The Journal of

RELIABILITY, MAINTAINABILITY, AND SUPPORTABILITY IN SYSTEMS ENGINEERING

—

Winter 2015

RMS Reliability, Maintainability and Supportability Partnership

Table of Contents

WINTER 2015

Introduction

JAMES RODENKIRCH

I asked Dr. Russ Vacante to send his input for the "Introductory editorial" section and he responded with a thought provoking article centered on our country's focus on rewards and privileges and how the drive or emphasis on educational and national security paths is losing its "luster," courtesy of a greater foci on wealth and social recognition. Well done, Russ! I encourage all of you to consider submitting an introductory editorial piece on any wide range of topics. The subject doesn't have to be "RMS-centric"—our four articles provide a sufficiency of that. Please—submit your thoughts...jump in, the water is fine.

Our four articles run the gamut of RMS-related topics. First off, we have a new foreign author, Michail Bozoudis, a Senior Engineer in the Hellenic Air Force, stationed in Athens, Greece. Mike approached me two months ago about submitting his article on *A Stochastic Model for Availability Projections*. I couldn't have been more pleased with the way it turned out and hope Mike can solicit more articles from other EU RMS practitioners...a much needed way to expand the scope and treatment of RMS by publishing foreign author efforts.

Second, Chris Feudo walks us through the problems associated with viewing and treating the protection of physical assets and electronic assets as different domains independent of one another. His article, *Security Fusion Resolved: Dynamically Converging Cyber and Physical Infrastructures into a Single, Integrated, and Interoperable, Common Operating Picture*, focuses our attention on the absolute need to converge the cyber and physical boundaries for Critical Information Protection security resolution and extend an organization's awareness of potential security operational and management exposures. This is Chris' first article submittal for our Journal, I believe, and I hope he prepares more submissions.

Third up is the submittal by Frank Straka, *Mechanical Accelerated Life Tests*. Frank presents a study of stress on a bracket used in an exercise cross trainer and discusses how to extrapolate accelerated life test results to normal operating conditions, using statistical analysis. Well done, Frank, and hope you consider more articles that reinforce our "statistical analysis roots."

Our fourth article, by Louis Gullo, *Design Failure Modes, Effects, and Criticality Analysis (D-FMECA) Process Explained*, describes the FMEA, FMECA and the Design-FMECA (D-FMECA) process. Louis introduces a new term, Additive Risk Priority Number (APRN) and discusses it in terms of the value to an analyst as compared to other methods for prioritizing failure modes for corrective actions when performing D-FMECAs.

There you have it - four terrific articles spanning the realm of RMS thinking and an Enterprise-wide editorial by our RMS President. Good reading to all. You are encouraged to provide feedback and comments to all of our authors and feel free to contact me for e-mail addresses.

The holiday season is here—enjoy it with associates and family—time is not on our side...so make each day count by staying in touch with loved ones and friends. ●

Rewards and Prestige Relevance to National Survival, Safety, and Security

RUSSELL A. VACANTE, PH.D.

This editorial provides a brief discussion of priorities as they relate to human survival, individual career paths and national welfare in the United States. Prima facially there doesn't seem to be a conscious and consistent conceptual package of cultural and national ethos pertaining to educational, career, wealth and national security paths. There appears to be a tension between what we need to do to ensure individual and national survival and jobs and professions, as we aspire and engage in a socio-economic system based on societal recognition and financial rewards. To say that modern day society is a mixed fabric containing many different threads of interests and opportunities is probably an understatement. The most that this editorial may accomplish is to expose the nature of these complex threads and question the degree to which they contribute to maintaining the fabric of U.S. society.

Sociologist Maslow established a hierarchy of "needs" (1) Physiological (survival), 2) Safety and Security, 3) Social needs (family and friends), 4) Esteem (self-esteem, confidence, achievement and 5) Self-Actualization (creativity, problem solving, authenticity, spontaneity)) that range from the very basic requirements pertaining to survival, security and safety to the more esoteric or abstract requirement of self-actualization1. When conceptualized in a pyramid as depicted below it becomes obvious that the fulfillment of human needs has to progress from the base up, each building upon the other.

