The Journal of

RELIABILITY, MAINTAINABILITY, AND SUPPORTABILITY IN SYSTEMS ENGINEERING

—

Summer 2017

RMS Reliability, Maintainability and Supportability Partnership

Table of Contents

SUMMER 2017

Introduction

JOHN BLYLER

Hello! My name is John Blyler. I have the honor to serve as the future editor of the RMS Journal. I knew James Rodenkirch, the former editor, for only a short while but the evident quality and care of his work on the journal will serve as a high baseline for my own efforts.

This issue contains a variety of timely topics. Our first two articles address software and security concerns in the global environment. The last two stories focus on a comparative study of reliability assessment techniques and improving reliability with a supply-chain sensitive automotive market, respectively.

Our first offering is by Katherine Pratt, President of Enviro-Logistics, Inc. She does a great job of taking a systematic, global look at the many weaknesses in the supply chain industry. I particularly like her cautions about the latest Internet-of-Things (IOT) technologies, among other areas. But she doesn't limit herself to merely technological concerns. For example, have you heard the expression "Control Tower" as a practice to foil intrusions into fourth-party logistics and logistics provider models? Her article covers many such topical terms across the breadth of the IT supply chain.

The second piece deals with the timely application of big data in cybersecurity. Its author is Douglas A. Samuelson, President and Chief Scientist of InfoLogix, Inc. He was part of a team for the U.S. Army Cyber Command and Second Army that created an integrated structure of large data sets with quick connections and analysis tools for real-world applications. This effort resulted in prototypes that could be created in a week to deliver functional web-based analytics at mission-relevant speeds. In practice, this framework emphasized moving operational intelligence closer to the source of the problem or attack. I like his analogy of hunting for cyber subs.

The third article moves us into the world of reliability assessment models and methods. Rather than examine yet another variant standard, the author takes a comparative look at three existing models. Egbert Touw is an Enterprise Performance Expert at Altran in Eindhoven, The Netherlands. He focuses on the software reliability of electronic control systems. His paper presents a multifaceted assessment technique that results from a comparative look at the existing CMMi and Automotive-SPICE process assessment requirements, as well as ISO-25010 based code assessment that identifies software reliability risk. The conclusion may not be what you expect.

The last article presents a Robustness Validation (RV) approach to the design of automotive memory components. This approach addresses reliability and safety margins between the design and actual application. I wrote this article based on a paper presented by the author, Valentin Kottler, Robert Bosch GmbH, at the IEEE International Electron Devices Meeting (IEDM) in December, 2016. The author described improvements in reliability as just one of the benefits in using the supply-chain sensitive Robustness Validation (RV) approach to qualifying non-volatile memory (NVM) components for the automotive electronic market. In general, RV is used to assess the reliability of electronic components by comparing the specific requirements of the product with the actual "real life values."

This article focuses specifically on automotive electronics and the application of RV as a more holistic approach than traditional standards, like Automotive Electronics Council (AEC) AEC-Q100, a failure mechanism based stress test qualification for packaged integrated circuits.

That's it for this issue of the RMS Journal! I hope you find it interesting and useful. Please feel free to submit or repurpose your own work for consideration in future issues. My contact information is provided below.

And finally, here's a shout-out to our latest website and newsletter sponsor, Mentor – a Siemens Company. You can look forward to future technical articles from this systems engineering giant.

Cheers, John

Global Supply Chain Vulnerabilities (Part II)

KATHERINE PRATT

Introduction

There are multitudes of e-platforms used within the U.S. and globally, each with their own set of vulnerabilities. In IT, a platform is any hardware or software used to host an application or service. Some are used mainly in industrial applications, such as robotics or real-time analytics factory automation. Others are the foundation of our business communications systems such as emails, computers, software, networking, telephone systems, inventory control systems, accounting systems, and customer relationship management systems.

While these systems offer wonderful advantages, they also have vulnerabilities that are being exploited by international economic "pirates." This article will explore these issues and offer prudent considerations.

Wireless Network Vulnerabilities

The type of attacks directed against Wi-Fi users includes access control attacks. Two out of three companies use business local area networks (LANs), but security continues to be their number one challenge. These attacks attempt to penetrate a network by using wireless or evading Wireless LANS (WLANs) access control measures, such as AP MAC filters or 802.1X port access controls.

So, if these systems are so problematic, why does industry continue to use them? Predictably, the answer is that WLANs can reduce network installation costs and make workforces more productive and improve corporate bottom lines. But a poorly secured WLAN can also leave a company's network vulnerable to misuse and attack, jeopardizing business assets.

Ethernet and Wi-Fi types of attacks include:

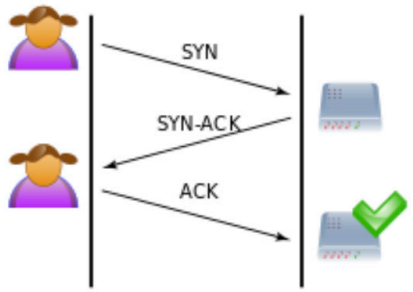
- Email worms and phishing attacks,
- Web-borne spyware and Trojan downloaders,
- TCP SYN flood, ICMP Ping-of Death
- Bad IP options, route poisoning

Physical Media and Data Link threats are different:

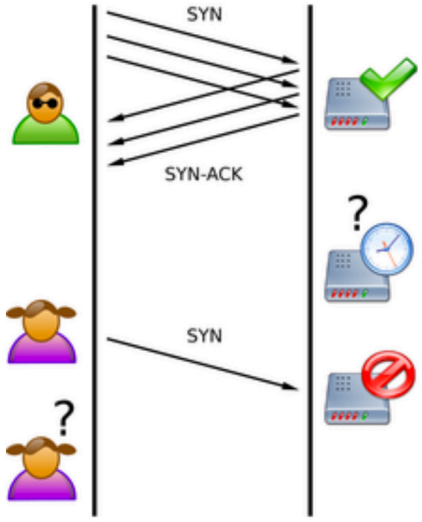
- CAT 5/6 cables limit access to Ethernet LAN
- Radio transmissions are unpredictable
- WLANs must be defended against new threats.

Here is an example of these problems:

This is a normal CP SYN connection between a legitimate user and a server. The three-way handshake is correctly performed:



On the following page is an example of CP SYN Flood. Here an attacker sends several packets but does not send the "ACK" back to the server. Thus, the connections are only half-opened and continuously consuming server resources. The legitimate user tries to connect to the server, but the server refuses because the attacker ties up its resources, and it is unable to open a connection, resulting in a denial of service.[1]



WLANs need to provide measures to address security vulnerabilities for:

- Confidentiality
- Integrity
- Availability
- Access Control
- Authentication

This above list can be applied to any technology for addressing security vulnerabilities. Obviously, disparate systems have unique and specific ways in which they must address each of the above areas.

WLANS use 802.11 frame relays, which is a packet switching telecommunication service that is designed for cost-efficient data transmission for intermittent traffic between LANS and between endpoints in Wide Area Networks (WANS). Currently 802.11 management and control frames have no integrity protection. This service has been in the process of being phased out since 2007, mainly because of the following challenges to this technology, such as:

Wireless "Sniffers," also know as WLAN Analyzers, which can easily capture 802.11 traffic. This includes MAC addresses, SSIDs (Local Area ID) and headers surrounding data, which also may possibly be visible. If the Protection is set to off, then eavesdroppers can see IP addresses, usernames, passwords, share names, and mail messages. If the protection is on, then the data payload is obscured.

Wireless Network Security Best Practices

Wireless networks have become a global corporate business norm. There are ways of securing WLANs by building the wireless LAN infrastructure using WLAN best practices, and selecting the Wi-Fi standards that best suit your network and security needs. Some of the easiest things you can do immediately are to insure your antivirus protection is up-to-date with personal firewalls and anti-spam, anti-spyware and privacy control features, however, do not forget to install the latest device drivers, too.

Even if you have discontinued or banned the practice of using Wi-Fi, it is likely your offices have been visited by unauthorized or rogue 802.11 devices. An inspection should also be made to determine if there are any rogue or unauthorized devices. Although it is relatively easy to detect one, it can be difficult to actually track them down for elimination.[2]

Systems Applications & Products (SAP) Supply Chain Management (SCM) Corruptions and Fraudulent Actions

SAP SCM is one of the most widely used global systems. It is a part of *SAP Business Suite*, used by business systems that store and process critical corporate data. It is used for supply chain management optimization, measuring optimal usage of resources to improve profitability. Retail industries will usually build their business processes around SCM systems. An unauthorized access can lead to control compromises over logistics processes. This system can be accessed through the Internet to give vendors a convenient remote access, but which also make it a perfect target for attack. There are many different kinds of SAP SCM fraudulent actions.

SAP SCM Sabotage

Sabotage is a typical risk. For instance, unauthorized modification of data can cause fraudulent financial losses. Because SAP SCM uses key business-processes based upon logistics, the system can be hacked to rely on erroneous data, resulting in the goods being sent to full warehouses that are unable to accept them, or the driver's route can be changed thereby delaying delivery to the warehouse by the promised delivery date, which can generate further financial penalties, as well.

SAP SCM Theft of Funds

Having gained control over SAP SCM, attackers can cause an income shortage or even transfer money to a different organization using an unauthorized access to SAP SCM. An attacker can transfer funds to an unknown bank account using a front company.

This is even more likely if the company's employees are in collusion with a third-party organization. The differences between the real costs of services and the costs entered deceptively may be used as a means of embezzlement. An attacker may even create false vendors and transfer money to these accounts. An example of such an operation occurred in Iraq, when with the help of a surreptitious vendor an order was made for bomb detectors and the total cost exceeded 55 million.

