testing
Location: Clinton, NJ
IO points: 126
Temperature: 600° F
Pressure: 1,200 PSIG

ExxonMobil
Energy lives here

40

40

End User collaborative development & field trials

2019-2020 | 2021+

Test Bed / Design → Build

User 1 → Field Trial
User 2 → Field Trial
⋮
User N → Field Trial

Collaborative Development

Individual Field Trials
Multiple system integrators

Collaboration Partners:

Aramco Services Company, Reliance, ExxonMobil, BASF, GP Georgia-Pacific, ConocoPhillips, Dow, Linde

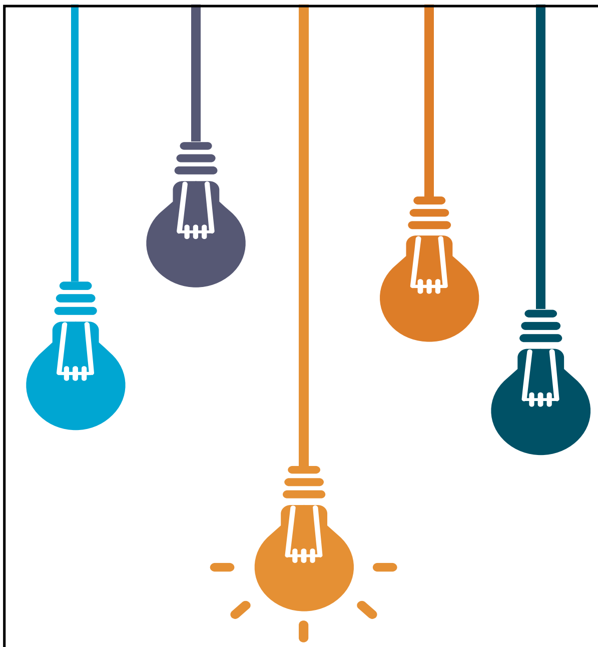
- Use O-PAS™ standards as available
- Multiple, parallel field trials
- Share non-competitive learnings among collaboration partners
- OPA Test Bed with Yokogawa for systems integration operational in The Woodlands, TX

ExxonMobil
Energy lives here

41

41

42



Summary

Change to process automation industry is here !

Open Process Automation Standard (O-PAS^{TM}) provides foundation for open, interoperable, secure systems

OPAF provides roadmap for business and technology ecosystem
Your company and industry needs an active voice to represent and defend your interests

Significant progress is being achieved- systems have been built from Proof of Concept to actualization in test beds

End users, system integrators and suppliers need to work adoption into their plans

43

43

Reliance
Industries Limited

Thank You

44

44

Dated 03rd, May 2023

Technical Paper for Petroleum and Power Automation Meet 2023 from

Fluke Technologies Pvt Ltd.,

(Global Leader in Manufacturing Testing and Measuring Instruments)

Fluke Corporation is a Global leader in manufacturing industrial test, measurement, and diagnostic equipment. Found in 1948 by John Fluke Sr., Fluke has helped define and grow a unique technology market, providing testing and troubleshooting capabilities that have grown to mission critical status in manufacturing and service industries. Fluke products are extensively used in Power, O&G, Metals and other heavy industrial segment.

From industrial electronic installation, maintenance and service to precision measurement and quality control, Fluke tools help keep business and industry around the globe up and running.

Fluke has achieved the top position in every market in which it competes. The Fluke brand has a reputation for portability, ruggedness, safety, ease of use and rigid standards of quality.
A wholly owned subsidiary of Fortive Corporation (NYSE: FTV), Fluke is a multi-national corporation headquartered in Everett, Washington, USA. Manufacturing centers are in the USA, the UK, Asia, and The Netherlands. Sales and service subsidiaries are in Europe, North America, South America, Asia, and Australia.

Market Segments
The Fluke product lines are beneficial for professionals in a variety of markets. Primary segments are listed below and include a brief description of the types of Fluke tools used along with their typical applications.

<u>Calibration</u>
Fluke has acquired global leadership position in the calibration marketplace with products in the line of Electrical, Temperature, Pressure, Flow, RF & Software. The Fluke Calibration line of calibrators, standards, calibration software products, and support equipment provide exacting standards for companies and government organizations who rely on tightly calibrated instruments for their quality and standards programs, as well as to meet strict international quality requirements.

<u>Industrial/Electronic Service Installation and Maintenance</u>
Today, electronics are integrated into an increasing number of electrical and electro-mechanical systems. Fluke's comprehensive line of digital multimeters, electrical power analyzers, thermal imagers, insulation resistance testers, accessories, plus the integrated ScopeMeter™ handheld test tools, are being used by a growing number of service technicians, plant engineers and installation and maintenance technicians. These tools provide them the ability to troubleshoot these complex new systems and detect problems quickly.

What is Calibration ?

- **Calibration is the activity of checking, by comparison with a standard, the accuracy of a measuring instrument of any type.**
- **It may also include adjustment of the instrument to bring into alignment with the standard.**

What are calibration standards?

Calibration standards are master instruments which can either be of measuring or sourcing standard that are more accurate than the devices that requires to be calibrated in a particular discipline. The standard’s accuracy varies depending on the Unit under test that needs to be calibrated; most professionals recommend using a calibration standard that is at least four times more accurate than the device being calibrated.

How Fluke implements the IIOT in providing best Testing & Calibration Solutions :

Fluke calibration products are built to be interfaced with a host at a high speed using LAN / RS232 / GPIB communication interface. The products are developed with remote protocols and drivers that helps software to easily communicate with the product for a bi-directional communication. Fluke Calibration, Asset Management and Reporting software helps performing Automatic Calibration and customized report generation. Asset Management tool pushes an auto-mail when any product / Device under test gets due for calibration. Workflow management module can be integrated with this software to track the product status once it is received in the lab for calibration until it is sent back. The calibration data gets stored in a database which gets installed over a server enabling the authorized once to access the calibration reports remotely.

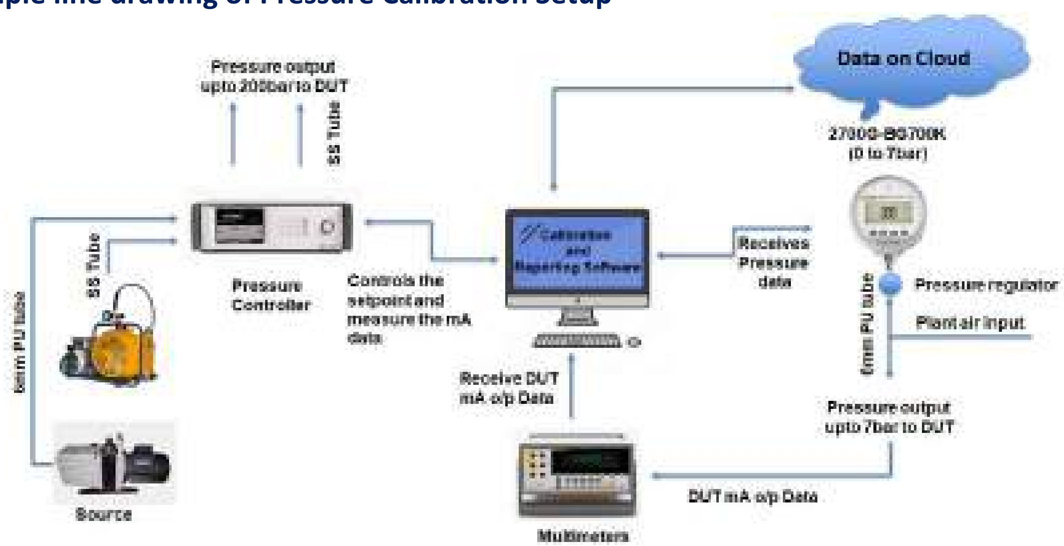
Our customers also get the Automation touch with portable products as Fluke field instruments comes with latest cutting edge technology known as Fluke Connect™. This software collects, stores and makes viewable machine data from more than 80 Fluke tools and sensors. Measurements can now be stored in the cloud, where teams can always access the data on their smart device or computer. Whether the maintenance and reliability team is gathering data from condition monitoring sensors or from portable test tools, they now have all the data they need to make critical decisions and complete necessary jobs. Some of the key features includes Taking live readings on-the-go, Trending and graphing data, Receiving alarms from anywhere, etc.

Make in India

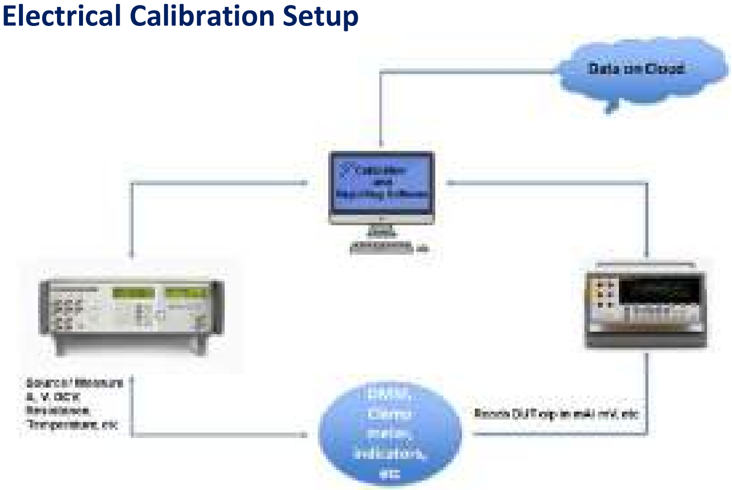
Fluke develops software solutions and test benches in India with a focus on Make in India Initiative.

Illustrations :

Sample line drawing of Pressure Calibration Setup



Sample line drawing of Electrical Calibration Setup



The Industrial Internet of Things (IIOT) the concept of interconnected applications, equipment, and technology- is more than just an abstraction. The IIOT is the idea that connections between the digital (e.g., mobile devices and computers) and physical worlds (e.g., plant equipment and test equipment) improves information exchange.

The practical applications of IIOT to plant operations may not seem clear at first, but when compared to more traditional methods of tackling operational challenges at the plant, the advantages become evident.

One way to understand the key differences is to compare two approaches to three-phase motor failure -- smart technology versus traditional analysis.

The problem: Three-phase motor failure

As often happens, a plant faces a problem motor, one that has been replaced twice in the past six months. Finding the root cause of motor failure is the task at hand. After finding that the insulation in the windings is breaking down, the technicians at the service shop think the motor might be running hot. They are not sure if is being caused by electrical power quality problems, mechanical wear or environmental or operational stresses that degrade the motor performance. It's therefore determined that a team is needed to collect current, voltage, power quality and temperature measurements in order to isolate the fault and identify the root cause.

What types of calibration standards does Fluke Calibration manufacture?

Fluke Calibration manufactures multiple types of calibration standards as below:

Temperature calibration standards

- Standard platinum resistance thermometers
- Temperature baths and furnaces (Liquid / Dry)
- Multifunction Calibrators
- Super Thermometers
- Multichannel Temperature Scanner / DAQ
- ITS-90 fixed-point cells
- Maintenance apparatus
- Liquid nitrogen comparison calibrator
- Resistance bridges
- Standard resistors and much more.

Pressure & Flow calibration standards

- Piston gauges
- Deadweight testers
- Pressure controllers and calibrators
- Pressure comparators and digital pressure gauges
- Portable/handheld pressure calibrators
- Flow calibration standards

Electrical & RF calibration standards

- Multi product calibrator
- Oscilloscope Calibrator
- 8.5 digit multimeter
- Primary Standard AC / DC Source etc
- Power & Energy Calibrator
- RF Calibrators and Sensors

Conclusion:

One accurate
measurement
is worth
a thousand
expert opinions

A trusted calibration means less worry, fewer questions and more time being productive.

Accurate and stable calibration equipment impacts business results (e.g. quality, efficiency, less waste)

Fluke latest technology products and solutions:

- Enhance the Operational Efficiency by providing automation
- Error free calibration since less manual activity involved.
- Increase productivity as the DUT's are communicated bi-directionally.
- Ensures Proactive and Predictive maintenance with asset- management.
- Improves Customer Service with Live status tracking & access to reports through cloud systems.
- More Connected Devices with data on cloud for continuous monitoring
- Process Data Management

  And much more!!

**** END ***

INCREASING POLYMERIZATION REACTOR EFFICIENCY THROUGH AI/MACHINE LEARNING

Sh. Ashok Kumar, Manager (PC O&M)
GAIL (INDIA) LIMITED, NEW DELHI
E-Mail: akumar07@gail.co.in

KEYWORDS
Artificial Intelligence, Machine Learning, Deep Neural Networks, Digital Twin, Analyzers, Industry 4.0, Regression, Decision Tree, Polymerization Reactors

ABSTRACT

The quality of the product output from the Refining Equipment is totally dependent the feed quality it is getting as an input. The key components in the measurement of feed composition of inputs as well as the output is the Analysers. there are vast variety of Analysers available in the market today like gas Chromatographs, Liquid chromatographs, NDIR analysers and analyser probes for O2, humidity etc. the accuracy of measurements from these instruments depends upon a lot of factors. There are higher chances of getting errors in the results. These errors contributes huge losses in terms of ENERGY, EQUIPMENT Refining EFFICIENCY, degraded Product Quality and Financial losses. One old approach to overcome this Particular Problem is by installing redundant system of Sample Analysers but this Approach requires huge capital cost and Increased Maintenance man hours. So this Paper discuss about an alternative solution to this using Artificial Intelligence/ Deep Learning in Digital and Data Driven way. The AI/ deep learning Solutions discussed in this paper overcomes the shortcoming of old Approach. The Paper primarily focused on the application Deep Learning Algorithms like Linear regression, KNN model, Decision tree Regression, random forest regression and Neural net Regression to PREDICT the INPUT and OUTPUT feed composition measurement of a refining equipment/Reactor as it is done by the Analyser system. This approach acts as a Redundant to analyser system in case the Physical Analyser has breakdown. The AI that is making the Predictions is trained and made robust using PAST historical data. The Case considered in this paper is of Gas phase, FLUIDIZED bed Technology based polymerization REACTOR which produces LLDPE (linear low Density polyethylene) and HDPE (high Density Polyethylene) as a product. The Reactor considered is of LLDPE-2 unit Of GAIL (India) Limited, PATA petrochemical complex. The INPUT Parameters that the AI will be predicting will be like mole percentage of Ethylene ,1-Butene , Hexane , Hydrogen, Methane, Nitrogen, pentane etc. the OUTPUT parameters that the AI model will Predicting will be like MI(melt index) and Density of polyethylene powder produced by the reactor. The AI model is

applicable to any polymerization reactor when trained for particular environment variables. The Potential benefits of the Technology is that it eliminates the Capital cost required to setup a redundant product and Feed quality analysis system. AI models Trained robustly gives more accurate results than the Physical Analysis system hence they improve REACTOR efficiency. It's also improves the Energy efficiency of the REACTOR by eliminating the Poor quality production due to Analyser system breakdown. The system acts like DIGITAL TWIN of Physical Analysers thus a significant step towards INDUSTRY 4.0.

INTRODUCTION

Oil and Gas Sector Comprises Range of Energy Intensive Industries at Each levels i.e. Upstream, Midstream and Downstream. In order to make the Fossil fuel available for final consumption as a Fuel certain amount of Input energy is consumed for its processing. The Downstream section of Oil and gas sector deal with the final processing of hydrocarbon to meet the quality required for further applications. Hence this section is most energy intensive and quality sensitive. The Efficiency of downstream processing section plays a vital role in reducing the energy consumption. Hence an energy efficient Processing will result in less carbon foot printing also less CO2 emissions per ton of hydrocarbon processed. Product quality and Production downtime are vital parameters to achieve energy Efficiency. If production downtime is reduced as well as quality of the product is superior then ultimately it will lead to higher energy efficiency as well as higher equipment/plant life. This paper primarily focuses on improving efficiency of polymerisation reactor of a Petrochemical plant which falls under downstream industries. This paper talks about improving the Production quality by improving reactor feed component measurement through advanced technologies such as ML\AI, Big Data Deep Learning, Digital Twining, Cyber physical systems. We will also see how these technologies could be leveraged to reduce downtime. These discussed technologies could also be leveraged as a tool for RCA (root Cause Analysis) of analytical Measurement system breakdown. Traditionally we use Analysers or redundant Analysers for the measurement of feed components to a Polymerisation reactor or Processing Equipment. There are variety of Analysers available with us like Gas Chromatographs, Liquid Chromatographs, PH, moisture Analysers etc. Measurements of these analysers tells us Feed characteristics. If these measurement Instruments malfunctions or have a breakdown then this severely affects production, production quality, production efficiency and energy loss. Traditionally we use an approach of making these systems redundant that is also a capital intensive and less robust. This paper proposes alternative approach that is more robust and also uses current technology trends of INDUSTRY 4.0. In a Data driven way.

This paper proposes a framework for Machine Learning-based Analytical Measurement system, which is distinguished from traditional perspectives. This framework eliminates the dependency on expert experience and knowledge. Industrial historical data are utilized to iteratively generate dynamic models according to the changes in environments. This study provides solutions to and a reference for industrial big data analysis and model training, especially in the petrochemical industry. The

framework and approach proposed in this paper can be generalized to other petrochemical manufacturing industries to introduce a new way to improve their economic benefits through improved Analytical measurement. Gas Chromatographs are mainly focused in this Paper.
The paper is further divided into Main content that talks about Machine learning, digital twin, Existing analyser setup, Parameter selection for Analyser modelling, Data Collection process, Data Cleaning process, Machine learning Models, Model training, prediction by models, then comes the Analysis\observations , Results and recommendation.

MAIN CONTENT

The Design of Polymerisation reactor in the any Petrochemical Industry mainly depends upon the type of technology that have been adopted i.e. any one from solution phase, slurry phase and Gas phase. The polymerisation reactor considered as a subject for this paper is of GAS PHASE FLUIDIZED BED reactor. The Reactor produces Polyethylene in powder form which is separated using its product Discharge system. The reactor takes Ethylene as monomer, 1-Butene as Co-monomer, hydrogen, nitrogen, N-pentane and ISO-pentane as raw inputs. The especially developed Ziegler-Natta Catalyst is used for polymerisation. UNIPOL- UNIVATION, USA is Licensor of the Plant. It has a Name plate capacity of 400KTA. The Polymerisation reactor can produce both HDPE (high density Polyethylene) as well as LLDPE (Linear Low Density Polyethylene) grades. Two Basic Schematics of the Reactor as below.

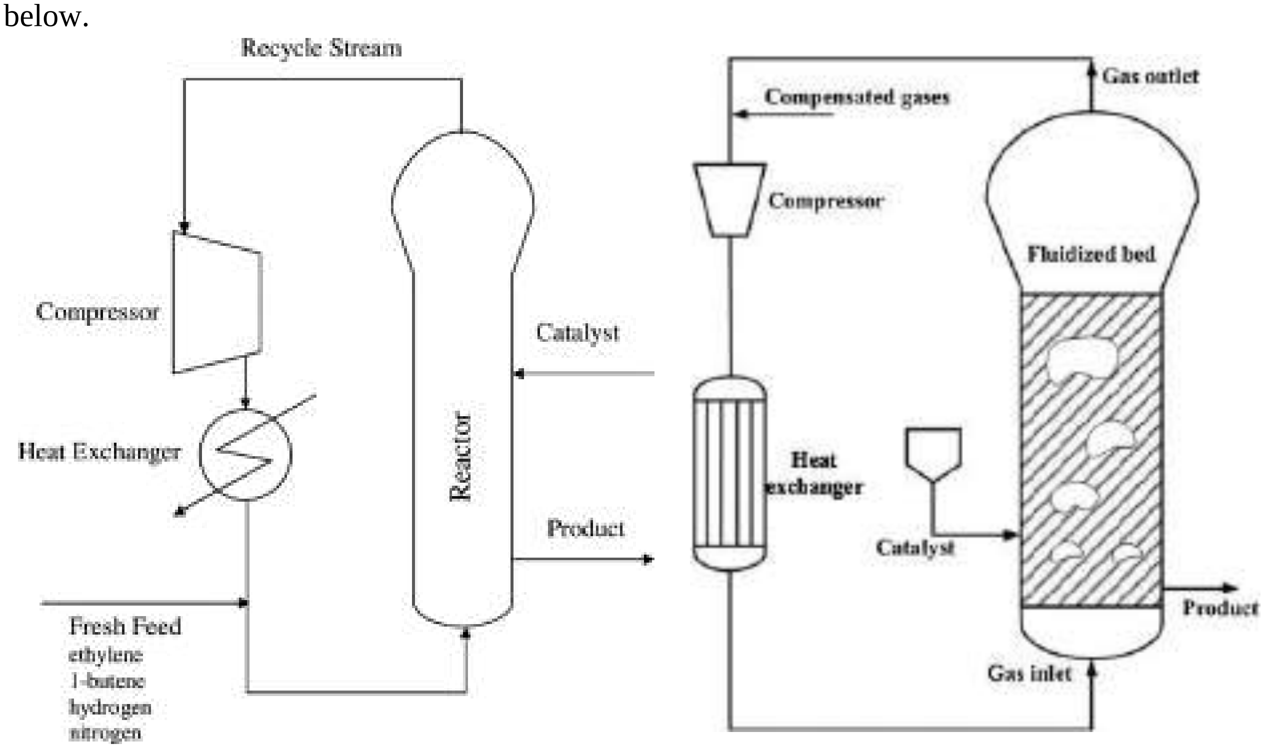


FIGURE-1: REACTOR SCHEMATIC DIAGRAMS

It can be seen clearly the raw inputs are freshly feed to the existing Recycle loop of the reactor as per the first schematic. The Analytical measurement takes place from recycle loop as discussed further.

EXISTING ANALYSER SETUP AND FEED MEASUREMENTS

Analytical Feed Composition measurement system consists of two Gas Chromatographs. These gas Chromatographs continuously take fresh sample of Recycle loop of Reactor for measurements of Feed Composition in mole percentage. The Output of these Analysers is electrical in nature which is fed to DCS for monitoring and control of reactor and Polymerisation reaction. Below mentioned schematic explains more clearly. Mole Percentage of Ethylene, 1-Butene, Hydrogen, nitrogen and Pentane/ICA is measured by These Analysers.

Thus Availability and Accuracy of these analysers is crucial for production and Product quality. There are multiple factor that can be seen in schematic that affects Gas chromatographs accuracy like components of Primary Sampling system, secondary Sampling system, oven temperature, sample pressure, filtering system and significant others.

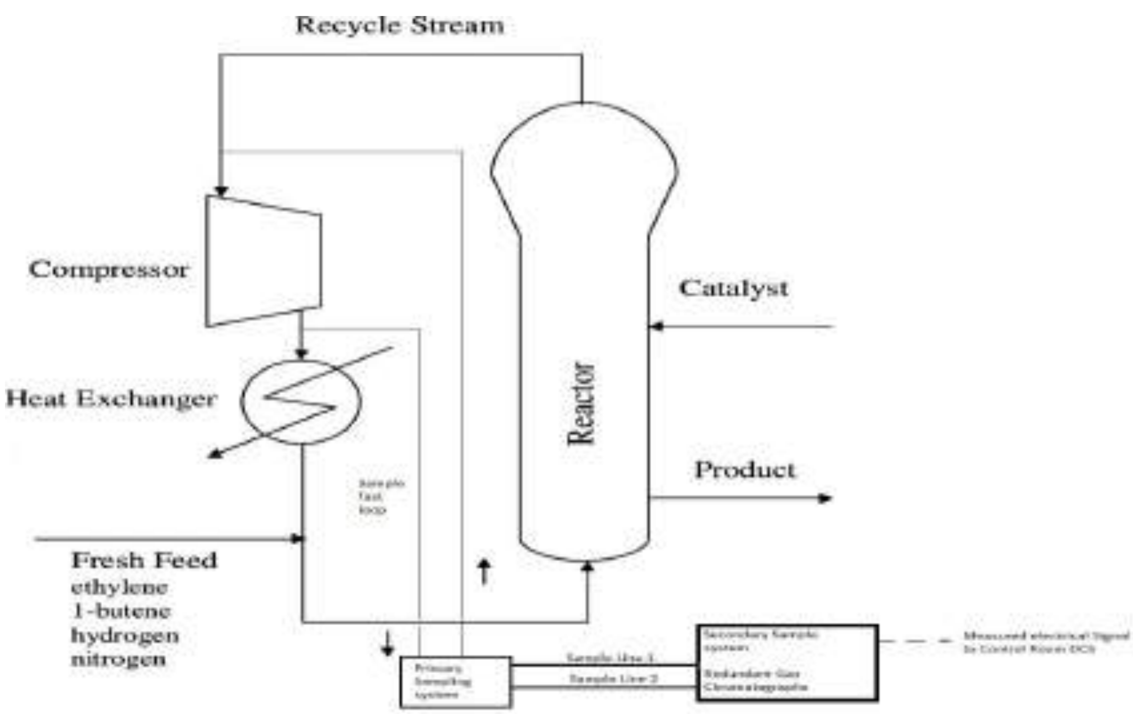


FIGURE-2: FEED COMPOSITION MEASURMENT SETUP

MACHINE LEARNING AND DIGITAL TWINS

Machine learning (ML) is a field of inquiry devoted to understanding and building methods that 'learn', that is, methods that leverage data to improve performance on some set of tasks. It is seen as a part of Artificial intelligence (AI). Machine learning algorithms build a model based on sample data, known as training data, in order to make predictions or decisions without being explicitly programmed to do so. Machine learning algorithms are used in a wide variety of applications, such as in medicine, email filtering, speech recognition, agriculture, and computer vision, where it is difficult or unfeasible to develop conventional algorithms to perform the needed tasks. Machine learning can be divided further into Supervised Learning, Unsupervised Learning, Re-enforcement Learning and dimensionality Reduction etc. this paper will make use of supervised machine learning Algorithms.

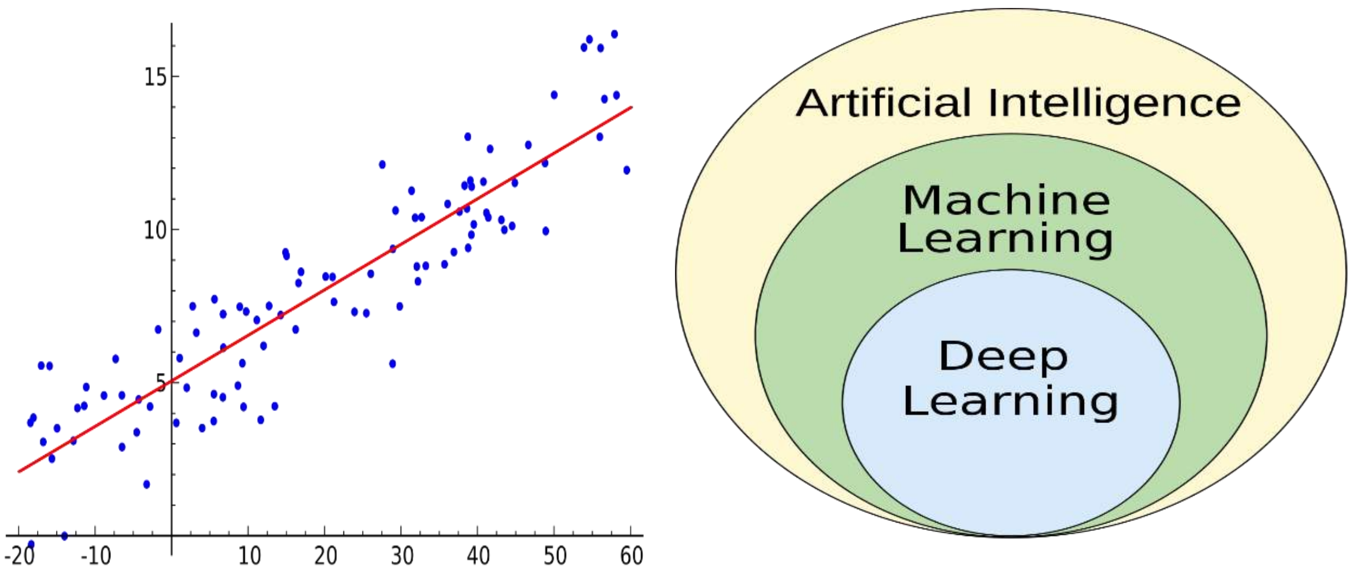


FIGURE-3: MACHINE LEARNING ALGORITHMS

Digital twinning uses AI, machine learning, and IOT (Internet of Things) technologies to create a digital copy, or model of physical objects, processes and systems. They are designed to be as close to their originals as possible, regarding their properties and behaviours, and use real-time data from sensors to constantly update themselves to reflect any changes of their real-world twin. Digital twins can also be used to test a number of scenarios without the limitations, costs or consequences of doing the same thing in the real world. Industrial applications of this technology are used to forecast and analyse future situations to predict possible risks. This makes it useful for improving production efficiency, production planning, and machine functionality. The model developed in this paper can be deployed as a Digital Twin of existing Analyse System. The deployed model will get real time data of feature variable as inputs to predict composition of feed similar as a normal physical analyser does.

