the newsletter of
RELIABILITY, MAINTAINABILITY, & SUPPORTABILITY

March 2016 • Volume 20 • Issue 1

THIS EDITION

Published Quarterly

John Blyler

Resiliency Needed for Smart Recovery Systems: *Is resiliency emerging as a richer version of reliability and a higher systems priority over optimization?*

Resiliency has been proposed as yet another needed capability for today's ever-increasingly complex, "smart" systems. Understandably, system architects and design engineers may be reluctant to add yet another "ilities-like" requirement to an already long list that includes reliability, maintainability, safety, and more.

What is resiliency, especially when applied to the engineering of complex hardware-software embedded systems? What is the difference between resiliency and reliability with feedback and control? Or the difference between resiliency and maintainability in terms of some measure of repairability that would restore partial or full functionality over a specified period of time and in a specified environment? What are some of the quantitative measures of a resilient system? This paper will attempt to answer these questions.

Definitions

First, to help avoid semantic entanglements, let's define a few terms. In general, a resilient system is one that can recover from a failure. INCOSE defines resilience as the capability of a system with specific characteristics before, during and after a disruption to absorb the disruption, recover to an acceptable level of performance, and sustain that level for an acceptable period of time. Further, it lists the main attributes of resilience as capacity, flexibility, tolerance and cohesion.[1]

The IEEE adds a security element to resilience by defining it as a combination of trustworthiness and tolerance.[2] Wikipedia describes resilient control systems as those that maintain a state of awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature.[3]

It's noteworthy that resilience is not defined in the usual reliability terms of subsystem or component MTBF and MTTR numbers. As Jim Rodenkirch notes[4], resiliency is the extended part of the reliability problem that deals with what can "go wrong" across the breadth of the system-of-system (SOS) domain and the time required to "undo the wrong" to return the system to an acceptable—albeit different—level of operation.

Resiliency has been described as a richer metric than reliability, as resilient systems have the capacity to survive, adapt and grow in the face of change and uncertainty.[5] In today's world of complex embedded systems, resiliency might be equated with "smart recovery" systems,

1 Resilient Systems Working Group, *https://www.rmspartnership.org/*

2 Resilience in computer systems and networks *http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5361311&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5357317%2F5361202%2F05361311.pdf%3Farnumber%3D5361311*

3 Wikipedia, *https://en.wikipedia.org/wiki/Resilient_control_systems*

4 "Understanding Resilience's Role in Designing Reliable Complex Systems," by Jim Rodenkirch

5 "Evaluating System of Systems Resilience using Interdependency Analysis," Seung Yeob Han, Karen Marais, and Daniel De Laurentis, School of Aeronautics and Astronautics, Purdue University

Eitan Yakoobinsky, Guest Editorial

Level of Repair Analysis (LORA) Challenge

At the earliest stages of system development, the challenge for ILS engineering is to influence the design so that an optimum system Life Cycle Cost (LCC) is realized. My lesson learned from many years of Integrated Logistic Engineering in the Electronics Defense industry is to start using the COMPASS STAT tool to address LORA before the system configuration is fielded and perform needed trade studies before "system configuration freeze."

One of the ILS team's main goals must be—present the best LORA report before a new system is fielded. However, there are a few challenges/unknowns to be aware of when developing a new system LORA:

1) Unknown field reliability for spare parts and consumables.
2) Unknown future cost for spares and consumables.
3) Support Equipment (SE) for LRU & SRU may not be designed yet.

A world class design objective—develop a reliable system(s) with a "minimum footprint,"—is achievable by ensuring:

continued on page 7

those that contained the capacity to evaluate and act on situational inputs via microprocessor hardware, software and connectivity to other systems like the Internet.

Unlike reliability, maintainability and systems safety, resilience is less of a specific topic and more of an over-arching set of considerations and design principals that help a system recover from a disruption. For our purposes, we are considering designed-in resilience, as opposed to intrinsic resilience, where the latter is the focus of material science, psychology and ecology.