SAP SCM Vulnerabilities

SAP SCM uses SAP Netweaver Application Server ABAP (AS ABAP) as a main platform. Currently there are about 80 vulnerabilities specific to the different modules of SAP SCM. In 2007, a Gateway-service vulnerability was discovered

that could potentially compromise SAP server access, allowing any of the operating system (OS) commands to be run.

In May 2016, it was revealed that there are at least 36 organizations worldwide affected by SAP vulnerabilities. The Invoker Servlet, a built-in functionality in the SAP NetWeaver Application Server Java systems (SAP Java platforms), contains a vulnerability that was patched in 2010 however, it continues to affect outdated and misconfigured SAP systems. The Invoker Servlet vulnerability affects business applications running on SAP Java platforms, residing on the SAP application layer, so it is independent of the OS and database application that supports the SAP system.

Exploitation of the Invoker Servlet vulnerability gives unauthenticated remote attackers full access to affected SAP platforms, providing complete control of the business information and processes over these systems, as well as potential access to other systems.[3]

Radio-Frequency Identification (RFID) Tag

RFID is an automatic identification technology, and unlike a barcode, which relies on a visual line-of-sight scan to transmit data, RFID relies on radio waves. The data from the RFID tag (i.e., transponder) is presented to the user by an electronic receiver.

RFID can help companies to manage many elements of their business such as parts, tools, returnable containers, vehicles, and much more. RFID are often used to notify shippers when a shipment has arrived at port. RFID tags are available in various frequencies, however, the ultra-high frequency (UHF) is the one used for supply chains. Typically, higher frequencies offer more bandwidth, data exchange and a higher communication range.[4]

Active RFID Tags or Wi-Fi tags can readily communicate directly with standard Wi-Fi infrastructure without any special hardware or firmware modifications and can co-exist alongside other Wi-Fi clients such as laptops and VoWLAN phones.

Multimode RFID Tags enable tracking of reusable shipping containers from a manufacturer, a distributor and a retailer using a combination of Wi-Fi Active RFID and passive RFID. Such a device may also include the capability to use tag magnetic signaling proximity communication devices as well.

RFID can be used to notify when a shipment has arrived at port.

Typically, there are blind spots at ports, railroad depots and at airports—this is likely to occur wherever goods are transferred between transportation modes or carriers. Legacy systems, such as the Electronic Data Interchange (EDI) system is currently used in supply chain communications to provide information about goods, but usually only at certain checkpoints. Because of system latency, it is only able to process messages in batch mode.

Big Data is now supplanting these legacy systems, because it is able to not only determine an accurate estimated time of arrival (ETA) of goods, but it enables the buyer to know several days in advance when the shipment will actually arrive, facilitating better planning and coordination of support services. This improved lead-time has enabled a return on investment to meet purchase order deadlines, and improved market response.

There has been an increase in theft of inventory at airports and on roads around the world. Theft costs shippers billions of dollars each year. Companies such as Savi Cloud Subscription are able to track shipments and can alert law enforcement authorities if the cargo leaves a designated geographical "fence," and to help them to recover stolen goods.[5]

Challenges such as privacy and data security remain active problems. New strategies addressing digital disruption include designing the SC operations around the intersection of suppliers, products, and customers. By offering highly individualized, focused products, customizing customer services to include buying anywhere, collect anywhere, and return anywhere capabilities using flexible channels.

By leveraging the full spectrum of digital technologies, such as investing in analytics, mobility and cloud, plus artificial intelligence, intelligent products and IoT, this facilitates higher levels of value to be achieved in terms of both profitability and revenue growth. Another advantage is offering smooth scalability to accommodate scaling SC up or down as circumstances warrant, and therefore enabling easier optimizing or duplicating processes, detecting errors, and adding or reducing partners as needed.

A digital design network will need to be designed to deliver increased competitiveness. By using value chain analysis, the value-creating activities can be identified that are core to the newly designed digital supply chain. Then the digital supply chains can be restructured as networks, and equipped with new capabilities embedded by digital technologies.[6]

Software Vulnerabilities

Manufacturer software vulnerabilities are typically disclosed on the site CVE Details. In the past 10 years Microsoft has disclosed 3,157 security flaws in its

products. About 50 percent of these involved errors that allowed malicious code execution, and exploits were created for 192 of them. An exploit is a weakness in a computer system or program that uses software, data or commands to carry out some form of malicious intent, such as a denial-of-service attack, Trojan horses, worms or viruses.[7]

Microsoft's buffer overflow vulnerability in the Server Service allowed attackers a way to remotely execute malicious code on vulnerable systems, and another flaw allowed wormable exploits leading to millions of systems worldwide to become infected. Whereas Oracle has had over 3,100 disclosed vulnerabilities, and ten percent were in 2015 alone. While Apple products had over 2,600 vulnerabilities in the last ten years and twenty-six percent were in just the last year. Others with relatively high numbers of vulnerabilities include Cisco, Adobe and IBM. Even thumb driver USBs controller chips were found to be vulnerable to reprogramming, which would enable them to be used to surreptitiously carry out malicious tasks, such as stealing data and files, or installing malware, redirecting traffic and infecting other USB devices.

Traditionally, application developers' security focus has been limited to static code analysis and fuzzing techniques. Today's reality is that secure application deployment principles must extend from the infrastructure layer through the application and include how the application is deployed. There is a concerted ongoing effort to anticipate where future cyber crime will be focused and where the new battlegrounds are in terms of actors—hackers, criminal, nation states and threats.[8]

Internet-of-things (IoT) Vulnerabilities

The internet-of-things (IoT) is turning people's homes into automated living spaces that promise extra convenience. Often people talk about these technologies and IoT, as if this smart automation technology applied only to gadgets and infrastructure. However, for any device to be categorized as IoT, it needs connectivity and the ability to be able to receive, process, and transmit digital information similarly as to a computer. Additionally, it needs to be able to connect to the Internet and communicate with other smart machines around it. An example of this is when the phone rings, the TV's volume automatically decreases.

Gartner predicted that by 2018, there would be over a billion connected devices in use, and that figure is for smart homes alone. Japan and Germany, two of many urban areas, have embraced this particular technology, to the point of necessity. There is no unified regulating body within this industry to instill functional and security standards of these devices' manufacturers, and this can lead to multiple security issues of privacy and safety, forward going. This technology, when applied to wearable's such as fitness trackers, can record a user's exact location, and therefore, is potentially vulnerable from tracking, or even personal attack. Not all smart devices have basic built-in security measures.

As many IoT device functionalities are reliant on cloud-based components supplied by the companies that manufactured them, it would be prudent to enquire what support would be available for the product if the manufacturer goes out of business, or gets absorbed by other organizations. An example of this problem occurred with the 246 padlock in Japan, which shut down its service this year. This padlock enabled users to lock or unlock the device by using a key accessed by a smartphone app. The users were left with no other option than waiting until the battery ran out in about 180 days. The companies offered refunds, but only those who could physically return the locks, were eligible.

Currently smart applications are only available on a single operating system. Predictability, this encourages widerscaled attacks. Trend Micro using controlled settings was able to determine it was possible for attackers to remotely snoop on smart car data and even to alter the status of automated gas tank gauges.

There are some go-to things that can be done to minimize these e-intrusions. First, become familiar with the functionality of your device(s). If your IoT devices offer encryption capabilities, make certain they are on by default. Check your default setting (passcodes supplied by the manufacturer) and change them if necessary to ensure your privacy and security. Create a strong router password right after you set it up. When setting up a home network, instead of the widely used, and easily compromised Wired Equality Privacy (WEP), you can opt for the Wi-Fi Protected Access II (WPA2) protocol.

By also setting up the firewall to only allow traffic on specific ports, you can significantly cut down on potential network-probing attempts. Also, by setting up a guest network for your devices, this limits the devices' ability to talk to each other and potentially pass on malicious commands or content. Frequently changing your passwords can ban outsiders from accessing your router and devices. Also make sure to use unique passwords for each of your home IoT devices.

Since a number of IoT devices can be controlled through mobile devices via an app, your smartphone also needs protecting. Here, standard mobile

security guidelines apply. Much like smart devices, make sure your phone is updated with the latest firmware version. Installing a mobile security app can also prevent malicious apps or codes from running on your phone.

Ultimately, manufacturers limit your systems' internal security, and they should be able to keep compliance on track and save their companies from future business headaches by conducting risk assessments and security audits. Integrating security in the devices' endpoint Software Developers' Kit (SDK) can do this. Security solutions for SDKs should allow manufacturers to block attack attempts, perform risk assessments, and secure their IoT platforms before a new firmware or patch is released.[9]

Global Supply Chains Threated by Cyber Hackers

The International Maritime Bureau (IMB) called for vigilance as a response to the rising incidence of cyber attacks targeting carriers, ports, terminals and other transport operators. The criminals are installing spyware within these transport operators' IT networks. Usually they target personal devices, where cyber security is less adequate. Hackers make use of social networks to target truck drivers and other operational personnel who travel extensively, to ascertain routing or overnight parking patterns. These criminals look to extract information such as release codes for containers from terminal facilities or passwords to discover delivery instructions.

The U.S. Government Accountability Office warned about possible threats to U.S ports. These criminals typically target containers with illegal drugs, high value cargo or human trafficking.[10]

U.S. Congressional Hearings on Cybersecurity

During a House Committee hearing on March this year, Bruce Schneider, a fellow of the Berkman Klein Center at Harvard University, asked for the establishment of a new governmental agency devoted to cybersecurity. The US House Committee on Energy and Commerce held the hearing "Understanding the Role of Connected Devices in Recent Attacks," with several expert witnesses. He suggested that benchmarks be set, but not the methods for achieving them. When pressed for his rationale for establishing a new Cyber Security agency, he further elaborated upon the inadvisability of having different rules if a computer has wheels, or propellers, or makes phone calls, or is in your body. Whenever innovation can be used to create catastrophic risk, such as shutting down all the power plants, then, this industry requires proper oversight.[11]

Risk Mitigation: the Supply Chain Safety Net

Historically, shippers expanded their sourcing, manufacturing, and distribution, which created fragmented SCs. Since 2008 when the great recession affected the global economy, shippers rationalized their networks to be more efficient, drive velocity, reduce costs and improve service quality. This strategy of fewer redundancies increased their exposure to risks.