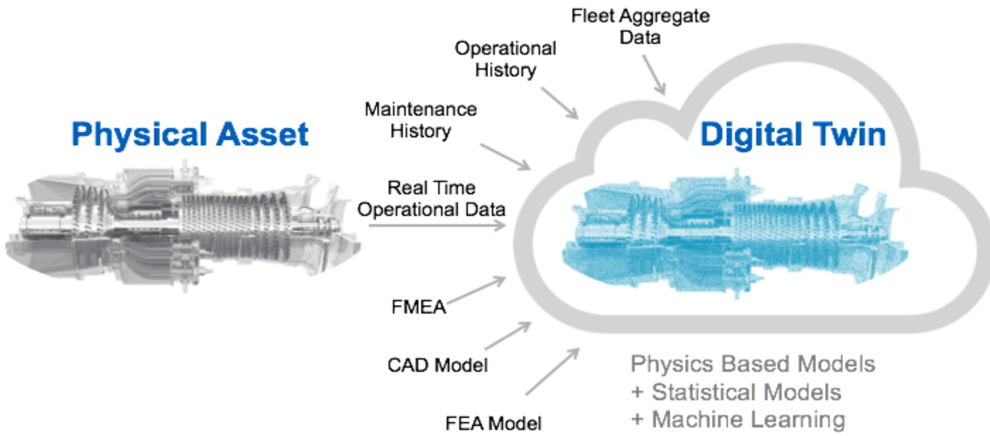


FIGURE-4: DIGITAL TWIN

IDENTIFICATION AND SELECTING PARAMETERS FOR ANALYSER VALUE PREDICTION MODELS

Parameters are most crucial part of any Machine Learning model since the model prediction accuracy also depends upon how correlated the selected parameters are. In this model of Analysers, that is going to predict the mole percentage composition of feed components. Following are the parameters that are most relevant as feature inputs for the reactor and Recycle loop gas composition.

- ✓ ETHYLENE FEED FLOW
- ✓ NITROGEN FEED FLOW
- ✓ COMONOMER FEED FLOW
- ✓ ICA FEED FLOW
- ✓ HYDROGEN FEED FLOW – LOW CV
- ✓ HYDROGEN FEED FLOW – HIGH CV
- ✓ RECOVERED LIQUID FEED FLOW
- ✓ PPB FLOW
- ✓ REACTOR PRESSURE
- ✓ REACTOR TEMPRATURE
- ✓ REACTOR BED WEIGHT
- ✓ REACTOR CYCLE GAS FLOW
- ✓ PURGE HEADER FLOW

Parameters that the Model will be predicting as Targets or outputs are as follows:-

- ✓ NITROGEN MOLE %
- ✓ H2 HIGH MOLE %
- ✓ H2 LOW MOLE %
- ✓ CH4 (METHANE) MOLE %
- ✓ C2H6 (ETHANE) MOLE %
- ✓ C2H4 (ETHYLENE) MOLE %
- ✓ C4H8 (1- BUTENE) MOLE %
- ✓ C4 INERT MOLE %
- ✓ N-C5 PENTANE %
- ✓ ICA MOLE %

After Selection of Parameters for Supervised machine learning model the next steps are collecting the data of selected variable from DCS (distributed control System) HISTORIAN for a selected time.

DATA COLLECTION FROM EXISTING STORAGE HISTORIAN

Since the model is supervised machine learning model hence the model needs to be trained. To train the supervised machine learning model its needs a lot of data. In this case the data that we are extracting from the HISTRIANs will be our training data as well as the test data to test the model. The historical data from historian was collected in CSV file for both Feature and target variables as mentioned above. There were a total of 65535 SAMPLES with a sampling period of 5 minutes. The period we selected was of 8-months starting from April to December of 2021 for which the plant was under production.

EXPLORATORY DATA ANALYSIS (EDA)

Exploratory Data Analysis refers to the critical process of performing initial investigations on data so as to discover patterns, to spot anomalies, to test hypothesis and to check assumptions with the help of summary statistics and graphical representations. The data that was collected from HISTORIAN will be analysed with the help various Data Analysis techniques as Discussed below.

PAIR PLOTTING THE EXISTING DATA EDA-1

The first exploratory data Analysis that was done on the data was to pair plot all the variables including features and targets. SEA BORN package in python was used to pair plot each variable with respect to each other to see what type of distribution they follow and if there are any outliners present inside our data. The following is multivariable distribute of the data. There are two images shown below.\the first image is pair plot of 23 variables with respect to themselves hence created a matrix of 23x23 plots. The second image shows the zoomed version of first in which we can see actual distribution.

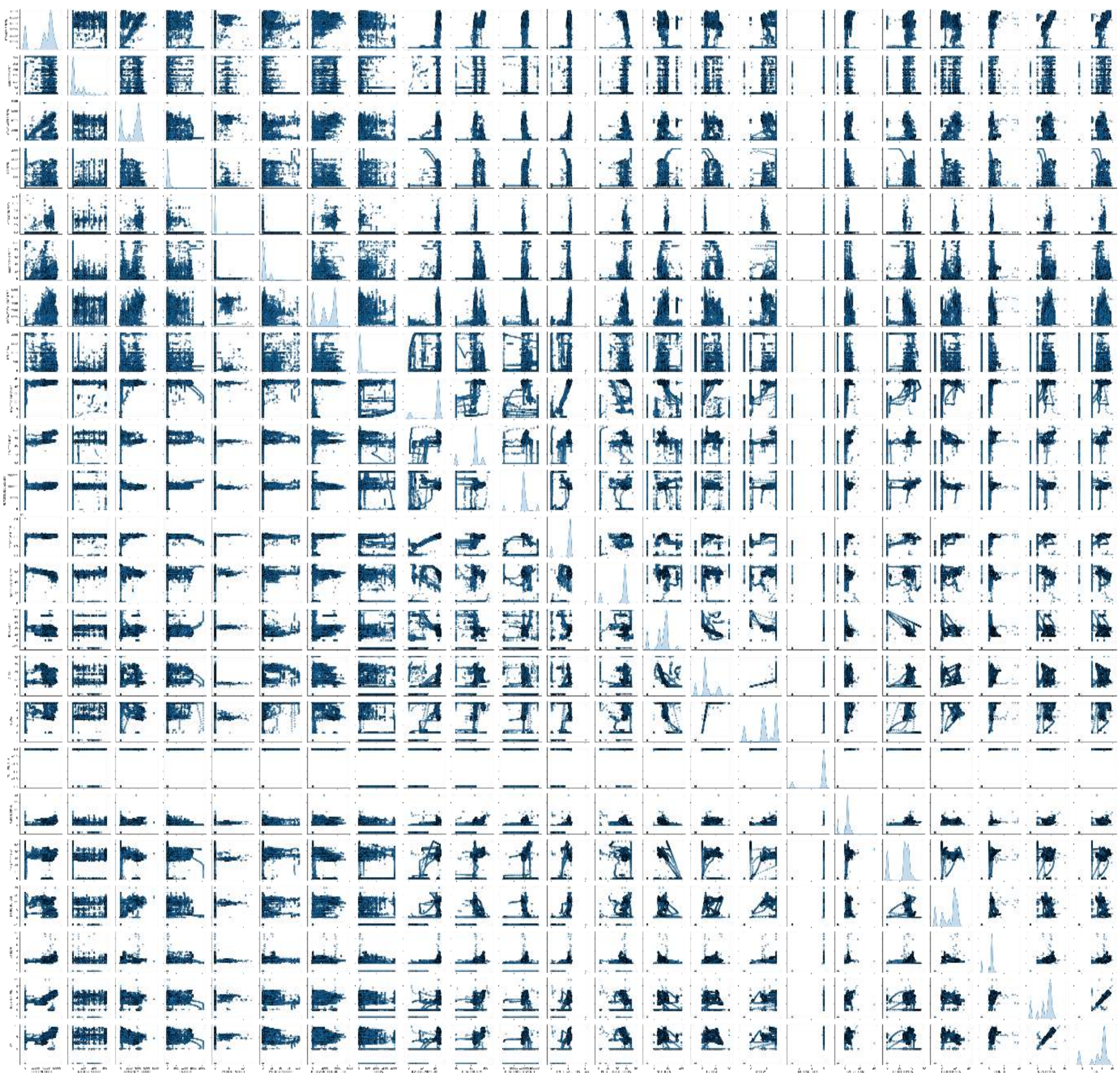


FIGURE-5: PAIR PLOT IMAGE 23X23

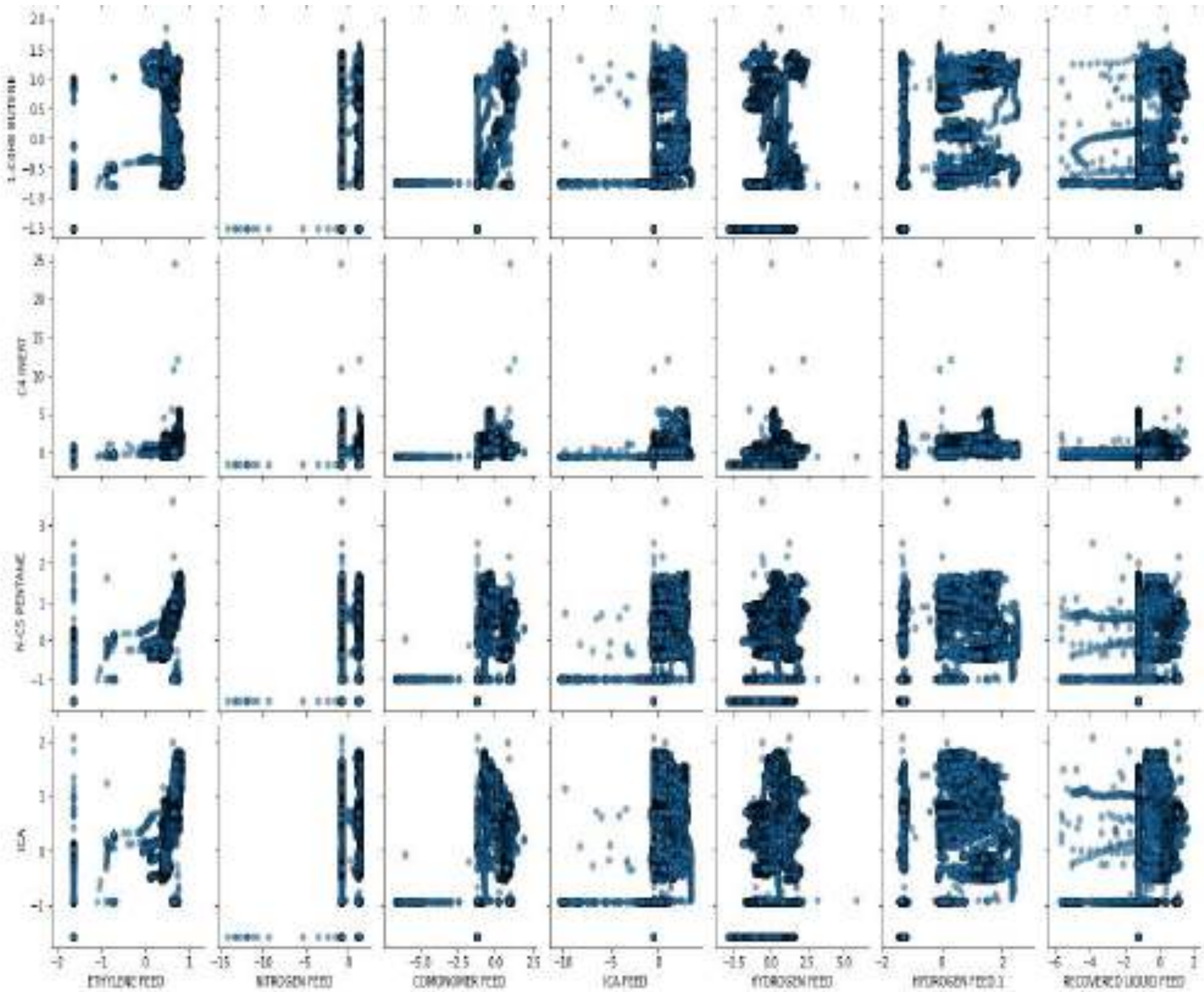


FIGURE-6: ZOOMED PAIR PLOT 23X23

This is observed from pair plotting that not all the variables are following the normal (not ideally GAUSSIAN) distribution. There are certain outliners present inside our dataset that need to be removed in further steps.

CORRELATION DATA PLOTS AS EDA-2

To find out which variables are more correlated with which variable and to what extent they are correlated. Whether that correlation is positive or negative in nature. Thus to look more into correlations among features and target by calculating the SPEARMANS's correlation and visualize the results using the HEATMAP. The following is the SPEARMAN's correlation HEATMAP of our data.

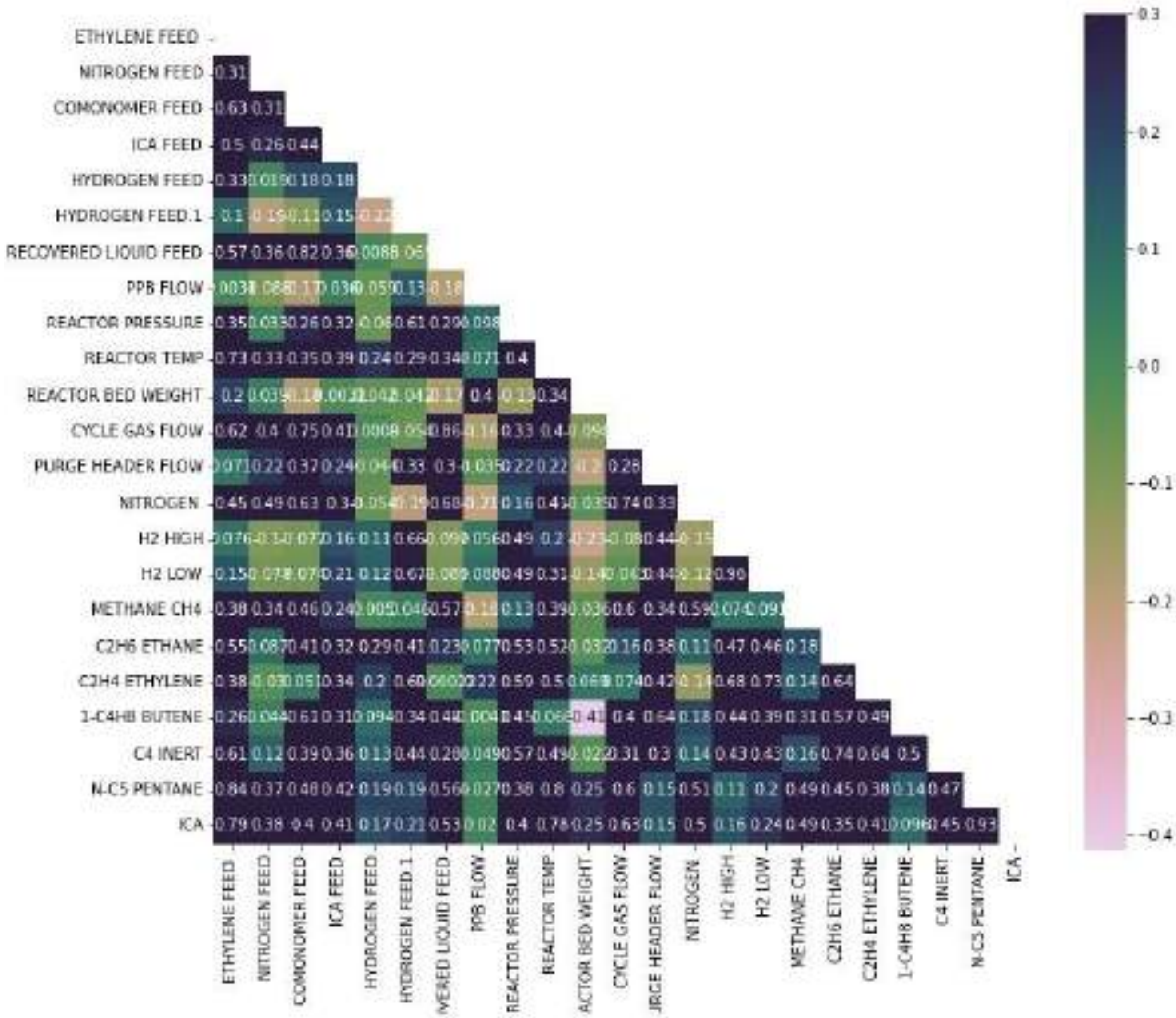


FIGURE-7:-SPEARMAN'S CORRELATION HEATMAP PLOT

As it can be seen the heat map diagram 0.4 being the highest positive and-0.4 being the least value all the have a discrete value of correlation with each other. A value close to zero or zero is indicated very negligible or no correlation. Hence As a common practice, any feature with very low correlation is excluded for prediction But in this case low correlation variable are still kept as a feature.

DATA PREPARATION FOR MODEL TRAINING AND TESTING

As it has been seen in the above Exploratory data analysis that the data can not to be passed straight-out to models for training because it is skewed, not normalised and also have certain outliners present in this data also. Hence following steps will be performed with this data to prepare it for model training.

TEST AND TRAIN DATA SPLITTING

This step is necessary in order to separate what is going as training data and what for testing. Test-Train split will be performed on the data frame available with us.

Train and Test Splitting from the Data Frame

```
[ ] n = len(df_heatmap)
    df_train = df_heatmap[0:int(n*0.7)].astype(np.float32)
    df_test = df_heatmap[int(n*0.7):].astype(np.float32)
```

As shown above 70:30 split is performed on the dataset means for example out of 100 samples 70 will be used as training dataset for model and 30 will be used as test dataset.

DATA NORMALIZATION

It is known before from the pair-plot that most distributions seem skewed. In order to improve the prediction performance, later on, it's better to do a normalization (may be called as scaling). Normalization is a technique to transform the data (without changing it) to be better distributed. SCIT-LEARN library of python is used to do the normalisation. There are several normalization techniques; the widely used are standardization (by transforming with the mean and standard deviation) and min-max (with minimum and maximum value). After trying all the methods, the power transform technique using YEO-JOHNSON method was more effective.

Normalizing the Training Data Sets

```
# normalize using power transform Yeo-Johnson method
scaler = PowerTransformer(method='yeo-johnson')

## ColumnTransformer
ct = ColumnTransformer([('transform', scaler, train_features)], remainder='passthrough')

## fit and transform
df_train_norm = ct.fit_transform(df_train)

## convert to dataframe
df_train_norm = pd.DataFrame(df_train_norm, columns=colnames)
df_train_norm
```

OUTLINERS DETECTION AND REMOVAL

Pair-plotting as it was done EDA shows that there are outliners present inside the dataset. Those outliners need to be removed in order to increase our model prediction performance. SCIT-LEARN libraries of python offers certain outliners removal techniques such as Isolation Forest, Minimum Covariance using Elliptic Envelope, Local Outlier Factor, and One-class Support Vector Machine. Alongside these, the most widely used outlier removal method, yet basic, is using the standard deviation method.

All 5 methods are implemented. There are two ways that can be used to compare which method performs the best outlier removal. One way is to count the data before outliers removed and the data after outliers removed for each method.

```
Number of points before outliers removed                       : 45872
Number of points after outliers removed with Standard Deviation: 44717
Number of points after outliers removed with Isolation Forest  : 22936
Number of points after outliers removed with Min. Covariance   : 41284
Number of points after outliers removed with Outlier Factor    : 32110
Number of points after outliers removed with One-class SVM     : 41287
```

FIGURE-8:-DATA POINTS REMOVAL COMPARISON

As it can be seen from above image Isolation Forest removed the most outliners followed by Outliner factor, Min. Covariance, one-Class SVM and Standard deviation. As it is already known that fewer outliner removed is better hence One-Class SVM and Standard Deviation are the winners.

SELECTION OF BEST OUTLINER REMOVER TECHNIQUE

Out of One-Class SVM and Standard deviation let's consider following box-plots of dataset before and after the outliner removal after all 5 methods.

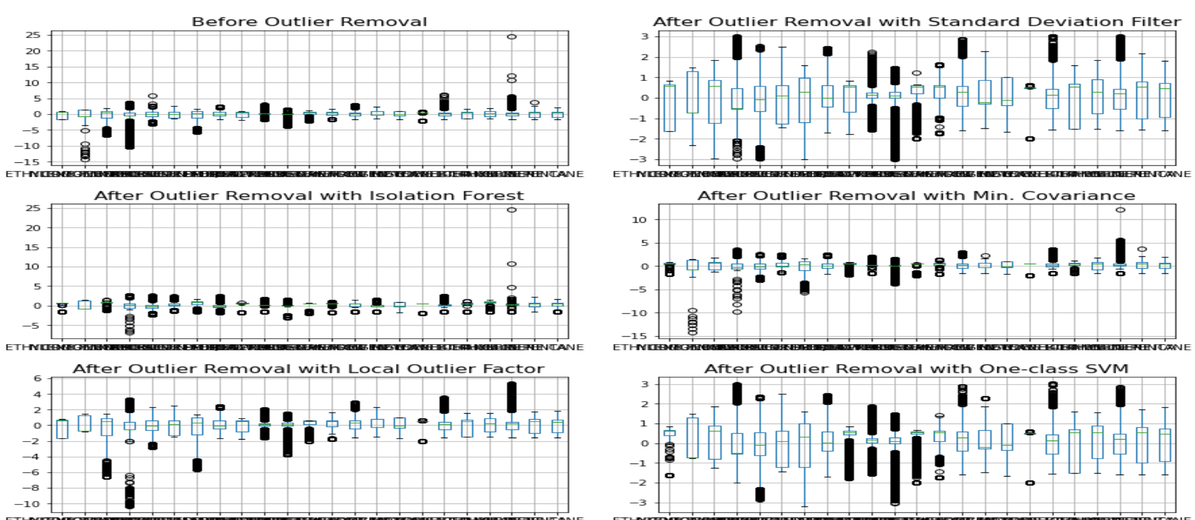


FIGURE-9:- BOX PLOT COMARISON OF DIFFERENT TECHNIQUES

Firstly it must be understood that box-plot represent the represents min, max and median values of a distribution as described in the below image.

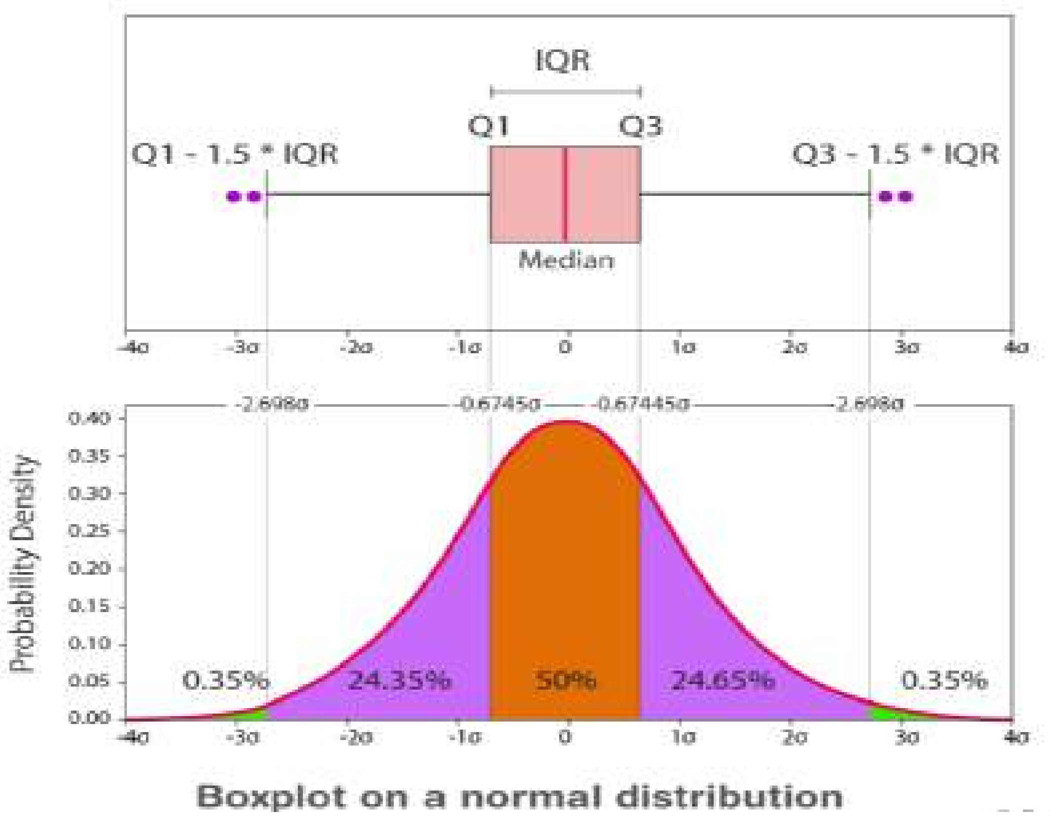


FIGURE-10:- EXAMPLE FOR BOXPLOT

Considering fewer outliners and more of a Gaussian distribution in the dataset One-Class SVM rises as a winner.

REGRESSION TECHNIQUES IN MACHINE LEARNING AND MODELS

Regression is a technique for investigating the relationship between independent variables (features) and a dependent variable (outcome\Targets). It's used as a method for predictive modelling in machine learning, in which an algorithm is used to predict continuous outcomes. Solving regression problems is one of the most common applications for machine learning models, especially in supervised machine learning. Algorithms are trained to understand the relationship between independent variables (features) and an outcome or dependent variable (targets). The model can then be leveraged to predict the outcome of new and unseen input data, or to fill a gap in missing data. Regression analysis is an integral part of any forecasting or predictive model, so is a common method found in machine learning powered predictive analytics. Following are the models that are taken into consideration for prediction of feed compositions using Features as listed above in inputs. Best model suited for Analyser data will be selected as final model based upon model score calculated.

LINEAR REGRESSION

Linear regression is a predictive analysis algorithm. It is a statistical method that determines the correlation between dependent and independent variables. This type of distribution forms a line and hence called a linear regression. It is one of the most common types of predictive analysis.