A good analogy that ties resiliency, reliability and maintainability together is provided by Ivan Mactaggart, Principal Systems Engineer at Dstl, and President-Elect INCOSE UK - INCOSE: "My car is reliable in that it starts every time and has never broken down. The vehicle is reliable in part due to scheduled maintenance by a trained mechanic, which helps it performs the primary transportation function. However, it is not resilient to a head-on impact with another vehicle, in which case it may no longer perform its primary function. It is not resilient to that shock. I might be able to return the car to a normal (acceptable) level of performance with repair. Or the damage may be too severe to repair."

Resiliency might have been added to the design of the car by selecting a hybrid architecture—gas and electric. Though the severity of the accident might damage both systems, as well. If one considers the system to extend beyond the car, the resiliency can be added with public transportation—until the car is repaired or replaced. Public transportation is a more limited option in that it can travel compared to a car, but it might be acceptable. At least, it returns some level of transportation function to the overall system.

Kenneth Lloyd, CEO of Systems Science at Watt Systems Technologies, explains that resiliency relates to the continued functional integrity (at some level) despite component failures (and other perturbations) through a range of operating conditions. Reliability relates component failures to MTTR and MTBF independent of functional integrity.

What does this tell us about resilience in the context of the systems engineering "ilities" disciplines such as reliability, maintainability, and safety, etc? Our previous automotive shows that resiliency has strong connections to reliability and safety. This is one reason why many argue that resiliency is not a separate and distinct discipline from the other "ilities." Rather, resiliency depends upon the other "ilities," in the same way that safety depends upon reliability, etc.

GOOD NEWS FROM FLORIDA INSTITUTE OF TECHNOLOGY AND THE RMS PARTNERSHIP

The RMSP has established a new partnership with the Florida Institute of Technology (FIT) that promises real benefits to its members!

In cooperation with FIT, the RMSP will now offer Continuing Education Units (CEU) of credit for training in reliability, maintainability, and sustainability. These courses will be provided both online and onsite.

Professional logisticians will be able use the courses to meet annual training requirements, as well as, for professional development. A short description of training courses are available at *www.rmspartnership.org*.

Requests for training can be discussed with Dr. Russell A. Vacante at: president@rmspartnership.org

Measuring Resilience

How does one design for resiliency? This question assumes that resiliency is a measurable quantity. There is some debate on this point. The over-arching nature of resiliency may be one reason why measurements are difficult, e.g., multiple threats, multiple failure modes and multiple recover modes. These issues make it hard to predict the resilience of a system.

According to the Systems Engineering Body of Knowledge (SEBok)[6], a resilient system must possess the four attributes of capacity, flexibility, tolerance and cohesion. Let's concentrate on the first one as a metric for resilient systems. According to Rodenkirch, the capacity attribute allows the system to withstand a threat. "Resilience allows for the capacity of a system to be exceeded, forcing the system to rely on the remaining attributes to achieve recovery."

If engineers can quantify the capacity of a system to withstand failures, then that quantity can serve as a measure of resilience. In the case of SOS, resilience can be defined as the level of performance achieved relative to different levels of failure. Capacity is required to withstand these various levels of failure.

In a related study, researchers at Purdue University[7] considered the challenge in measuring resilience. To perform this measurement, they first defined two types of SOS resilience: conditional and total. Conditional resilience is the ratio of the percentage of SOS performance in response to a failure in a particular system or combination of systems. This can

6 Systems Engineering Body of Knowledge (SEBok): *http://sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK)*

7 06377904.pdf (IEEE) "Evaluating System of Systems Resilience using Interdependency Analysis"

A Unique Systems Engineering Program (SEP)

FIRST
M.S.S.E. Degree Program in Texas - 1994
Weekend Format M.S.S.E. Degree Program - 2002

Founding Director
Professor of Practice
jerrell@lyle.smu.edu

FIRST
Ph.D. S.E. Degree Program in Texas
Applied Science (S.E.) - 2004
Systems Engineering - 2009

Jerrell Stracener

DEGREES AND CURRICULUM

- M.S. and Ph.D. Systems Engineering Degree Programs
- 21 graduate courses developed and maintained in response to industry and government needs
  - 5 core courses
  - 16 elective courses
  - 3 courses in development
- Developed by SEP Development Team Subject Matter Experts in industry/government

FOCUS

- Customer focus
  - U.S. Aerospace and Defense Systems Developers
    - Contractors
    - Government
- SEP course focus
  - Aerospace and Defense Systems Design & Development
  - Current U.S. DoD OSD and military services, policies, directives, guides, standards, procedures and methods
  - Commercial Best Practices