Over the past several years, there have been several natural disasters sending shock waves though supply chains: Iceland's Eyjafjallajökull volcano eruption in 2010, the earthquake and tsunami that struck Japan in March 2011; severe floods in Thailand that followed four months later; and Hurricane Sandy in the U.S. in October 2012.

Global supply chains, by design, are fraught with risk. Lately, supply chains are being optimized, such as offshoring for cost purposes, and keeping inventories low for just-in-time efficiency. All of this builds even more risk into their networks.

SCM builds in strategies for managing risks, which include:

1. Physical mitigation: Safety stock, multiple suppliers, and excess capacity.
2. Analytical mitigation: Sales and operations planning, forecasting, and collaboration. Emphasis can be placed on control towers, and real-time visibility over both transportation and materials movement.
3. Financial mitigation: Focus is on financial risk problems.

Nearshoring is a process of locating production nearer to demand, which can shorten the SC and reduce risk and volatility. Shippers can also turn to third-party logistics and forwarding partners as an extra measure of security. These value chain partners can provide cover in terms of facilities, IT systems and labor, and even pre-positioning materials or inventory in certain areas, to position materials closer to the point of consumption. Nearshoring and regionalization may reduce transportation costs and increase demand agility, but these strategies may also help with currency fluctuations. Currency flux has a greater impact on transportation than any other function.

The term "Control Tower" in SCM is the practice of providing a technology to foil intrusions into fourth-party logistics and logistics provider models—this means having dedicated teams working closely with customers to manage material flows through systems and processes. There are companies that can provide shared customer operations in Europe,

North and South America and Asia. These towers can comprise anywhere from 10 to 20 multi-lingual operations personnel, conceivably providing 24/7 visibility across a common global platform.

The best protection against SC risk is developing a sense of probability—in spite of the fact that not all risks are equal. Some companies are able to use predictive analytics to drive competitive advantage. There are even companies that offer probability-based blackout models down to the street level, when planning for major weather events.

Compared to physical and analytical mitigation tactics, financial risk management is an area largely overlooked in SCM. GSCM also has to consider the less stable currencies around the world. When getting pricing for a service such as shipping, it is prudent to consider where the shipment is originating from, the currency it is using, and what the anticipated exchange rate might be. If you have a value chain and every agent in that chain is hedging its risk, the accumulation of hedges can be significant. By the time all the individual hedges are added up at each point, they can equal 25% of the cost of the product.[12]

Clearly, there are ongoing vulnerabilities with GSCM—how does one begin considering pro-active strategies for if not mitigating these disparate threats, then, perhaps minimizing them? Telecon, a banking and energy company IDT Corporation in Newark, NJ uses a combination of three products from Palo Alto to protect its network: Wildfire network detection software; Traps, for end point protection, acquired from Israel-based Cyvera, and Global Protect, which allows IDT to extend the benefits of WildFire and Traps to mobile devices and computers that leave the office. This software combination replaces the need for IT staffers to detect malware, disconnect the computer from the network, upload the file to the antivirus lab, and it does this in near real-time. Hackers also use automation, so this levels the "playing field."[13]

Big data, both structured and unstructured, continues to offer challenges in managing the magnitude of this potential resource. With the ever-growing data volumes, it is becoming clear that maintaining a focus on just real-time information may make the task of achieving some sort of coherent use of this data possible. The goal is now to be able to use real-time data for real-time decision-making to become a real-time business. Currently mobile devices, social networks, and real-time information are driving big data architecture and analysis tools.[14]

The federal government is also taking notice about the practices of consumer data collection and usage practices. The Federal Trade Commission (FTC) issued orders to nine companies in the data broker industry, requiring them to provide information on their usage practices, as there are significant privacy implications.[15]

There is a dramatic increase in Big Data heists, such as the massive plastic card data theft in South Korea, which affected 20 million card holders at Lotte Card and Nonghyup Bank, plus 40 million KB Kookmin card holders were affected.[16]

Conclusion

The above are technology-based types vulnerabilities, however, there are other kinds of vulnerabilities when evaluating current GSCM practices. For instance, if the U.S. is obtaining all of these GSCM products aboard, this implies we are not keeping supply inventories here.

Nor are we training our people to do the manufacturing work that is being done overseas, and this is creating a skills-gap. As a result of this skills shortage, businesses are unable to meet customer demand and this leaves their ability to implement new technologies while achieving productivity targets threatened.

While the manufacturing industry is facing the need for 3.4 million workers, there is an expected shortage of 2 million workers in the U.S. over the next decade.[17]

This leaves us vulnerable...very vulnerable, particularly in case of a dramatic climate event, war, or pestilence.

So, the word to the wise is evigilo! ●

References

1. Wikipedia.com, "SYN Flood" https://en.wikipedia.org/wiki/SYN_flood
2. "How to Counter Wireless Threats and Vulnerabilities" www.Brightcove.com
3. SAP SCM Security https://www.us-cert.gov/ncas/alerts/TA16-132A
4. "Wi-Fi Location-Based Services 4.1 Design Guide" http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/WiFiLBS-DG/wifich6.html
5. "Sensing Change" by Yasmin Ghahremani CFO.com 11-22-16 http://ww2.cfo.com/supply-chain/2016/11/sensing-change/
6. "The Way Forward: The Digital Supply Network" by Kris Timmermans Nov. 22, 2016 CFO.com http://ww2.cfo.com/accounting-tax/2016/11/way-forward-digital-supply-network/
7. "What Does Exploit Mean?" PCTOOLS http://www.pctools.com/security-news/what-does-exploit-mean/
8. "The 10 Worst Vulnerabilities of the Last 10 Years http://img.deusm.com/darkreading/2016/05/1325425/04-shellshock.jpg

9. "Securing Smart Homes" http://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-smart-homes
10. U.S. Government Accountability Office http://www.gao.gov/key_issues/overview
11. "Understanding the Role of Connected Devices in Recent Cyber Attacks" https://youtu.be/BvId5-0295U
12. "Risk Mitigation: Supply Chain Safety Net", by Joseph O'Reilly Jan 2014 http://www.inboundlogistics.com/cms/article/risk-mitigation-supply-chain-safety-net/
13. "Latest Network Security Threats prompt one question: 'Are we next", by Steve Zurier http://searchnetworking.techtarget.com/feature/Latest-network-security-threats-prompt-one-question-Are-we-next
14. "Big Guide to Big Data", TechTarget http://www.computerweekly.com/feature/How-to-tackle-big-data-from-a-security-point-of-view
15. "Managing big data privacy concerns: Tactics for Proactive Enterprises", by Lynn Goodendorf, TechTarget http://searchsecurity.techtarget.com/feature/Managing-big-data-privacy-concens-Tactics-for-proactive-eterprises
16. "Get Ready for Big Data Heists" by Leonid Bershidsky https://www.bloomberg.com/view/articles/2014-01-22/get-ready-for-big-data-heists
17. "The Skills Gap in U.S. Manufacturing 2015 and Beyond" http://www.themanufacturinginstitute.org/~/media/827DBC76533942679A15EF7067A704CD/2015_Skills_Gap_Report.pdf

Using Big Data in Cybersecurity: Operations Research Analysts Search for 'Cyber Subs'

DOUGLAS A. SAMUELSON

Reprinted by permission, Douglas A. Samuelson (2016) Using Big Data in Cybersecurity. OR/MS Today 43(5):20-23. Copyright 2016, the Institute for Operations Research and the Management Sciences, 5521 Research Park Drive, Suite 200, Catonsville, MD 21228 USA.

Defending U.S. cyber assets such as computer network, operational and intelligence systems against adversaries is one of the most critical tasks the U.S. military faces. The U.S. Army Cyber Command and Second Army (ARCYBER & 2A) has implemented a new, big data approach to address the challenges inherent in this task, exemplary not only for what it is accomplishing but also as a model for how to conduct analytical studies in a fast-paced, complicated setting. The team has created an integrated structure of large data sets, quick connections between them and readily usable tools to enable swift analyses by operators in deployed real-world missions. They can create prototypes in a week and deliver functional web-based analytics at mission-relevant speeds—in often three weeks or less.

In a recent presentation at the Center for Strategic and International Studies, one of the most prominent and respected defense "think tanks" representatives in the country, Lt. Gen. H. R. McMaster, pointed out the ARCYBER & 2A team as an especially good example of how analysis should be done in support of military missions. It is his job to know, as he now serves as deputy commander of the Training and Doctrine Command (TRADOC) and director of TRADOC's Army Capabilities Integration Center. He is noted both as a successful combat commander, especially as a brigade commander in Iraq in 1991, and as a provocative, iconoclastic thought leader. He

wrote one of the most highly regarded critiques of U.S. military policy and doctrine in the escalation of the Vietnam War[1] and managed to continue to advance in the Army, no small feat.

Lt. Col. Cade Saie leads the small team that built the capability, along with Maj. Isaac Faber, who recently returned to graduate school for Ph.D. studies, and Maj. Ross Schuchard. "Cyber is different," Maj. Faber explained. "Traditional statistics don't work because everything is incredibly non-linear. There's a high false positive rate, so operational commanders lose interest pretty quickly if you can't do better."

The characteristics of these types of systems require adaptation in operations research approaches, as well as a re-thinking of military tactics. Formal O.R. approaches such as regression and optimization give way to rapid adaptation and generating multiple options. Additionally, the traditional military tactics become transformed into a rapid feedback loop between defender and adversary, so the operators' analytical requirements change along with the pace of action.

