ISA Delhi Section

Setting the Standard for Automation™

Advanced Substation Automation & Cyber Security

- Amit K Aglave , Sukhraj Singh & Tarul Sahgal
(FLUOR)

ISA-D: “Fertiliser , Food and Pharma Symposium-2022”

Fluor – Business Groups

A global, publicly traded **professional and technical solutions** provider

Designs and builds well-executed, capital-efficient facilities for clients on six continents

110-year heritage providing solutions for clients

Global execution platform serving clients in over **60** countries

#259 on the 2022 **FORTUNE® 500** list

41,000 employees spread across **90** offices in **29** countries executing projects globally

ENERGY SOLUTIONS

Production & Fuels
- Asset Decarbonization
- Carbon Capture
- Energy Storage
- Gas Processing & Gas Treating
- Gasification
- Heavy Oil Upgrading & Oil Sands
- Hydrocarbon Transportation – Pipelines
- Hydrogen
- Offshore Oil & Gas Production
- Onshore Oil & Gas Production
- Petroleum Refining
- Renewable Fuels & Biofuels
- Sulfur Recovery
- Sustaining Capital Projects
- Utilities & Offsites

Chemicals
- Battery Chemicals
- Chemicals & Petrochemicals
- Chemicals & Plastics Recycling
- Green & Sustainable Chemicals
- Polysilicon

Liquefied Natural Gas
- LNG

Nuclear Project Services
- Small Modular Reactors (SMRs)

URBAN SOLUTIONS

Advanced Technologies & Life Sciences
- Advanced Materials
- Animal Health
- Biotechnology
- Data Centers
- Fast-Moving Consumer Goods
- Food & Beverage
- Medical Devices
- Pharmaceuticals
- Semiconductors
- Smart Batteries
- Specialty Products

Infrastructure
- Aviation
- Bridges
- Commercial & Institutional
- Heavy Civil
- Infrastructure O&M
- Ports and Marine Terminals
- Public-Private Partnerships
- Rail and Transit
- Renewable Energy
- Telecommunications
- Toll Roads & Highways

Mining & Metals
- Fertilizers
- Metals
- Metals Process Expertise
- Mining
- Mining Process Expertise

TRS Staffing Solutions
- Staffing Resources

MISSION SOLUTIONS

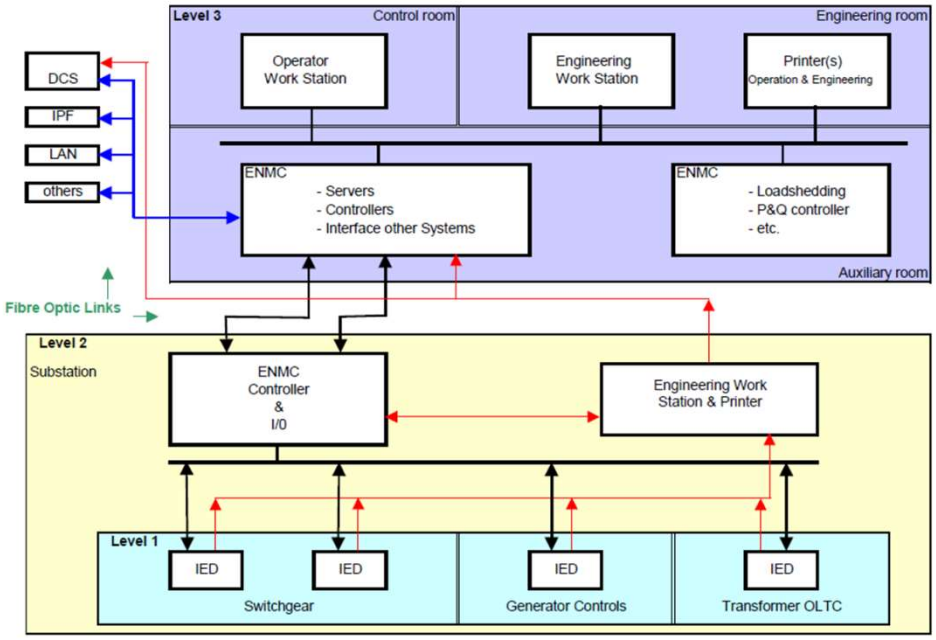
Defense
- Base Engineering & Construction
- Base Operations Support
- Capital Projects
- Contingency Construction
- Emergency Response & Recovery
- Facilities/Equipment Operations & Maintenance
- Life Support & Logistics Services
- National Security