Unique by Design™

An Unconventional University Model
Conceived, Developed, and Delivered in *Working* Partnership
with Aerospace and Defense Contractors and U.S. DoD

FACULTY AND STUDENTS

- Most SEP faculty are (or have been) employed by aerospace and defense organizations
- Majority of SEP students are employed full-time by the aerospace/defense sector—industry/government

PARTNERSHIPS

- On-going development and research projects staffed by Subject Matter Experts affiliated with
  - Defense Contractors
  - Aerospace Companies
  - U.S. DoD OSD
  - U.S. Air Force, Army, Navy
  - Sandia National Labs
  - NASA

FIRST
SEP (and only SEP) with Long-Term Aerospace and Defense Systems Development Contractor Focus

Established
1994

FIRST
North Texas SERC Member - 2008

SMU | LYLE School of Engineering

be thought of as a particular performance measure that indicates how much performance is maintained for failure in a given set of systems.

Total resilience shows how performance is degraded as the total level of component system failures increases. According to the researchers, resilience patterns for the system are influenced by two factors: architecture type and system-level risk of the SOS. The architecture determines the general shape of the resilience pattern. The goal is to architect a system design that recovers to the highest level of performance possible after the failure.

In contrast to the resilience pattern, the system-level risk determines the scale or magnitude of the pattern, that is, how the system performance degrades as systems fail.

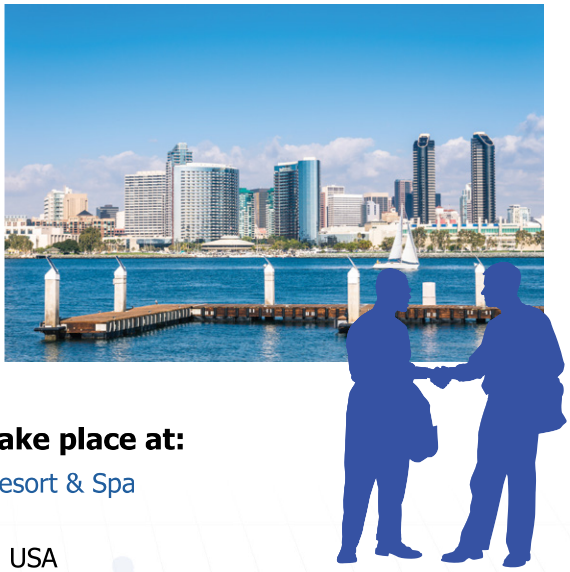
In the Purdue paper, researchers determine the two most critical systems of a multi-component threat detection SOS using the conditional resilience metric. They demonstrated that adding a communications link between these two systems increased the resilience, resulting in higher expected performance and slower expected performance degradation as a result of system failure. The goal now is to develop resilience patterns for more complex interactions.

The Purdue study show that some attributes of a resilient system can be measured. Treating resilience as an evolving, richer function of reliability might help facilitate further interest and study of this upcoming system design consideration. Finally, there is a need to place a greater emphasis on recoverability instead of just optimal states in the engineering of systems, which is another reason to consider augmenting reliability with resilient design. ●

International Applied Reliability Symposium

Join the conversation!

June 21 - 23, 2016 in San Diego, California



Reliability engineering has never been more important than in today's economic environment. Whether you are just beginning your reliability journey or you are a weathered veteran, the International Applied Reliability Symposium (ARS) has something for you. This reliability and maintainability conference provides a forum for expert presenters from industry and government to come together with reliability practitioners from all over the world to discuss the application of reliability principles to meet real-world challenges.

To register or for more information:

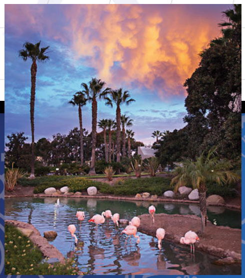
Website: http://www.ARSymposium.org
E-mail: Info@ARSymposium.org
Phone: 1.888.886.0410 or +1.520.886.0410

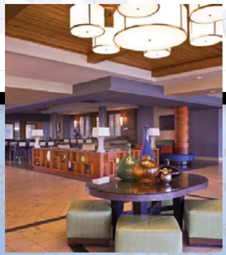
The Symposium will take place at:

Coronado Island Marriott Resort & Spa
2000 Second Street
Coronado, California 92118 USA

- **Gain insights from results-oriented presentations and tutorials**
- **Network with industry professionals**
- **Explore solutions from sponsors and exhibitors**

Please contact us for information on sponsorship and exhibitor opportunities.