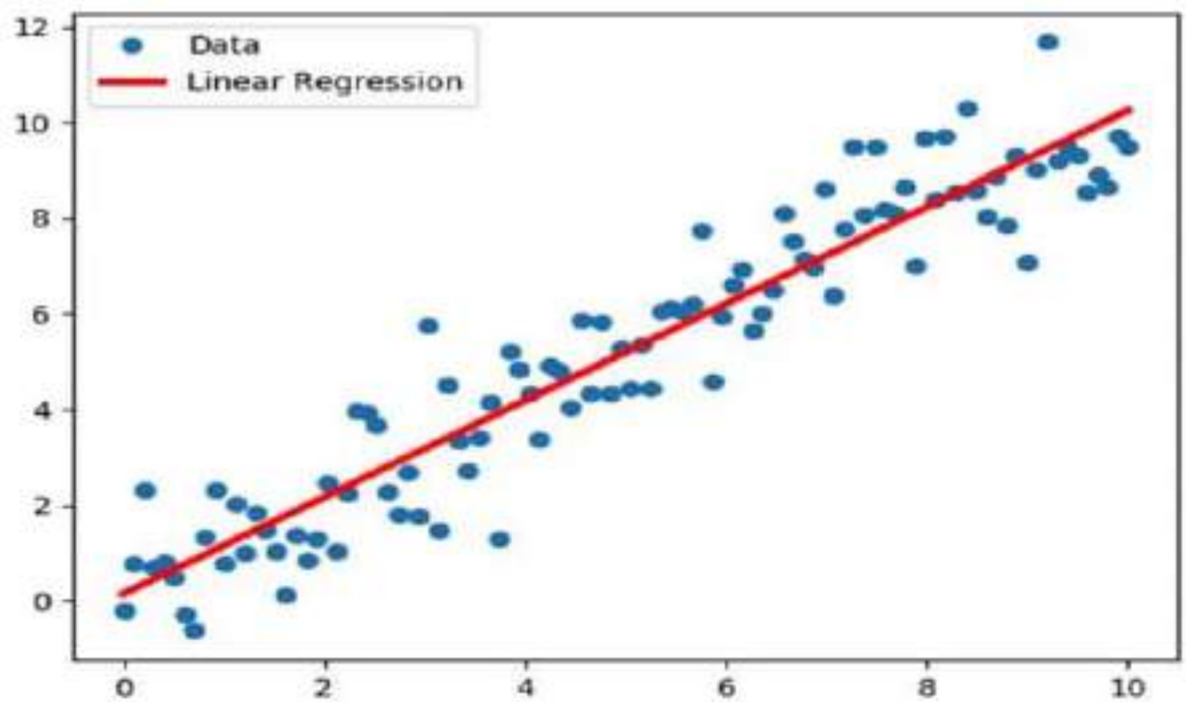


FIGURE-11:-LINEAR REGRESSION ALGORITHM

DECISION TREE REGRESSION

A decision tree is a supervised machine learning model used to predict a target by learning decision rules from features. As the name suggests, we can think of this model as breaking down our data by making a decision based on asking a series of questions.

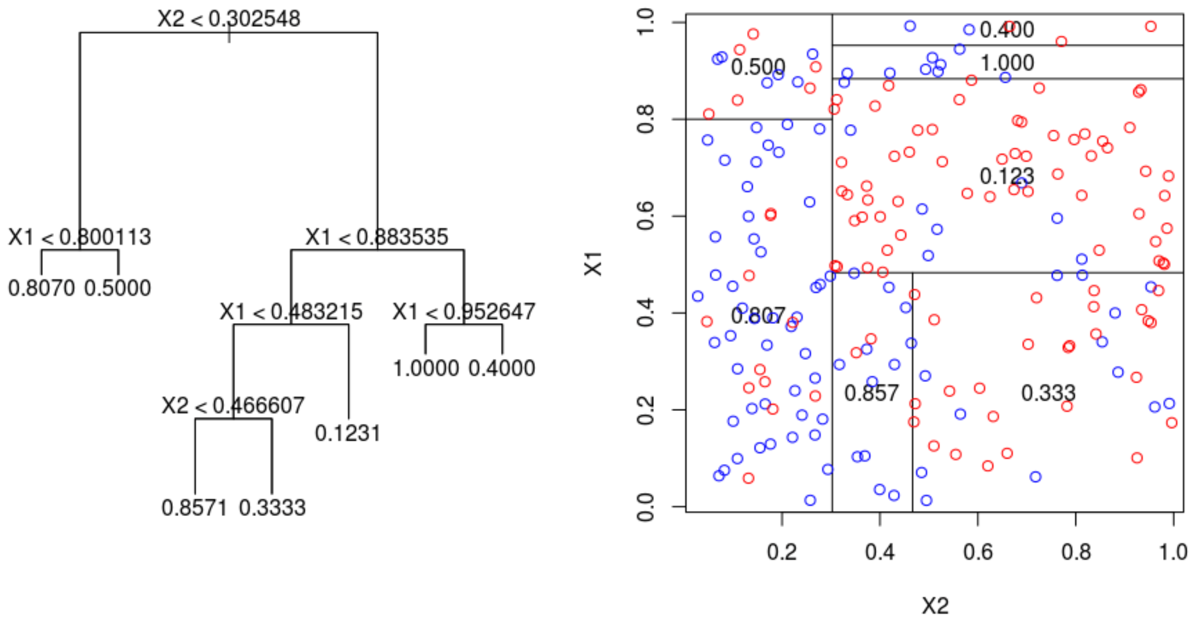


FIGURE-12:- DECISION TREE ALGORITHM

SUPPORT VECTOR MACHINE (SVM) REGRESSION

Support Vector Regression is a supervised Machine learning algorithm that is used to predict discrete values. Support Vector Regression uses the same principle as the SVMs. The basic idea behind SVR is to find the best fit line. In SVR, the best fit line is the hyperplane that has the maximum number of points. SVM can also be used for classification problems. The Image below depicts the working of model and Dependant (Features) variable and independent variable (Targets) relations.

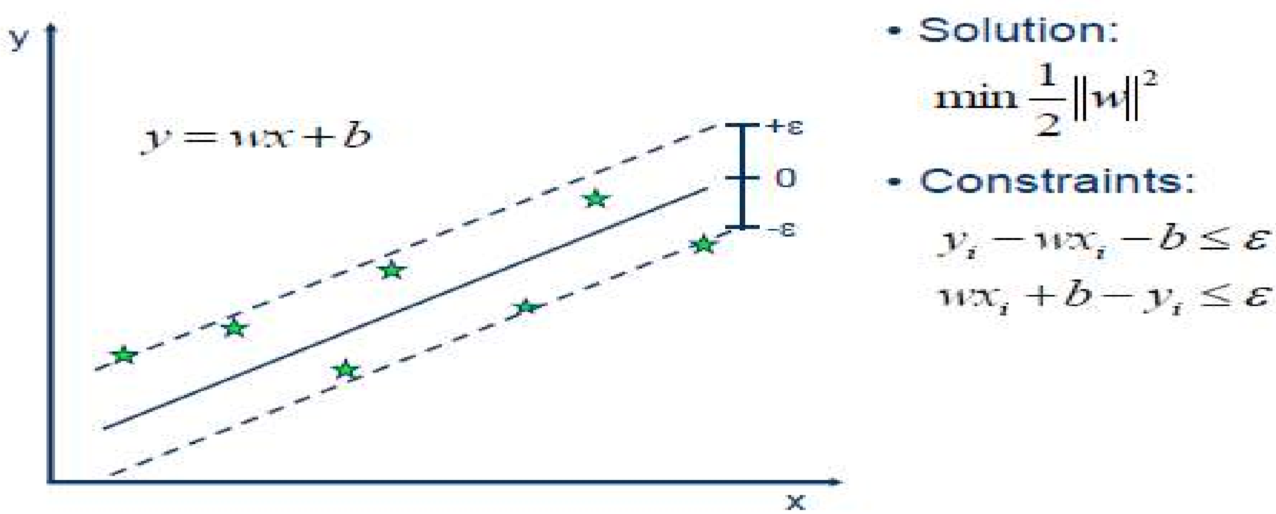


FIGURE-13:- SVM ALGORITHM

KNN REGRESSION

KNN algorithm can be used for both classification and regression problems. The KNN algorithm uses 'feature similarity' to predict the values of any new data points. This means that the new point is assigned a value based on how closely it resembles the points in the training set. It uses different type of methods to calculate distance between two points like EUCLIDEAN distance, MANHATTAN distance and HAMMING distance.

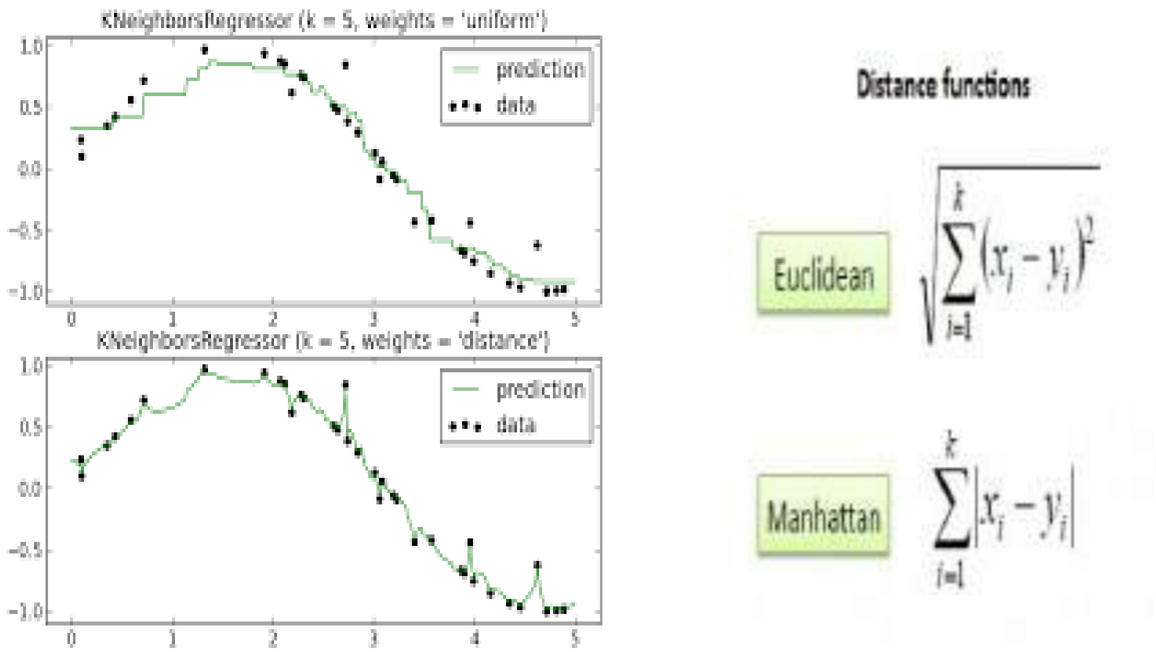


FIGURE-14:- KNN ALGORITHM

GRADIENT BOOST REGRESSION

Gradient boosting Regression calculates the difference between the current prediction and the known correct target value. This difference is called residual. After that Gradient boosting Regression trains a weak model that maps features to that residual.

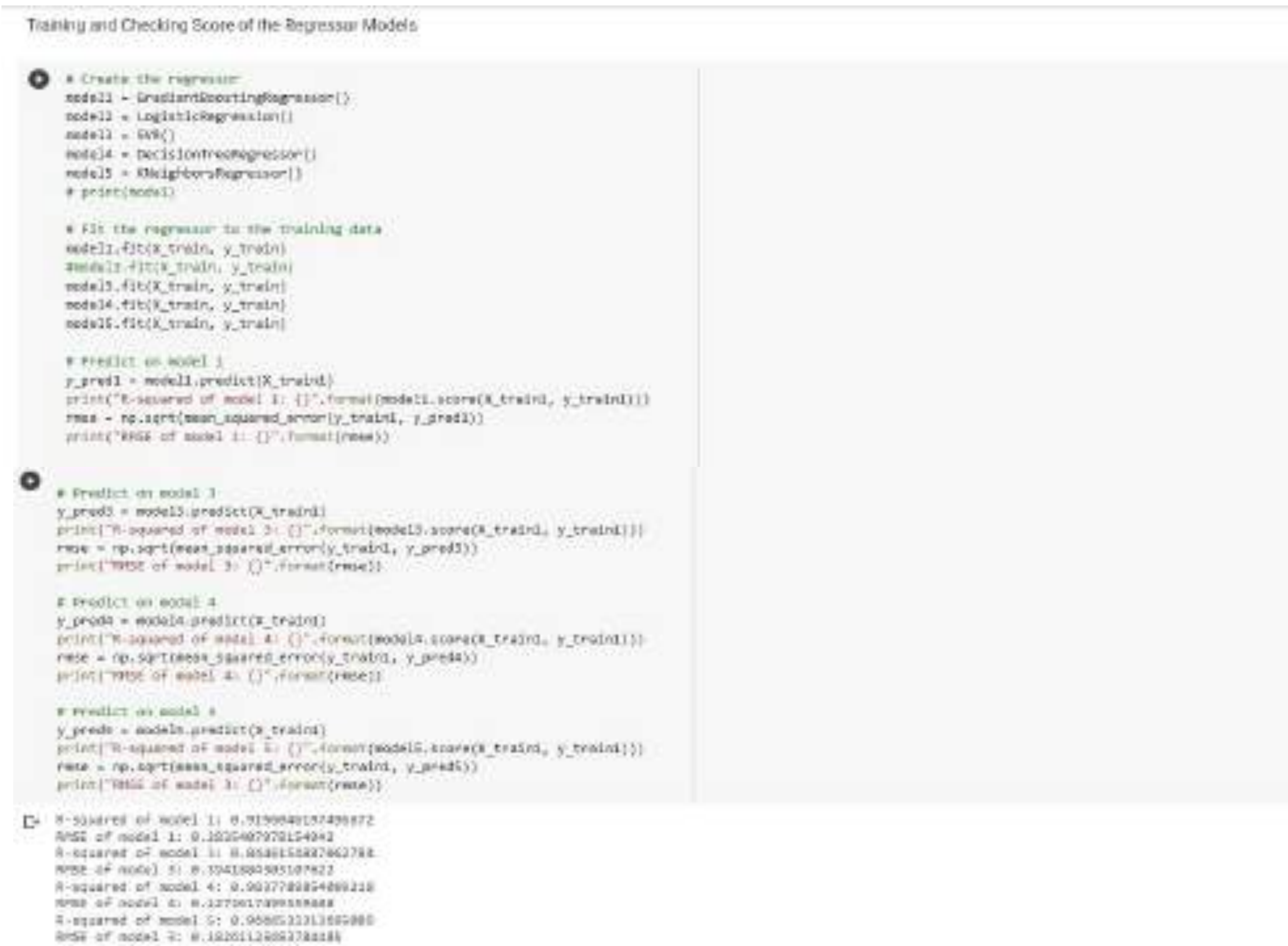
The algorithm tries to minimize the MSE (Mean square Error) function. Thus the model tries to fit the predicted output of model to actual target. This is clearly depicted in the figure below with an example of golfer trying to put the golf ball into the flag hole in minimum no of shots.

MODELS TRAINING AND MODELS SCORES

Machine learning offers variety of Regression models as discussed above. To check which regression model works best with the selected data, above discussed popular regression models will be trained with training dataset that we prepared earlier steps. Finally model scores will be calculated using R-Square and RMSE (root mean square error methods).

The model which is getting best score on the training dataset will be selected as a final model for feed composition prediction. For implementation of Analytical measurement data prediction framework as a DIGITAL TWIN of exiting analyser setup, the selected best model will be replicated for each target (Mole% of N2, H2 high, H2 low, CH4, C2H6, C2H4, C4H8, C4-INERT,N-C5, ICA etc.).

Just for the evaluation and representation purpose we are selecting C2H4 (ethylene mole %) as target against all the 13 features (NITROGEN FEED FLOW, ETHYLENE FEED FLOW, COMONOMER FEED FLOW Etc.). The images below depicts the model training and their scores.


Training and Checking Score of the Regressor Models

```
# Create the regressor
model1 = GradientBoostingRegressor()
model2 = LogisticRegression()
model3 = SVR()
model4 = DecisionTreeRegressor()
model5 = KNeighborsRegressor()
# print(model1)

# Fit the regressor to the training data
model1.fit(X_train, y_train)
#model2.fit(X_train, y_train)
model3.fit(X_train, y_train)
model4.fit(X_train, y_train)
model5.fit(X_train, y_train)

# Predict on model 1
y_pred1 = model1.predict(X_train1)
print("R-squared of model 1: {}".format(model1.score(X_train1, y_train1)))
rmse = np.sqrt(mean_squared_error(y_train1, y_pred1))
print("RMSE of model 1: {}".format(rmse))
```

```
# Predict on model 3
y_pred3 = model3.predict(X_train1)
print("R-squared of model 3: {}".format(model3.score(X_train1, y_train1)))
rmse = np.sqrt(mean_squared_error(y_train1, y_pred3))
print("RMSE of model 3: {}".format(rmse))

# Predict on model 4
y_pred4 = model4.predict(X_train1)
print("R-squared of model 4: {}".format(model4.score(X_train1, y_train1)))
rmse = np.sqrt(mean_squared_error(y_train1, y_pred4))
print("RMSE of model 4: {}".format(rmse))

# Predict on model 5
y_pred5 = model5.predict(X_train1)
print("R-squared of model 5: {}".format(model5.score(X_train1, y_train1)))
rmse = np.sqrt(mean_squared_error(y_train1, y_pred5))
print("RMSE of model 3: {}".format(rmse))
```

```
R-squared of model 1: [illegible]
RMSE of model 1: [illegible]
R-squared of model 3: [illegible]
RMSE of model 3: [illegible]
R-squared of model 4: [illegible]
RMSE of model 4: [illegible]
R-squared of model 5: [illegible]
RMSE of model 5: [illegible]
```

FIGURE-14:- DETAILS OF MODELS

As it can be noted from above images we have four models for predictions named as MODEL1, MODEL3, MODEL4 and MODEL5. These four models apply following Regression algorithms as Listed below.

MODEL1 --- Gradient Boosting Regression

MODEL3 --- SVM Regression

MODEL4 --- Decision Tree Regression.

MODEL5 --- KNN Regression

The R-square and RMSE of these four model is as below

```
R-squared of model 1: 0.9196046197496672
RMSE of model 1: 0.2835407978154942
R-squared of model 3: 0.8446154887062784
RMSE of model 3: 0.3941884303107622
R-squared of model 4: 0.9837789854099218
RMSE of model 4: 0.1273617499559688
R-squared of model 5: 0.9666531313695089
RMSE of model 3: 0.18261125683784485
```

FIGURE-15:- MODEL SCORES

As it can be seen clearly that MODEL4 which is Decision Tree Regression Outperformed the remaining three models with a score of R-Squared equals 0.98377 and RMSE equals 0.1273.

The much desired outcome of any Machine learning Regression model is R-Squared close to 1 and RMSE close to Zero.

PREDICTIONS BY MODELS AND RESULT COMPARISON

Model Score from above discussion shows that MODEL4 outperformed the remaining three regression models in score parameters. The next Examination is how the Prediction from these model looks like on the plots of TRUE DATA and PREDICTED data for considered Target variable i.e. C_2H_4.