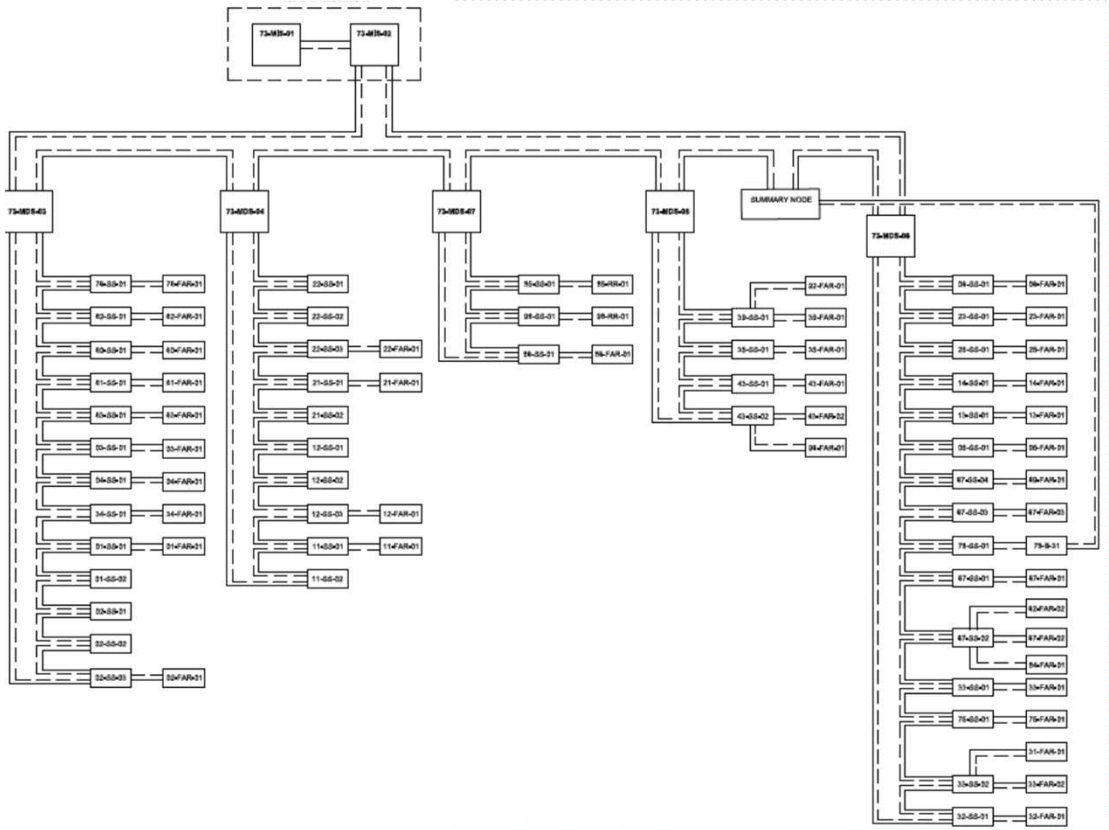
Intelligence
- Intelligence Services

Nuclear & Civil
- Decontamination & Decommissioning
- Emergency Response & Recovery
- Environmental Remediation
- Laboratory Management
- National Security
- Nuclear Operations & Management
- Nuclear Power Plant Support Services
- Site Closure Management
- Waste Management

FLUOR®

Substation Automation - Block Diagram & Backbone Network





FLUOR®

Substation Automation System - Functionality & Scope

1

Monitoring

- Status
- Alarms
- Remote Metering (e.g. Power Import/Export, Overall Plant Power Factor)

2

Control

- Power Control, e.g. Transformer OLTC
- Object Control, e.g. CB Operation (Remote Operation prevents arc flash issues)
- Generator Operation Mode
- Turbines (MW Control, Frequency Control, Mode Change etc.)
- Active and Reactive Power Control
- Load Shedding : Manual/Automatic, Loss of Power Source, Frequency Drop Overload

3

Analytics

- Disturbance Data Recording; Trip Events; Fault Analysis
- Historical Data Processing - Early Detection Of Equipment Failures; Reliability Analysis – MTBF/MTTR
- Renewable Energy Generation Forecast; Prediction Algorithms
- Asset Monitoring/Management
- Digital Twin

4

Maintenance

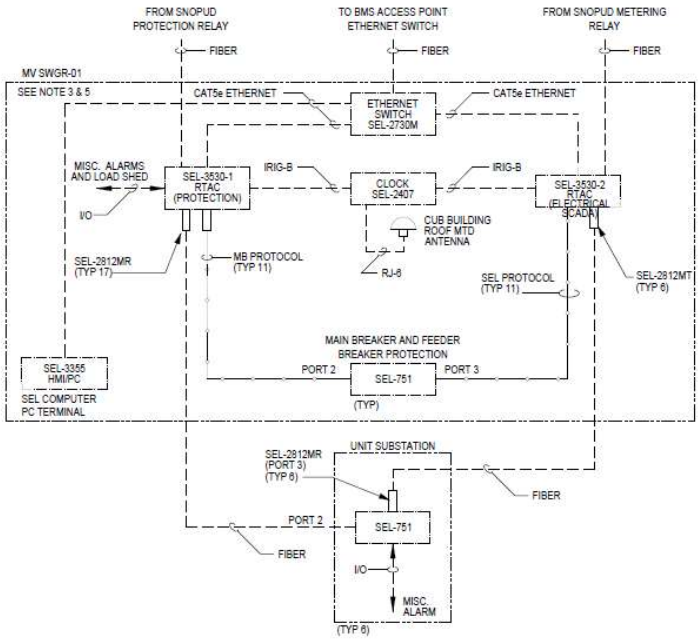
- Outage Management
- Switching Procedure Management
- RMRS – Remote Maintenance Reliability Support