Organized by ReliaSoft® SRC SYSTEM RELIABILITY CENTER

Global Issues, Local Perspectives!℠

Europe South America North America India Asia Pacific Middle East

Dr. Lloyd H. Muller, CPL

Forged Quality: A Loggie's Concern

The concept of Just in Time (JIT) manufacturing has been around for a long time. Developed in large part by Mr. Taiichi Ohno of Toyota, it solved a lot of expensive inventory problems. Among them, from the perspective of post-war Japan were:

1) a lack of available cash by which inventories could be purchased.
2) a lack of space for the storage of large inventories.
3) a lack of natural resources for use in manufacturing thereby requiring expensive raw materials to be imported.[1]

Toyota's success with JIT has been vaunted around the world. In fact, Lee Iacocca, president of Chrysler motors, credits this management technique for saving his company when it was bankrupt. As he wrote in his autobiography:

To save money, we set up a system where parts would be shipped at the last possible moment. This is known as "Just in Time" inventory, and it's a good way to cut costs. The Japanese have been doing it for years...[2]

Unfortunately, JIT has a weakness that is being exploited by Chinese vendors. Specifically, Chinese upline vendors are harvesting used parts from old systems and selling them as new to their customers. Consequently, component parts that must be installed immediately on assembly lines allow no time for quality control. What is received is what is placed into all sorts of electronic assemblies such as computers, flight controls, etc. As a consequence, inherent reliability, maintainability and supportability standards falter. If the quality is not there, then the standards that drive operational availability will not be there. Below is an image of what harvesting means.

http://search.aol.com/aol/imageDetails.

This practice is attracting governmental reviews. The FBI did a probe in 2008, and 3,500 bogus parts were found that were valued at $3.5 million. Fortunately, no dangerous consequences were found, but such was not the case with other investigations.[3] The Canadian Broadcasting Company investigated this problem in the Royal Canadian Air Force, and the results were disturbing. The Chinese fakes were installed in navigation equipment which led to pilots seeing blank screens instead of the vital information they needed to fly their airplanves safely.[4]

Ultimately, this problem has created Congressional interest. Senate Armed Services Committee Chairman Carl Levin (D-Mich) in 2011 reported Navy P-8 Poseidon ice detectors defective due to counterfeit parts. The Chinese government refused to participate in the investigation or react to the Senator's findings.[5]

Finally, US SENATE, May 21, 2012 reported: "INQUIRY INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN"[6] This inquiry was based on Defense Department (DOD) findings in which a US firm, American Vision Tech, implicated. "The result could be systemic loss of a key capability in… critical military equipment." As a consequence of these findings, the Defense Federal Acquisition Regulations (DFARS) now requires contractors to detect and avoid counterfeit parts.[7]

Thus, it is a sad consequence for an effective management system that was designed to reduce waste, improve quality, and lower costs. Instead of these benefits, many companies and government agencies are being required to revert back to inefficient post receipt inspections to avert disastrous accidents. ●

1 "Just in Time Manufacturing." *Wikipedia. https://en.wikipedia.org/wiki/Just-in-time_manufacturing#Evolution_in_Japan.* 18 Feb 2016.

2 Iacocca, Lee. *Iacocca: an Autobiography*. New York, NY: Bantam Books. 2007. Kindle Location: 3378-89.

3 Morgan, David. "FBI Probes Counterfeit China Computer Parts." Washington, DC: Washington Post. http://www.reuters.com/article/us-usa-china-counterfeit-idUSN0952813820080510. 4 Feb 16.

4 Weston, Greg. "Fake parts in Hercules aircraft called a genuine risk." CBC News. http://www.cbc.ca/news/politics/fake-parts-in-hercules-aircraft-called-a-genuine-risk-1.1345862. 4 Feb 16.