One of the key principals in advocating the inclusion of O.R. methods in cyber, Maj. Gen. John Ferrari (U.S. Army Director of Program Analysis and Evaluation), handpicked the team in 2014. He described the problem, referring back to the roots of operations research, as "searching for cyber subs." As in the World War II search for attackers, the essential idea is to place the analysts with the field commands, close to the situations of interest, and have them work closely with operational commanders to define the challenges, produce prototype solutions and rapidly implement. Showing agreement with Ferrari's sentiment, U.S. Army Cyber Command's Lt. Gen. Edward Cardon chartered the creation of a small ORSA (operations research/systems analysis) cell within the command. By taking this approach, Lt. Col. Saie amplified, "Analytics is then embedded into the daily operations routine."

The ARCYBER ORSA team spent the first year after its founding in late 2014 doing some traditional O.R. analyses and modeling, developing some cyber operations metrics, and defining requirements for a big data platform that would support the expansion of advanced analytics and cutting-edge O.R. techniques and dissemination of those techniques to operators.[2] "We had a big data platform that couldn't be leveraged by operators," Lt. Col. Saie stated. "We needed to create a framework for the ORSA community to participate more readily in analytics with tools widely available in the field such as R or Python."

The focus so far is on just defensive operations, such as intrusion detection and response. The effort to date has also been limited to unclassified data, possibly "For Official Use Only," but not more restricted than that. The key is assembling patterns of low-level anomalies that are not of much interest by themselves but might, in combination, indicate something worth investigating.

The Building Blocks: Use Cases

The data platform the team built now integrates several dozen live data streams. Defenders identify use cases, that is, activities that are to some extent out of the ordinary, and they and the analysts then build analytics to address operational needs in response to the use cases. Most of these analytics now integrate regression, clustering, time series and visualizations—and heavily emphasize open source software.

Current data assembly relies on a

global sensor grid that relays alerts to a central repository, consolidated by a commercial software product known as a Security Incident and Event Manager (SIEM). Queries can be complicated to formulate and slow to execute, with results that an analyst must then manually evaluate. It is difficult to answer complex questions or support even moderate mathematical algorithms. Verifying actions and their effects at multiple levels of activity is also difficult.

Big data technologies enable drastic increases in query speed and data storage limits by leveraging parallel computing. These technologies also create dynamic computing environments to support more advanced analytical tools and methods. Hence, the vision for the future is a federated network of cyber analytics platforms; that is, the data sets are all compatible in terminology and structure and therefore can easily be viewed and studied in combination.

To move toward the new structure, the team gathers problems from the Defensive Cyber Operations (DCO) community as part of the community's routine functioning. Then, the problem is given to a development partner (Center for Army Analysis, the U.S. Military Academy at West Point, the Naval Postgraduate

School or the Air Force Institute of Technology) or remains in-house for resolution via analytic development. Once the first version of an analytic is complete, it is deployed on a big data training system and used/validated by DCO community members. After feedback is incorporated, the revised analytic is then deployed onto an operational platform where it then becomes part of the operational workflow for the consuming organization.

The analytics range from simple (providing sorted counts) to moderate (providing interactive network flows) and finally to complex (such as Bayesian change point detection). Some of the most immediate impact of the work was simply observing workflow processes and creating capabilities within analytics that automated some analyst tasks, such as generating reports. This simple act of addressing a time-consuming aspect of the cyber analyst workflow had a double benefit: helping the team gain operators' trust and solidifying the rapid analytic development framework. Over a small period of time to test the framework, the team worked closely with a small group of personnel, with a wide range of specialties, to develop a group of use cases and, from there, to produce analytics which helped to identify certain types of malicious behavior and thwart numerous unauthorized communication attempts.

In broad terms, analytics may employ a range of standard descriptive displays, some statistical tools, and innovative data exploration methods to find patterns of activity that are identified as potentially of interest but that would tend to elude more traditional approaches. In Medicare fraud detection, combining data from different types of claims often yields findings that would not have been apparent from just one source—for example, hospital surgery claims without associated claims from a surgeon and an anesthetist, or reasonable-looking numbers of services allegedly delivered within a short time span in several different places. A similar idea of combining disparate data sources and looking for connections among events that seem innocuous by themselves applies in cybersecurity threat detection.

Another parallel to Medicare claims analysis is that the anomaly of interest may not be an outlier. Rather, it might be a number of events, each quite unremarkable by itself, with unusual frequency—or even a set of events with less variation than typical. In Medicare claims, for example, an event of interest could be a provider with a high volume of claims and no claims with values that trigger a range check, when some such values are often observed in general. The absence of typical variation suggests that the provider may be submitting false claims for services that were never rendered; they know enough to fake unremarkable claims, but not to fake typical variation. Similarly, in cybersecurity monitoring, a "too regular" log of activity on the system could be an indicator of a log file being spoofed to conceal an intrusion.

These examples do not describe the actual use cases ARCYBER has pursued, but they are meant to illustrate the principles of reasoning in this field. In the view of some people especially knowledgeable in this topic area, too much specificity, even based on unclassified information, could reveal too much to prospective adversaries. ARCYBER produced a report, "The Rapid Analytic Development Framework,"[2] that describes many of the analytical tools and use cases in greater detail, along with a more detailed description of the command and its activities. Although an unclassified version is available, even that version of the report has distribution limitations and must therefore be requested from the organization.

Closely Embedding Analysts with Operators

The examples briefly summarized here and expounded in detail in the RADF report illustrate the kinds of analytics, based on use cases identified by operators, the analytical team has conducted. What is most important, however, is how the analysts do this. "We sit next to the operator," Maj. Faber says, "and we're very adaptive. We put an extreme premium on change. We have tight iterative feedback, changing approaches, getting new problems. Our goal is a simple

solution evolving to more complex with continual feedback. With this approach, parties stay interested because they stay involved. The end user is involved from inception to delivery."

The analytical focus is on reducing false positives and identifying low-level events of potential interest. False positives are common and a serious challenge. Maj. Faber recounted, "Routine scans to see how many Windows 10 machines were active on a network set off intrusion alerts." To detect the subtle elements that do not set off intrusion alerts but are more meaningful, a key analytical approach is finding correlations between heterogeneous data sets. "At some point in the future," he went on, "we hope offensive and defensive data sets will talk easily, at some level of classification."

Concentrating on operator-identified use cases drove the implementation and the data architecture. The development and improvement of the large, integrated data platform provided the capability to ingest and process mission relevant data actively and quickly. The team automated inclusion of network activity reports and other incident data. Standardizing some formats greatly eased the task of comparing. An additional financial benefit was enabling commands to do more analytical tasks in-house rather than having to rely on other agencies or commercial providers.

Summary

The Army Cyber Command and Second Army's Rapid Analytic Development Framework, built on a big data and parallel computing architecture, has produced striking improvements in defensive cybersecurity operations and provides a powerful example of how to integrate OR/MS into a real operating setting. "Placing analysts on station," integrating them into the operational team to identify and address problems quickly and adaptively, as Philip Morse famously recommended during World War II, remains the most effective approach to using OR/MS professionals' talents. ●

For more on the topic of cybersecurity from Doug Samuelson, see the September/October 2016 of Analytics magazine: http://analytics-magazine.org/

References

1. H. R. McMaster, 1996, "Dereliction of Duty: Johnson, McNamara, the Joint Chiefs of Staff and the Lies That Led to Vietnam," Harper.
2. U.S. Army Cyber Command and Second Army, 2016, "The Rapid Analytic Development Framework." Point of contact: U.S. Army Cyber Command and Second Army, 8825 Beulah Street, Fort Belvoir, Va.

Multi-faceted Reliability Assessment Techniques: An Industrial Case Study

Method for Gaining Software Reliability Insights of a Supplier's System

EGBERT TOUW

Editor's Note: The following work was first published in the 2017 IEEE International Conference on Software Architecture Workshops (ICSAW). It is used here with permission from the IEEE (see end of article). References have been removed to meet copyright issues but are available on the IEEE website: http://ieeexplore.ieee.org/document/7958430/

A note about the assessment method used in this study. The author explained that all assessments conducted in this case study were based on collecting evidence from available documentation (direct and indirect) and participant's interviews (oral affirmations). This historical data made it very difficult to calculate any probability of failure of the software.

As quoted in the reference (MIL-STD-882E for System Safety), "the assessment of risk for software, and consequently software-controlled or software-intensive systems, cannot rely solely on the risk severity and probability. Determining the probability of failure of a single software function is difficult at best and cannot be based on historical data. Software is generally application-specific and reliability parameters associated with it cannot be estimated in the same manner as hardware. Therefore, another approach shall be used for the assessment of software's contributions to system risk that considers the potential risk severity and the degree of control that software exercises over the hardware."

Thus, a software risk assessment code (RAC) classification method was used to express the reliability risk. For each practice that is assessed in this case study a reliability classification is added in the Excel based assessment tooling according the distribution in Table 1. Reliability classification for code coverage will be "1." When all software code is covered by tests (satisfaction=Fully) the chance is low that defects are not found. Reliability classification for code coverage will be "4." According to the author, the method applied in this paper fulfills the requirements of the Software Engineering Institute's Assessment Requirements for CMMi® (ARC) [11] and the Automotive SPICE® process assessment model [12].

This case study describes the application of three combined assessment reference models that result in a measurable and reproducible insight in quality aspects of complex systems. In this case insight is given in the software reliability an electronic control system. A multifaceted assessment technique is presented that meets both the CMMi and Automotive-SPICE process assessment requirements and identifies the practices in the product lifecycle processes that might introduce not-found faults in software. An in depth TMMi based test assessment technique identifies reasons why not all introduced faults are found. As the third technique an ISO25010 based code assessment identifies reliability risk areas in the software code. Qualitative assessment data obtained from documentation study and interviews is translated in a reproducible software reliability number. Based on detailed observations and findings improvement proposals are reported that increase obviously the overall reliability number when implemented. The three presented assessment techniques are

commonly applied in high tech industry as well as in automotive industry however not in the described powerful combination. The multi-faceted assessment techniques can rather simply be made more specific for the automotive application by exchanging the CMMi reference model by Automotive-SPICE.