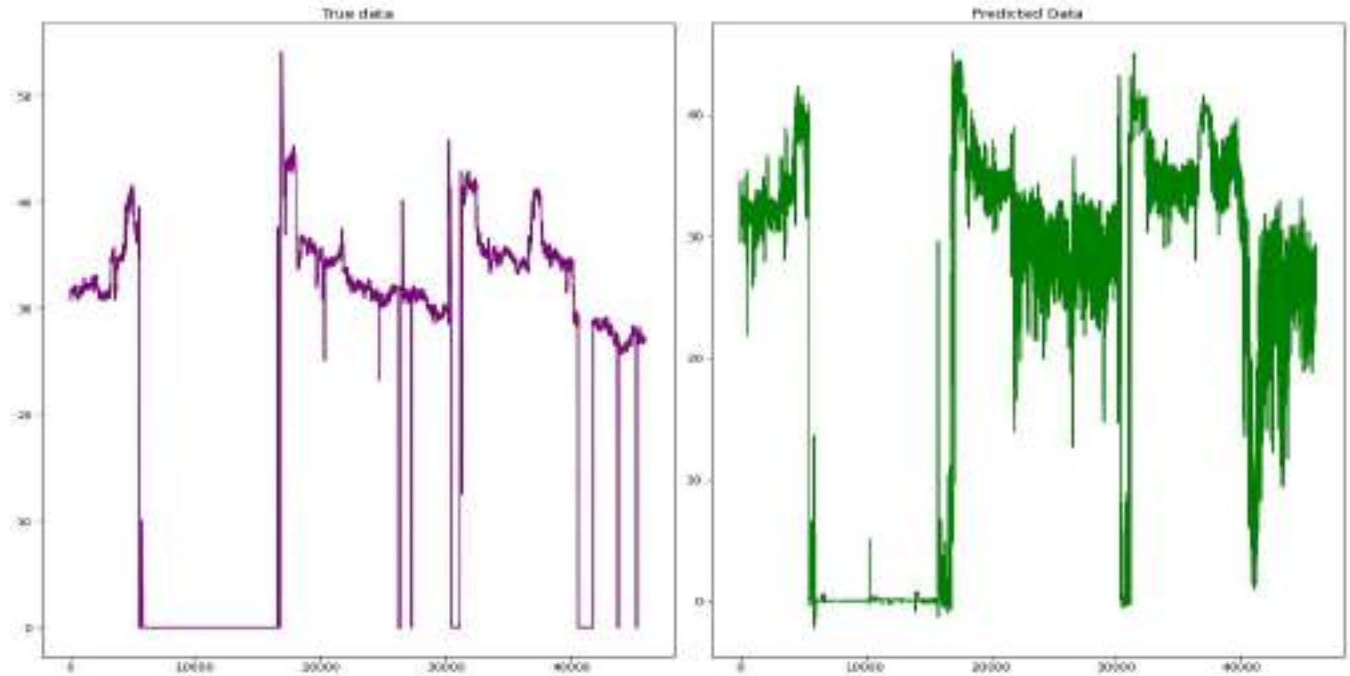


FIGURE-16:- C2H4 PREDICTION VS ACTUAL PLOTS FOR MODEL-1

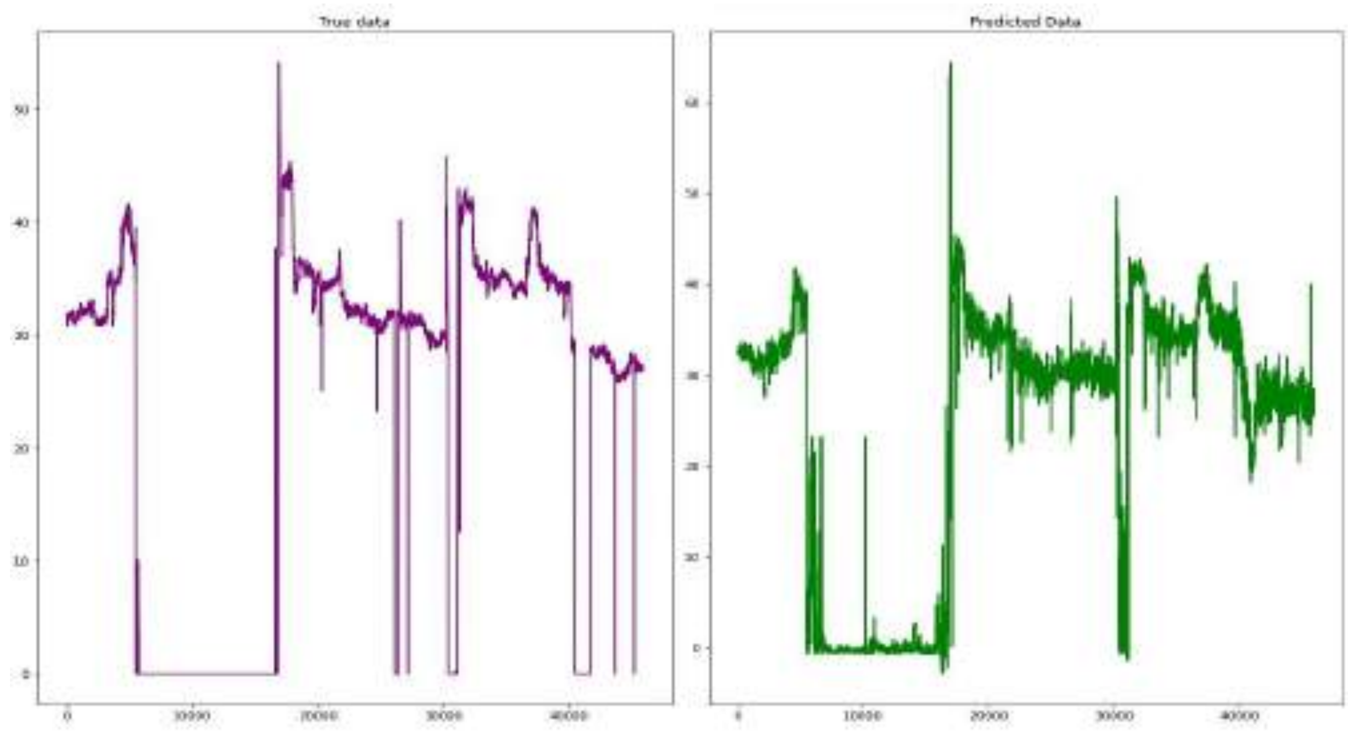


FIGURE-17:- C2H4 PREDICTION VS ACTUAL PLOTS FOR MODEL-3

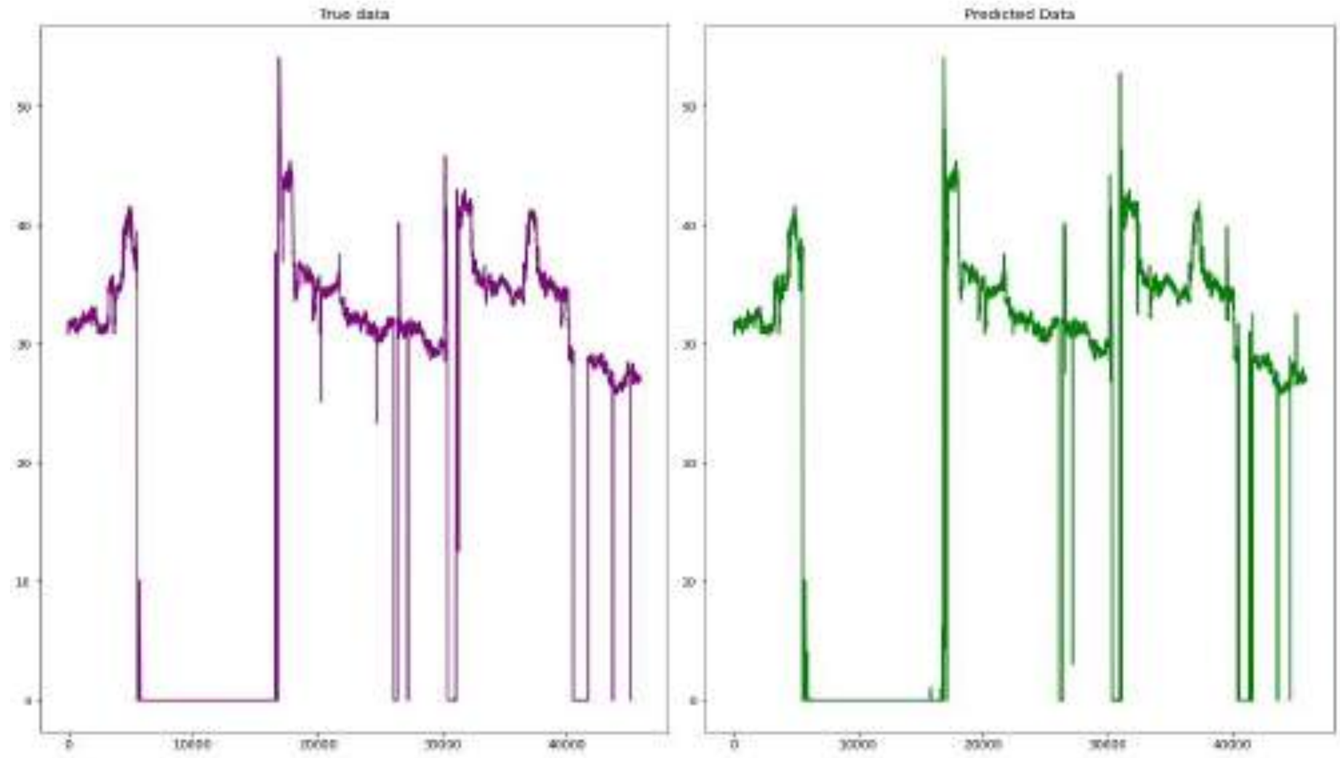


FIGURE-18:- C2H4 PREDICTION VS ACTUAL PLOTS FOR MODEL-4

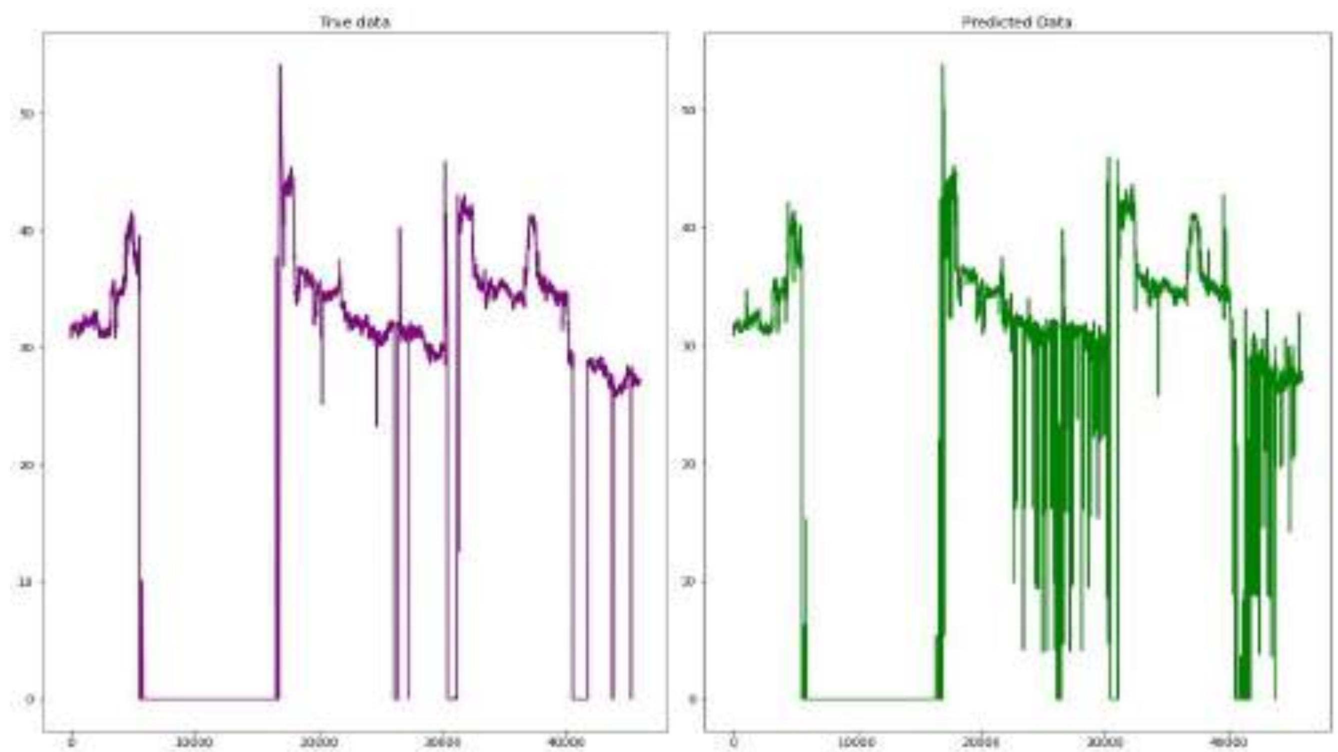


FIGURE-19:- C2H4 PREDICTION VS ACTUAL PLOTS FOR MODEL-5

The prediction results also states that the MODEL4 is a clear winner in this test also because the plots shows that the Prediction results from MODEL4 matches much closely with the Actual data. Hence MODEL4 is selected as a final model for prediction of remaining targets (9 remaining) also. The features (total 13) for the remaining targets will remain same as they were for C2H4 prediction.

ANALYSIS/OBSERVATIONS

In Supervised machine learning domain for prediction of unknown Variable (dependent Variable/target variable) which depends upon Independent variable (Features) regression proves to be an excellent technique. In regression machine learning we select a regression model then we train the selected machine learning model with clean dataset then we use that model in production for prediction. In this case we followed the approach step wise by doing EDA of the data first then cleaning the data for training of the data then Four model were selected for prediction then out these Four models one best performing model suited for dataset was selected based on Model score parameters. Thus a final Model which is MODEL4 in this case is selected for deployment in our DIGITAL TWIN framework for physical Analyser sets. The MODE4 will do the prediction for FEED COMPOSTION parameters of Recycle Loop of the Rector based on the FEED FLOWS, REACTOR PARAMETERS as features.

RESULTS AND CONCLUSION

Artificial Intelligence/Machine learning, deep learning and Digital Twin technologies are the Current trends of INDUSTRY 4.0. These technologies largely depends on huge amount of data. These technologies can also solve Industrial problem related to PRODUCTION efficiency improvement, ENERGY efficiency improvement, Downtime Reduction, Production QUALITY improvement, Reducing CARBON FOOTPRINTING and NET ZERO emission which otherwise seems very difficult to solve with traditional technologies and Capital intensive. As it was discussed above the machine learning model developed above will be highly beneficial in Tangible and Intangible benefits listed below.

RECOMMENDATIONS

The above Discussed framework can be expanded to other refining processes and refining Equipment to achieve greater Deeds in term of higher ENERGY efficiency as well as production efficiency in a Data Driven way. There are two types of architectures that are highly popular for INDUSTRY 4.0 i.e. CLOUD based and on premise based. Machine learning models like that we discussed could be deployed in both architectures. Below mentioned images describe the on premise implementation that we opted which can be scaled for other processes in an industrial complex.

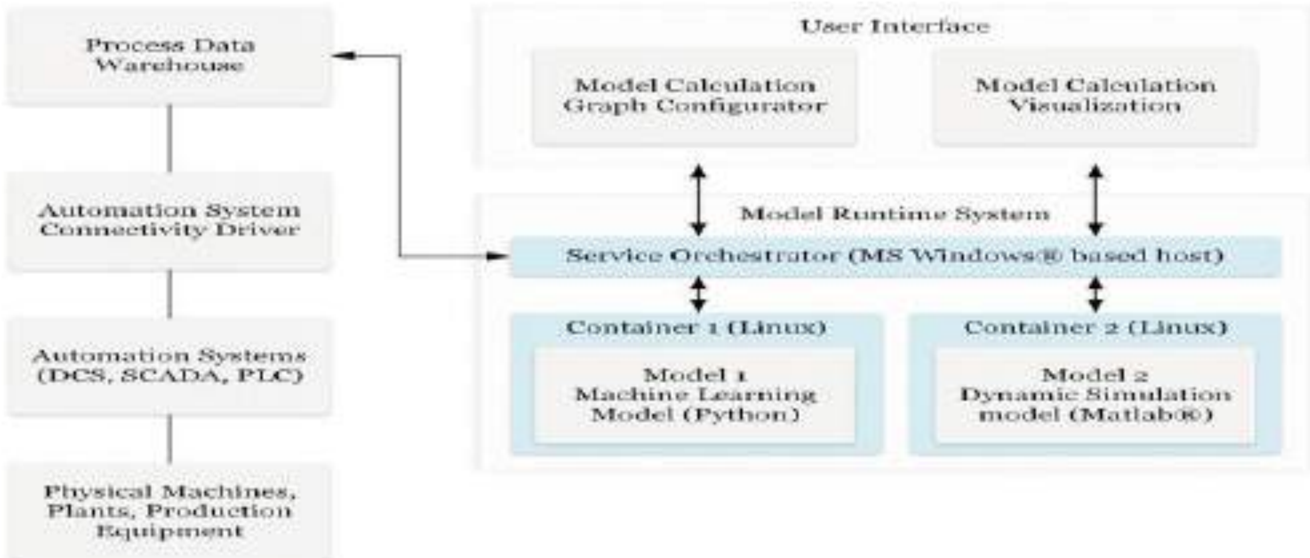


FIGURE-20:- DATA FLOW DIAGRAM FOR MODEL HOSTING

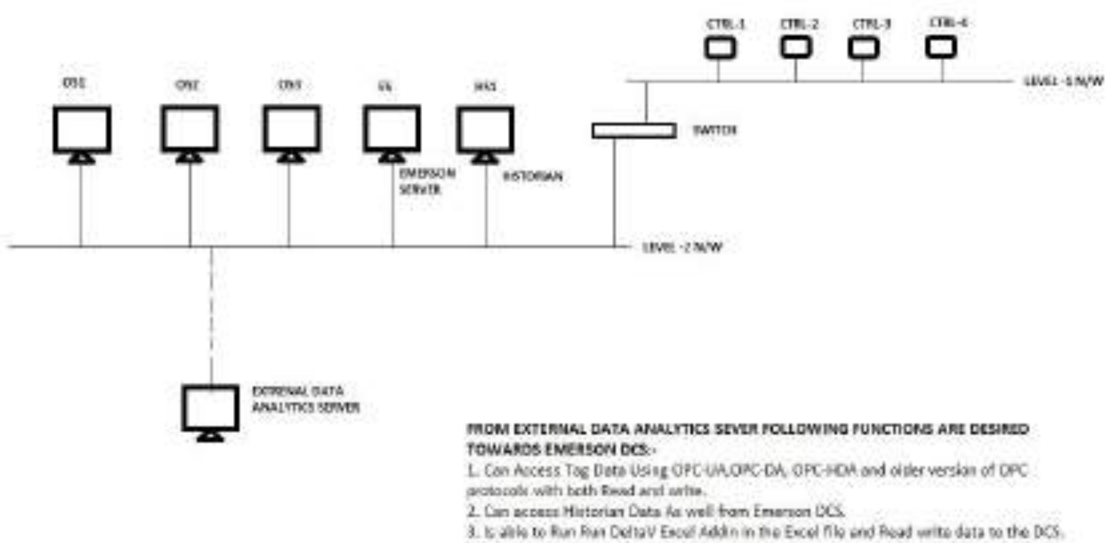


FIGURE-21:- NETWORK ARCHITECTURE DIAGRAM FOR MODEL HOSTING

REFERENCES

1. Miskinis, C. (n.d.). *Digital Twin Data Gathering versus advanced machine learning*. Challenge Advisory. Retrieved December 28, 2022, from https://www.challenge.org/insights/machine-learning-vs-digital-twin/
2. Author links open overlay panelTsega Y.MelesseaEnvelopeMatteoBollobValentina DiPasqualeaFrancescoCentrobStefanoRiemmaa, Y.MelesseaEnvelope, T., a, MatteoBollob, b, DiPasqualea, V., FrancescoCentrob, StefanoRiemmaa, & Abstract A technological gap to monitor fruit quality evolution in the food supply chain is causing a huge waste of fruits. A digital twin is a promising tool to minimize fruit waste by monitoring and predicting the status of fresh produce throughout its l. (2022, March 8). Machine learning-based digital twin for Monitoring Fruit Quality Evolution. Procedia Computer Science. Retrieved December 28, 2022, from https://www.sciencedirect.com/science/article/pii/S1877050922002095
3. Sarkar, P. (2022, October 7). Digital Twin Modeling using machine learning and constrained optimization. Medium. Retrieved December 28, 2022, from https://towardsdatascience.com/digital-twin-modeling-using-machine-learning-and-constrained-optimization-401187f2a382
4. Panel QingfeiMinaYangguangLuabZhiyongLiuaPersonEnvelopeChaoSuaBoWangc, A. links open overlay, QingfeiMina, a, YangguangLuab, b, ZhiyongLiuaPersonEnvelope, ChaoSua, BoWangc, c, twins, A. D., Zhang, Y., Yuan, Z., Yaqoob, I., Wu, K.-J., Wen, J., Tao, F., Schleich, B., Santos, M. Y., Rehman, M. H. U., … Alidi, A. S. (2019, May 31). Machine Learning Based Digital Twin Framework for production optimization in Petrochemical Industry. International Journal of Information Management. Retrieved December 28, 2022, from https://www.sciencedirect.com/science/article/abs/pii/S0268401218311484
5. Dasani, S. (2018, December 3). *Evolving industrial standards in the era of Digital Twins and Industry 4.0*. Medium. Retrieved December 28, 2022, from https://medium.com/@sdasani/evolving-industrial-standards-in-the-era-of-digital-twins-and-industry-4-0-66965461bde1
6. *Digital Twin: The new power of real-time cloning*. Bangkok Bank Innohub. (2022, August 10). Retrieved December 28, 2022, from https://www.bangkokbankinnohub.com/digitaltwin/

BIOGRAPHY

Sh. Ashok Kumar graduated in Instrumentation and Control Engineering from NIT JALANDHAR. He is highly Motivated Oil and Gas Professional focused towards improving the Energy efficiency of Refining processes in Oil, gas and petrochemical Industries. The Advance technologies like AI/ Machine Learning, IIOT, INDUSTY 4.0, DIGITAL TWIN and Deep Learning deeply Fascinates him. His current engagement is PATA petrochemical Complex of GAIL (INDIA) LIMITED. He looks after Automation, Control and Monitoring of Process plant. He is continuously exploring the applications of AI/ Machine Learning in Process Plants to improve their Production efficiency as well as Energy Efficiency to meet Net-Zero emissions. He has also presented Papers in external as well as internal Knowledge sharing Seminars/Conferences and have won awards and recognitions.

Maximize Value through Integrated Renewable Power Management System

Renewable electricity capacity has seen record growth in recent years. During COP 26 commitments, Prime Minister Narendra Modi announced the “**Panchamrut”** with the aim of making India Energy independent Country. This is geared to make India energy independent before the country completes 100 years of its independence in 2047.

However, transitioning to cleaner energy systems or scaling up existing ones is a complex undertaking for power producers. Wind turbines, solar arrays, lithium-ion batteries, hydrogen electrolyzers and hydroelectric power all use a wide variety of automation software and technologies. As renewable portfolios grow, the number of applied technologies will multiply, increasing learning curves and adding complexity to operations as solutions from different vendors require additional integration. At the same time the future of power requires integrated hybrid energy systems where renewable and traditional generation, energy conversion and storage technologies are combined to increase the resiliency and reliability of the grid while helping to balance the supply of clean electricity.

While the benefits of hybrid power systems are clear, bringing them to life is complicated, Our Case Study talks about Dedicated Renewable Power Automation Technology and Software Portfolio that expertly managed integrated renewable energy generation and storage. This is a single set of purpose-built software and solutions that supports different technologies in one standardized, intuitive system.

Emerson software and solutions for renewable assets provide a secure, purpose-built digital automation foundation with multi-vendor and multi-asset interoperability. At the same time, our battery energy management systems enable safe operations and optimize charge and discharge for maximum production and lifecycle.

Emerson’s energy storage management software optimizes operations and supports a reliable power system through energy management, load-levelling, reserves and black start or backup power. Our software gathers, contextualizes and securely delivers realtime and historical data to key stakeholders providing accurate, actionable intelligence that enables better decision-making and higher revenues. Our flexible solutions are scaled to meet the needs of standalone renewable assets or hybrid applications that includes Wind, solar, and hydro, providing full operational visibility across all assets to increase performance, improve efficiency and reduce costs.

Jyotsna Joshi

Business Director

Sustainability Decarbonisation

Emerson Automation Solutions, India

Shubhi Goel
Senior Marketing Manager
Power and Water Solutions

Enhancing Polyethylene Reactor Operation & Efficiency by enabling Advanced Process Control using online inference of Polymer properties: Melt Index & Density

- Nishchay
GAIL INDIA LIMITED, Auraiya

KEYWORDS

Advanced Process Control, Recursion, Reactor Modeling, Polymer properties

ABSTRACT

Major difficulty affecting control of product quality in Polymerization reactor is lack of suitable online polymer property measurement. We have referred a scheme developed to predict melt index and density in UNIPOL Polyethylene reactor. Theory based models are derived to predict quality variables from the available on-line temperature and gas composition measurements. Adjustable parameters in these models are updated on-line using infrequent laboratory measurements and recursive parameter estimation. Application of this methodology is illustrated using operating data from our LLDPE2 (UNIPOL PE) reactor. Using such methodologies along with latest recursive techniques, we can predict important polymer parameters and thus enable Advanced Process Control by providing operator feature to provide set point for it after validating it wholly. Knowledge of product property deviations from desired targets is required so that plant operators can take corrective actions to reduce the quality of off-grade material and produce with consistent quality product.

INTRODUCTION

Common problem in polymer industry and thus in our plants is the lack of on-line measurement technology for product quality variables. While with standard instrumentation systems, one can measure reactor temperature, pressure, flow rate and gas composition continuously, but key quality variables such as molecular weight (inference variable Melt Index) and copolymer composition (inference variable Density) measured offline in quality control laboratories. These delayed and infrequent quality measurements provide essential feedback for process control. Combining this information from on-line and off-line measurements with process models can lead to improved estimates of quality variables between samples and hence improve product property controlling. In this paper, a scheme to obtain polymer quality variables in UNIPOL PE swing plant fluidized-bed polyethylene reactor is presented. The development of a recursive technique for updating model parameters using offline MI and density measurements is described.

FORMULATING MODEL FOR POLYMER PROPERTIES

In UNIPOL process (LLDPE-HDPE swing plant), copolymerization of ethylene and Butene-1/Hexane is carried out in a fluidized bed reactor. The melt index and density of the polymer in the bed depend on catalyst properties, reactant gas composition, and reactor temperature. The reactor is well instrumented with temperature, pressure and flow sensors. Gas compositions are measured by on-line gas chromatographs. Melt index and density are measured every several hours in the quality laboratory. These analyses require up to one hour, when the lab results become available, they are used to adjust the reactor operating conditions to ensure that on-specification polymer is produced.

Instantaneous melt index and density models developed by McAuley [1991] for UNIPOL PE reactor, these are as follows:

$$\ln(MI) = k_7\left(\frac{1}{T}-\frac{1}{T_0}\right) + 3.5\ \ln\left(k_6 + k_1\frac{[M_2]}{[M_1]} + k_2\frac{[M_3]}{[M_1]} + k_3\frac{[\mathrm{H}_2]}{[M_1]} + k_4\frac{[R]}{[M_1]} + k_5\frac{[I]}{[M_1]}\right)$$

$$\rho = p_0 + p_1\ln(MI) - \left\{p_2\frac{[M_2]}{[M_1]} + p_3\frac{[M_3]}{[M_1]}\right\}^{p_4}$$

Similarly derived Instantaneous models for UCATJ type catalyst whose outlook too is similar in equation as given by McAuley, UNIVATION given models are as follows:

ln (MI) = 23.97 - 7094.0/(T+273) + 2.762 * ln (Z1)

R^2 = 0.9929

Density = 0.968490 – 0.088390 * (Z2)$^{0.5}$ + 0.002129 * ln (MI) (g/cm^3)

R^2 = 0.9810

Z1 in high density, rest all remains same in equation:

Z1 = H2/C2 + 0.277*C4/C2 + 0.537*C6/C2

Where Z1 defined differently in High density as well in Low density, for low density:

H_2/C2	=	hydrogen / ethylene ratio
C4/C2	=	butene / ethylene ratio
C6/C2	=	hexene / ethylene ratio
T	=	temperature (°C)
Z1	=	H_2/C2 + 0.5*C4/C2 + C6/C2
Z2	=	0.01 + C4/C2 + 2.5*C6/C2
MI	=	melt index (g/10 min)

Cumulative melt index and density models

In UNIPOL reactors, solid polymer particle phase is mixed well by turbulent action of gas phase. New polymer added continuously to the bed by the polymerization of monomers and accumulated leaves the bed in frequent small batches via Product discharge system. Hence, the mixing and residence time behavior of the solid phase usually approximated by that of an ideal continuous stirred tank. Instantaneous polymer with weight average molecular weight M_{wi}, Melt index MI_i and density p_i is fed continuously to the mixer at a mass flow rate P_R equal to the instantaneous polymer production rate. The well mixed bed contains a mass of polymer M_P, which has cumulative weight average molecular weight M_{wc} , cumulative Melt index MI_C and cumulative density p_c. If there is no net accumulation of polymer during short period of time, then $P_R\Delta t$ kg of new instantaneous polymer enter the bed and subsequently same quantity of cumulative leaves. After the time, Δt, the mass fraction of new instantaneous polymer in the reactor will be $P_R\Delta t/ M_P$ and the mass fraction of old cumulative polymer will be 1- $P_R\Delta t/ M_P$. Thus, the new weight average molecular weight and density are given by:

$$\overline{M}_{wc}(t+\Delta t) = \frac{P_R \Delta t}{M_p}\overline{M}_{wi}(t) + \left(1 - \frac{P_R \Delta t}{M_p}\right)\overline{M}_{wc}(t)$$

$$\frac{1}{\rho_c(t+\Delta t)} = \frac{P_R \Delta t}{M_p}\frac{1}{\rho_i(t)} + \left(1 - \frac{P_R \Delta t}{M_p}\right)\frac{1}{\rho_c(t)}$$

Deriving using above weight and density approximation we get cumulative models for MI and density, which are as follows:

$$MI_c^{-0.286}(t) = \exp(-h/\tau) MI_c^{-0.286}(t-h) + \{1 - \exp(-h/\tau)\} MI_i^{-0.286}(t-h)$$

$$\frac{1}{\rho_c(t)} = \exp(-h/\tau)\ \frac{1}{\rho_c(t-h)} + \{1-\exp(-h/\tau)\}\frac{1}{\rho_i(t-h)}$$

Where ,

$\tau = M_p/P_R$ is the solid-phase residence time

Gas compositions in the reacor are measured periodically using on-line gas chromatographs. Since the gas sampling interval, h, is very small with respect to the polymer-phase resitdence time, τ, little error is incurred by assuming that the instantanoeous properties remain constant over the gas sampling interval.

These are the model froms used in on-line inference scheme [McAuley 1991]. All that is required to predict cumulative melt index and density estimates are initial estimates of MI_c and p_c , estimates of the parameters k =(k_1, k_2…. K_7) and p =(p_1, p_2,… p_4) in the instantaneous property equations of McAuley but in out case it's UNIVATION given equations and a series of gas compostion, temperature, production rate and bed mass measurements.

Application of Recursive prediction error method for Property estimation

Similar approach as used by McAuley if we implement in our case by using simplified approach of one varying paramater only in both density as well Melt Index, we get :

$$\text{Z1} = ko + \frac{H2}{C2} + \frac{0.277 * \text{C4}}{C2} + \frac{0.537 * \text{C6}}{C2}$$

$$\text{Z2} = po + 0.01 + \frac{\text{C4}}{C2} + \frac{2.5 * \text{C6}}{C2}$$

Updating ko on-line has intiutive appeal because it accounts for the effect of changing impurity levels on MI.

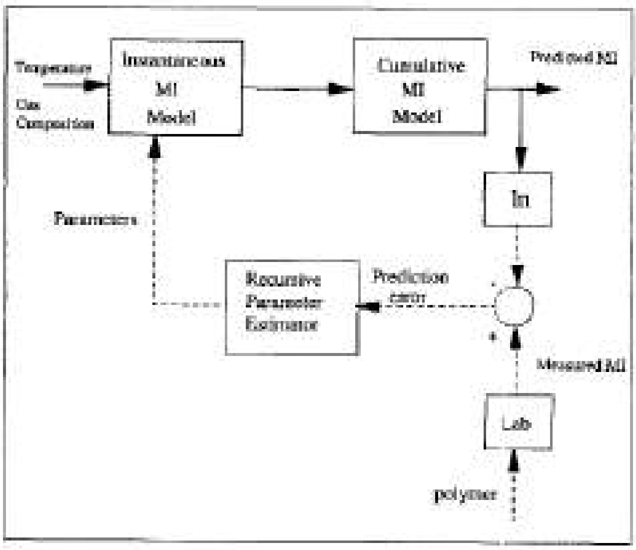


Figure 1 Scheme for RPE; ln(MI) used as 'y'

As RPE (Recursive prediction error) approach is used which has generic equations and their extended version used by MacGregor [1991] is as follows :

$$y = f[\underline{\theta}, \underline{u}(t-1), y(t-1)]$$

$$\hat{\underline{\theta}}(t) = \hat{\underline{\theta}}(t-1) + \underline{L}(t-1)\epsilon(t)$$

$$\epsilon(t) = y_{\text{meas}}(t) - y[\underline{\theta}(t-1)]$$

$$\underline{L}(t-1) = \frac{\underline{Q}(t-1)\underline{Z}(t)}{\lambda + \underline{Z}^T(t)\underline{Q}(t-1)\underline{Z}(t)}$$

$$\underline{Q}(t) = \frac{1}{\lambda}\underline{Q}(t-1) - \frac{\underline{Q}(t-1)\underline{Z}(t)\underline{Z}^T(t)\underline{Q}(t-1)}{\lambda + \underline{Z}^T(t)\underline{Q}(t-1)\underline{Z}(t)}$$

$$\underline{Z}(t) = -\frac{\partial \epsilon}{\partial \underline{\theta}} = \frac{\partial y}{\partial \underline{\theta}}$$

$$\underline{Q}(t) = \frac{\text{Cov}[\underline{\theta}(t)]}{\sigma_e^2}$$

$$\hat{\underline{x}}^*(t \mid t) = \hat{\underline{x}}^*(t \mid t-1) + \underline{K}^*[\underline{y}(t) - \hat{\underline{y}}(t \mid t-1)]$$

{ Modified version with constant Gain term K^*}

Since error variance in ln(MI) is independent of magnitude of MI unlinke error variance of MI itself which changes with MI magnitude. So we assume 'y' in RPE equation as ln(MI) or p, when proceeds further for calculation.

Initially K* was estimated from some plant data to minimize the sum or squared prediction errors later it is iterated using subsequent measured lab values. Error is calculated as differnce among the predicted readout and actual lab results, which will drive parametrical changes in model, having variable term dependent upon it only.

OBSERVATIONS

Derived equations and specified equation when tested with data provided by licensor UNIVATION for various grades in steady state, seems showing well responsive.