Maslow's hierarchy of needs model also applies to national priorities within the structure of the nation-state. That is, the two basic needs identified in the pyramid must be well-established in order to ensure the survival of the nation-state. Following this train of thought, it is not far-reaching to envision that societal rewards and prestige would be bestowed upon those whose careers are directly responsible for and engaged in supporting the physiological and safety and security needs of the nation-state. However, this notion seems to be turned upside down in the U.S., and also most likely in other countries. Self-actualtization and self-esteem in the U.S. apparently reap rewards and privileges over other needs within Maslow's hierarchy.

In the U.S., rewards and privileges come in the form of wages and material possessions, such as, houses, cars, planes and yachts. Some of the highest salaries are associated with athletic achievements. In 2015, the top four ranking salaries in the NFL were in the $23 million dollar range.2 A similar salary structure exists for the top 2015-2016 NBA players. Dozens of other sport figures also earn handsome salaries well into the millions of dollars. Within the context of Maslow's needs hierarchy, the rewards and prestige of achievements of professional athletics has little, if anything, to do with the preservation and survival of the nation-state.

The disparity between rewards, prestige and risk and U.S. priorities, is amply displayed in other professional and

1 Maslow's hierarch of needs, Wikipedia, https://www.google.com/search?q=maslow+hierarchy+of+needs&espv=2&biw=1522&bih=900&tbm=isch&tbo=u&source=univ&sa=X&ved=0CDAQ7AlqFQoTCMP-tquA98gCFQpxPgodD, visited 11/10/2015.

2 NFL Salary Rankings, 2015 Cap Hit Rankings, http://www.spotrac.com/nfl/rankings/, visited 11/10/2015.

non-professional career fields. Active soldiers are often in harms way on a daily basis. Yet the basic pay of an enlisted E-9 with over 16 years of service is a mere $5,299.00 per month. An Army major with over 16 years of service is $7,354.00 per month.3 Senior level Army executives, with more than 20 years of service receive a basic monthly pay of $16,072.00.4

You may be surprised to learn what the pay scale is for our nationally celebrated high risk-taking astronauts. Civilian astronaut salaries are keyed to the civil service, or government, pay scale. In 2012, the minimum starting pay for an astronaut was $64,724 to a maximum of $141,715.00.5 According to the government pay scale chart, this is the same salary received by government G-11 through G-14 employees sitting safely behind their desks. We have to ask ourselves, knowing the years of rigorous academic and technical screening and competition that astronauts undergo, whether the rewards and prestige of competitive athletes should overshadow astronauts.

Similar questions can be raised in the context of other high paid professions in the U.S. The highest median income in 2012, reported by the U.S. Department of Labor, is attributed to seven surgical medical professionals. Their medium annual pay is equal to or greater than $187,200.00 per year.6 Citing 2013 salary statistics, it is reported that "the best lawyers" earn more than $187,199 annually with the lowest earning less than $55,170.00, with an average annual salary of $131,900.00.7 The Glassdoor Blog, ranks lawyers as seven out of twenty-five of the highest paying jobs in "demand."8 By comparing societal rewards and prestige bestowed upon physicians and lawyers, according to Maslow's hierarchy, their contribution to the physiological, safety and security needs of the nation greatly exceed that of our war fighters despite the little degree of risk to their well being. However, doctors' and lawyers' rewards and prestige, in contemporary American society, pales in comparison to that of professional athletes—the latter group being the furthest removed from national survival, security and safety concerns.

It is perplexing from a national security and safety perceptive that engineers, scientists, and professional positions in defense and related industries, seldom, if ever rank among the highest paying or most in demand jobs. I am also astonished by one report that ranks post secondary teachers', i.e., college professors, wages 293 out of 300 in the U.S. Professional educators that have enormous influence and responsibility for developing career paths for our children rank especially low in terms of rewards and prestige in our society.