5 Reed, John. "Counterfeit Parts Found on P-8 Posiedons." *Defensetech. http://defensetech.org/2011/11/08/counterfeit-parts-found-on-new-p-8-posiedons/*. 4 Feb 16.

6 *http://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf . 6 Oct 15. http://www.ibtimes.com/why-pentagon-finding-counterfeit-chinese-electronics-critical-military-equipment-701214. 6 Oct 15*

7 http://www.nixonpeabody.com/files/169899_Government_Contracts_25JUNE2014.pdf. 6 Oct 15

THE SYNTHESIS PLATFORM®

Upgrade to Version 10 today!

WEIBULL++® ALTA® DOE++® RGA® BLOCKSIM® RENO®

λPREDICT® XFMEA® RCM++® RBI® MPC® XFRACAS®

ENTERPRISE PORTAL

Best-in-class software,
integrated reliability solutions

The **Synthesis Platform** provides **intelligent integration** between reliability program activities and tools, while simultaneously **facilitating effective cooperation** across engineering teams of any size.

Version 10 offers new features in individual Synthesis applications and significant platform enhancements, such as:

- **Option to implement a Synthesis Enterprise Portal (SEP) website**
- **Integrated Project Planner for reliability milestones and tasks**
- **Easier to Find and Filter analyses, with more graphical Dashboard overviews**
- **Display and track Key Performance Indicators (KPIs)**
- **Automated Watches and Alerts for actions and metrics**

http://Synthesis.ReliaSoft.com/version10.htm

ReliaSoft®

Editorial, from page 1

1) All fielded spares are consumables (e.g., very high reliability, unrepairable and low cost)
2) There are no requirements for fielding SE or special tools.
3) Minimum Operation & Support (O&S) documentation required.
4) Minimal Operation & Support (O&S) training.
5) Two level(s) of maintenance, O/L and Depot.

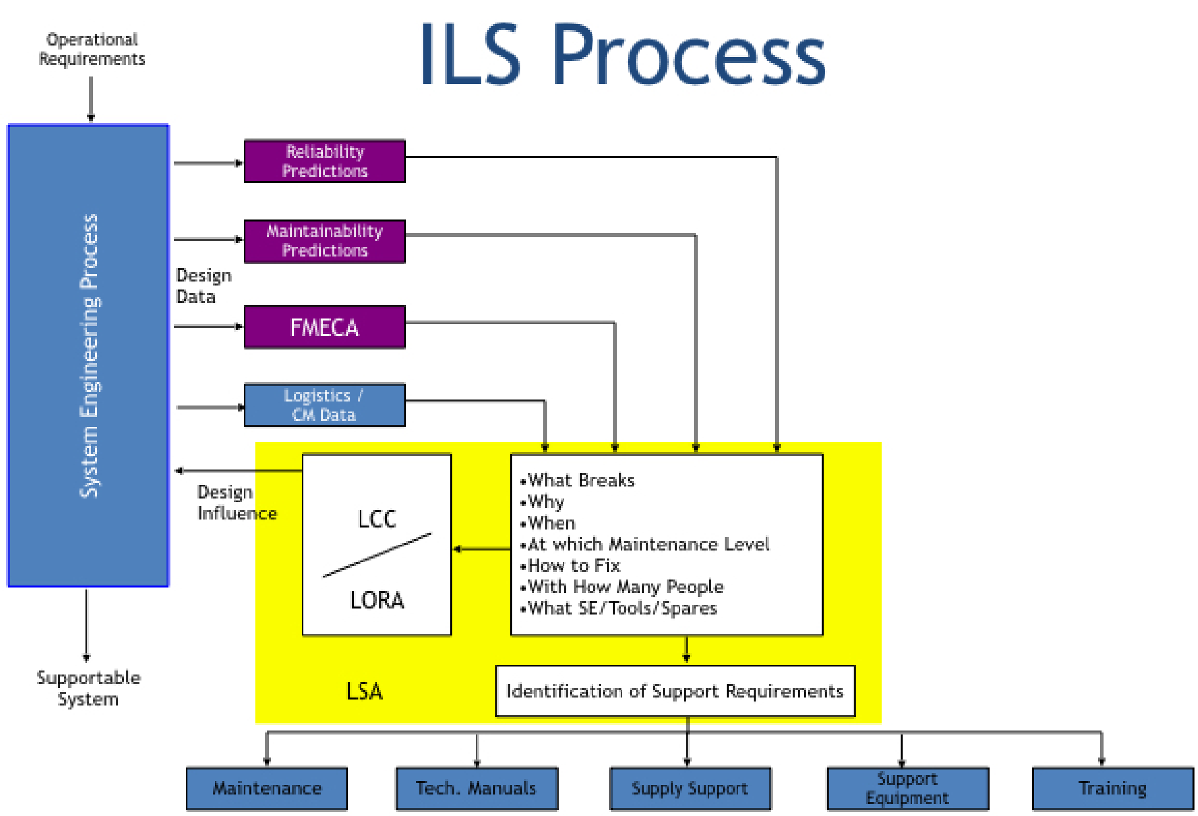
Several "cautionary notes":