FLUOR®

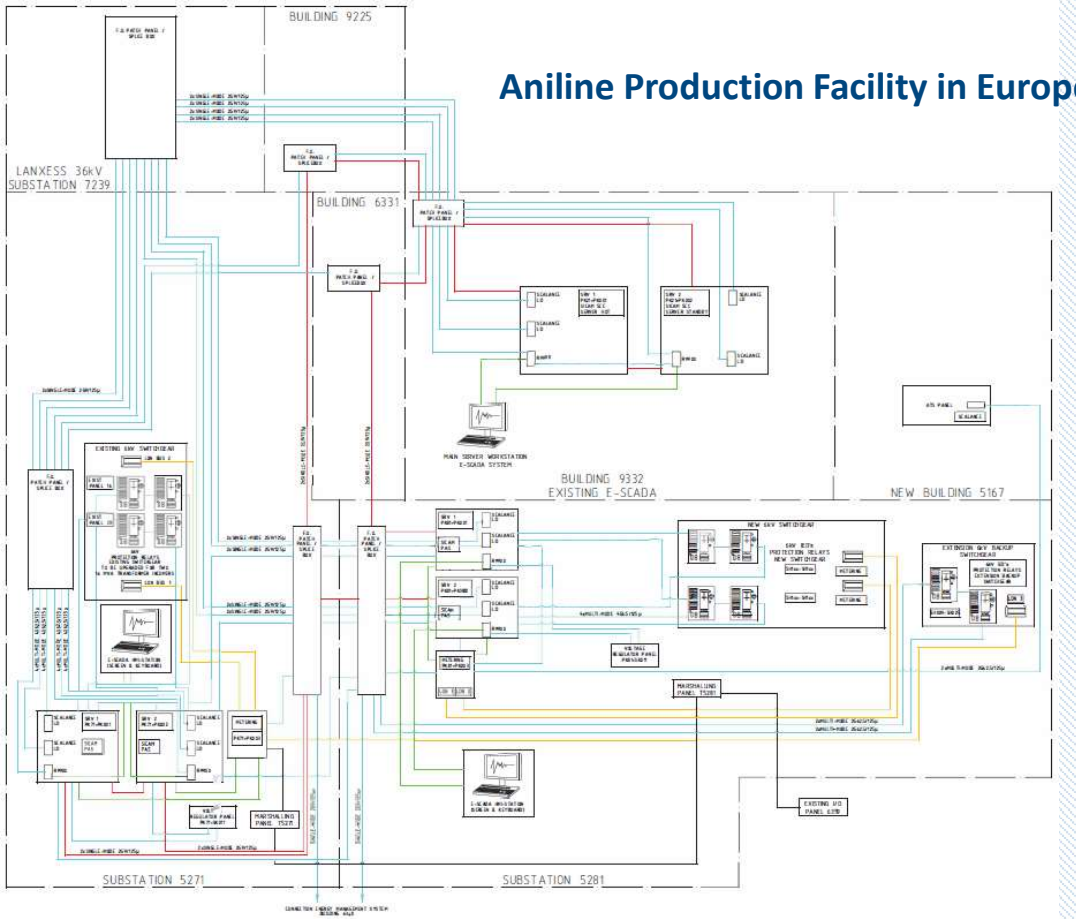
Typically Monitored Equipment Parameters / Status / Alarms

Equipment	Typical Parameters / Status / Alarms
Switchgear / MCC **(All voltage levels)**	- CB/Contactor Status (Open/Closed/Tripped/Racked-out) - Local/Remote Control Status; ATS Status (Manual/Auto) - Total Power Failure - SF6 Leakage/Gas Pressure Low - Fault Trips like UV; Dead Bus; PT Fuse Failure - Metering Functions (Current, Voltage, Freq, Power, PF etc.) - Interlocks & Intertrips
Transformer	Alarms & Trips for - Oil/Winding Temp High, Bucholz, PRV, Oil Level Low, Common Trouble etc. (ENMCS Interface through Switchgear IEDs)
Motor **(All voltage levels)**	**Alarms**: Over Temp, Load Unbalance, Earth fault, Locked Rotor **Metering Functions:** Current, Voltage, Freq, Power, PF etc.
AC / DC UPS & BMS	**Alarms**: Rectifier Failure, Fan Failure, Over Temp, DC Out of Tolerance, Earth Fault, MCB Trip, Battery Discharged, Bypass On **Monitoring:** AC/DC Voltage/Current, Battery Charge Status, Battery Temp.,
EDG **(ENMCS Interface through GCP)**	**Engine Alarms & Status** - Over crank, Over Speed, Coolant Temp. High, High Bearing Temp., Low Fuel Level, High Vibration, Oil Temp/Pressure, Jacket Water Temp, Control Supply Tripped Alarm, Engine Battery Status **Generator Alarms & Status** - Stator Winding Temp High, Under/Over Voltage, Under/Over Freq, Voltage Regulator Fault, Exciter System fault, Cooler Air Temp High, Generator CB Status (Open/Closed), Metering Functions (Current, Voltage, Freq, Power, PF etc.)
Building Alarms **(For systems like Fire & Gas, HVAC etc. in Substation / Control Room etc.)**	- Smoke Detected, CO Detected - Building Temperature High - Loss of Pressurization
Misc. Systems **(VFDs, EHT, Cathodic Protection, Thyristor Control Panels)**	Low Voltage Alarm, Earth fault, RTD Damage, Common Trouble Alarm, Protection Watchdog