Further, test results based upon cumulative reactor modeling are as follows:

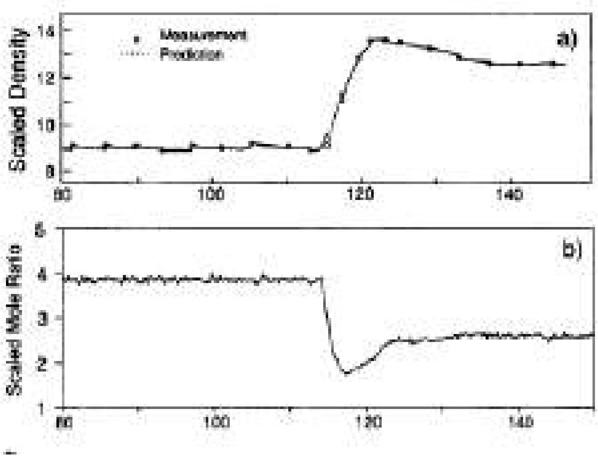


Figure 2 Density change with molar ratio

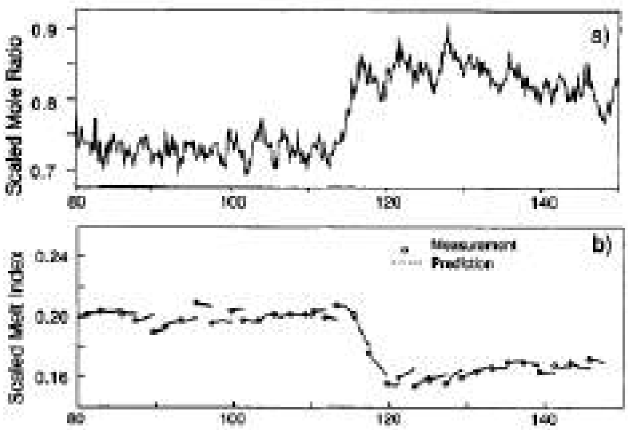


Figure 2 Melt index change with molar ratio

Refer figure 2 and figure 3, we can observe that circles show measurement value while lines in between is values based upon inference which provide us continuous readout of critical polymer properties which help in controlling them more prudentially.

CONCLUSION

This scheme consists of theoretically based models along with Licensor specified models, which relate melt index and density to reactor operating conditions. When both Licensor specified instantaneous models and cumulative models clubbed along with recursion techniques, one can easily predict critical polymer properties: Melt index as well as density.

Further synchronization with DCS system for updating parameters as per RPE (least square algorithm) method is done. After subsequent tuning of parameters, we will get working model in DCS for inference, which will let us enable Advanced Process Control by providing control of these property parameters directly in place of manual intervention currently in practice for controlling these polymer properties.

RECOMMENDATIONS

Incorporation of Recursive Prediction Error (Least square method) algorithm in DCS to be done along with usage of models specified by Licensor Univation and cumulative models developed by McAuley for predicting Melt Index and Density. This will help operator in Grade changeover and in case of Process disturbances as lab results are only available when disturbances happened and causes formation of large amount of production as Off-grade production. Prediction can not only reduce human error probability in deriving important polymer properties, it will also result in enhanced On-spec production by reducing Off-grade production.

REFERENCES

1. On-line inference of Polymer properties in an Industrial Polyethylene Reactor – K.B. McAuley and J.F. MacGregor.
2. Univation Vol II – Process Technology.
3. Section III- Process Flow Diagram and Material Balance //PDDR to GAIL only

ACRONYMS

PE	Polyethylene
DCS	Distributed Control Systems
RPE	Recursive Prediction Error
MI	Melt Index
UCATJ	Univation Catalyst J

BIOGRAPHIES

Sh. Nishchay was born in Bhiwani, Haryana, India in the year 1995. He graduated in Electronics (Instrumentation & Control) engineering from Thapar University, Patiala, Punjab. He joined department of Instrumentation in GAIL INDIA LIMITED at its Gas Processing & Petrochemical site in Auraiya as Senior Engineer (Petrochemical Maintenance – Instrumentation) in 2017. At present he is working as Manager (Petrochemical Maintenance – Instrumentation) and associated with design, engineering, maintenance & procurement of Instrumentation & Control systems used at Petrochemical & Gas processing plant. He has participated in various Technical paper presentation seminars in GAIL. His Technical suggestion related to Operational enhancement has even awarded as “Best Technical Suggestion year 2022” on GAIL Foundation Day at GAIL PATA.

Hydrogen Automation: A Promising Pathway for Sustainable Energy Systems

Praseed Sahu
Manager, Project Development
GAIL (India) Limited, Noida

Mukul Gupta
Chief Manager, Sustainability Development
GAIL (India) Limited, Pata

ABSTRACT

The increasing global demand for clean and sustainable energy has led to the development of hydrogen automation technologies that are transforming the way we produce, store, and distribute energy. Hydrogen is not only the most abundant element in the universe, it could also play an essential role in tomorrow's energy mix - from fuelling cars, trains, trucks and ships to generating electricity and heating buildings. Green hydrogen has emerged as a promising solution for achieving the Net-Zero emissions target set by several countries worldwide. Hydrogen has been utilized and manufactured in the chemical and petrochemical sector for over a century. Green hydrogen, produced using water electrolysers, is generated from renewable energy sources. Currently, there are four types of electrolysis used and being further developed: Alkaline, PEM, AEM, and solid oxide. However, the first two are the most commonly used today. With an increasing number of hydrogen plants, the technology is becoming more mature, resulting in better efficiency, longer operational time, improved safety, and plant availability at a reduced cost.

Process control instrumentation plays a crucial role in the hydrogen industry, aiding in process control, safety, and efficiency. It is particularly critical for processes that operate under unsteady conditions. Instrumentation can be found in various stages, starting from the production of hydrogen through electrolysis plants, measuring hydrogen flows at the interfaces between different companies, during transportation via pipelines or tankers, and ultimately used for re-electrification in combined cycle power plants.

Hydrogen as the lightest element differs from others in many aspects. It has a high specific energy content, explaining why it can also be used as a rocket fuel. It is light, thin and highly flammable. Thus, the process equipment including the instrumentation must be suitable and designed for the safe handling of hydrogen. Special design of all the materials is essential for use with hydrogen. Hydrogen permeates through metals and leads to an embrittlement if not treated correctly.

This paper provides an overview of the role of automation in the hydrogen industry, highlighting the potential of hydrogen automation to enable the transition to a low-carbon economy.

KEYWORDS

1. Sustainable Energy 2. Net-Zero 3. Electrolysers 4. Low Carbon Economy

INTRODUCTION

The Paris Agreement is a legally binding international treaty on climate change. It was adopted by 196 Parties at the UN Climate Change Conference (COP21) in Paris, France. Its overarching goal is to hold "the increase in the global average temperature to well below 2°C above pre-industrial levels" and pursue efforts "to limit the temperature increase to 1.5°C above pre-industrial levels." India at the 26th session of the Conference of the Parties (COP26) to the United Nations Framework Convention on Climate Change (UNFCCC) held in Glasgow, United Kingdom, expressed to intensify its climate action by presenting to the world five nectar elements (Panchamrit) of India's climate action.

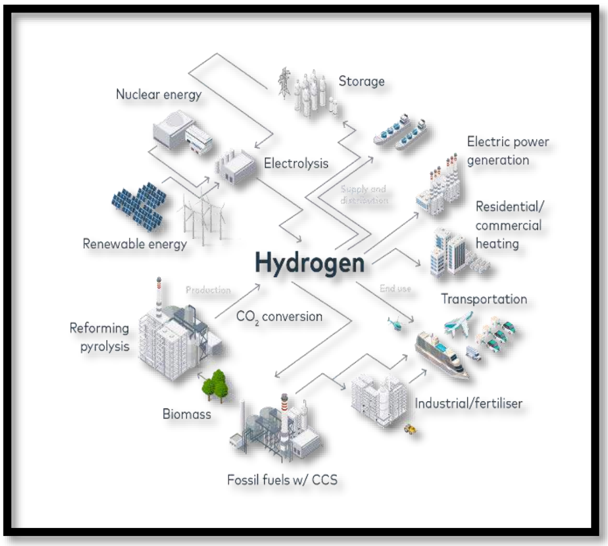
This update to India's existing NDC translates the 'Panchamrit' announced at COP 26 into enhanced climate targets. The update is also a step towards achieving India's long-term goal of reaching net-zero by 2070. In line with this, the National Green Hydrogen Mission was approved by the Union Cabinet, with the intended objectives of: Making India a leading producer and supplier of Green Hydrogen in the world.

Process control instrumentation takes a pivotal role in the hydrogen industry. It is applied for process control, its safety and, helps to make the process even more efficient. It is especially important for processes operating under unsteady conditions. Instrumentation can be found from the producing electrolyser plants via the measurement of hydrogen flows at the interfaces between different companies and during its transportation over pipelines or tankers until used for re-electrification in combined cycle power plants.

HYDROGEN CONTROL AND AUTOMATION ARCHITECTURE

The anatomy of a hydrogen hub can be divided into four segments: hydrogen production (making it), hydrogen storage and hydrogen transportation (moving it), and electrical power generation (using it).

Each of these segments can then be divided further. Hydrogen production, for example, will occur through a variety of different processes from many different producers. Production methods will range from existing fossil fuel facilities using steam methane reforming that will likely be modernized by adding carbon capture units, to new electrolyzer and biomass facilities. Hydrogen that is produced across these processes will then need to be transported to either storage facilities or electrical power generation units. These different pieces will need to be monitored effectively and controlled efficiently to ensure a robust hydrogen network.



The Hydrogen value chain, Courtesy: Woodplc

The salient features of a control system architecture are:

(a) **Integrated (SCADA and distributed / embedded) controls**: In order to get an accurate depiction of what is happening across an entire hydrogen hub, the control system should supervise electrolyzers and other hydrogen generation units, monitor pipeline activity, control electrochemical fuel cell interface with the power grid, and interface with safety instrumented systems (SIS). This means data from PLCs, DCS and SIS systems will all converge to a central location with the help of remote/SCADA systems. Advanced applications will need to be evaluated for integration between hydrogen hubs and both the electric grid and natural gas grid, to manage grid balance.

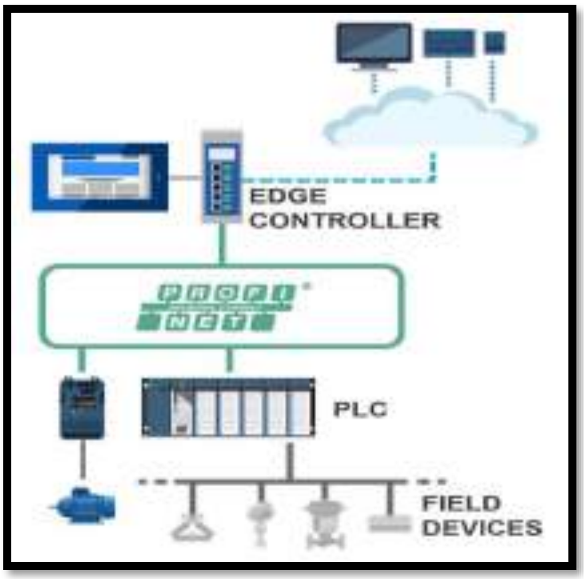
(b) **Safety systems**: As hydrogen can be highly volatile, safety system implementation is a crucial piece of hub integration. Because hydrogen usage is well established across industries, regulations, guidelines, and codes and standards already exist to facilitate safety guidelines around the industrial use of hydrogen. In addition to existing regulations, systems have already been put in place to establish codes and standards that facilitate hydrogen and fuel cell commercialization. Layer of protection analysis (IEC 61511/ISA84) will continue to govern safety integrity level (SIL) implementation for safety instrumented systems (SIS).

(c) **Human-machine interface (HMI), alarms and production, demand analytics**: The HMI should be structured so that operators are quickly alerted to abnormal conditions and can take immediate action to rectify any issues. High performance graphics, following ISA-101 HMI standard should be developed so that operators are presented with useful information rather than being overloaded with data points. Display hierarchy is critical to the development of hydrogen hub HMI because of the vast network of assets that are integrated to a central system. Analysis should be done in advance to determine how to structure this hierarchy as well as how to best integrate future assets as they become connected to the hub.

(d) **Alarm rationalisation**: A robust alarm system will be an important part of the hydrogen hub's central control system for operators to be quickly alerted to abnormal conditions across the entirety of the hydrogen hub. Alarm rationalisation (as per ANSI/ISA-18.2) will minimize the number of alarm activations and nuisance alarms. Following rationalisation, the alarm system will result in a rapid response from control room operators who learn that the alarm system can be trusted to only report on necessary events, thereby reducing complacency.

(e) **IT/OT infrastructure**: Technology advancements in recent years have led to a push for the convergence of IT and OT systems, but it is important to understand the purpose of each system. OT systems prioritize maintaining reliable and safe production operations while IT systems prioritize securing business data. Multiple different private entities will form hydrogen hub networks composed of differing equipment vendors and communication technologies. Careful planning is required so businesses can share vital production data with the entire hub, while protecting their own business networks and ensuring overall system security and integrity in line with Industrial Control Systems (ICS) is based on IEC/ISA 62443. The hydrogen hub in turn will likely require its own independent IT network infrastructure. Early planning of this network architecture allows communication to be streamlined across the networks associated with all involved private entities.

(f) **Cybersecurity**: Integral to IT/OT infrastructure planning is cybersecurity. Traditional IT risk assessments do not fully capture process risks at the OT level as highlighted by ANSI/ISA/IEC 62443. This is where new cyber risk assessments as part of CHAZOP (Control Systems HAZOP methodology) is useful. Performing CHAZOP allows us to systematically identify key risks at the OT level that have health, safety and environmental implications. Performing a CHAZOP will help stakeholders and decision-makers identify true risks across the hydrogen hub and take appropriate mitigation measures.



A portfolio of PLCs, edge controllers and HMI/SCADA software can be integrated with intelligent field devices to provide a complete automation and IIoT solution for the safe and efficient production of hydrogen. Courtesy: Emerson

ADVANTAGES OF AUTOMATION

Due to the distributed nature of hydrogen production, solutions must address a range of automation requirements, while providing exceptional connectivity. Digital platforms and methods for automating hydrogen production offer the following advantages:

- Provide reliable deterministic control in harsh field conditions
- Offer options for redundancy
- Be scalable and modular for expanding and converting infrastructure
- Support fast-track designs
- Enable open and interoperable connectivity in the field
- Incorporate native security
- Include cloud connectivity and data management for remote access and detailed analysis.

Designers need PLCs, both compact and high-performance models, with IIoT capabilities to effectively transfer data and inform better decisions. More advanced equipment needs the extra computing capabilities of edge controllers, or even industrial PCs, to execute innovative control schemes and to closely integrate operational technology (OT) field equipment with information technology (IT) to deliver best performance.

It is important to consider whether an automation partner offers a breadth of complementary elements such as safety devices, instrumentation, analyzers, and valves — especially as each of these items becomes more intelligent and readily networked with control platforms. Availability of asset management system, maintenance and support services ensures investment protection.

AREAS IN HYDROGEN PRODUCTION CHAIN WHERE AUTOMATION CAN BE OF IMPORTANCE

(a) **Corrosion monitoring**: Hydrogen production skids can be subject to product streams with excessive corrosion-causing sulfur. Modern PLC controls must connect to analytical instruments to enable real-time gas purity analysis, detect problematic conditions, advise operators, and even automatically add inhibitors to improve plant safety by maintaining equipment integrity. Advanced corrosion detection instruments can be integrated to track equipment degradation.

(b) SMR (Steam Methane Reforming) optimization: Operators want to run SMRs at the maximum possible efficiency, but overly aggressive steam firing leads to unacceptable pressure increases, equipment failure, and even personnel injuries. Edge controllers go beyond basic PLC automation by performing advanced calculations with local and external data to determine the optimum operating setpoints within safe boundaries, and to ramp steam injection up or down to avoid unplanned disruptions.

(c) Leak prevention: Hydrogen leaks represent an extreme hazard anywhere, but especially so at storage units. It is extremely important to integrate instrumentation and remote I/O with automation to detect leaks and command the systems to a safe state. With the right measurement technologies, it is possible to monitor hydrogen tank lining conditions, thus avoiding leaks.

(d) Fueling stations: Fueling station are widely distributed. However, they have many of the same needs for automation and condition monitoring as hydrogen production equipment, plus they need to work autonomously, while interacting with supervisory systems for commercial reasons. IIoT-capable PLCs provide a cost-effective and right-sized solution to control smaller local installations, while integrating IT-friendly data connectivity.

CHALLENGES IN HYDROGEN AUTOMATION

As the smallest and lightest element, incorrect handling can have catastrophic consequences. Therefore, electrolyzer components must be reliable and built for hazardous environments to protect people and property.

It is particularly important to work with a supplier who has a wide range of measurement, control and electrical devices specially designed to improve the reliability and safety in the hazardous areas of electrolysers. In addition to valves, valve systems, flow meters, regulators and pressure transmitters, they should also contain intelligent technologies, such as scalable process control and safety solutions. These should be able to reduce operational complexity, lower risks and improve the performance of green hydrogen plants. Site-wide security system functions are also relevant.

The challenges in hydrogen production and distribution extend through the supply chain in conversion, storage, and transport. Reliable controls are needed to address this hazardous energy source. These include shut-off and metering valves, high pressure regulators, pneumatic actuators, and solenoid valves. Reliable control and safety circuits provide the precision necessary to maintain adequate pressure and flow rates and ensure hydrogen purity. Sensors should be integrated for remote monitoring of pressure, temperature, and flow rates. When using intelligent devices, data can be collected to improve productivity, monitor plant status, and ensure high operating yields.

CYBERSECURITY IN HYDROGEN AUTOMATION PROCESS SYSTEMS

Operational Technology (OT) is becoming increasingly digital and internet-connected. This introduces security concerns for OT commonly used in federal facilities, where typically security had not been an issue before.

Previously, most OT was non-connected and had minimal cybersecurity vulnerabilities—but as new efficiencies and functionalities for enhanced flexibility and resilience are added, cybersecurity vulnerabilities need to be continually monitored and addressed. As more connected technologies, control systems, and distributed energy resources are added to federal facilities, installations, and campuses, it is more important than ever to consider cybersecurity. Poor cybersecurity posture can result in vulnerabilities that leave a facility open to an attack that can result in data corruption, financial harm, physical equipment damage, disruption of services, and even loss of life.

Due to the complexity and cost of acquiring new equipment, technology, and operational systems, OT is frequently not replaced at the same rate as consumer or informational technologies. Thus, federal facility managers and operators face additional challenges in protecting legacy systems from cybersecurity threats, especially given that these systems are not likely to have the same cybersecurity protective capabilities as modern technology and may risk disruption if traditional IT cybersecurity protection and detection capabilities and solutions are applied.The recent ransomware attack on Colonial Pipeline is just the latest to underline the vulnerability of energy infrastructure to attacks by criminals or state actors. As the IEA has outlined, despite the gains digital technologies bring, they have significantly expanded potential vulnerabilities.

Modern, leading solutions such as Honeywell Experion DCS, Safety Manager and ControlEdge PLC have embedded cyber security capabilities that are ISASecure certified. This offers robust cybersecurity built into OEM package control systems so that end users can build cyber-secure plants. OEMs and end users also benefit from secure remote connectivity to their assets, while mitigating the threat from bad actors.

FUTURE IN HYDROGEN AUTOMATION

Hydrogen's many potential uses, directly as a carbon-free fuel or to store and transport renewable energy, are about to make hydrogen invaluable in substantially lowering man-made CO2 emissions and integrating renewable energy into the industry's value chains all over the world, into the transportation as well as the power and building sectors.

Environmental stewardship is one of the most important issues of the 21st century and hydrogen fuel producers are rising to the occasion. By scaling up hydrogen production, fuel producers can bring us closer to a zero emissions world.

REFERENCES

1. Nishadi Davis, Control systems integration: The hydrogen hub backbone, Woodplc
2. Jim Cahill, Jorg Brahm, Overcoming Challenges in Hydrogen Production and Distribution, Emerson Automation Experts

AUTHOR PROFILE

Praseed Sahu is a mechanical engineer having more than 9 years experience in mechanical upkeep of mega scale petrochemical complex. A graduate in Mechanical Engineering from NIT Rourkela, he currently works in Projects Development department of GAIL (India) Limited where he is responsible for Green

Hydrogen and Renewables project investments.

He is part of the team executing India’s first large scale green hydrogen plant in GAIL Vijaipur. He has also been selected for the prestigious Indian Engineering Services conducted by UPSC in 2015.

Mukul Gupta is a vibrant performance-driven professional with more than 13 years of experience in Sustainability & Environment Management with India’s major Maharatna Company GAIL (India) Limited. He is currently working as Chief Manager at GAIL's Premier Natural Gas based Petrochemical Plant at Uttar Pradesh.

Mukul Gupta has done BE in Environmental Engineering from Delhi Technological University (Previously Delhi College Of Engineering, DCE in the year 2009 followed by PG diploma in Environmental Law from National Law School, Bangalore, in 2015.

Alarm analysis and optimization aiming to maximize yield with enhanced safety integrity for petrochemical plants.

Manu Mehta, Vivek Sethi

GAIL (India) Limited, Pata

ABSTRACT

Alarms are basic building blocks for a concrete safety system. Industrial alarm systems are very critical for the efficient and safe operation and control of plants and maintain system integrity. Alarms are used to inform the operator about possible process deviations from the normal so that the operator can take appropriate corrective action prior to triggering of unforeseen scenarios.

One of the widespread issues currently in production plants is alarm and event overload. This is partially as a result of formerly independent systems that are integrated for more effective operation. Each operator then has to monitor an increasingly wider area and consequently deal with more alarms. Without rigorous alarm rationalization efforts, alarm flooding becomes a serious problem and increases the risk of safety and environmental incidents.

Alarm Management system should have capabilities for extensive analysis and fast decision making for sustained Industrial operations in refinery and Petrochemicals.

- Analyse the alarm frequency within the predefined period
- Identifies chattering
- Monitors Real-time frequency
- Create shift-wise report of alarms
- Histogram of daily alarms
- Correlation of independent alarm

The purpose of Alarm Information Management System is to provide a centralized alarm information over and above the alarm summary information provided to operator through DCS. This system is used for acquiring, sorting, and transforming the raw alarm data into intelligent and actionable information.

KEYWORDS

Alarm rationalization, ISA18.2, Chattering alarms, Standing Alarms, DCS, EEMUA, Alarm Flooding.

INTRODUCTION

Alarm Information Management System (AIMS) is an alarm management package, which gathers alarm information from various sub-systems and presents the desired meaningful analysed data for information and further analysis.

The purpose of Alarm Information Management System is to provide a centralized alarm information over and above the alarm summary information provided to operator through DCS. This system is used for acquiring, sorting, and transforming the raw alarm data into intelligent and actionable information.

SIGNIFICANCE

One of the widespread issues currently in production plants is alarm and event overload. This is partially as a result of formerly independent systems that are integrated for more effective operation. Each operator then has to monitor an increasingly wider area and consequently deal with more alarms. Without rigorous alarm rationalization efforts, alarm flooding becomes a serious problem and increases the risk of safety and environmental incidents.

There are a number of alarm management standards and guidelines such as ISA-18.2-2009, IEC 62682 and EEMUA 191 that help us rationalize our alarm systems. Plant operators are often faced with a high number of alarms and abnormal situations. ISA SP18's goal is to provide a useful set of guidelines for developing and maintaining alarm systems. They are therefore unable to respond quickly enough. In addition, a poorly applied alarm management philosophy may result in excessive alarms that can cause operators to routinely ignore these alarms due to the information overload.

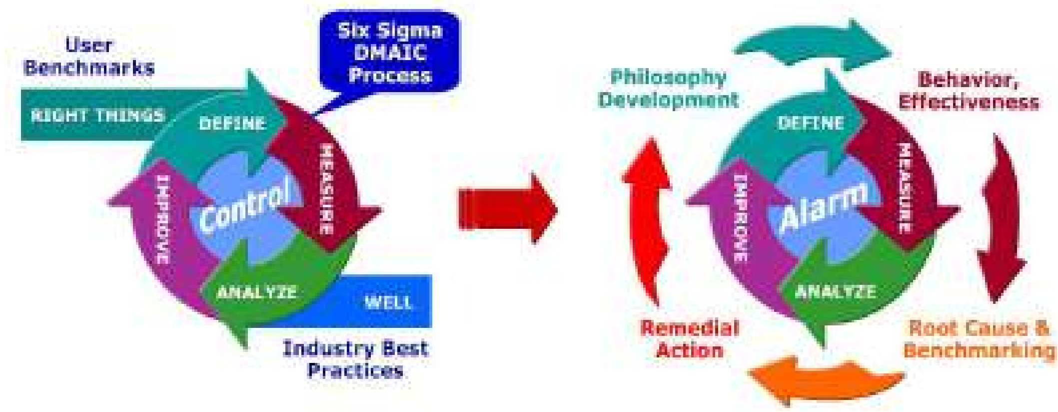
Alarm Information Management System (AIMS) is an alarm management package, which gathers alarm information from various sub-systems and presents the desired meaningful analyzed data for information and further analysis.

According to the Engineering Equipment and Material Users Association (EEMUA), for example, the DCS operator can effectively address up to 150 alarms a day, which averages out to an alarm every ten minutes. An alarm every five minutes or 300 alarms a day is still considered manageable. Of course, the reality is much different. Typical alarms for a large refinery could average over 14 thousand per day.

Long Term Average Alarm Rate in Steady Operation	Acceptability
More than 1 per minute	Very likely to be unacceptable
One per 2 minutes	Likely to be over-demanding
One per 5 minutes	Manageable
Less than one per 10 minutes	Very likely to be acceptable

EEMUA Criteria for Steady State Operations
(Source: EEMUA Publication No. 191)

The push for operational excellence in plants today is also driving the need for more effective alarm management. Plants are operating closer to their limits than ever before, and users are continuously looking for new ways to increase operational excellence by reducing downtime, increasing productivity, and implanting real time performance management (RPM) strategies for their plants. Effective alarm management strategies are a key component in achieving all of these goals. The need for effective alarming is increasing dramatically in spite of the fact that most alarm systems are not effectively used. As alarm systems become less effective, they diminish the effectiveness of all automation.

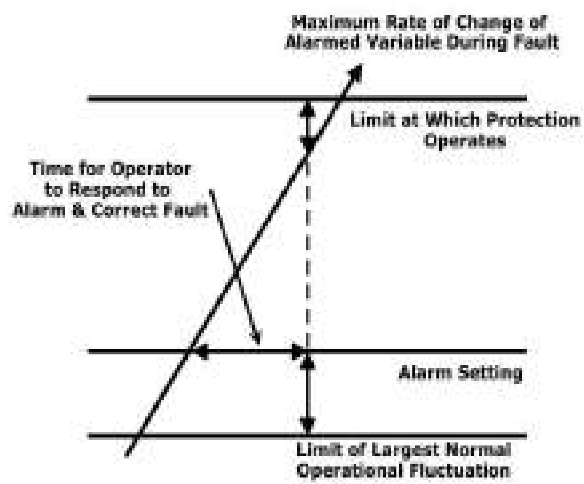


The Correlation of Operational Excellence to Alarm Management

Define relates to Philosophy Development, Measure relates to determining Alarm Behaviour and Alarm Effectiveness, Analyse relates to Root Cause Analysis and Performance Benchmarking, and Improve relates to the Remedial action necessary

Alarm Settings Must Give Operators Appropriate Time to Respond to Faults

Source: EEMUA Publication 191to align the prevailing implementation with the Alarm Philosophy. Finally, Control relates to Alarm execution.