- Unfortunately these objectives are hard to achieve and, potentially, verifiable only after deployment.
- To verify the new design meets system requirements, suppliers use high cost sophisticated test equipment that should not be used in the field.
- The developer/manufacturer (supplier) shoots for high production yields and saves time by verifying each part not separately but at system level proof of design.

With all of the above to work through, the preferable way to address LORA is through the use of the COMPSS STAT tool. During the design stage the system configuration, LRU, SRU, parts and consumables data are input to the COMPASS tool, along with engineering estimates (reliability, parts cost, SE cost, documentation cost as well as maintenance and training cost). With this approach the entire development and deployment team will begin understanding and measuring the initial system Life Cycle Cost (LCC), as well as the probability of influencing the system configuration and drive down the system's overall LCC.

As the development proceeds deployment of the final system begins, periodic updates to COMPASS STAT data—e.g., updated data and refined maintenance tasks at each repair level, including distribution of spares and consumables—will go a long way towards enduring a robust LORA and optimized system LCC.

See below the system design process for the role Integrated Logistics Support (ILS) Engineering plays and the correct "insertion point(s) for a completed LORA.



To be an effective ILS engineer / manager you must understand the ILS need(s) by:

- becoming integrated early on into the design team.
- ensuring "best trade study tools" such as COMPASS STAT are: populated with accurate data, utilized correctly and utilized early on in the design/development phases. ●

About the Authors

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.*

Eitan Yakoobinsky *is an accomplished Product Support Leader with 10+ years of experience as Integrated Logistics Support (ILS) engineering and management, Program Management, Engineering Lead and Production Management in the defense Electronics Industry.*

He has achieved customer success through close collaboration with Quality, Supply Chain, and Development Engineering. He has implemented and Managed Reliability Improvement Program that improved airborne system MTBD from 50 hours to 1500 hours. He drove 30% reduction of Life Cycle Cost (LCC) of JHMCS system by analysis and trade study. He maintained preferred supplier status by actively collecting users feedback.

Lloyd H. Muller *is also widely versed in the academic elements of logistics. Bringing his wealth of practical experience to education, he has taught at universities located both in the United States and in foreign countries. Among them are the University of Maryland, Emery Riddle Aeronautical University, La Verne University and Middle East Technical University in Ankara Turkey. He has also been a logistics instructor for the United States Navy. Currently, he is an associate professor of logistics for Florida Institute of Technology. He is also the Vice President for Curriculum Development with the RMS Partnership Inc.*

Besides these duties, Dr. Muller is a Past President of SOLE, The International Society of Logistics. Beyond these teaching experiences, he has written numerous articles and books on many aspects of the discipline.

INTERESTED IN CONTRIBUTING?

If you are interested in sharing your knowledge in future editions, please contact Russ Vacante at:

president@rmspartnership.org

Articles can range from one page to five pages and should be of general interest to our members.

RMS/LOGISTICS & SYSTEMS ENGINEERING ON-SITE SHORT-COURSE OFFERINGS

Provide Us Your Training Requirements and the RMS Partnership will provide tailored training that will exceed your expectations. For Additional Information contact Russ Vacante at *president@rmspartnership.org*

AUTHOR OPPORTUNITIES

Author opportunities for the RMS Professional Journal "The Journal of Reliability, Maintainability and Supportability in Systems Engineering":

Contact the Journal Editor, Jim Rodenkirch at:

rodenkirch_llc@msn.com.