Substation Automation – Topology Examples



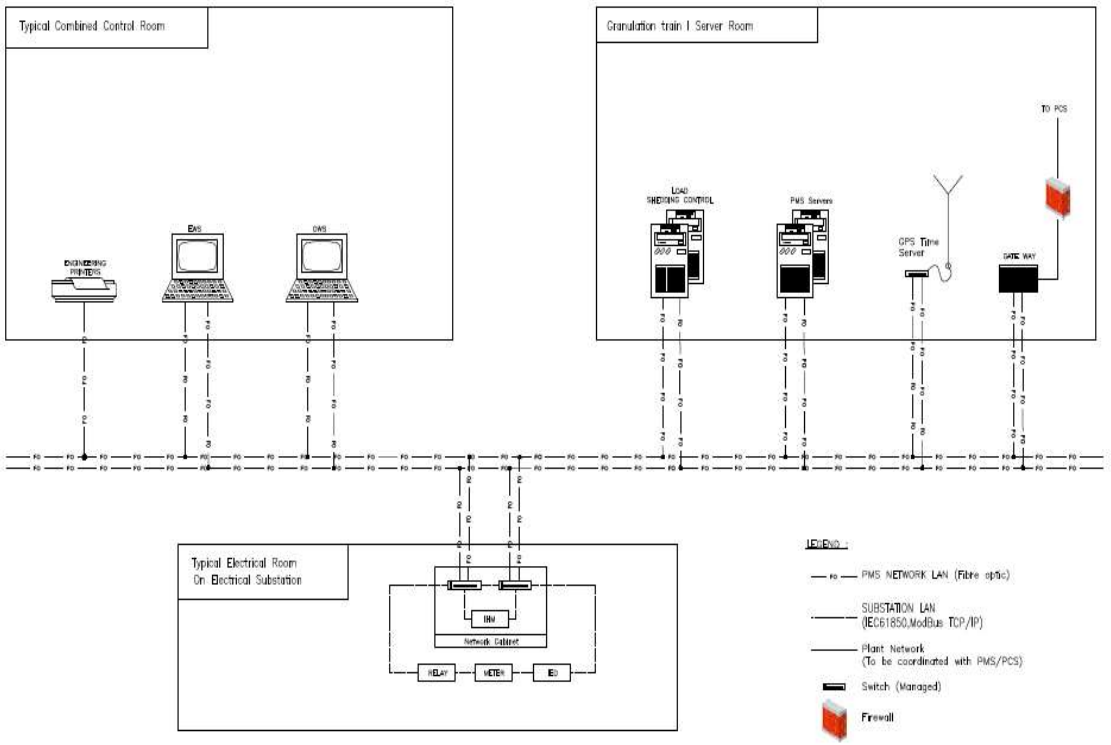
Biomanufacturing (Cancer Drug) Facility in US



Aniline Production Facility in Europe

FLUOR®

Substation Automation – Topology Examples



Phosphate Production Facility in Middle-east

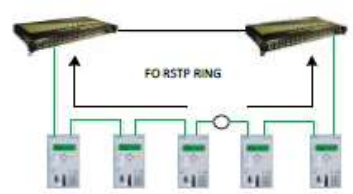


Figure 24: Normal Operation

Figure 25:: Link failure

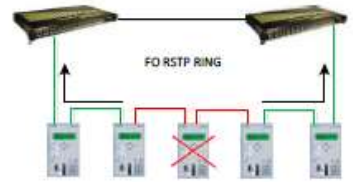


Figure 26:: Device Failure

FLUOR®

Substation Automation – Technical Parameters / System Specification

Response Time

- Start-up after Power Breakdown for Satellite Unit (e.g. 30 sec), Central Unit (e.g. 2 min);
- Issuing a command in response to operator's command (e.g. 1 sec);
- Updating information on the screen after change of value (direct/indirect)(e.g. ½ sec)