Alarm Settings Must Give Operators Appropriate Time to Respond to Faults
Source: EEMUA Publication 191

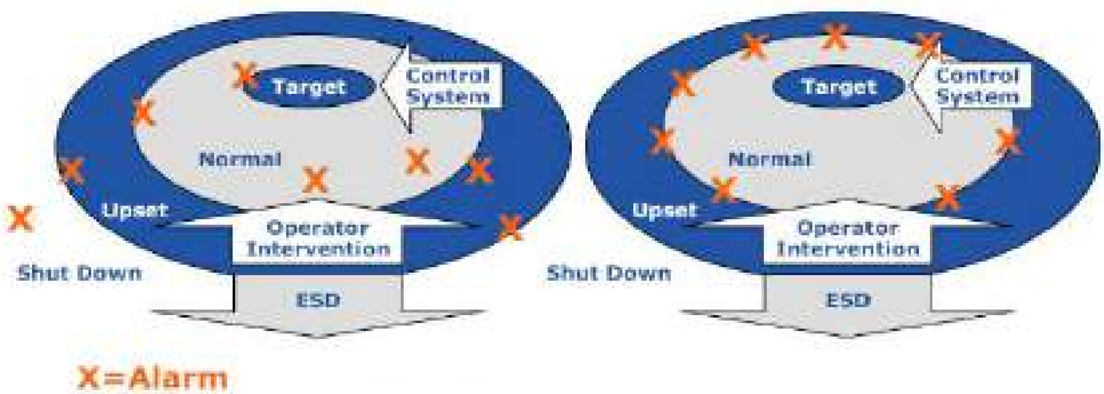
PHILOSOPHY AND RATIONALIZATION

There are actually two parts to this step. The first is the development and maintenance of the alarm philosophy. This document needs to cover everything anyone needs to know about this alarm system implementation. It should be considered the design definition.

The second part is the alarm rationalization. This systematic process optimizes the alarm database for safe and effective operation. It usually results in a reduction of the number of alarms, alarm prioritization, validation of alarm parameters, evaluation of alarm organization, and the number of alarms assigned to an operator, and finally alarm presentation.

Selection of alarm settings is one topic to which the EEMUA guidance devotes a significant amount of time. EEMUA's position is that alarms should be set at the point where the operator must take action. If alarms are set too conservatively, then they are triggered within normal operating parameters.

Conversely, if alarms are set outside the normal operating range of the plant, it is too late for the operator to take action.



An Effective Alarm Should Mark the Point Where the Operator Should Take Action
Source: EEMUA Publication 191

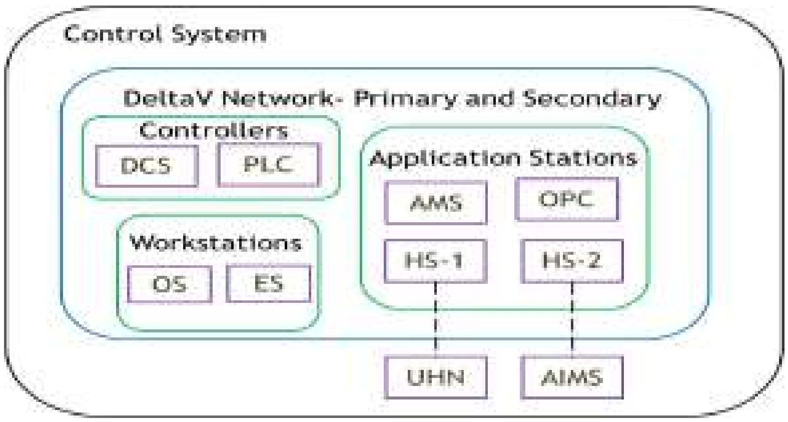
Area	Benefits
Safety	Reduced risk of human injury and incidents.
Unplanned Downtime	Avoid plant shutdown, lost product, and associated costs.
Information Management	Avoid nuisance alarms, improved fault tracing.
Role of the Operator	Give operator more time to focus on the process, creating knowledge workforce.

Key Areas of Alarm Management Justification

CASE STUDY

Systemic enhancement of Alarm & Information Management System contributing to overall reduction in alarms by 10%

Emerson DCS have SUPRA Alarm Information Management System which captures data from Historian through ODBC connectivity. Alarm server handles multiple date-time formats, event definition – alarms, operator actions, system diagnostic messages and track configuration changes whereas client is used for logical representation of alarms and events.

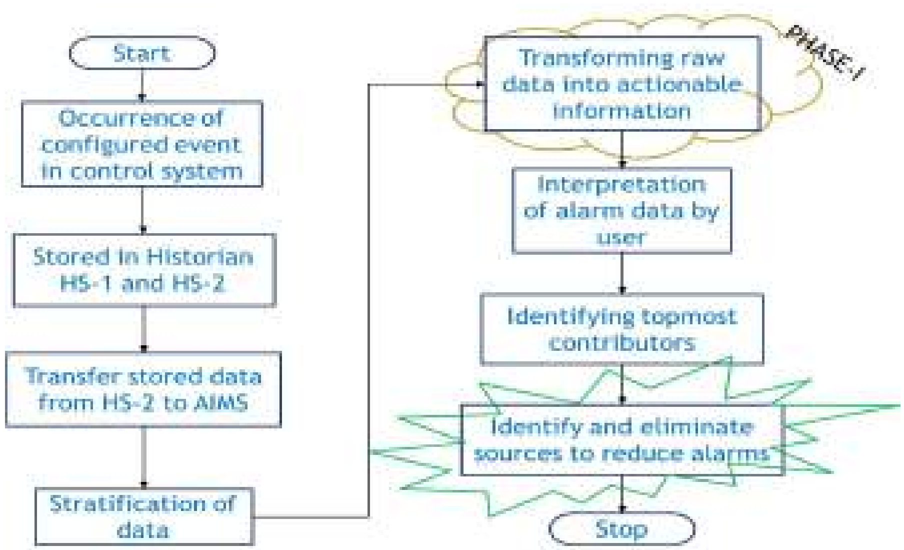


System Architecture

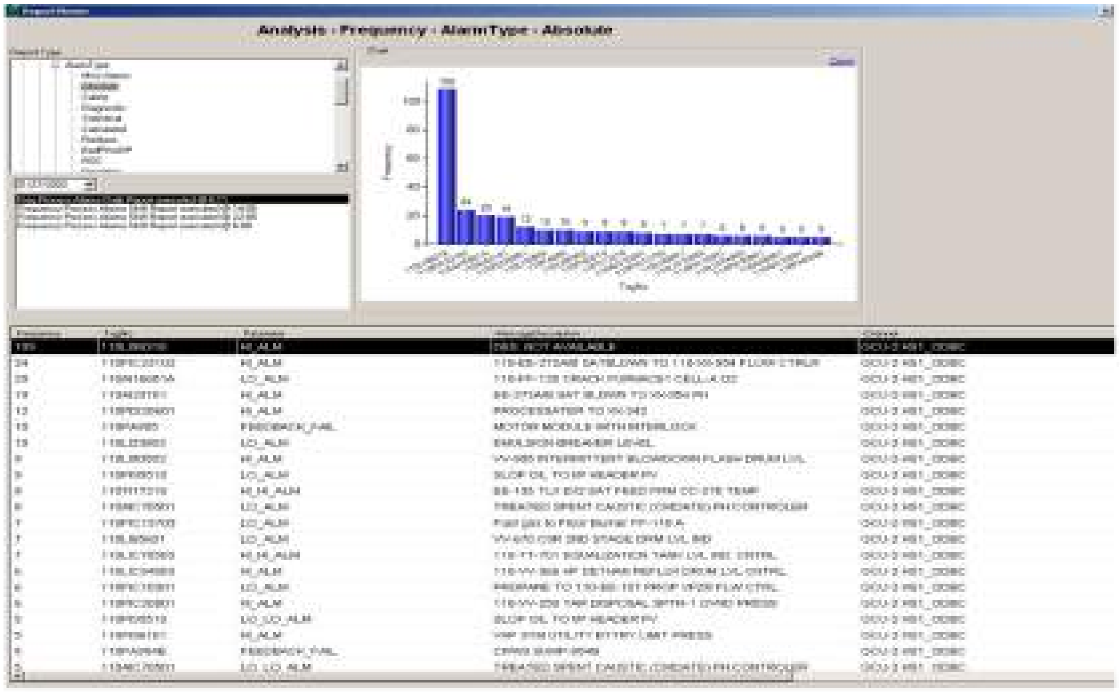
The following types of alarms are acquired by AIMS.

- Process Alarms
- System Alarms
- Operator activities
- Maintenance alarms

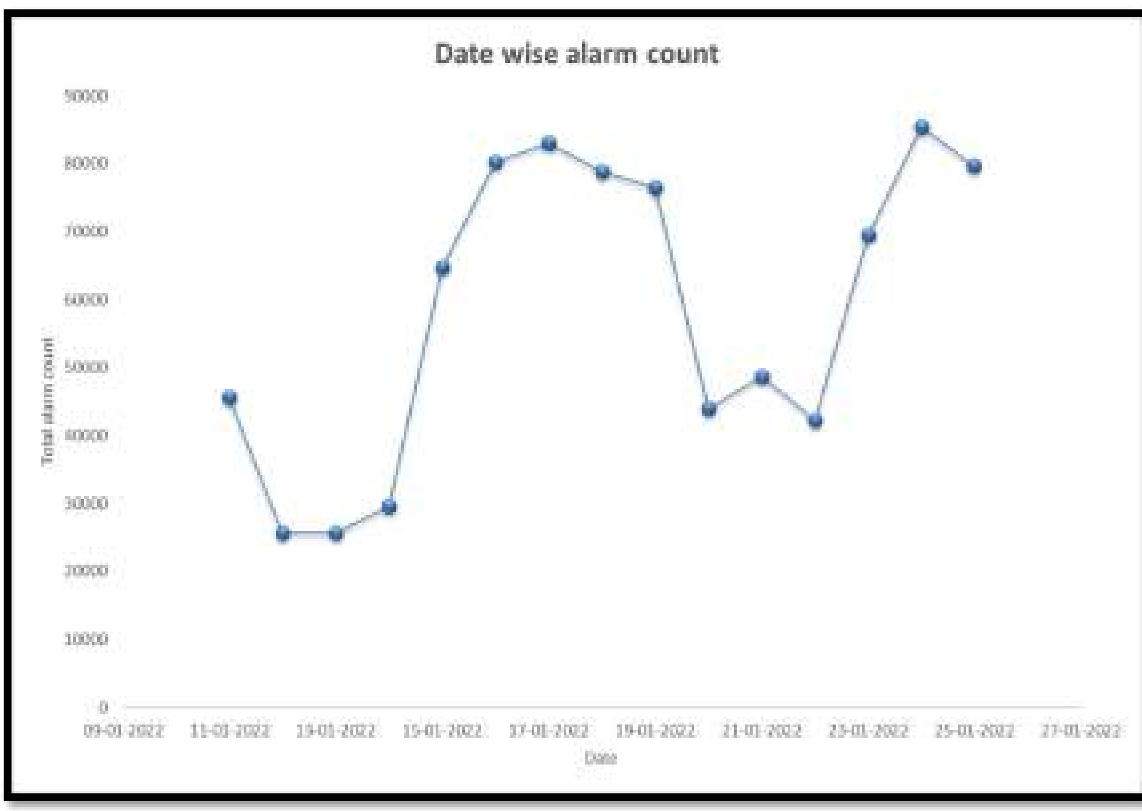
<u>High Level Flow Chart</u>



Samples of application interface of AIMS system are shown below:



Frequency Analysis Trend – Absolute



Underutilization of AIMS System	Below Spec Server	Maybe	Additional Software maybe required which require upgraded software
	Connection issue	No	All physical connections checked
	Interface	Maybe	Current interface for alarm and event display is not productive
	Requisite software	Yes	The current software used for display has limited capabilities
	Database connectivity	Yes	It is observed that there is gap in data collection due to overloading
	Sorting Tools	Yes	The alarm data available is not in a form which can enhance utility
	Vendor support not available	No	Vendor support is available.

Cause Effect Matrix

CHALLENGES

1. Database connectivity

It was observed that continuous connectivity to the historian database is hindered because of overloading of virtual printer. The virtual printer was not able to push data to the AIMS system and needed to be restarted at least once in a day. Due to this data gaps were created in alarm collection.

2. Requisite Software

Alarm server handles multiple date-time formats, event definition – alarms, operator actions, system diagnostic messages and track configuration changes whereas client is used for logical representation of alarms and events. The client software is not up to the mark and provides only limited reports and trends.

3. Sorting Tools

The data collected by alarm server cannot be utilized by other common Microsoft analytical tools for further analysis. Discussion was done with vendor to convert the collected data into a form which can be easily ransformed into multiple actionable information.

4. Interface

The current interface in which we observe alarm and event is ineffective and it was discussed with vendor to prepare a dashboard which displays suitably segregated data.

SOLUTION DEVELOPMENT

The stated capabilities of AIMS remain underutilized due to lack of presentable reports which enable logical processing of events and facilitate assessment of dynamic plant scenarios.

The system shall be able to carry out statistical analysis on the alarm data gathered and generate actionable reports based on a logical combination of states, conditions and events. Some examples of such reports are:

- Alarm count by area
- Alarm Flood report
- Symptomatic alarms report

- Standing alarms over time
- Shelved alarm report

Along with these reports a single window dashboard which would display **daily alarm count area wise**, would be helpful in analyzing the overall status of alarm and event history by comparison with baseline.

IMPLEMENTATION

Step 1: Establishment of dependable database connection

As established, the connection of AIMS server to historian database was not robust. To make sure that there is no gap in data collected and continuous availability of Alarm and event data a solution was provided by vendor which did not require any additional software or hardware. The data collection method was changed from virtual printer to ODBC (Open Database Connectivity) connectivity which is an open standard Application Programming Interface (API) for accessing a database. After establishing connection through ODBC the problem of **database connectivity** was resolved.

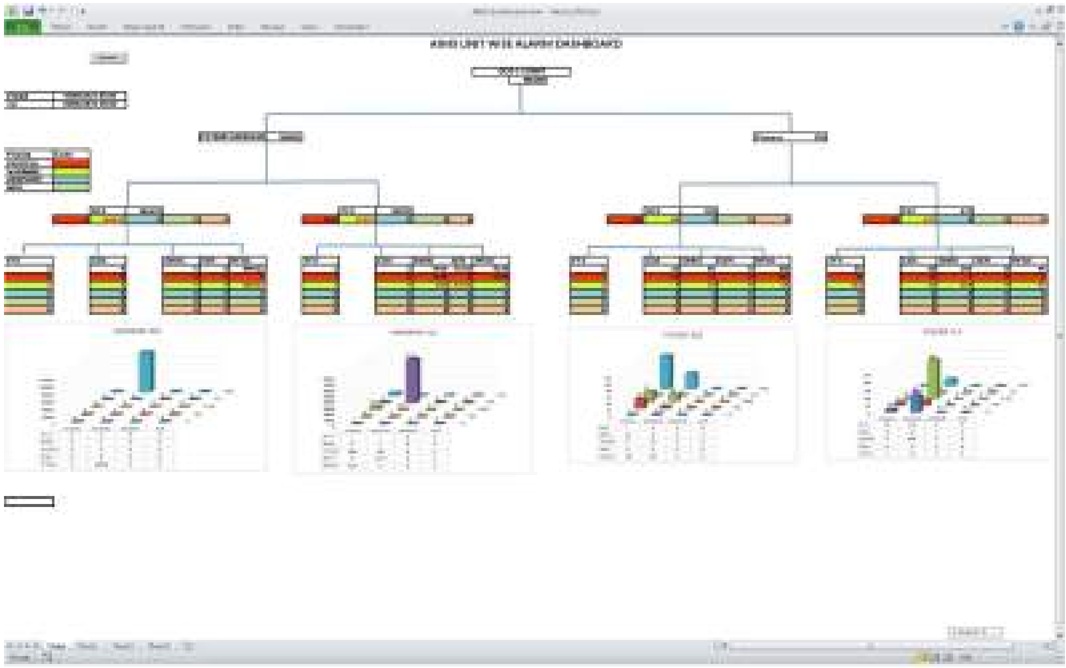
Step 2: Installation and configuration of add-in software

Once it was established that database flow is now smooth next step was to install the add-ins required for fulfilling our objective. Vendor recommended "SAMA XL reporter for AE" as per specification and requirement put forward by us. This add-in provides the capability of data collection from Server to Microsoft Excel. We can also generate different kinds of report as per our requirement.

Step 3: Development of dashboard and report generation

Once the add-in was installed system was ready to capture data in MS Excel so that dashboard can be prepared. As this required repeated programming and testing, the system was required to be disconnected from DeltaV network. To facilitate this, remote assistance was provided by SUPRA service engineer for further programming in house by UJJWAL-3 team. Then, for testing purpose the system was required to be connected again to the DeltaV network so that data can be collected for a day or two and then testing is carried out.

After rigorous effort of our team for around six months the dashboard was finally ready to use. Since the data is readily available in Excel format all the statistical capabilities of excel can now be capitalized for analysis of alarm data. Some examples of the same are as shown below:

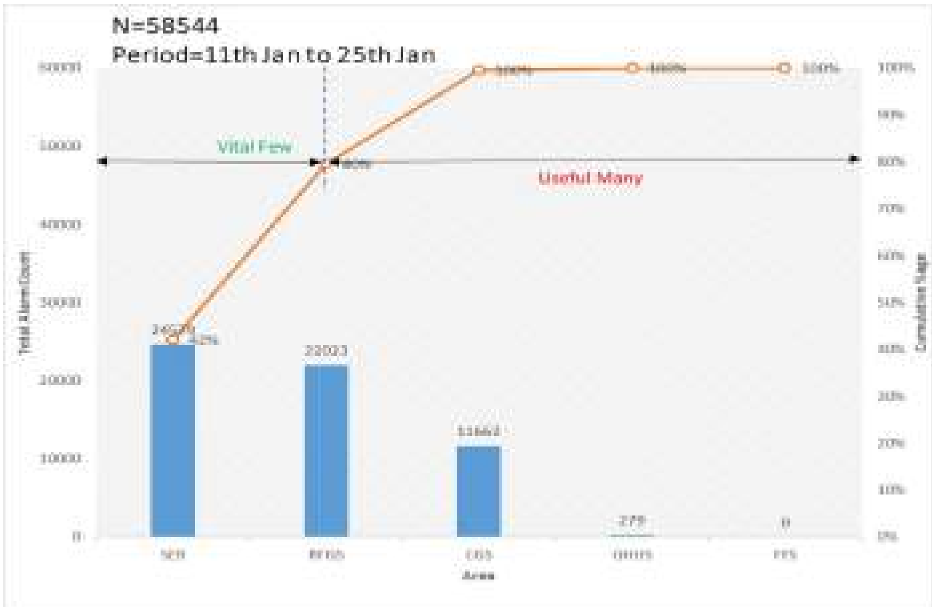


Complete Dashboard

Along with dashboard some useful reports are also configured which readily provides actionable data which can be utilized for analysis and daily tracking of effectiveness of actions taken by us to reduce the quantum of nuisance alarms for both chattering and standing categories.

Step 4: <u>Data analysis and alarm reduction</u>

From the dashboard we extracted the total alarm count related to system and carried out pareto analysis of same.



Pareto of alarm count dated 16.01.2022

On further drilling the individual causes were segregated to eliminate the system alarms and changes were made in the modules to eliminate the module errors which were generating nuisance alarms. Some of the common errors on which work is being carried out are as follows:

1. Field Device Failure
2. Unresolved References
3. IO Unassigned
4. Unassigned action block
5. Input Transfer Error

CONCLUSION

Before implementation of the project the alarm data was not available in usable form. Also, there was no way of segregating the alarm area wise which is now readily available in dashboard.

After implementation of solutions developed in this project problems related to connectivity of AIMS systems is resolved and data is now available in a form through which we can easily carry out statistical analysis of alarms. The daily reports generated are useful in tracking the effects of action taken to reduce the alarms.

<u>Benefits achieved:</u>

1. Alarm data is now available **in MS Excel**, so all the statistical capabilities of MS Excel can be exploited to carry out Alarm analysis. This analysis can now be used to preventively address system related issues.
2. Major contributors were identified and necessary measures are ongoing to achieve the target of reducing the alarms and events by 10%.
3. Since the spurious alarms are reduced, improved analysis of machine trips can be carried out due to decluttering of event database.
4. **Seamless connectivity** of AIMS system to the historian is established and there is no gap in data collection.

GLOSSARY

Control System: A collection of devices (termed as controllers) that directs or regulates the working of equipment or assists in maintaining process parameters in a plant.

Control Network: It is a network of nodes that collectively monitor, sense, and control or enable control of an environment for achieving optimum performance.

HMI: The hardware or software through which operator interacts with control system.

Usability: Usability refers to how successfully operator can use a software to accomplish the goals of the plant.

UX: User Experience encompasses all aspects of the end user's interaction with software or application including how it looks and feels

Alarm: A displayed message usually coupled with an audible horn that is automatically generated whenever a pre-defined condition is detected, such as a faulty instrument or an abnormally high or low measurement.

AIMS: Alarm Information Management System provides a centralized alarm information over and above the alarm summary information provided to operator through Operator station.

REFERENCES

- Holifield, Bill and Habibi, Eddie: The Alarm Management Handbook, Second Edition: A Comprehensive Guide; August 31, 2010
- Van Camp, Kim (Emerson Process Management) and Stauffer, Grosdidier, Pierre (Ph.D., P.E.); Conner, Patrick (P.E.); Hollifield, Bill; Kulkarni,
- Sarmir: A Path Forward for DCS Alarm Management; published by Plant
- Automation Services, Inc.
- Exida – Stauffer, Todd (Director – Alarm Management Services, exida): You Asked: Alarm Management - Setting a new Standard for Performance, Safety, and Reliability with ISA-18.2; published in Canadian Process Equipment & Control News; December 2009

BIOGRAPHIES

Sh. Manu Mehta was born in Meerut, India in the year 1987. He graduated in Instrumentation and Control Engineering from Bharati Vidyapeeth College of Engineering, Delhi. He joined GAIL (India) Ltd. in the year 2009. He also completed MBA in Oil & Gas from UPES, Dehradun in 2015.At present, he is working as Chief Manager, Instrumentation department, Petrochemical Maintenance in GCU-II, Petrochemical Complex, Gail Pata. He has myriad experience of over 13 years at Gas Cracker Unit, both old and new plants specific in Gas fired Furnace controls and safety systems.

LATEST TRENDS AND FUTURE OUTLOOK OF PRESENT DAY DCS

Arupjyoti Saikia

Engineers India Limited-Gurugram

ABSTRACT

This paper outlines the most visible technological trends for DCS in recent times including a future out-look assessment of the popular DCSs. Even after 45 years since its debut in 1975, the key DCS elements have not changed significantly. But, certainly, over the period of time a DCS system has benefited from the advancement of software and hardware in terms of computing power, speed and operational efficiency, ease of integration and enhanced functionality, security and reduced footprint. All such major developments including futuristic trends are presented here as assessed across the major DCS systems.

Disclaimer: any *mention of DCS make, models etc in this paper is in no way meant for any endorsement, but for examples purpose only. The names are appearing in the context of the development & usage of the technologies*.

KEYWORDS

OPC UA, NAMUR Open Architecture, Hyper Convergence, IT/OT Integration, Digital Twin, Autonomous plant, Industry 4.0. IEC 61499

INTRODUCTION

The DCS was commenced in 1975. Both Honeywell and Japanese Electrical farm Yokogawa introduced their own independently produced DCS at roughly the same time, with the TDC 2000 and CENTUM systems respectively. Present day major DCS brands in Process, Fertiliser, Power industries are ABB, Emerson, Honeywell, Rockwell Automation, Schneider, Siemens, Yokogawa etc. Whereas the Asia Pacific region is witnessing the highest market growth in the period of 2019 - 2024 followed by the Latin America and Africa, even after 40 years, the key DCS elements have not changed significantly. But, certainly, over the period of time a DCS system has benefited from the advancement of software and hardware in terms of computing power, speed and operational efficiency, ease of integration and enhanced functionality and security.

For end users and for consultants, it would be of great interest to have a general review of the ***"what is happening, what is the future like"*** in the world of DCS.

Therefore, a comprehensive study is carried out to capture the most visible technological trends of the DCS in recent times. This study also includes the future out-look assessment of the popular DCSs.

OPC UA

OPC DA (Data Access) is the predecessor of OPC UA (Universal Access). OPC DA which relies heavily on Windows Distributed Component Object Model (DCOM), is not a truly open standard, behaves poorly in a disconnected state, does not work very well with firewalls, and only works in Windows. To overcome these drawbacks of OPC DA, the OPC Foundation developed OPC UA with the below features (a.) Open- available for anyone to use (b.) Cross platform- it is not tied to one single operating system or programming language (c.) Increased protocol security- provides users access to authenticity, authorisation, integrity and confidentiality. It is a technology based on IEC 62541 framework, a framework that provides vendors with an independent platform allowing secure and reliable information exchange.

Deployment of OPC UA in DCS speeds up and improves the accuracy of the system integration. OPC UA can be important in modernizing DCSs for Industry 4.0. Industry 4.0 is the fourth industrial revolution, defined by incorporating advanced technologies such as IoT, Big Data, and Artificial Intelligence. OPC UA allows these technologies to be seamlessly integrated with DCSs, which can help improve industrial processes' efficiency, flexibility, and performance.

Utilization of OPC UA protocol in DCS promises to deliver broad communications benefits which intends to reduce security risks, while improving overall compatibility and flexibility.

NAMUR OA

NAMUR Open Architecture (NOA) is a futuristic plant automation system approach. The most simplified architecture here is the deployment of OPC UA for converting all proprietary interfaces to convert to open interfaces with a highly reliable IT infrastructure as described above.

HYPER CONVERGENCE & VIRTUALIZATION OF PC

Virtualization of PC and use the virtual machine in DCS would potentially reduce hardware and possibly reducing footprint. The virtual machine (VM) runs on a "thin client" HMI and Virtualized DCS project development ecosystem. Virtualization concepts are being widely deployed in peripheral DCS servers and slowly making inroads to the core system level.

Hyper Convergence Infrastructure (HCI) is a step further. Underpinned by virtualization technology, Hyperconvergence is gradually making strong hold in the IT world. HCI is a software defined unified system that combines all the components of a traditional data center e.g. storage, compute, networking and management into single appliance.

HCI delivers simplicity and flexibility, scalability, data security as compared to legacy infrastructure. Integrated storage, servers and networking devices are designed to be managed as a single entity across all instances of an HCI. HCI environment saves cost in below capacities including (a.) data center power and space (b.) Management Efficiency (c.) Data Efficiency (d.) High Availability (e.) Scalability (e.) Data Protection. (f.) Ease of upgradation without depending on single vendor.

Virtualization solution through hyperconverged infrastructure (HCI) in a DCS offers easy scalability to help organizations future-proof their operations while also improving their sustainability, efficiency and overall performance. Virtual Unit Operation Controller (UOC)™ provides features whereby Configured applications can be tested and validated in the cloud or locally in the Virtual environment and then downloaded to the physical UOC without reassignment or further testing and validation.

REMOTE FIELD MOUNTED IO

"Remote I/O enclosure at field" approach got several benefits, which includes reducing cost, improving the overall project schedule as it can reduce or eliminate marshalling. Electronic Marshalling is aimed at replacing the traditional process I/O modules with either "smart" I/O modules or single-point smart signal conditioners. It promises reduced footprint, environment flexibility, I/O flexibility, ease of expansion/revamp, integrated barriers, App based troubleshooting.

DCS OEMs provide solution for a remote I/O system for mounting directly in the field. Zone 2 Remote I/O architecture allows I/O cards to be installed remotely from the controller. Intelligent Enclosures are specially being developed for use in hazardous area.

INTEGRATION OF OT & IT

Operational Technology (OT) and IIoT coupling in DCS is a step towards Industry 4.0 realization.

While the modern organizations grapple with two worlds of IT and OT, today, the worlds of IT and OT are converging. Advances in technologies such as the Internet of Things (IoT) and Big Data Analytics are systematically allowing the *digital information world* to see, understand and influence the *physical operational world*. When implemented properly, IT/OT convergence can merge business processes, insights and controls into *a single uniform environment*.