I. Introduction

In the automotive domain where system availability and system performance is very important, reliability management becomes crucial. In the main focus areas concerning safety and reliability of automotive safety-critical electronic control systems [13] there is a serious need for accurate assessment techniques that provide insight in quality aspects like safety and reliability, in particular of software components. System reliability depends on all processes in the product lifecycle, design, production as well as maintenance. The probability of failure over time can be predicted based on the age of parts or components in the system. There are just a few parameters needed (age and failures) and statistical models [8] to predict reliability of hardware parts. Software reliability however cannot be predicted based on age and failures of the software component. Software does not wear out over time and a lot more parameters have influence on the quality of software [7]. The probability of software failure depends on the number of faults in software that have not been found during the development process and the risk that these not-found faults will ever come to expression. On top of this it must be accepted that with every change on a released software product new faults are introduced that will not be all detected and resolved during the change implementation process. Changes on software in a released product affects software reliability in a negative way. For this reason also service and maintenance processes for software need to be taken into account in the case study. For getting insight in software reliability, assessment models, like Automotive SPICE [6] and CMMi [3][4] have proven to be more accurate than statistical models.

Software quality aspects and in particular software reliability is hard to measure. Although software reliability growth models (SRGMs) have been developed to estimate or simulate software reliability measures such as the number of remaining faults, software failure rate, and software reliability [14] there are no existing tools or techniques that are able to give our customers insight in the software reliability risks and status of their products. To the best of our knowledge, a multifaceted assessment technique that looks at fault injection processes as well as at fault finding processes and at the remaining faults in the software by means of a code assessment, is not known. Most of the current research on assessment approaches on software reliability focus on the fault injection processes which are always related to the design processes of the software [10]. The described assessment techniques give integral insight in different quality aspects where causes can be linked to effects and observations to realistic improvement recommendations. The rest of the paper is organized as follows: Section II covers an introduction in defect removal effectiveness. Section III describes 3 types of quality areas that will be addressed in this paper. Section IV outlines the multifaceted assessment method. Section V discusses the results of the case study. Finally, Section VI describes some improvement proposals and how they worked out in practice and future work that is foreseen for the described assessment techniques.

II. Defect Removal Effectiveness

A simple metric for effectiveness for defect removal is described by S.H. Kahn [1] and depicted in Figure 1. It is the ratio of faults found by test cases (Ntc) to the total number of faults (Ntot) reported during the test cycle (by test cases or by side effects)

$$TCE = 100 \times N_{tc} / N_{tot} [\%]$$

The Traditional Fault Injection Model [9] (Figure 1.) basically says that given

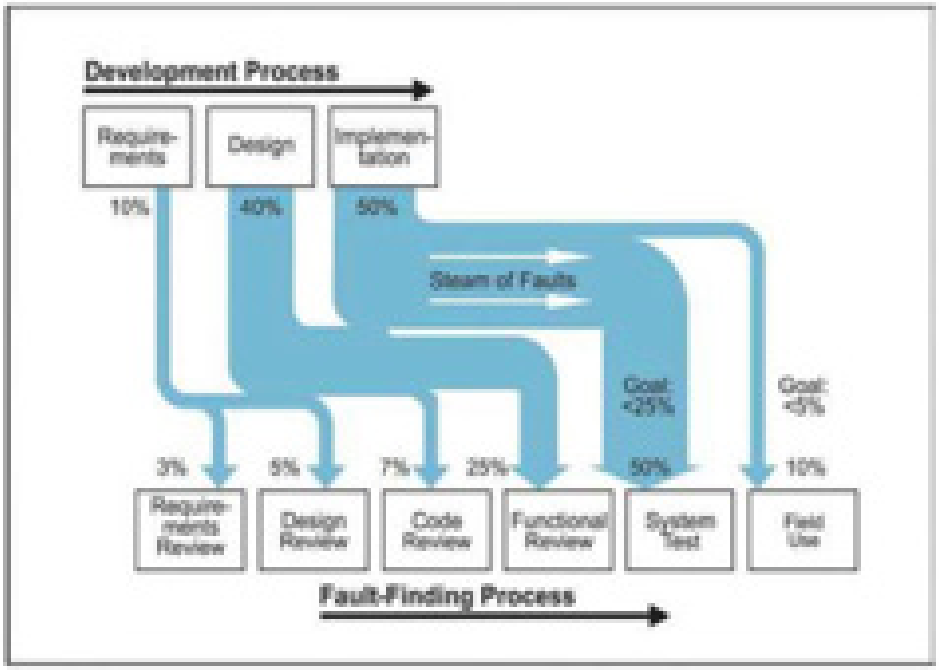


Figure 1 – Traditional Fault Injection Model

a software project—you have defects being "injected" into it (from a variety of sources) and defects being removed from it (by a variety of means). This high level model is good to use to guide our thinking on reasoning about defects and defect processes.

Defect removal effectiveness in this case study is defined as to deliver a product with the fewest defects which is: to minimize the number of defects that go in and maximize the number of defects that are removed. On top of this the case study evaluates the ability of a product supplier to service and maintain the product in such a way that when a not-found defect comes to expression, the problems will be resolved without being noticed by the end-user during field use.

Fact is with software, there will always be some defects left that might express themselves somewhere in the future when external conditions or use of the product changes causing the product stops functioning as specified.

Software reliability in this case study is defined as: The Probability of failure-free software operation for a specific period of time in a specified environment.

III. Insight in Software Quality

In this case study insight is obtained in the development and maintenance processes that are applied to create and service the product during its lifecycle. By combining process assessment techniques with a code assessment we also get insight in the software defects that were not found and resolved during the development process but were left in the code base.

Process Quality

In this case study only those process areas have been assessed that have any influence on injecting or removing defects in the software code. The CMMi for development [3] and CMMi for service [4] are used as reference assessment models. CMMi based models are selected because they all have the same structure and identical assessment procedures can be applied. Furthermore it won't take much effort to adjust the Excel based recording and analysis tooling to the defined scope of the assessment. From the CMMi for Development, eight process areas have been selected: Requirements Management (REQM); Process & Product Quality Assurance (PPQA); Configuration Management (CM); Requirements Development (RD); Technical Solution (TS); Product Integration (PI); Verification (VER); Validation (VAL). From the CMMi for Service, four process areas have been selected: Service Delivery (SD); Service System Development (SSD); Incident Resolution & Prevention (IRP); Service Continuity (SC). These process areas are included to assess defect identification and resolution during the maintenance phase of the product lifecycle.

Test Quality

In this case study the processes for removing defects are assessed more in depth applying a number of relevant process areas from the TMMi [5]. The TMMi reference model contains the same structure as other CMMi based models. Focus on Test strategy; Test design; Test execution; Test environment; Test documentation and Traceability. The assessment team judges on how efficient and effective the chosen test strategy is applied, if test strategy, test cases, test environment and plans are adjusted based on actual test metrics and results and in what way the assessment results affect the reliability of the software.

Code Quality

In this case study, software code is assessed against software quality aspects referenced in ISO25010 [2]. This standard describes 6 main quality categories; Functionality, Reliability, Usability, Efficiency, Maintain-ability and Portability. The case study focus will be on: Reliability (Maturity, Availability, Fault Tolerance, Recoverability) and Maintainability (Modularity, Re-use-ability, Analyzability, Modifiability, Testability) of the software components. For the other quality categories adequately detailed requirements were provided.

The main tool applied during the code assessment is; "Understand"—a multi-platform tool for code analysis and comprehension of large code bases. It enables code comprehension by providing flow charts of relationships and building a dictionary of variables and procedures from the provided source code. The following subjects are investigated: Method size; Cyclomatic Complexity; Fan in/out, Cyclic Dependencies, Dead code; Coding rules [21]; Code smells. Duplicated Code has been identified with the tool "CopyPasteDetector" (CPD) from the PMD-suite of Sourceforge. Next to this assessors will look into: Archive structure; Product variants; Reliability mechanisms and Engineering practices [15], [16], [17], [18], [19], [20].

After analysis of the results from the tooling combined with the information from interviews with members of the development organization, the assessment team will identify a number of software reliability related risk areas in de codebase. Also a number of not found defects will be identified apart from the conclusion that they will ever cause a failure of the product.

IV. Assessment Method

See Editor's note.