Lastly, in keeping with the theme of higher formal education, it is obvious, but may not be intuitive for most, that the brightest and most knowledgeable individuals graduating from our colleges and universities often don't reap the highest paying or most prestigious positions in American society. Far above and beyond the salaries of professional athletes are the incomes of franchised team owners, CEO's of multinational corporations, entrepreneurs, bankers and stock brokers whose contribution to the survival, security, and safety of the nation-state cannot be closely examined due to intentional lack of transparency. While war fighters, police officers, firemen and women, and many other professionals engage in life risking careers, we can't say the same for those who receive the greatest rewards and prestige in the U.S.

The above discussion is not meant to reach a conclusion of the rights and wrongs of America's socio-economic priorities. It is, in part, to shed some light on how greater U.S. societal values get reflected in our system of formal education, which in turn, can have long-term consequences for the United State's survival, safety and security. This editorial is not an argument against the rewards and prestige received by professional athletes and other entertainers as opposed to urging for greater societal awards and prestige to be shared with those who provide for our survival, safety and security.

This editorial is a call for an overhaul of our system of higher education. Students should be provided with a preparatory course enlightening them to potential career paths, as well as, associated rewards and benefits. Once students gain a more comprehensive understanding of the thousands of career opportunities available to them, the pressure will build in colleges and universities to offer a broader curriculum. Courses that can provide advice, guidance and tools on how to become a CEO, a military general, an anesthesiologist, a senator, or even a president would be widely accepted by college bound students.

On the other hand, if this editorial gets readers thinking that the system of rewards and prestige within the U.S. has little direct bearing on enhancing the survival, safety and security of the U.S., especially given the global challenges facing us today, then the time may have come to petition decision makers for relevant and timely change. ●

3 U.S. Army, My Army Benefits, http://myarmybenefits.us.army.mil/Home/Benefit_Library/Federal_Benefits_Page/Basic_Pay.html?serv=147, visited 11/10/2015.

4 Id.

5 Universe Today, Astronaut Today, http://www.universetoday.com/41252/astronaut-salary/, 4/16/2014.

6 U.S. Department of Labor, Top 50 Highest-Paying Occupations by Median Hourly Wages, http://www.careerinfonet.org/oview5.asp?Level=Overall, visited 11/10/2015.

7 U.S. News & World Report, Lawyer Salary Outlook, http://money.usnews.com/careers/best-jobs/lawyer/salary, visited 11/10/2015.

8 Glassdoor Blog, http://www.glassdoor.com/blog/highest-paying-jobs-demand/, visited 11/10/2015.

A Stochastic Model for Availability Projections

MICHAIL BOZOUDIS

Introduction

In 2014 the Hellenic Air Force (HAF) F-16 Weapon System Support Program Office (WSSPO) initiated a study aiming to optimize the F-16 Materiel Availability. Alongside the operational requirements, the provided resources and logistic procedures had to be considered. The rationale behind this effort was to enhance the F-16 fleet sustainability, after 25 years of operation:

> *"Determining the optimum value for Materiel Availability requires a comprehensive analysis of the system and its planned use, including the planned operating environment, operating tempo, reliability alternatives, maintenance approaches, and supply chain solutions. Materiel Availability is primarily determined by system downtime, planned and unplanned, requiring the early examination and determination of critical factors such as the total number of end items to be fielded and the major categories and drivers of system downtime."*[1]

The HAF F-16 WSSPO utilized a stochastic model written in the *Wolfram Mathematica*© language. The model runs a Monte-Carlo simulation routine to generate pseudorandom times to failure (*TTF*) and turnaround times (*TAT*) for a critical spare part. Historical RAMS data were utilized to estimate the distribution parameters for the part's *TTF* and *TAT* distributions. The model enabled availability projections under different scenarios of operating tempo (*OPTEMPO*), spare part *TTF*, *TAT*, and stock levels. In practice, it served as a tool for the identification of the less costly approach towards maintaining the F-16 fleet availability at the desired level. Eventually, the F-16 WSSPO came up with realistic proposals to enhance the F-16 fleet sustainability.