Today, the OT world is rapidly adopting new IT practices such as virtualization, cloud, AI, agile DevOps and Edge computing.

HYBRID DCS

A hybrid DCS integrates distributed control technology with the full functionality of a multi-purpose PLC. It brings out cost effectiveness.

Hybrid DCS is an automation system allowing to engineer, operate and maintain entire plant in a single common database. There are examples where the DCS is empowered by their most powerful legacy PLC controllers combined with cyber-secured architectures, and improved system availability and workflows.

ADDING HUMAN ELEMENTS

Adding human element to new console design for the operator who sits there for 8-12 hours controlling a volatile process taking critical decision is already taking place, bringing plethora of innovation in the console design.

Human Interface Stations (HIS) are designed to minimise operation errors and losses by using the mental model of plant operators to offer intuitive Look & Feel operability, based on Human Factors engineering. Ergonomically designed Console increases operator effectiveness by providing faster response, reducing fatigue, and increasing situational awareness.

DCS & ECS INTEGRATION AS PER IEC 61850

IEC 61850 is a global standard for Ethernet-based communications and system architecture in substation automation and power distribution systems.

IEC 61850 interface protocols enable integration with the Electrical Control System (ECS) in a single control platform through DCS. Therefore, the strategy is to take benefit of both the world of Process and Electrical operations and automation. With Profinet, IEC-61850 and an industrial Ethernet, it is expected that the DCS will be able to tightly integrate electrical system packages along with instrumentation for process control into a common system. However presently such applications are limited to the power plant operations mainly.

IEC-61850 uses Ethernet as backbone communication and it enables DCS controller integration for medium and high voltage electrical equipment. Used with electrical power distribution and substation equipment, IEC-61850 is being deployed within medium and high voltage drives, switchgear, motor starters, relay protection, generator and transformer protection, excitation and synchronization. DCS integration with IEC-61850 includes control, monitoring, asset monitoring, time stamp and integrated configuration tools to program the Intelligent Electrical Devices.

MAIN AUTOMATION CONTRACT

Another radical approach is the project execution through Main Automation Contract (MAC). A MAC is engaged to supply, coordinate, and/or manage all automation related aspects (e.g. Process Control System, APC, Analytical Systems, Field Instruments, Electrical Systems, Safety Systems, Automation Design & Engineering, Operations and Management & Training etc.) of a major capital project.

CLOUD BASED DCS SYSTEM, WEB BASED DCS SYSTEM

Cloud-based DCS system advantages include remote access and control, scalability, cost-effectiveness, advanced data management, and improved availability. These cloud-based DCS advantages can ultimately lead to improved efficiency, reliability, and safety of industrial processes. Web based DCS is being developed for improved usability, scalability and global collaboration. It provides accessibility from any device, without installing local DCS software and licenses and simultaneous access to multiple users from any location. As cyber security threat is alarming and real, there are efforts to address and mitigate current and future cybersecurity vulnerabilities. ISA/IEC-62443-4-2, "Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components", provides the cybersecurity technical requirements for components that make up an industrial automation and control systems (IACS), specifically the embedded devices, network components, host components, and software applications. The standard, which is based on the IACS system security requirements of ISA/IEC 62443-3-3, System Security Requirements and Security Levels, specifies security capabilities that enable a component to mitigate threats for a given security level without the assistance of compensating countermeasures. Standard security features like the ability to centrally manage antivirus scans, virus signature file updates, host-based intrusion detection systems and data loss prevention systems are adopted by some of the OEM's.

DECENTRALIZED CONTROL

Future DCS systems will move towards decentralized control architecture that allows for independent and adaptive control of different subsystems or devices in a process. This will provide more flexibility, and scalability and can improve the system's overall performance.

ADVANCED ANALYTICS

Advancements in data analytics and processing power will enable more advanced analytics capabilities in DCS systems, such as real-time process modelling, predictive maintenance, and optimized control strategies.

INTEGRATION WITH OTHER SYSTEMS

DCS systems will continue to integrate with other systems such as ERP, MES, and SCADA, providing a seamless integration of various plant systems and improving the overall efficiency of the plant. DCS increasingly integrating with other plant systems such as Laboratory Information Management Systems (LIMS) and Maintenance Management Systems (MMS). This is to provide a seamless integration of various plant systems and can help to improve the overall efficiency of the plant

AI AND SIMULATION BASED DIGITAL TWIN

AI and simulation based Digital Twins collaborate DCS because digital twins in particular tuned by AI, *can do things, that people can't*. All plants, irrespective of their maturity levels, are primed to identify and adopt digital technologies to move toward autonomy with the ultimate goal for *an autonomous plant* to keep pace for de-carbonization "Net Zero" goal as set in COP26 forum. A move to autonomous plants requires a digitally enabled approach to transform across the three fundamental aspects of the operating system -i.e. *Technical system, Management system, and People system*. Digital Twins (DT) is one of the most important enablers of digital integration for such an autonomous plant.

IEC 61499 -FUNCTION BLOCKS FOR DCS DESIGN

IEC 61499 defines a component-based modelling approach using function blocks. Function block is different than software block insofar as, a function block captures functionality that can be implemented as software or hardware or a combination of both. This standard was conceived because an increasing portion of the intellectual property (IP) related to the domain of industrial automation is now being expressed in the form of software. This standard stimulates economic

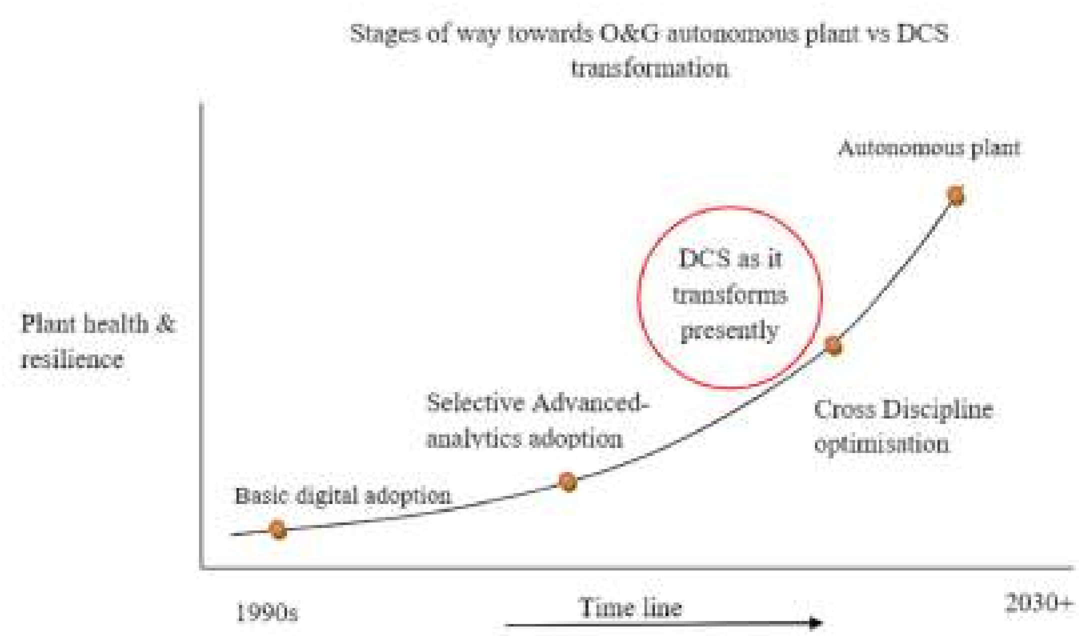


Fig-1

design and enables faster and easier reconfiguration. The standard's approach in dealing with DCS architecture is unusual when compared to other standards and their use in the domain of control and automation

CONCLUSION

DCS is emancipating from the conservative system architecture approach and infusing fresh ideas and technologies of the mainstream computing, and as a result, the DCS systems have typically become more open, more distributed, more integrated with safety and hazardous area barriers. This trend will continue to supplement for achieving the goal of *an autonomous plant* (Fig-1)

REFERENCES

- IEC 61805, 62541, 61499.
- NAMUR
- Websites of various DCS OEMs
- Control Engineering Magazines
- Timothy E Carone "Future Automation- Changes to Lives and Businesses"-World Scientific-2019 ISBN 978-981-3142-33-6

ACKNOWLEDGEMENT

The author is deeply grateful to HOD(Instrumentation) EIL, for his encouragement and guidance in materializing this paper.

BIOGRAPHY

Sh. Arupjyoti Saikia is serving as a Dy. General Manager (Instrumentation) in **Engineers India Limited-Gurugram**. He has over 23 years of experience which includes R&D, Maintenance and Engineering. As an Instrumentation & Control Professional he has extensive experience in execution of various Oil & Gas industry projects such as MRPL phase III PFCCU, GAIL Pata GCU-II, IOCL BS-VI, and overseas assignment, Dangote-DRPP and presently CBR-CPCL. He has published two papers in international Journals, two papers in Petrotech-2006, 2019, three in ISA Delhi-2015, 2019 & 2023 and one in FCRI Palakkad "Flowtek-G" Global Conference -2017. He holds B.E degree in Instrumentation & Control form Gujarat University and MBA from IMT-CDL Ghaziabad. He is a TUV certified Functional Safety Professional and Certified Blockchain Expert from Blockchain Council.

Dated 03rd, May 2023

Technical Paper for Petroleum and Power Automation Meet 2023 from

Fluke Technologies Pvt Ltd.,

(Global Leader in Manufacturing Testing and Measuring Instruments)

Fluke Corporation is a Global leader in manufacturing industrial test, measurement, and diagnostic equipment. Found in 1948 by John Fluke Sr., Fluke has helped define and grow a unique technology market, providing testing and troubleshooting capabilities that have grown to mission critical status in manufacturing and service industries. Fluke products are extensively used in Power, O&G, Metals and other heavy industrial segment.

From industrial electronic installation, maintenance and service to precision measurement and quality control, Fluke tools help keep business and industry around the globe up and running.

Fluke has achieved the top position in every market in which it competes. The Fluke brand has a reputation for portability, ruggedness, safety, ease of use and rigid standards of quality.
A wholly owned subsidiary of Fortive Corporation (NYSE: FTV), Fluke is a multi-national corporation headquartered in Everett, Washington, USA. Manufacturing centers are in the USA, the UK, Asia, and The Netherlands. Sales and service subsidiaries are in Europe, North America, South America, Asia, and Australia.

Market Segments

The Fluke product lines are beneficial for professionals in a variety of markets. Primary segments are listed below and include a brief description of the types of Fluke tools used along with their typical applications.

Calibration

Fluke has acquired global leadership position in the calibration marketplace with products in the line of Electrical, Temperature, Pressure, Flow, RF & Software. The Fluke Calibration line of calibrators, standards, calibration software products, and support equipment provide exacting standards for companies and government organizations who rely on tightly calibrated instruments for their quality and standards programs, as well as to meet strict international quality requirements.

Industrial/Electronic Service Installation and Maintenance

Today, electronics are integrated into an increasing number of electrical and electro-mechanical systems. Fluke's comprehensive line of digital multimeters, electrical power analyzers, thermal imagers, insulation resistance testers, accessories, plus the integrated ScopeMeter™ handheld test tools, are being used by a growing number of service technicians, plant engineers and installation and maintenance technicians. These tools provide them the ability to troubleshoot these complex new systems and detect problems quickly.

What is Calibration ?

- **Calibration is the activity of checking, by comparison with a standard, the accuracy of a measuring instrument of any type.**
- **It may also include adjustment of the instrument to bring into alignment with the standard.**

What are calibration standards?

Calibration standards are master instruments which can either be of measuring or sourcing standard that are more accurate than the devices that requires to be calibrated in a particular discipline. The standard’s accuracy varies depending on the Unit under test that needs to be calibrated; most professionals recommend using a calibration standard that is at least four times more accurate than the device being calibrated.

How Fluke implements the IIOT in providing best Testing & Calibration Solutions :

Fluke calibration products are built to be interfaced with a host at a high speed using LAN / RS232 / GPIB communication interface. The products are developed with remote protocols and drivers that helps software to easily communicate with the product for a bi-directional communication. Fluke Calibration, Asset Management and Reporting software helps performing Automatic Calibration and customized report generation. Asset Management tool pushes an auto-mail when any product / Device under test gets due for calibration. Workflow management module can be integrated with this software to track the product status once it is received in the lab for calibration until it is sent back. The calibration data gets stored in a database which gets installed over a server enabling the authorized once to access the calibration reports remotely.

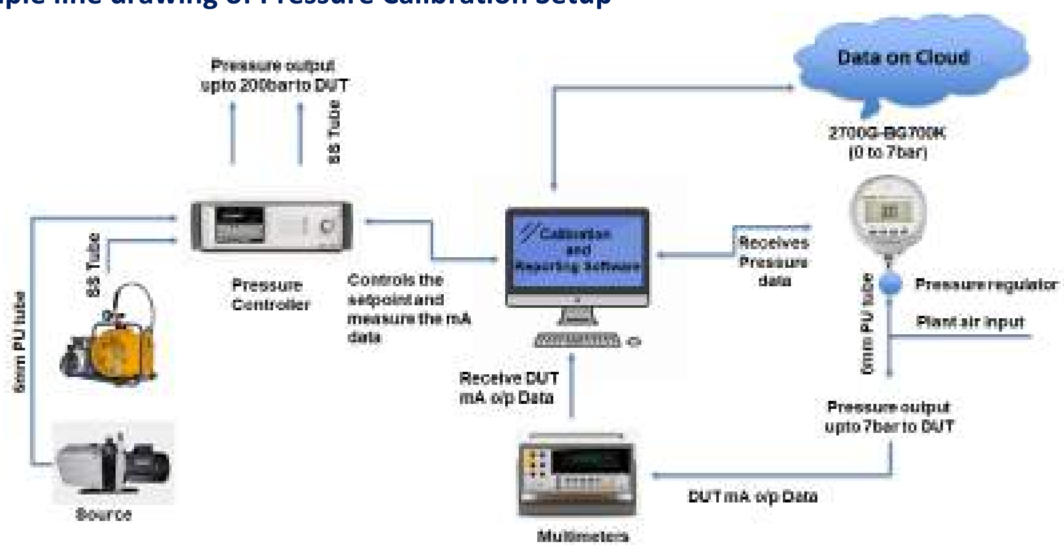
Our customers also get the Automation touch with portable products as Fluke field instruments comes with latest cutting edge technology known as Fluke Connect™. This software collects, stores and makes viewable machine data from more than 80 Fluke tools and sensors. Measurements can now be stored in the cloud, where teams can always access the data on their smart device or computer. Whether the maintenance and reliability team is gathering data from condition monitoring sensors or from portable test tools, they now have all the data they need to make critical decisions and complete necessary jobs. Some of the key features includes Taking live readings on-the-go, Trending and graphing data, Receiving alarms from anywhere, etc.

Make in India

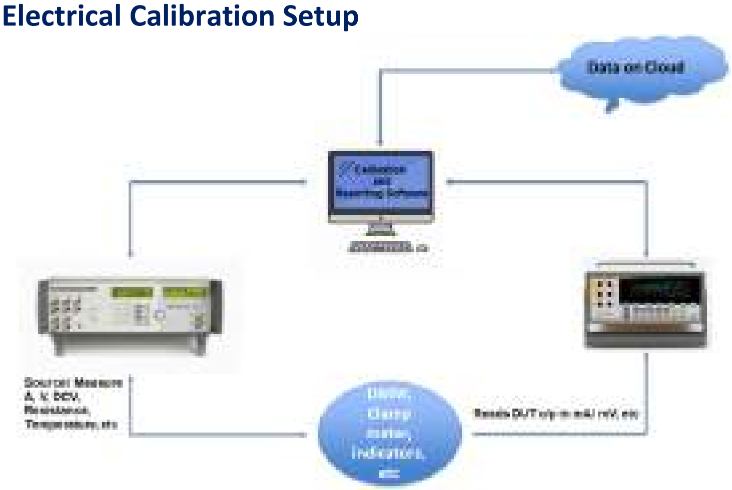
Fluke develops software solutions and test benches in India with a focus on Make in India Initiative.

Illustrations :

Sample line drawing of Pressure Calibration Setup



Sample line drawing of Electrical Calibration Setup



The Industrial Internet of Things (IIOT) the concept of interconnected applications, equipment, and technology- is more than just an abstraction. The IIOT is the idea that connections between the digital (e.g., mobile devices and computers) and physical worlds (e.g., plant equipment and test equipment) improves information exchange.

The practical applications of IIOT to plant operations may not seem clear at first, but when compared to more traditional methods of tackling operational challenges at the plant, the advantages become evident.

One way to understand the key differences is to compare two approaches to three-phase motor failure -- smart technology versus traditional analysis.

The problem: Three-phase motor failure

As often happens, a plant faces a problem motor, one that has been replaced twice in the past six months. Finding the root cause of motor failure is the task at hand. After finding that the insulation in the windings is breaking down, the technicians at the service shop think the motor might be running hot. They are not sure if is being caused by electrical power quality problems, mechanical wear or environmental or operational stresses that degrade the motor performance. It's therefore determined that a team is needed to collect current, voltage, power quality and temperature measurements in order to isolate the fault and identify the root cause.

What types of calibration standards does Fluke Calibration manufacture?

Fluke Calibration manufactures multiple types of calibration standards as below:

Temperature calibration standards

- Standard platinum resistance thermometers
- Temperature baths and furnaces (Liquid / Dry)
- Multifunction Calibrators
- Super Thermometers
- Multichannel Temperature Scanner / DAQ
- ITS-90 fixed-point cells
- Maintenance apparatus
- Liquid nitrogen comparison calibrator
- Resistance bridges
- Standard resistors and much more.

Pressure & Flow calibration standards

- Piston gauges
- Deadweight testers
- Pressure controllers and calibrators
- Pressure comparators and digital pressure gauges
- Portable/handheld pressure calibrators
- Flow calibration standards

Electrical & RF calibration standards

- Multi product calibrator
- Oscilloscope Calibrator
- 8.5 digit multimeter
- Primary Standard AC / DC Source etc
- Power & Energy Calibrator
- RF Calibrators and Sensors

Conclusion:

One accurate measurement is worth a thousand expert opinions

A trusted calibration means less worry, fewer questions and more time being productive.

Accurate and stable calibration equipment impacts business results (e.g. quality, efficiency, less waste)

Fluke latest technology products and solutions:

- Enhance the Operational Efficiency by providing automation
- Error free calibration since less manual activity involved.
- Increase productivity as the DUT's are communicated bi-directionally.
- Ensures Proactive and Predictive maintenance with asset- management.
- Improves Customer Service with Live status tracking & access to reports through cloud systems.
- More Connected Devices with data on cloud for continuous monitoring
- Process Data Management

  And much more!!

**** END ***

Technical Paper: Digitalization & IIOT Concepts for Process Industry

Suresh Jan **Head Process Industry**

Content

1. Idea of NOA
2. Architecture/ Technology Scheme
3. Digital Twin solution

1. Idea of NOA

NOA stands for NAMUR Open Architecture, and it is a concept to bring modern technologies around "Industry 4.0" into older process plants.

The NAMUR is a user organization of mainly German chemical companies like BASF or Bayer. It was founded after second world war. Meanwhile they have over 140 members and became worldwide important. In over 40 workgroups, technical recommendations for process and chemical industry are elaborated. The NAMUR publishes periodically "NE" s which
stands for "NAMUR Empfehlung" (NAMUR Recommendation). An example is one of the first NE, which recommend using a 4…20mA instead of 0…20mA to detect sensor failures.

It is a fact that process plants have a long lifetime compared to a car production plant e.g. This makes it harder to bring new technologies like the Profinet Fieldbus into the plant. The NAMUR searched for ideas to bring new technologies into the older plants and founded the NOA concept.

Another fact is that a lot of unused data is in a process plant. The sensors became more and more complex and the have a lot of information inside which are not transferred to the control system because the connection is still a 4…20mA signal. This additional data could help to
improve the plant by doing asset management, predictive maintenance or artificial intelligence.

A typical architecture of a plant in general is the "Automation Pyramid" with an ERP system
in the top and a sensor/actor layer in the bottom, in between control system layers.

A main requirement of almost all plant operators is not to change the main control system.

This brings up the idea of a "Side Channel" to place smaller additional controllers for new additional functionalities. Another main requirement of the plant operators was that these new plant components must be safe against unauthorized access from outside which add the topic that this side channel has to be OPEN and SECURE.

Figure 1: NOA Pyramid

NOA concept is mainly for older plants were new technologies are not integrated and with the help of New technology components it can be done .

Newer process plants, which already have HART interfaces on each input module or with integrated predictive maintenance functionalities e.g. are not in focus of this concept!

2. Architecture/ Technology Scheme

The target of this NOA concept is to place additional devices in the NOA side channel, which allows to collect data from the plant without touching the existing control system. These devices must be secure from “IT” view.

Examples:

- A controller must have a protected user interface with user and password. Other (Data) Interfaces must have a protection as well like OPC UA it has.
- The security on sensor lever can be: HART communication with READ ONLY functionality, a signal splitter on 4…20mA or current transducer for energy measurement or an additional sensor which is not connected to the main control system.
- To use existing fieldbuses requires a careful planning and a security concept for the specific fieldbus.
- The collected data has to be transferred to a target (Internal Cloud, Internet Cloud or DCS System e.g.) on a save and protected way. This can be made with a VPN tunnel by an mGuard Security Router.

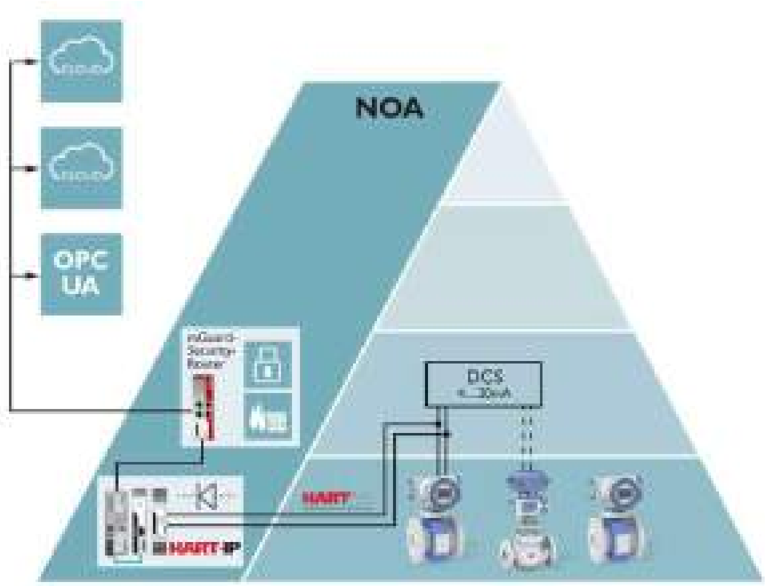


Figure 2: NOA with HART connection to existing process plant sensors

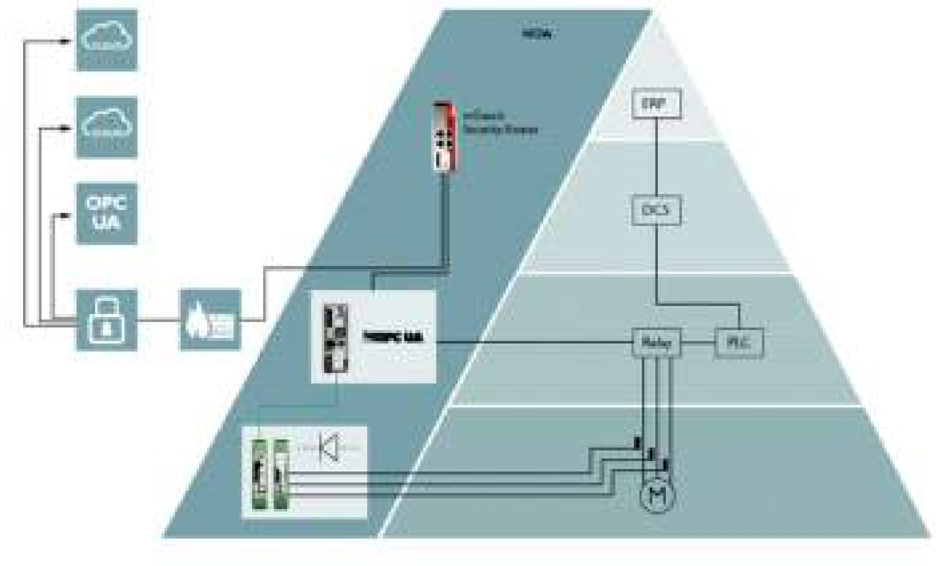


Figure 3: NOA with Motormanager EMM 3-XXX and current transducer

3. Wether the new NOA concept or a traditional data collector in a plant Phoenix Contact has a good and very large portfolio for this task. Beginning with 4…20mA signal splitter of the MCR/ MACX family, the modular HART Gateway or the Motor manager Modules for energy measurement and many more. A conversation with the customer helps to find the right devices fitting to the customers' needs and requirements.

Key device of this solution is the PLCnext controller. It has…

- Security functionalities (Restricted access with user + password, HTTPS…)
- OPC UA Interface for a protected communication with higher systems
- Open Source Platform for High Language Data Applications and Cloud connections • Docker® Functionality, which makes it easy to install applications like IIOT Server
- Access to almost all Fieldbuses by using the Axioline Family
- Complete IO Modul Portfolio
- ATEX Zone 2 Approbation
- Attractive Price

3.1 Digital Twin

By using the HART GW, the AXC F 2152 with an 8GB PLCnext SD Card and an IIOT Server of the company. We can offer a smart solution for collecting all unused HART data of connected sensors.

The IIOT Server has a pool of 1800 description files of HART sensors (eDD, FDI) integrated, which allows the access of all HART parameters of the connected sensors instead of the standard commandos of a solution without this IIOT Server. The factor is 3…10 times more data from each sensor. Depends on the complexity of the sensor.

During the installation is an internet connection necessary, after the setup and download of the data package the internet connection can be disconnected, what a requirement of the most customers is the interface to the customer is OPC UA .