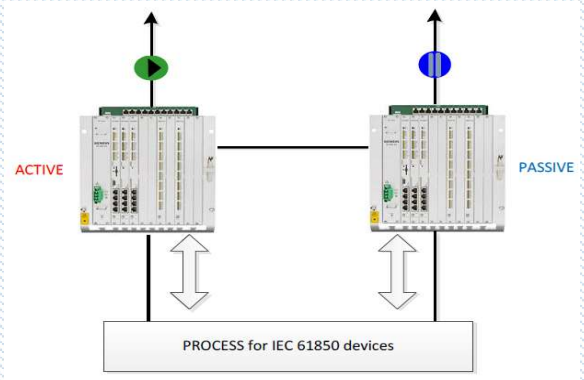
Accuracy

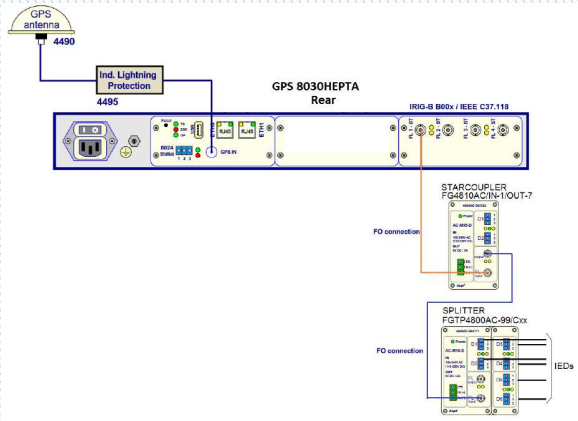
- Time Stamps (e.g. 1ms); Analogue/Digital Measurements; Minimal Pulse Width detected

No. of Data points

Interface Parameters

- Communication Protocol, Redundancy, Version, Base Speed (like 100fx. 10sx etc.)
- Physical Interface: Cable Type, Connector Type

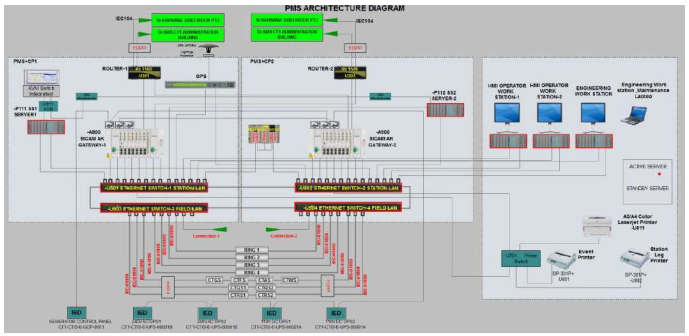


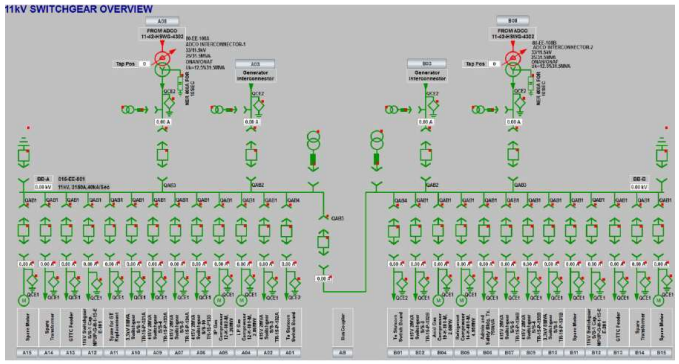


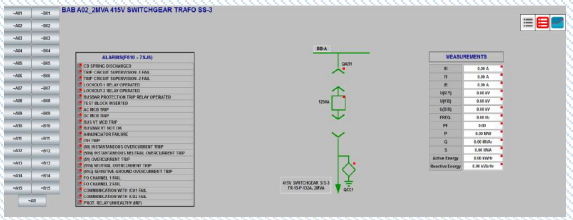
FLUOR®

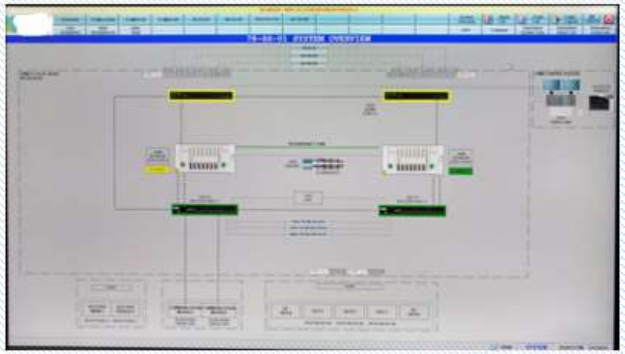
Substation Automation – HMI Display

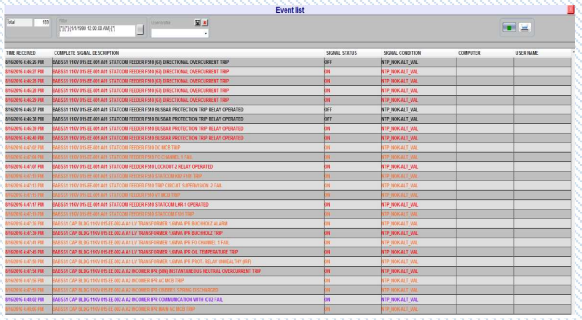
- Alarm Management – Priority/Criticality
- Event Log
- Tagging
- Operating/Fault Status
- Energy Accounting
- Helpfile/Training Manuals/Catalogues
- Topological Network Coloring
- Maintenance/ Outage Management/ Switching Procedure Management