Key practice		REQM	PPQA	CM	SD	IRP	SSD	SC	RD	TS	PI	VER	VAL
SG 1													
	SP 1.1	4	1	4	4	2	4	4	4	4	4	4	4
	SP 1.2	4	1	4	1	2	4	4	4	4	4	4	4
	SP 1.3	4		4			4			4	1	1	4
	SP 1.4	4											
	SP 1.5	4											
	SP 1.6												
SG 2													
	SP 2.1		1	4	4	4	4	2	4	4	4	4	4
	SP 2.2		1	4	4	4	4	1	4	4	4	4	4
	SP 2.3				2	4	4	1	4	4		4	
	SP 2.4					4	4			4			
	SP 2.5					4	4						
	SP 2.6					4							
SG 3													
	SP 3.1			4	4	4	4	1	4	4	4	4	
	SP 3.2			4	2	4	4	1	4	4	2	4	
	SP 3.3				4	4	4	1	4		4		
	SP 3.4						4		2		4		
	SP 3.5								4				
GG 2													
Commitment to Perform	GP 2.1	4	2	4	4	4	4	4	4	4	4	4	4
Ability to perform	GP 2.2	4	2	4	4	4	4	4	4	4	4	4	4
	GP 2.3	4	1	4	4	4	4	4	4	4	4	4	4
	GP 2.4	4	1	4	4	4	4	4	4	4	4	4	4
	GP 2.5	4	1	4	4	4	4	4	4	4	4	4	4
Directing Implementation	GP 2.6	4	1	4	4	4	4	4	4	4	4	4	4
	GP 2.7	4	1	4	4	4	4	4	4	3	3	4	4
	GP 2.8	4	1	4	4	4	4	1	4	4	4	4	4
Verifying Implementation	GP 2.9	1	1	1	1	1	1	1	1	1	1	1	1
	GP 2.10	4	2	4	3	4	4	4	4	4	4	4	4
GG 3													
Ability to perform	GP 3.1	4	1	4	4	2	1	1	4	4	4	4	4
Directing Implementation	GP 3.2	1	1	1	1	1	1	1	1	1	2	1	4
Capability on scale 1-4		3,65	1,19	3,68	3,30	3,48	3,63	2,55	3,64	3,67	3,48	3,55	3,82

Overall Score	3,30

TABLE 2 – SOFTWARE RELIABILITY SCORES

V. Case Study Results

This case study is based on an assessment assignment to Altran. [Editor's Note: Altran is listed as and engineering and R&D service company, www.altran.com] In this project, the objective is to help the customer to get an insight in software reliability of one of the systems they buy from their supplier. To achieve this, we have performed a multi-faceted process/code assessment as described above on the development and service processes and on the software code base at the premises of the supplier.

A. Process Assessment Results

Table 2 shows the results in a rating table where each practice for each assessed process area has been rated according to and following the classification in Table 1.

The overall software reliability score for the assessed system is 3,30 on a scale of 1-4.

To be able to understand Table 2 it is needed to have more insight in the content and structure of the CMMi based models [3],[4]. The Abbreviations and Acronyms in Table 2 are given as follows (Abbreviations for described Process Areas are described in chapter IV of this paper.):

SG1, SG2, SG3; Specific Goal 1, 2 and 3 which are not depicted in this table. See [3], [4]. These goals are different for each Process Area.

GG2, GG3; Generic Goal 2 and 3 which are not depicted in this table. See [3], [4]. These goals are always the same for each Process Area.

SP1.x, 2.x, 3.x; Specific Practice. These practices are specific for each process area.

GP2.x, GP3.x; Generic Practice. These practices are always the same for each Process Area.

Discussion on high performing parameters (rated 3,4)

Supplier appeared to have a professional development and service organization with enthusiastic, well trained and ambitious staff. Supplier documented the overall development process and followed a stage gate model for managing the product development process. A professional Application Lifecycle Management (ALM) tool supported the development workflows. Trace-ability from requirements to design, integration, verification, validation to the released product is in place. Development and test teams apply an agile way of work using modern tools and techniques e.g. continuous integration and continuous delivery methods. The supplier's service organization was prepared to take the product into service but first the production of the product had to be started. The quality organization was prepared to manage quality issues in case they should occur.

Discussion on low performing parameters (Rated 1,2)

Supplier's development organization did not implement the QA-role in the development teams. This resulted in all kinds of small errors in dates, numbers, names, internal reports and records in the Application Lifecycle Management Tooling. Since these are all not functionality related errors, engineers did not check on it. In future these errors will slow down the service/maintenance processes significantly since it will be difficult to find the right historic data and sources. It is expected that the same kind of small errors occur in the software documentation, problems reports and change history.

All development workflows were implemented in ALM, however, criteria for completion of tasks or workflows are not implemented. This makes it very difficult to establish a definition of completion for intermediate development processes and for the final released product. This will also make it difficult to check if an engineer has really completed his/her tasks. Since hardly any measurements were defined on processes there is no data as basis for improvement.

The service organization is well prepared for their future task. A service organization and a service system has been established but the supplier cannot prove its effectiveness since the product has not been taken into production and there are no service level agreements in place.

B. Test Assessment Results

The test assessment part focused in more detail on how test effort is spread over the different project phases, see Table 3.

In general the supplier implemented a well-organized, professional test organization with well-trained professionals using modern tools and techniques. Test process, procedures and work instructions were well documented and accessible for all team members.

Most obvious result from test point of view is that functional requirements coverage has been measured from the beginning to the end. However the supplier cannot show what percentage of the software code has been covered by the applied test cases. There is a serious risk that there is code in the product with unknown functionality that has not been

	Unit Test	Integration Test	System Test	User Acceptance Test
Run Frequency	At code checkin, after build	After build	Per release	Per release
Test Automation	Yes	Partly	Partly	No
Edge Cases	Yes	Yes	Yes	No
Functional Tests	Yes	Yes	Yes	Yes
Non-functional Tests	Yes	Yes	Yes	No
Regression Tests	Yes	Yes	Yes	Yes
Tests Coverage	No	No	Yes	Yes

Table 3 – Test Cases

tested. These kind of faults in software that are not detected in an early stage (unit test) will be very difficult to find and when they are found in a later stage they will be difficult to resolve.

Since during the requirements analysis phase a Failure Mode and Effect Analysis (FMEA) has been made in which the more critical functions were indicated as high risk, supplier has chosen for a risk based testing approach. During this FMEA software has not been regarded as a separate component in the system with its own specific failure modes. Software components have not been tagged as high risk. So for software there is no risk based testing approach applied. It can be concluded that the supplier does not follow its own risk based testing strategy for software testing. It is highly probable that critical software components have not been tested well enough and therefor there is a reasonable chance on not-found defects in these software components.

C. Code Assessment Results

Code subjects judged against quality standard ISO 25010 are depicted in a Code Quality Index spider web diagram Figure 2.

Archive structure and Product variants were rated on standard. These subjects are under control by the project. Since there are several software components acquired from third parties and other components that are not planned to be touched in the project there is no control on the quality of those components. Still the supplier was surprised by the analysis of their codebase. The supplier expected far less coding rule violations, too big components, cyclic dependencies, dead code, code smells and code duplications than what resulted from the code assessment. Coding rules and the MISRA standard [17], [21] are applied on new code and code that needed to be changed, which is good. In particular third party software components contained many code rule violations that makes coding rules on third party software components a risk for reliability. Supplier admitted that they introduced cyclic dependencies, but was convinced that this would not cause any extra reliability risk since the software was tested extensively. A high fan-in and fan-out results in high risk for reliability. Several components have a very high complexity number compared to the standards in industry. Complex constructions were found, variables names are sometimes cryptic that obviously will cause delay during maintenance of the software.

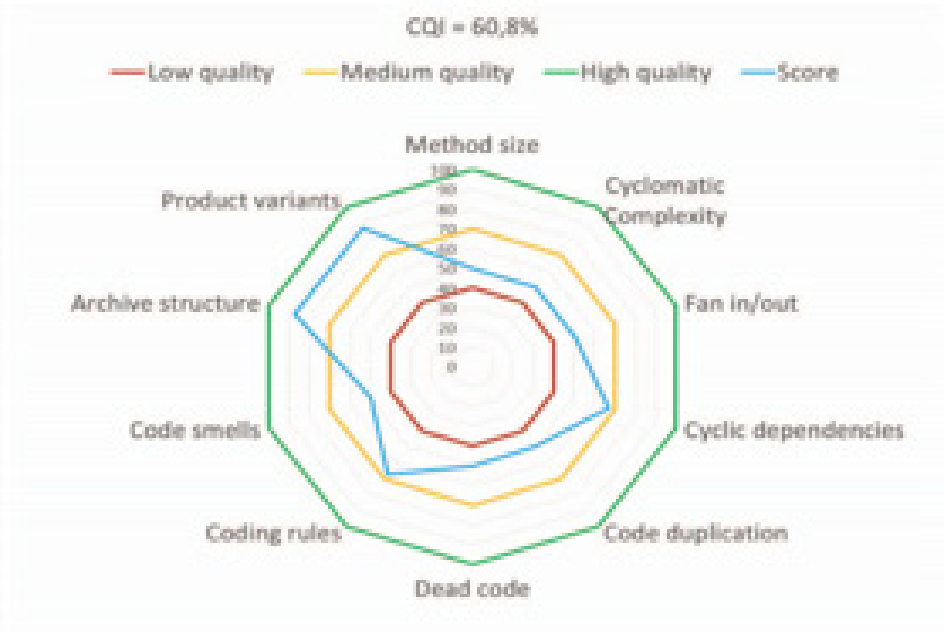


Figure 2 – Code Quality Index

Main reason for the big surprise at the supplier about the quality status of the software code is that they did not measured the code quality parameters themselves. Supplier was also not used to measure on process and test quality parameters.

VI. Conclusion and Future Work

On process quality it was advised to add a quality assurance role to the project team or development organization that would check on efficiency and effectiveness of the defined development processes and applied standards. The project team had a vacancy on this role for several months and now with the assessment report on the table the project team got their QA-resource immediately. It was also not a surprise for the supplier that it was advised to implement a good definition of completion for all development tasks and procedures. The project team started immediately with adding criteria to the workflows in their ALM tooling. Now they can start measuring on the processes and the new QA resource can report his findings based on data.

On the test quality it was advised to approach software as separate system components with their own failure modes. When software is regarded a system component on its own, the critical software components can be tested with a risk based testing approach. The testing approach for software is not dependent anymore on the criticality of the required functionality. It has also been advised to start measuring “code coverage” (the

percentage of the code that has been tested) to avoid having code and functionality that has never been tested. The supplier indicated that the test improvement proposals will be implemented in the next project.

On the code quality it was advised not to touch third party code that has already been verified and validated in the system knowing that with every change on existing software new defects are introduced that might not be found before release. In the future the supplier should set quality requirements on software code they buy from third parties. Since the supplier was surprised on the low quality of the code they were advised to start measuring on code quality. The supplier will buy a license on the software analysis tool "Understand." Based on the results of this tooling the supplier plans to implement in each new project some software reengineering activities that will improve the overall quality of the code over time.