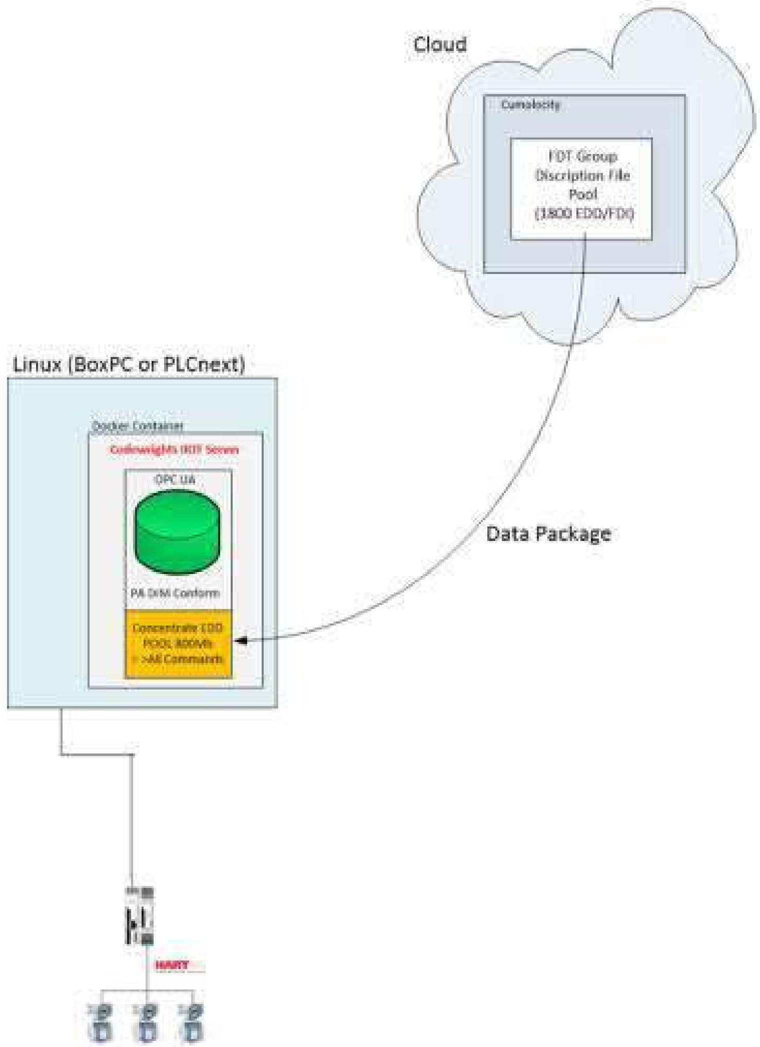


Figure 4: IIOT Server: Description file pool

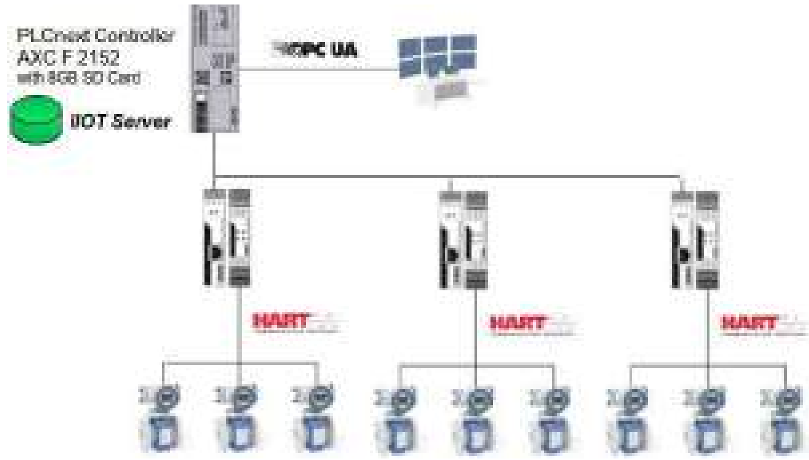


Figure 5: Digital Twin Technologie Scheme

One controller OPC UA integrated can handle up to five full extended HART Gateways with 40 connected sensors = 200 sensors in sum.

- This solution needs no application programming. The IIOT Server will be installed by using
  the Docker functionality. For the installation an application engineer is necessary.
- A field engineer has to install the physical HART connections. Several terminals are useable.
- **In the most cases a loop check is necessary after the installation**.

GLIMPSES OF ISA (D) PAST EVENTS

POWAT 2009, Habitat world on 24-25 April 2009

POWAT 2010, Hotel Sheraton on 28-29 May 2010

PNID 2011, Hotel Taj Palace on 26th Sep. 2011

POWAT 2012, Hotel The Grand on 13-14 Jan 2012

PNID 2012, Hotel Taj Palace on 5th Oct. 2012

at PNID 2013, Hotel Taj Palace on 3rd Oct. 2013

POWAT 2013, Hotel Hyatt on 12-13 April 2013

PPA Meet Eros Hotel on 10-11 April 2015

PPA Meet, Eros Hotel on 8-9 April 2016

PPA Meet, Eros Hotel, New Delhi on 21-22 April 2017

PPA Meet, Eros Hotel, on 20-21 April 2018

PPA Meet, Taj Palace Hotel, on 3rd & 4th May 2019

GLIMPSES OF ISA (D) PAST EVENTS

Total 2021

Total 2021

LDP 2023 Shillong

Cyber Security Program 2023

Cyber Security Program 2023

Cyber Security Program 2023

Fertilizer Symposium 2015

Fertilizer Symposium 2016

Fertilizer Symposium 2017

Fertilizer Symposium 2018

Fertilizer Symposium 2019

Fertilizer Symposium 2022

GLIMPSES OF ISA (D) PAST EVENTS

Students Visit IOCL Panipat 2023

Students Visit IOCL Panipat 2023

Students Visit IOCL Panipat 2023

SIL Certification 6th Batch

SIL Certification 7th Batch

Monthly Meet

AGM 2015

AGM 2016

AGM 2017

AGM 2018

AGM 2019

AGM 2021

Smart & Safety Integration Solutions

ARMTEL
Industrial communication systems

Armtel is an experienced R&D and manufacturer of smart industrial communication systems.

We combine engineering traditions with advanced technologies to create reliable products to ensure effective communication and safety in any industrial environment.

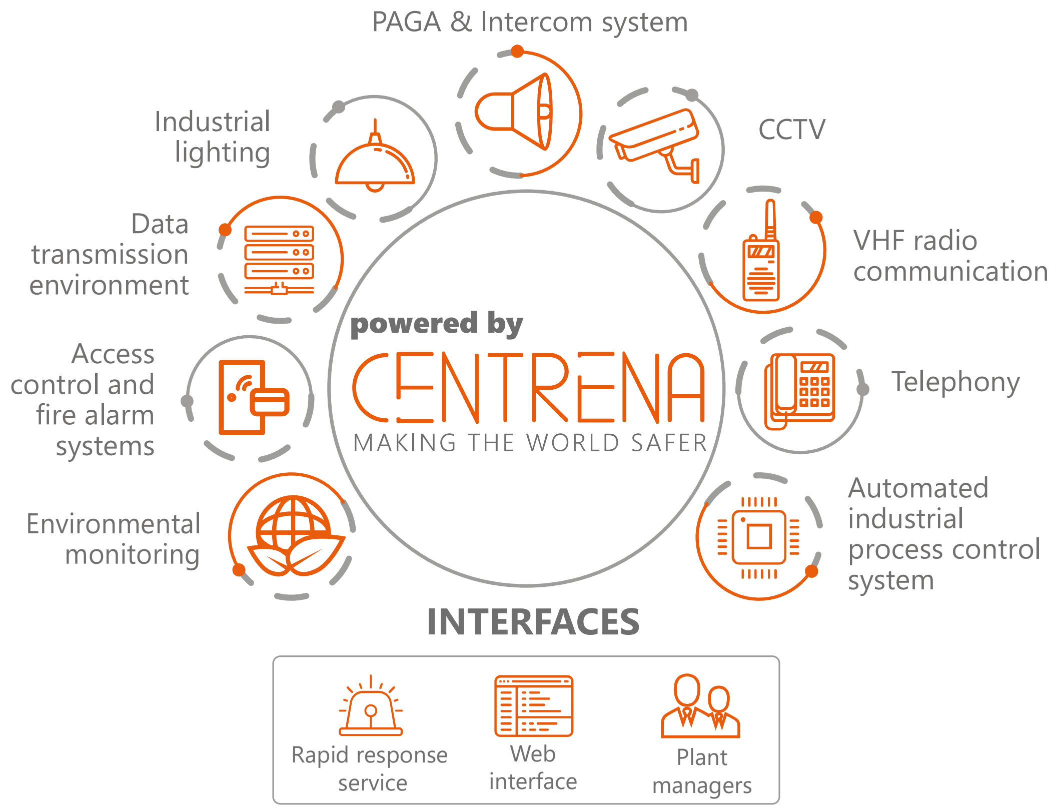
Armtel delivers high quality and ensures reliability of its product thanks to its highly professional team of experts, application of advanced technologies and focus on product development.

Armtel also develops digital solutions for oil and gas, power, chemical, transportation and other industrial verticals. One of the latest solutions is CENTRENA Control Centre which is a hardware and software package that integrates independent security and equipment management systems in a single user interface to monitor and ensure trouble-free and continuous operation and production.

The CENTRENA Control Centre is a software that integrates various security systems, i.e. video surveillance, access control, Armtel PA/GA systems to monitor equipment and services and to form a complete communication, emergency and evacuation system.

CENTRENA is a digital solution to support decision-making and equipment management to ensure the overall production safety. The CENTRENA monitoring system allows to integrate and easily manage geographically distributed infrastructure in a single platform to ensure real-time monitoring of production assets.

The CENTRENA Control Centre boosts production safety and efficiency, minimizes risks of accidents and equipment downtime, reduces costs while contributing to business growth and investment attractiveness.



OUR CUSTOMERS

IndianOil, CPCL, LUKOIL, ONGC MRPL, SIBUR, ROSNEFT, BHEL, GAIL, NOVATEK, ROSATOM, PDIL, QATAR STEEL, Bharat Petroleum, ONGC making tomorrow brighter (Oil and Natural Gas Corporation Ltd.), EIL, HMEL, TATNEFT, GAZPROM, RusHydro

SOLUTION

The system is designed to fully correspond to all customer's needs.

SERVICE

A collection of unique proposals that increase value of the product.

info@armtel.com

+91-9560355880

India
Corporate Edge Serviced office, Building 10, Tower A, First Level, DLF Cyber Hub, Cyber City, Gurgaon, Haryana

Russia
12 korp.1, Zaporozhskaya ulitsa, office 1/2, St. Petersburg

COMFIT

BEYOND REENGINEERING

TUBE FITTING

Connectors, Reducers, Adapters, Unions,
Port Connectors, Elbows, Tees, Component

PIPE FITTING

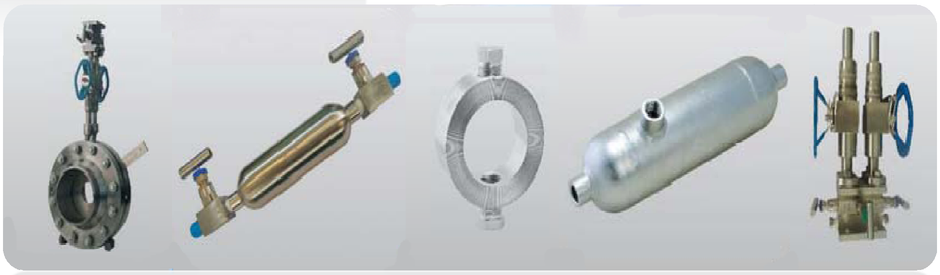
Nipples, Adapters, Bushings, Couplings, Connectors,
Unions, Elbows, Tees, Cross, Caps, Plugs, Gasket

INSTRUMENT VALVES

Needle Valves, Manifold Valves,
Monoflange Valves, Ball Valves,
Check Valves, Air Header Distributer

OTHER PRODUCTS

Pre Fab Hookup, Kidney Flange,
Orifice Assemblies, Flange Connector,
Flush Ring, Thermowell, Tee Filters,
Sampling Cylinder, Condensate Pot
Gauge Snubber, Syphon



Our extreme clients

EIL | NPCIL | IBR | HMEL | Tractebel Engineering suez | IndianOil | ONGC | THE LINDE GROUP | HP | Tecnimont ICB | KSS KazStroyService | TOYO

COMFIT & VALVES PVT LTD

Survey No. 23/1, Part-2, Laxmipura- Nandasan, Ahmedabad – Mehsana Highway,
Post- Nandasan – 382705 Tal.- Kadi , Dist- Mehsana , Gujarat (INDIA)
Phone - +91-9054009800, Email: info@com-fit.com , Website: www.com-fit.com

Sabu Jose | India Country Manager | +91 98958 11002 | sjose@ectpac.com

Headquarters

Energy Control Technologies

10664 Justin Drive

Urbandale, Iowa 50322 USA

FORBES MARSHALL

Real Time Vibration Analysis to Sustain Uptime of Critical Rotating Equipment

Uptime

Productivity

Safety

Real time monitoring of the running condition of plant machinery helps to get an indication of failures that could develop, causing plant shutdowns.

For over 75 years, Forbes Marshall has provided innovative products and services to help industries improve their process and energy efficiency. Our VibAssist™ is a machinery analysis and diagnostic software specially designed for rotating machinery like turbines, compressors, fans, blowers, motors and pumps. It detects abnormal symptoms from vibration characteristics or subtle changes in vibration. This helps proactive action to be taken, optimizing plant operation and enabling an uptime of >95%.

HACH®

Be Right™

Worried about unreliable ***TOC monitoring?***

Looking for Reliable and Robust TOC analyzer?

- **Versatile And Adaptable - B7000i Is Perfect for Any Environment**

  Offers Versatility with A Wide Measuring Range, Up To 6 Process Streams. Suitable for any measurement right from Drinking water to influent wastewater.

- **Saves Costs & Optimize Processes**

  With Certified high uptime (98.86%) and minimal maintenance B7000i helps in optimizing the maintenance costs and helping to achieve best optimization of the processes.

Let B7000i Take Care of It

- **Reliable Results, No Matter the Conditions**

  Smart design that includes self-cleaning sample line & reactor eliminates sample carryover, suitable for 30% salt content and particle size up to 2mm makes it perfect TOC analyzer for very challenging applications like Seawater and for influent monitoring.

- **True TOC measurement**

  Large tubing eliminates the need for filtration, clogging & sample contamination and provides large sample for oxidation. This leads to measurement of undissolved organic compounds and more representative sample.

- **Two Stage Advance Oxidation Tech – Complete Oxidation**

  Patented TSAO technique is very power oxidation at ambient temperature and pressure, ensuring complete oxidation. TSAO helps in minimal maintenance with once in 6 months maintenance requirement unheard in the industry.

CONTACT US

+91 99160 40249

sales_support_india@hach.com

in.hach.com

Life Is On | Schneider Electric

Delivering

SECURE

Cybersecurity services and solutions for all industries.

WANT TO FIND A HIGH QUALITY µMODULAR & MANUAL SAMPLING SYSTEM PROVIDER **FOR YOUR PROJECTS?**

SPIRARE ENERGY

Value propositions:
- *Representative sample*
- *Safe systems*
- *Zero emission to atmosphere*
- *Reduced cost of ownership*
- *Low & predictive maintenance (µSCS)*

DESIGN & ENGINEERING SERVICES

PRODUCT SELECTION SUPPORT

TECHNICAL SUPPORT

CUSTOM INTEGRATIONS

PRODUCT TRAINING

CUSTOMER SERVICE

AUDIT & PLANT SURVEYS

OVER **2500+** SAMPLING SYSTEMS ARE SUPPLIED AND INSTALLED AT DIFFERENT REFINERY, PETROCHEMICAL & CHEMICAL PLANTS

ABOUT US

Spirare Energy is a leading manufacturer and supplier of hydrogen H2 generation plants using Alkaline bipolar technologies ranging from 0.5nm3 to MW scale

We design, fabricate, assemble & test modular conditioning & closed Loop sampling systems for O&G, Petrochemical, Chemical and other market segments.

At Spirare Energy, we take pride in being a one-stop solution provider for instrumentation HOKE tube fittings & valves, GO regulators, and sampling packages in India.

WHAT WE DO

WHY US?

- Your trusted Hydrogen expert
- Not just a fabricator- your safe sampling solution provider
- One Stop Shop for Instrumentation Hook-up
- Committed to Quality & Reliability

12 Years H2

Experience Our Experience

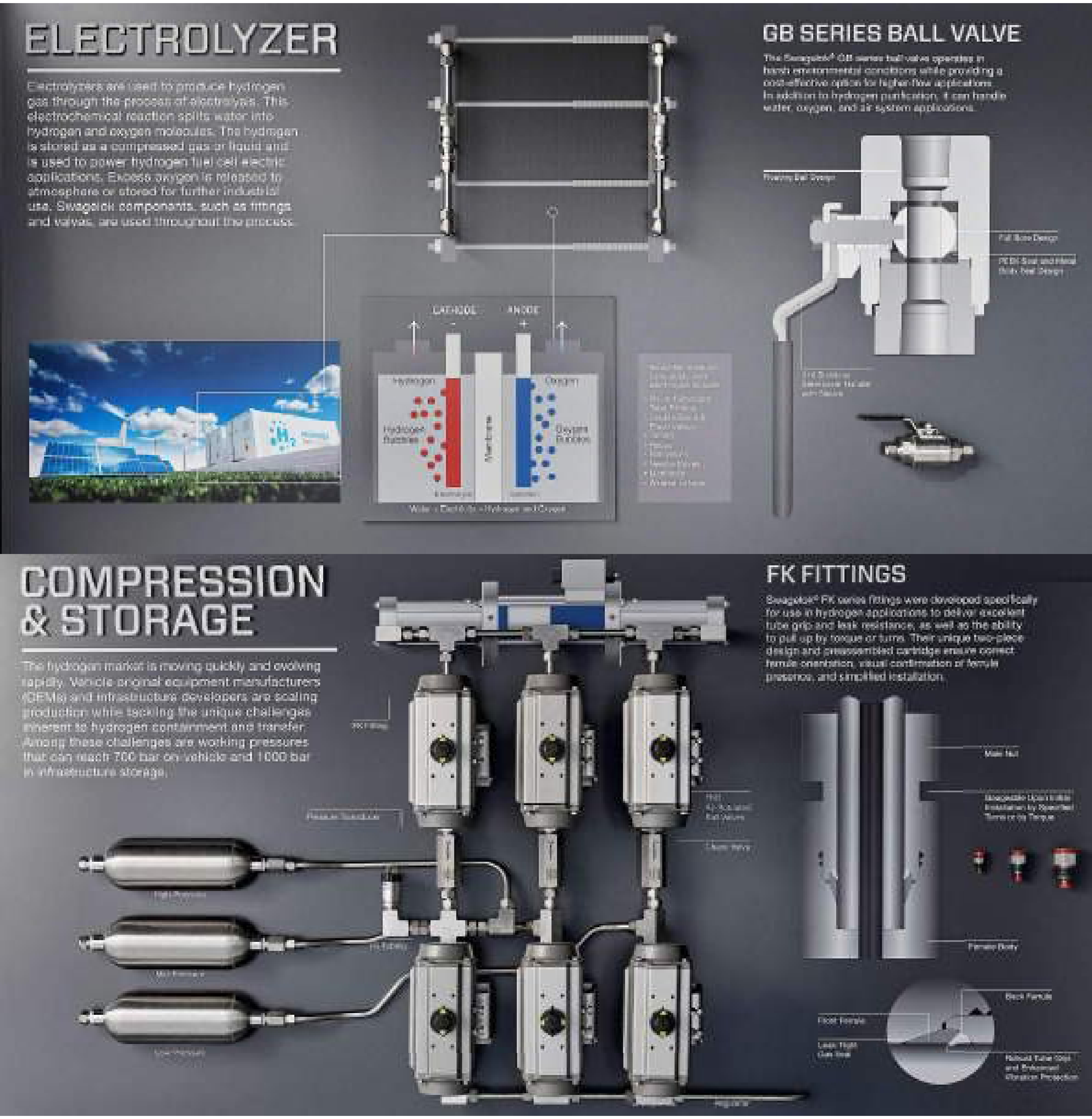
CALL +91 9560067525
+91 9958944519

www.spirare.co.in
spirare.sales@gmail.com

FLO PRESSURE
SAMPLING SYSTEMS

Swagelok Bangalore | Chennai | Delhi | Hyderabad

Hydrogen Solutions



Contact your authorized Swagelok sales and service center to learn more about our clean energy solutions:

Swagelok Delhi, 414, Bestech Chamber, B Block, Sushant Lok - I, Gurgaon - 122009, Phone: 0124 - 404 5632, Email: delhi@swagelok.com

Keep the Operation Running with the OT Zero Trust Approach

Keep the operation running.
Keep assets working.

txOne networks

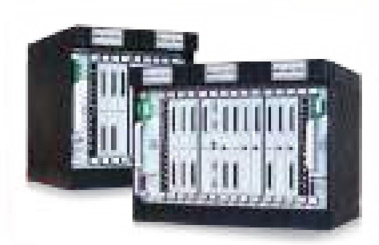
COMPRESSOR CONTROL AND PROTECTION

Field Proven Across the Globe

REDUCE SYSTEM DEVELOPMENT AND COMMISSIONING TIME

For over 145 years, Woodward has been collaborating with OEMs and end users to provide the technology, application expertise and support that you've come to trust from a market leader. Our field-proven prime mover and compressor controls and protection technologies are safely operating some of the world's largest compression systems. And, many major compressor manufacturers incorporate Woodward systems into their equipment.

Our integrated turbine-compressor and motor-compressor control systems maximize availability and performance in up-stream, midstream and downstream oil and gas applications, helping owners run their compression systems and process at peak efficiencies. All of our systems meet industry standards for machinery control and safety, and are fully tested in a dynamic simulation environment—enabling you to reduce both system development and commissioning time.

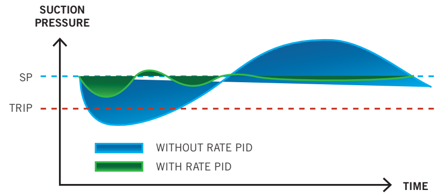


CUSTOM COMPRESSOR CONTROLS

Woodward's Integrated Compressor Control Systems utilize field proven hardware packages (MicroNet Plus or MicroNet TMR) and OEM qualified algorithms to improve compressor train performance, reliability, and protection. These purpose-built controllers are customized to meet the control, protection, and decoupling functionality required for the specific application's requirements

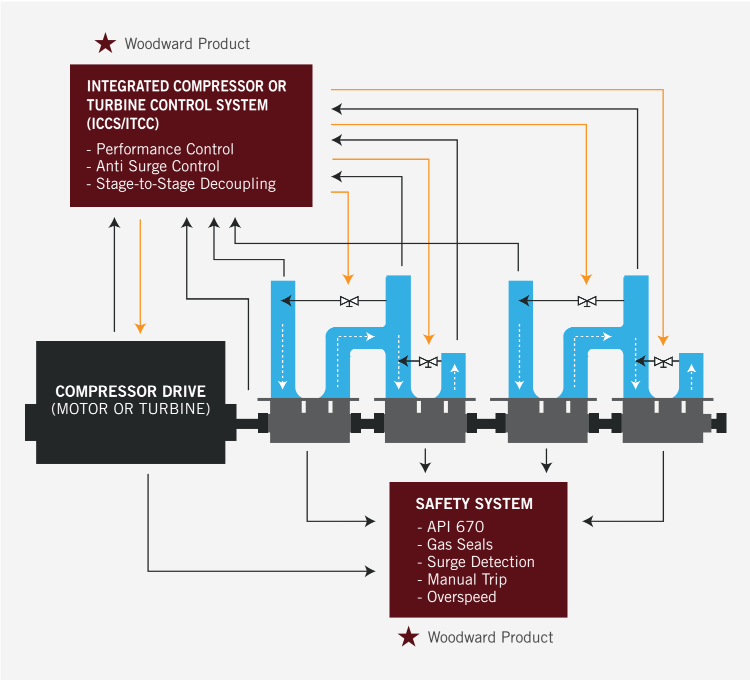
STANDARD COMPRESSOR CONTROLS

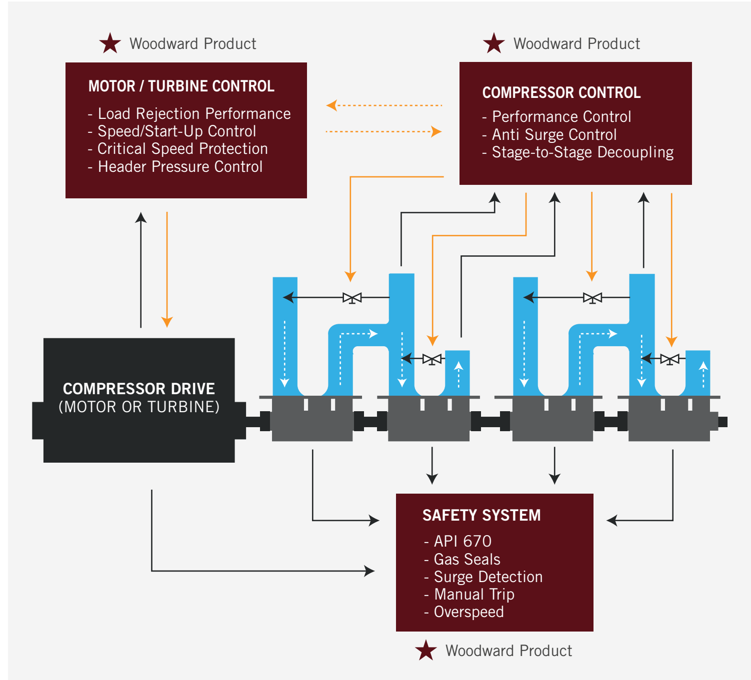
Woodward's Vertex and Vertex-Pro control product lines are designed to control and protect industrial sized axial or centrifugal compressors with one or two recycle loops only. These standard off-the-shelf controllers are field configurable allowing OEMs and or users to easily configure/select the specific control algorithm required for the specific compressor loop and application.



ADVANCED TECHNOLOGIES

Woodward has developed surge preventive techniques that help compressor users achieve peak performance of their process and minimize process disturbances. All our solutions are modeled in our advanced dynamic simulation program (NetSim) before being implemented in the control systems. Woodward's patented rate PID algorithms provide anticipative opening of anti-surge valves during process upsets to minimize overshoots and allow safe operations with minimal safety margins. Compressor turndown is maximized and higher product yields are achieved.





FIELD PROVEN

With over 40,000 steam or compressor controllers installed worldwide, Woodward's control systems have been proven to stand up to harsh environments, as well as mee the rigorous control requirements of OEMs and users in upstream, midstream, and downstream applications.

Robust product designs are leveraged to ensure long-term operation, no matter what the environment of application.

OEM QUALIFIED

OEM control system qualification is a stringent process in which details of the control system design, application architecture and performance are carefully scrutinized and tested by the OEM to ensure to meet performance requirements..

Woodward's advanced technology compressor and prime mover control algorithms and hardware are qualified and have become a standard on OEM systems throughout the world

GLOBAL SUPPORT

Colorado:
coloradofieldservice@woodward.com
+1 970-498-3609
turbinehelpdesk@woodward.com
+1 970-482-5811, option 7

Brazil:
vendas@woodward.com
+55 19 3708-4800

Europe:
fieldservice.europe@woodward.com
+31-23-5661257
helpdesk.europe@woodward.com
+31-23-5661239

China:
fieldservice.china@woodward.com
+86 (512) 8818 5515
helpdesk.china@woodward.com

Japan:
fieldservice.japan@woodward.com
+81-43-2132198
helpdesk.japan@woodward.com

India:
fieldservice.india@woodward.com
+91 (124) 439 9500

Middle East
fieldservice.middle-east@woodward.com
+971 26267 929
Saudi, +966 135 107 900

WOODWARD

ISA Delhi Section

PETROLEUM & POWER AUTOMATION MEET 2023

PLATINUM SPONSORSHIP

इंडियनऑयल IndianOil
2023 STRENGTHENING THE GREEN RESOLVE

EATON
Powering Business Worldwide

GOLD SPONSORSHIP

YOKOGAWA

SILVER SPONSORSHIP

PEPPERL+FUCHS
AXIS
BARTEC
PHOENIX CONTACT

SUPPORT SPONSORS

Delegate Kit, Knowledge Partner, Event Support, etc.

एनटीपीसी NTPC
EIL
EMERSON

SPONSORED BY

ARMTEL Industrial communication systems
RITTAL
FORBES MARSHALL
AIC
TOA DKK
ABSR
ADAGE
FLUKE
DelVal Flow Controls
txOne networks
Rockwin Flowmeter India Pvt Ltd
Life Is On Schneider Electric
Baker Hughes
COMFIT
Swagelok
BLISS ANAND
SPIRARE ENERGY
WIKA
Pyrotech
HIKVISION See Far, Go Further
EIP
Total Solutions
finder
Nocle
CONGMAX ELECTRO Your Partner in Control Solutions