Why Use the Stochastic Model?

The model was validated and published by Wolfram Demonstrations Project.[2] An analyst may download at no cost and customize the source code according to his needs. However, a *Wolfram Mathematica*© software license will be required to run the kernel.

An analyst who uses the model may anticipate the following benefits:

- Comprehend the relationship between the Materiel Availability, system *OPTEMPO*, critical spare part stock level, *TTF*, and *TAT*.
- Experiment with different scenarios, parameter combinations, and tailor the best solution by simply setting the controls in the user's menu at different positions.
- Choose the desired confidence level for future projections and evaluate the risk for any potential solution. Compared to a deterministic model, the stochastic nature of this model makes it more robust and pragmatic.
- Keep away from complex equations and calculations, yet be statistically correct. Make estimations that couldn't be performed analytically. Save computational effort and provide quick and sound responses.

1 US DoD Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3170.01C, 2007, page B-3.

2 *http://demonstrations.wolfram.com/SystemAvailability/*

- Perform RAMS cost-benefit analysis and evaluate alternative solutions. Support the decision making process.
- Evaluate the provision of Performance Based Logistics (PBL).
- Identify the optimal initial spare parts inventory, during the procurement of a new system. Avoid useless and costly stock surplus and reduce the logistic footprint.

Definitions

Materiel Availability[3] is a Key Performance Parameter (KPP) for a system's sustainment.

"It is a measure of the percentage of the total inventory of a system operationally capable (ready for tasking) of performing an assigned mission at a given time, based on materiel condition. This can be expressed mathematically as:

$$Availability = \frac{\text{number of end items operational}}{\text{total population of end items}}.$$

EQUATION 1

"Materiel Availability also indicates the percentage of time that a system is operationally capable of performing an assigned mission and can be expressed as:

$$Availability = \frac{\text{uptime}}{\text{uptime} + \text{downtime}}.$$

EQUATION 2

Criticality is a term with many implications. The following definitions derive from US DoD documentation[4]:

*"**Critical Application Item (CAI):** An item that is essential to weapon system performance or operation, or the preservation of life or safety of operating personnel as determined by the military services. The subset of CAIs whose failure could have catastrophic or critical safety consequences is called Critical Safety Item (CSI).*

***Critical characteristic:** Any feature throughout the life-cycle of a critical item, such as dimension, tolerance, finish, material or assembly, manufacturing or inspection process, operation, field maintenance, or depot overhaul requirement that, if nonconforming, missing, or degraded, may cause the failure or malfunction of the item."*

Critical Availability could be defined as the minimum acceptable availability level that enables the system to reach its intended purpose of use.

Materiel Reliability[5] is a supporting Key System Attribute (KSA) for a system's sustainment.

*"It is a measure of the probability that the system will perform without failure over a specific interval. Reliability must be sufficient to support the assigned capability needed. Materiel Reliability is generally expressed in terms of a **mean time between failures** (MTBF or MTTF), and once operational can be measured by dividing actual operating hours by the number of failures experienced during a specific interval:*

$$MTTF = \frac{\text{operating hours}}{\text{number of failures}}.$$

EQUATION 3

"Reliability may initially be expressed as a desired failure-free interval that can be converted to MTTF for use, as a KSA (e.g., 95 percent probability of completing a 12-hour mission free from mission-degrading failure; 90 percent probability of completing 5 sorties without failure)."