Software reliability is very important for complex systems. In this paper we applied a multiple-faceted assessment technique that is based on existing reference assessment models and techniques to get better insight in software reliability.

To demonstrate our techniques, a case study has been discussed. The results of the case study have been well accepted by our customer and by the supplier of this customer. Moreover, our approach can be applied in the automotive domain as it is and even be improved by exchanging some of the process assessment components by the parts from automotive reference models, such as A-SPICE [6].

In the meantime a team is working on bringing the separate assessment models into an overall model so that it will be easier to select the scope for future software quality assessments and set up a model for documenting, analyzing and reporting about this specific assessment assignment. ●

A Holistic Approach to Automotive Memory Qualification

The Robustness Validation approach in design of automotive memory components addresses reliability and safety margins between design and actual application.

JOHN BLYLER

Improved reliability is just one of the benefits claimed in using the supply-chain sensitive Robustness Validation (RV) approach to qualifying non-volatile memory (NVM) components for automotive electronic application. The following is a summarized and paraphrased coverage of a paper presented by the author, Valentin Kottler, Robert Bosch GmbH, at the IEEE IEDM 2016. —JB

Today's cars have many electronic systems to control motor, transmission, and infotainment systems. Future vehicles will include more telematics to monitor performance as well as car-to-car communication. As the number of electronic applications in the car increases so does the need for non-volatile memories to store program code, application data and more.

Automotive applications place special requirements on electronic components, most noticeably regarding the temperature range in which the components must operate. Automotive temperature ranges can vary –40 to 165 ºC degrees. Further, harsh environmental influences like humidity and long vehicle lifetimes are significantly additional requirements not typically found in most industrial and consumer products. Finally, automotive standards place high requirements on electronic component, system and subsystem quality and reliability. For example, it's not uncommon to demand a 1part per million (ppm) failure rate requirement for infotainment systems and a zero defect rate over the lifetime of the car for safety systems, e.g., braking and steering systems. PPM (parts per million) is a common measurement of performance quality.

These expectations place an additional challenge on components that will wear out during the lifetime of the car, namely, non-volatile memories. Accordingly, such components need to be thoroughly qualified and validated to meet reliability and safety requirements. Adding to this challenge are both the function of the electronic component and its location in the car, all of which creates a wide spectrum of requirements and mission profiles for electronic memory components.

Non-Volatile Memory (NVM) Components

One of the key components in automotive electronics is non-volatile memory, from which program code, application data or configuration bits can be retrieved even after power has been turned off and back on. It is typically used for the task of secondary storage and long-term storage. The size of the NVM in automotive systems can range from a few bytes to many giga-bytes for infotainment video systems.

The various types of NVM add to the range of available components. For example, a form of NVM known as Flash Memory can have NOR and NAND architectures. Further, there can be single and multi-level cell (SLC and MLC) flash

memory technologies. A qualification and validation approach that works for all of these types is needed.

Automotive application requirements can be very different from one application to another. Application requirements will affect the basic performance of memory device characteristics such as speed, write endurance, data retention time, temperature performance and cost effectiveness, noted Valentin Kottler, Robert Bosch GmbH. One particular application may require only a few write cycles of the entire memory. Another application may require the same component to write continuously for over one-half million cycles. Still, another application might require 30 years of data retention, which happens to be the typical 20 year life time of the car plus up to 10 years of shelf time if the supplier has to pre-produce the electronics that support that application.

The simultaneous fulfillment of all these requirements may not be possible in any cost effective way. What is needed is an approach to validation that is application specific. The trade-off is that application specific validation may need to be repeated for each new application that uses a given component. This can mean significant effort in validation and qualification.

Standard approaches using fixed stress tests—like the "3 lots × 77parts/lot approach"—will not be able to cover this wide spread of mission profile and the high variety just described. The Automotive Electronics Council (AEC) AEC-Q100 is a failure mechanism based stress test qualification for packaged integrated circuits.[1] The 3 lots × 77 parts/lot failure tests aims at a 1% failure rate with 90% confidence. [http://plot.nl/wp-content/uploads/sites/43/2014/07/Rene.pdf]

More importantly, this type of approach does not provide information margins (discussed shortly), which are very important for determining the PPM fail rates in the field.

For these reasons, the standard approach needs to be complemented with a flexible qualification methodology like the *robustness validation approach* as described on the ZVEI pages:[2]

"A RV Process demonstrates that a product performs its intended function(s) with sufficient margin under a defined Mission Profile for its specified lifetime. It requires specification of requirements based on a Mission Profile, FMEA to identify the potential risks associated with significant failure mechanisms, and testing to failure, "end-of-life" or acceptable degradation to determine Robustness Margins. The process is based on measuring and maximizing the difference between known application requirements and product capability within timing and economic constraints. It encompasses the activities of verification, legal validation, and producer risk margin validation."

Wikipedia defines robustness validation as follows:

"Robustness Validation is used to assess the reliability of electronic components by comparing the specific requirements of the product with the actual "real life values". With the introduction of this methodology, a specific list of requirements (usually based on the OEM) is required. The requirements for the product can be defined in the environmental requirements (mission profiles) and the functional requirements (use cases)." [https://en.wikipedia.org/wiki/Robustness_validation#Robustness_margin]

The Robustness Validation (RV) technique characterizes the intrinsic capability and limitations of the component and of its technology. It is a failure mechanism and technology based approach using *test-to-fail trials instead of test-to-pass* and employing drift analysis. Further, it does allow for an assessment of the robustness margin of the component in the application.

For clarification, the test-to-pass approach refers to an application where a test is conducted using specific user-flow instructions. Conversely, a test-to-fail approach refers to testing a feature in every conceivable way possible. Test-to-pass is an adequate approach for proof of concept designs but for end-product systems the test-to-fail is necessary to ensure reliability, quality and safety concerns.

The benefit of the robustness validation approach is that the characterization of the device capability would only need to be done once, explained Kottler. Subsequent activities would allow for the deduction of the behavior of the memory under the various mission profiles without repeating the qualification exercise.

Robustness Margin

Robustness Validation (RV) can be used as a holistic approach to NVM qualification. One way to visualize RV is to consider two memory parameters, i.e., endurance and temperature. The intrinsic capability of the NVM may be described as an area between these two parameters. Within that area are the hard requirements for the memory (NVM spec) and the application (application spec). The distance between the application spec, the remaining portion of memory and the NVM capability limit is called the "robustness margin."

In other words, the robustness margin is a measure of the distance of the requirements to the actual test results. It is the margin between the outer limits of the customer specification and the actual performance of the component [https://en.wikipedia.org/wiki/Robustness_validation#Robustness_margin]

The importance of the robustness margin is that it determines the actual safety margin of the component as used in the application verses its failure mode.

The overall capability of the device

including its quality and reliability is that its properties are determined and eventually designed throughout the product development life-cycle phrases:

- Product & technology planning
- Development and design
- Manufacturing and test
  - In order to prove whether the device is suitable for automotive usage, data is gathered from the early design phases in addition to qualification trial data.
  - Then, investigations are held of the performance of the device on a specific application condition.

Robustness Validation Applied to Memory Qualification

How then do you specifically apply the robustness validation approach to a memory qualification? Kottler listed four basic steps in his presentation (see in Figure 1). One should note that Steps 2 and 3 require input from the NVM suppliers. Further, the NVM supplier can run these exercises without input from Step 1 or output to Step 4. We'll now consider each of these steps more closely.

The first step is to identify the mission profile, which is used to describe the loads and stresses acting on the product in actual use. These are typically changes in temperature, temperature profile, vibration and working of electrical and mechanical fields, or other environmental factors. In order to qualify a non-volatile memory for a specific automotive application, an automotive Tier 1 supplier must therefore identify the sum of application requirements to the NVM and must assess whether and to which extent a given NVM component will fulfill them.

To specifically determine the mission profile, all NVM component application requirements must be collected, from electronic control unit (ECU) design, manufacturing and operation in the vehicle. This is usually done within the Tier 1 organization based on requirements from the vehicle manufacturer.

The second step requires identification of all relevant failure mechanisms. Specifically, it means mapping application requirements to the intrinsic properties and failure modes of the NVM component. This requires the competence of the component supplier to share their understanding of the NVM physics and design to identify all relevant failure mechanisms. Intensive cooperation of the NVM technology and product experts with the quality and reliability team on NVM supplier and Tier 1 sides are necessary to accomplish this step.

As an example, consider the typical requirements to an NVM component. These requirements include data retention, re-programmability and unaltered performance as specified over the vehicle lifetime and under various conditions in the harsh environment of a vehicle. According to Kottler's paper, some of the corresponding failure mechanisms in a flash memory include the various charge loss mechanisms through dielectrics, charge de-trapping, read, program and erase disturbs, tunnel oxide degradation due to programming and erasing, as well as radiation-induced errors. These mechanisms are already predefined by choices made at design of the NVM technology, memory cell and array architecture, as well as of the conditions and algorithms for programming, erasing and reading.