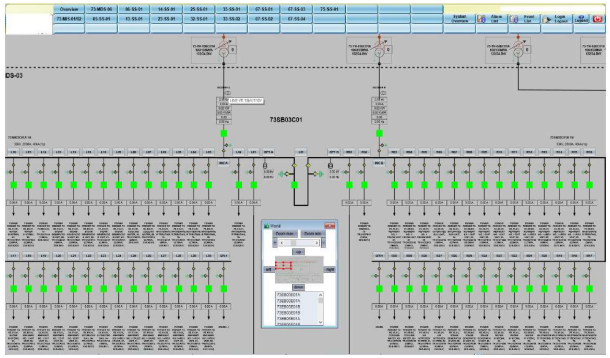


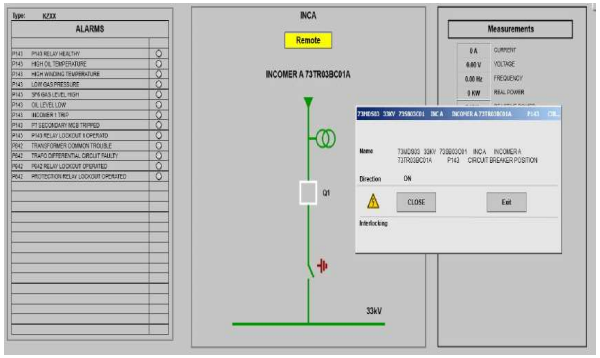


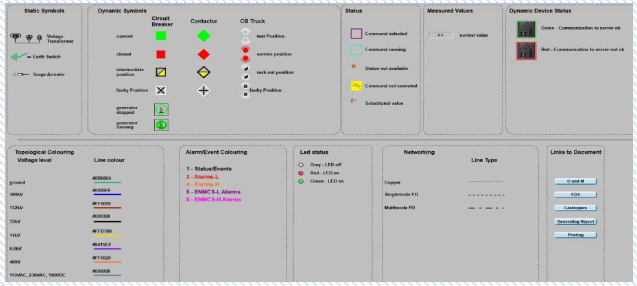
FLUOR®

Substation Automation – Study & Reviews

Study / Review	Purpose
• Safety and Operability (SAFOP) • SAFAN (Safety Analysis) • SYSOP (System Operability) • OPTAN (Operator Task Analysis)	- Defining the HMIs - Access Control & Authorization Levels for Operators, Engineers & Supervisors - EWS/OWS Functionality/Application
Failure Mode and Effect Analysis	
Load Flow, Short Circuit & Transient Stability Study	- Flow scenarios of active and reactive power







User rights of Group	Display only (default autologon)	Control Operation	Engineer	System Administrator
Navigate Through Various Displays	Yes	Yes	Yes	Yes
Acknowledge alarm	No	Yes	Yes	Yes
Control Operation	No	Yes	Yes	Yes
Access to digsi software, 3rd party software	No	No	Yes	Yes
Access to System Software	No	No	No	Yes
Exit From SICAM 230 Runtime	No	No	No	Yes
Logout after 30 Min idle Time	NA	Yes	Yes	Yes

FLUOR®

Substation Cyber Security – Are they Vulnerable?

Attacks on Electrical Grids

- 2015: Ukrainian power grid taken offline
- 2016: Ukrainian power grid taken offline (**yes, again**)

Other Attacks in Process Industry:

- 1982: Trans-Siberian pipeline explosion
- 2003: SQL Slammer brings down the Davis-Besse plant
- 2009: Conficker infects power plants in the U.S.
- 2010: Stuxnet discovered
- **2017: Attackers compromise Safety Instrumented Systems (SIS)**
- 2021: Major gas pipeline taken offline due to ransomware

Every System which uses a Microprocessor, PLC, PC infrastructure and/or internet is vulnerable!!!

Motives?

- Operational disruption
- Reputational loss
- Cyber terrorism
- Impact Safety
- Money

FLUOR®

How do we Protect?