In statistical terms, if *TTF* (denoted: *t*) derive from a probability density function (PDF) f(*t*), then:

$$MTTF = \int_0^{+\infty} t\, f(t)dt.$$

EQUATION 4

The Reliability or Survival function R(*t*) expresses the probability that a system will fail beyond the temporal point *t*:

$$R(t) = P(T > t) = 1 - F(t).$$

EQUATION 5

F(*t*) corresponds to the *TTF* cumulative distribution function (CDF). If *TTF* follow a three-parameter Weibull distribution[6], (4) becomes:

$$MTTF = \mu + \beta\Gamma\left(1 + \frac{1}{\alpha}\right),$$

EQUATION 6

Where Γ denotes Euler's Gamma function. Then, (5) becomes:

$$R(t) = 1 - F(t) = 1 - W(\alpha, \beta, \mu) = 1 - \left(1 - e^{-\left(\frac{t-\mu}{\beta}\right)^{\alpha}}\right) = e^{-\left(\frac{t-\mu}{\beta}\right)^{\alpha}}.$$

EQUATION 7

The function λ(*t*) denotes the **failure rate** (*FR*) at a timeframe *t*:

$$\lambda(t) = \frac{\alpha}{\beta}\left(\frac{t-\mu}{\beta}\right)^{\alpha-1}.$$

EQUATION 8

3 CJCSM 3170.01C, "Operation of the Joint Capabilities Integration and Development System," 2007, page B-3.

4 DCMA-INST 303, "Critical Safety Items (CSI)," 2013, page 14.

5 CJCSM 3170.01C, "Operation of the Joint Capabilities Integration and Development System," 2007, page B-4.

6 "Life Data Analysis Reference," 2014, ReliaSoft Corporation, Chapters 3 and 8.

When $\alpha > 1$, $\lambda(t)$ increases when t increases (increasing failure rate, *IFR*). When $\alpha < 1$, $\lambda(t)$ decreases when t increases (decreasing failure rate, *DFR*). When $\alpha = 1$ (the case of the exponential distribution), $\Gamma(1+1/\alpha) = \Gamma(1+1/1) = \Gamma(2) = 1$, and (6) becomes:

$$MTTF = \mu + \beta,$$

Equation 9

And (8) becomes:

$$\lambda(t) = \lambda = \frac{1}{\beta}.$$

Equation 10

When *TTF*~Exp(λ,μ), *FR* remains constant through time (constant failure rate, *CFR*). During the *CFR* period of the system's life cycle, the reliability function (5) becomes:

$$R(t) = 1 - F(t) = 1 - \text{Exp}(\lambda, \mu) = 1 - \left(1 - e^{-\lambda(t-\mu)}\right) = e^{-\lambda(t-\mu)}.$$

Equation 11

Operations or Operating Tempo (*OPTEMPO*) measures the utilization rate of the system:

$$OPTEMPO = \frac{\text{operating hours}}{\text{time duration}}.$$

Equation 12

Time duration may be measured in days, weeks, months, years, etc. Instead of operating hours, the analyst may use flight hours, distance in miles, number of missions, etc.

Turnaround time (*TAT*) is the time required to restore a system back to operational condition, after it failed. *TAT* may include the necessary time that takes for:

- Safe for maintenance procedures.
- Fault isolation.
- Remedy actions.
- Gaining accessibility, removal and installation of components.
- Operational checks.
- Removal and installation of the failed spare part/component.
- Obtain the required repair parts, consumables, special tools, support equipment.
- Packaging, handling, storage.
- Solicitation process (e.g., for repair center, for transporter, etc).
- Transportation of the spare part to be repaired.
- Repair at the repair center.
- Administration/logistic procedures.
- Await time.
- Other procedures.

Ground Rules and Assumptions

The stochastic model is based on the following assumptions:

- The system's attrition rate through the operating period under examination is zero.
- All the critical spare parts have zero operating hours at the beginning of the operating period.
- All the critical spare parts are available at the beginning of the operating period.
- The system fails when the critical spare part fails.
- The system Materiel Availability depends on no other factors than the critical spare part operational condition.
- Each operating system has one critical spare part installed.
- System availability is considered 100%, if the population of the operational spare parts equals or exceeds the system total inventory.

The expected system availability will tend to balance at a point, after a warm-up period. The warm-up period corresponds to the first months of operations, until those firstly failed parts begin to return from the repair center. If there is not a balance point, the system availability will go downhill until it drops at 0%. This is likely to happen when low reliability, long turnaround times and high *OPTEMPO* take place at the same time.