The third step focuses on trial planning and execution with the goal of characterizing NVM capabilities and limits with respect to the previously identified failure mechanism. As in the previous step, the competence and participation of the component supplier to provide insight into the physics of the NVM, as well as NVM quality and reliability. Acceleration life cycle testing models, parameters and model limitations need to be identified for each failure mechanism. The health of the NVM component related to the failure mechanism must be observable and allow for drift

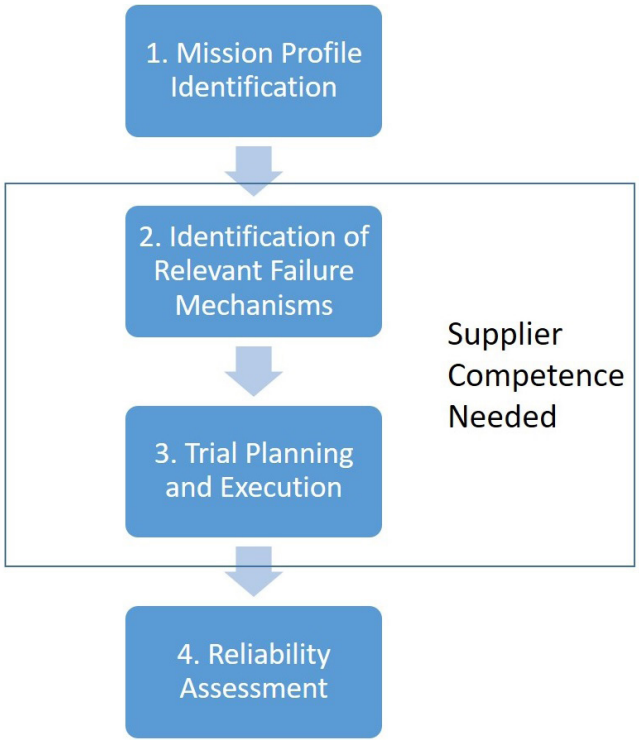


Figure 1 – Steps to apply the Robustness Validation approach to memory devices

analysis, e.g., by measuring the memory cell's threshold voltage variations.

How might the drift analysis be performed and by whom, i.e., the supplier or the Tier 1 customer? For example, will the flash memory provider be asked to give the customer more component data?

According to Kottler, the drift analysis will depend upon the flash memory manufacturer to measure data that is not accessible to the customer/end user. Generally, the latter doesn't have access to test modes to get this data. Only the manufacturer has the product characterization and test technologies related to their components.

The manufacturer and customer should work together to jointly define the parameters that need to be tracked. It is a validation task. The measurements are definitely done by the manufacturer but the manufacturer and customer should jointly interpret the details. What the customer doesn't need is a blank statement that the components have simply passed qualification. This "test to pass" approach is no longer sufficient, according to Kottler.

The trials and experiments for drift analysis need to be planned and jointly agreed upon. Their execution usually falls to the NVM supplier, being the only party with full access to the design, necessary sample structures, test modes, programs and equipment.

According to Kottler, the identification of an appropriate electrical observable is of utmost importance for applying Robustness Validation (RV) to NVM. Such observables may be for memory cell threshold voltage Vth for NOR flash and EEPROM, or corrected bit count for managed NAND flash memories. Both observables provide sensitive early indication on the memory health status and must therefore be accessible for qualification, production testing and failure analysis in automotive.

The fourth and final step in the Robustness Validation approach involves the assessment of the reliability and robustness margin of the NVM component against the mission profile of the automotive application. The basis for this assessment is the technology reliability data and consideration of the initial design features and limitations, such as error correction code (ECC), adaptive read algorithms (e.g., read retry) and firmware housekeeping (e.g., block refresh and wear leveling), noted Kottler in his paper.

Reliability characterization on technology and component level do not necessarily have to be separated. Combined trials may even be recommended, e.g., for managed NAND flash, due to the complex interaction between firmware, controller and NAND flash memory.

Benefits of the Robustness Validation Approach

The Robustness Validation (RV) approach provides a straight-forward way in which a semiconductor company might design and validate an NVM component that is acceptable in the automotive electronics market. Using RV, the supplier will enable its customers to assess the suitability of the component for their applications in the necessary detail.

The resulting NVM qualification and characterization report that results from the NVM approach should list the memory failure mechanisms considered and characterized. Further, the report should describe the acceleration models applied, and showing drift analysis data supporting a quantitative prediction of failure rate vs. stress or lifetime for each failure mode. According to Kottler, combinations of stresses are to be included according to previous agreements, e.g. data retention capability after write/erase endurance prestress, temperature dependent.

To some, the Robustness Validation approach may appear to cause significant additional qualification work. However, most or all of these reliability investigations are part of the typical NVM product and technology characterization during the development phase. For new designs, the optimized top-down RV approach may be applied directly. For existing NVM designs, this approach must be tailored to the agreement of both the NVM supplier and Tier 1 company, potentially re-running trials to complete the RV approach. Even so, some existing NVM components may not meet automotive qualification. It is therefore important to jointly assess the feasibility of the automotive NVM qualification by RV prior to the design-in decision.

The end result of the RV approach is an efficient solution to cope with the high requirements of the automotive market, "requiring a close cooperation along the value creation chain," noted Kottler.

Summary

The automotive expectations to non-volatile memory (NVM) components continues to grow due to market evolution, increasingly complex data structures and the demand for performance and endurance. Tier 1 and NVM suppliers must cope with this challenge jointly. By considering these expectations from the beginning of product and technology development, and by providing comprehensive data, the NVM supplier can enable the automotive Tier 1 to assess the NVM suitability for the application under a Robustness Validation (RV) approach. ●

References

1. AEC-Q100: Stress Test Qualification for Integrated Circuits—Rev. H, Spe. 2014, pp. 36-30
2. ZVEI "Handbook for Robustness Validation of Semiconductor Devices in Automotive Applications," 3rd edition, May 2015, pp. 4-20

About this Issue's Authors

Ms. Katherine Pratt is a leader in the development of environmental logistics as a career field. After 13 years as a logistics professional for major U.S. Corporations, Ms. Pratt founded Enviro-Logistics, Inc. Her firm provides business redevelopment, expansion, economic and environmental conversion services to commercial, environmental, and the defense industry sectors. Ms. Pratt is a Coordinator and provides Technical Support to the RMSP Partnership as the Membership Chair and Coordinator of Professional Activities. She was a senior member of the Society of Logistics Engineers (SOLE), a member of the Base Closure Initiative Committee, and a member of the Standing Committee on Environmental Applications. She was also the SOLE Rhode Island Narragansett Chapter Chairwoman. Ms. Pratt has published a variety of logistics and environmental articles. The published works are libraried in 140 libraries.

Mr. Douglas A. Samuelson is President and Chief Scientist of his own R&D and consulting company, InfoLogix, Inc., in Annandale, Virginia. He has been a Federal policy analyst, consultant, successful high-tech entrepreneur and executive, patented inventor, and an adjunct and research faculty member at several universities. He is a well-known columnist and feature writer for his profession's trade magazines, OR/MS Today and Analytics, and a former chair of its speakers' program. His R&D and consulting focus on risk-advised decision-making, cybersecurity and threat detection, machine learning, wargaming, health care policy, and disaster response and preparedness. He holds a doctorate in Operations Research from The George Washington University and a B.A. in statistics from the University of California, Berkeley.

Mr. Egbert Touw xxx

John Blyler covers today's latest high tech, R&D and even science fiction stories in articles, blogs, whitepapers, books and videos. He is an experienced physicist, engineer, journalist, author and professor who continues to speak at major conferences and before the camera. John has 23 years of experience as a systems engineer-manager in the commercial, DOD and DOE hardware-software electronics industries. Another 16 years of experience has gained in the technical trade and professional engineering journal markets. He was the founding advisor and affiliate professor for Portland State University's online graduate program in systems engineering. Also, John has co-authored several books on systems engineering, RF design and automotive hardware-software integration for Wiley, Elsevier, IEEE and SAE.

THE JOURNAL OF RELIABILITY, MAINTAINABILITY, & SUPPORTABILITY IN SYSTEMS ENGINEERING

Editor-in-Chief: John E. Blyler
Managing Editor: Russell A. Vacante, Ph.D.
Production Editor: Phillip S. Hess

Office of Publication: Post Office Box 244, Frederick, MD 21705
ISSN 1931-681x

Instructions for Potential Authors

The Journal of Reliability, Maintainability and Supportability in Systems Engineering is an electronic publication provided under the auspices of the RMS Partnership, Inc. on a semi-annual basis. It is a refereed journal dedicated to providing an early-on, holistic perspective regarding the role that reliability, maintainability, and supportability (logistics) provide during the total life cycle of equipment and systems. All articles are reviewed by representative experts from industry, academia, and government whose primary interest is applied engineering and technology. The editorial board of the RMS Partnership has exclusive authority to publish or not publish an article submitted by one or more authors. Payment for articles by the RMS Partnership, the editors, or the staff is prohibited. Advertising in the journals is not accepted; however, advertising on the RMS Partnership web site, when appropriate, is acceptable.

All articles and accompanying material submitted to the RMS Partnership for consideration become the property of the RMS Partnership and will not be returned. The RMS Partnership reserves the rights to edit articles for clarity, style, and length. The edited copy is cleared with the author before publication. The technical merit and accuracy of the articles contained in this journal are not attributable to the RMS Partnership and should be evaluated independently by each reader.

Permission to reproduce by photocopy or other means is at the discretion of the RMS Partnership. Requests to copy a particular article are to be addressed to the Managing Editor, Russell Vacante at president@rmspartnership.org.

Publication Guidlines

Articles should be submitted as Microsoft Word files. Articles should be 2,000 to 3,000 words in length. Please use ONE space after periods for ease of formating for the final publication. Article photos and graphics should be submitted as individual files (not embedded into the article or all into the same file) with references provided in the article to their location. Charts and graphics should be submitted as PowerPoint files or in JPEG, TIFF, or GIF format. Photos should be submitted in JPEG, TIFF, or GIF format. All captions should be clearly labeled and all material, photos included, used from other than the original source should be provided with a release statement. All JPEG, TIFF, or GIF files must be sized to print at approximately 3 inches x 5 inches with a minimum resolution of 300 pixels per inch. Please also submit a 100-125 word author biography and a portrait if available. Contact the editor-in-chief, John Blyler, at j.blyler@ieee.org for additional guidance.

Please submit proposed articles by October 1 for the Spring/Summer issue of the following year and April 1 for the Fall/Winter issue of the same year.