Network Segmentation

- Use the Purdue Model to ensure that the control network and other network segments at the facility are properly segmented with restrictive firewalls configured to block all traffic by default

Increase Detection Capabilities

- Build an Incident Response program specific to the ICS environment to be able to effectively contain and eradicate incidents in a timely manner

Increase Response Capabilities

- Build an Incident Response program specific to the ICS environment to be able to effectively contain and eradicate incidents in a timely manner

Conduct Risk Assessments

- Leverage existing frameworks such as ISA 62443 to identify gaps in the environment's cyber security and physical engineered controls

Awareness Training

- Ensure all computer-based users at a facility receive security awareness training, especially in identifying and not falling victim for phishing emails

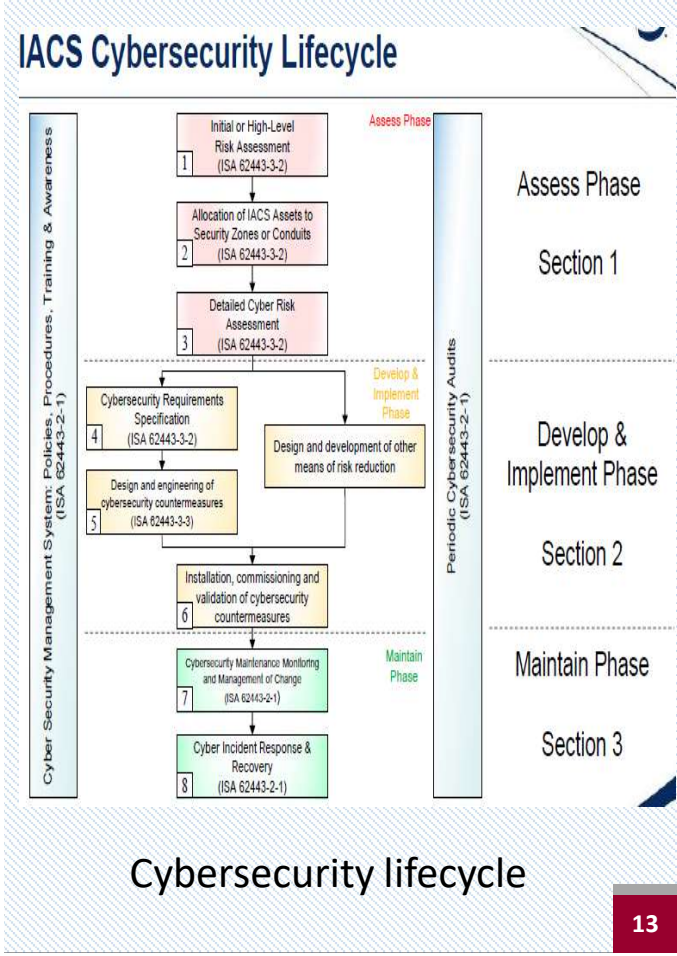
Secure Remote Access

- Use Multifactor Authentication (MFA) to secure remote access. Use other security controls such as dial back and monitored jump hosts as alternatives when necessary. Only activate when needed.

FLUOR®

Management of Cyber Security and Lifecycle

- Cybersecurity related management activities, all of which are necessary to ensure that objectives are met.
- Addressing the requirements of ISA84 series of standards as well as the IEC/ISA-62443 series of standards.
- Throughout lifecycle, risk assessment and management should be accomplished with respect to all identified cyber hazards or vulnerabilities.
- The high-level risk assessment can usually be performed at a corporate level to determine in general what high-level risks exist for their operations.
- A Cybersecurity requirements specification (CSRS) should be developed as a separate document to cover what is required to achieve and maintain the necessary security level(s) while not adversely impacting necessary IACS functions.



Cybersecurity lifecycle

FLUOR®

Cybersecurity Requirements Specification (CSRS) for the IACS

A **C**yber **S**ecurity **R**equirements **S**pecification (**CSRS**) shall be created to document mandatory security countermeasures of the **S**ystem **U**nder **C**onsideration (**SUC**) based on the outcome of the detailed risk assessment as well as general security requirements based upon company or site-specific policies, standards, and relevant regulations.

CSRS as a minimum to include:

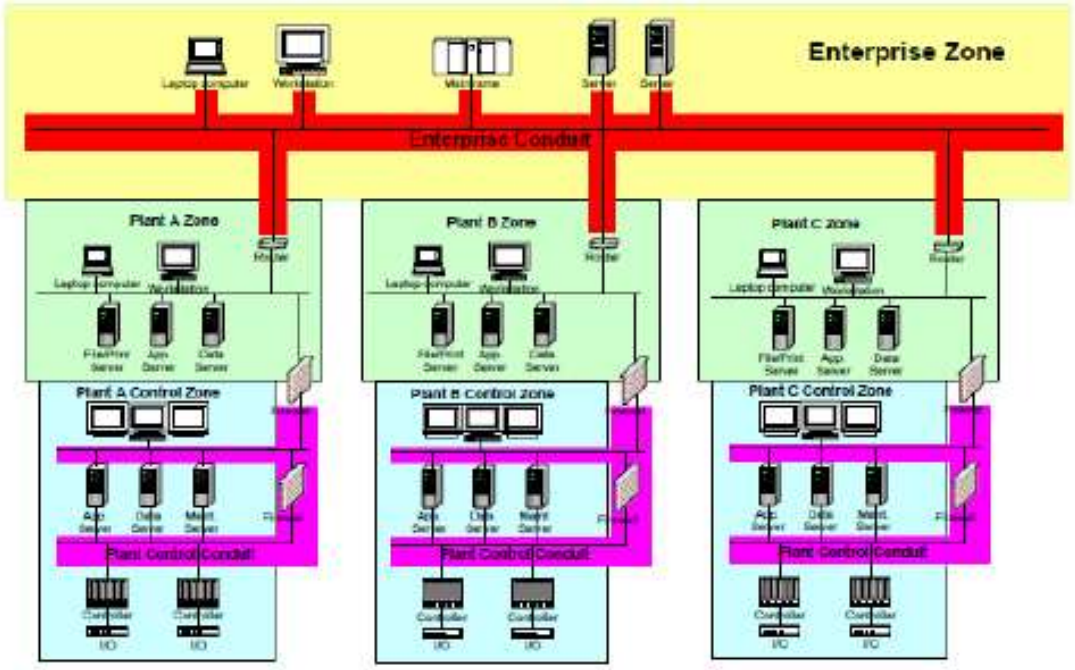
– SUC description & Purpose of the System
–Tolerable risk
– Zone and conduit drawings with Target Security Level (SL-T)
– Threat environment
– Organizational security policies & Countermeasures
– Operating environment assumptions
– Regulatory requirements

<u>The SUC can include multiple subsystems</u>

- Basic Process Control Systems (BPCS)
- Distributed Control Systems (DCS)
- Safety Instrumented Systems (SIS)
- Supervisory Control and Data Acquisition (SCADA)
- Substation Automation System
- Manufacturing Operation Management Systems (MES or MOMS)
- Historians

FLUOR®

Zone and Conduiting of the System



Zone & Conduit Drawings

- **Zone**: Grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization.
- **Conduit**: Logical grouping of communication channels that share common security requirements connecting two or more zones.

FLUOR®

Organizational Security Policies & Countermeasures

Security countermeasures and features that implement the organizational security policies shall be included in the CRS

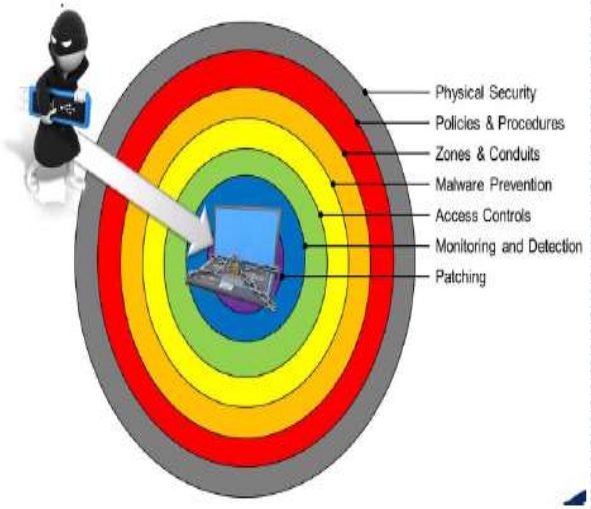
Protecting assets requires a defense-in-depth security approach, which addresses internal and external security threats

Utilize multiple layers of defense (physical, procedural, and electronic) at separate ICS levels by applying policies and procedures that address different types of threats

Selection of the cybersecurity countermeasures should be considered without degrading the achieved risk reduction

Selection of countermeasures is the technical process of risk management driven by organization's risk tolerance

Risk tolerance defined by initial/high-level risk assessment and Results of detailed risk assessment



FLUOR®

Cyber Security – Remember!!!

- First step of any assessment is a well reviewed design, documentation, and the specifications.
- IEC 62443 3-2 provides excellent guidance on cybersecurity risk assessment process and development of CSRS.
- Implement an integrated lifecycle approach with respect to cybersecurity and functional safety. Use PHAs to feed worst case consequences for compromise of SIS.

FLUOR®

References

- IEC 62439-1 : Industrial Communication Networks - High Availability Automation networks - Part 1: General Concepts And Calculation Methods
- IEC 62439-3 : High Availability Automation Networks - Part 3: Parallel Redundancy Protocol (PRP) And High-availability Seamless Redundancy (HSR)
- IEC 60794-1: Optical Fibre Cables – Part 1: Generic Specification
- IEC 61131: Programmable Controllers
- IEC 61850: Communication Networks And Systems In Substations
- IEC 61000: Electromagnetic Compatibility (EMC)
- ANSI/ISA–62443 - Security for Industrial Automation and Control Systems

FLUOR®

Questions

FLUOR®

Thankyou!!!

FLUOR®