The three-parameter Weibull distribution is the default distribution for times to failure. The reasons for this choice are:

- The Weibull distribution is well known and widely used in reliability analysis.
- The location parameter μ enables the modeling of a guarantee period (i.e., the spare part supplier offers immediate spare part replacement in case of failure within the first 50 hours of operation).
- Depending on the value of the scale parameter α, the Weibull distribution may model *DFR*, *IFR*, and *CFR* spare part lifetimes.
- The analyst may estimate the parameters of the three-parameter Weibull distribution from historical data. The data fitting process[7] is relatively easy, and most statistics software packages support it.
- It is relatively easy to generate a pseudorandom variable from a Weibull distribution and then build a simulation process. If U is uniformly distributed on (0, 1), then $W = \mu + \beta(-\ln(U))^{1/\alpha}$ follows a three-parameter Weibull distribution with shape parameter α, scale parameter β, and location parameter μ.

Also, the three-parameter lognormal distribution is the default distribution for turnaround times. The reasons for this choice are:

- Experience shows that historical

7 A cost-free tool for data fitting to a three-parameter Weibull distribution is available at: http://demonstrations.wolfram.com/FittingTimesToFailureToAWeibullDistribution/

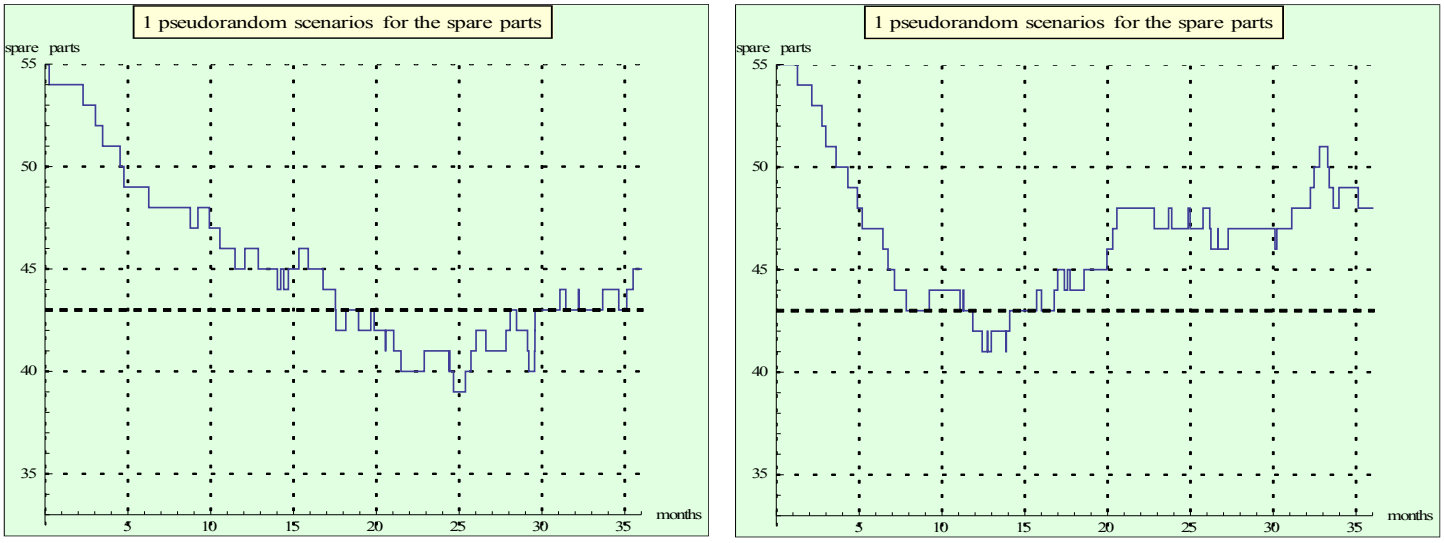


Figure 1 – Examples of paths for the remaining operational spare parts. The path goes down whenever a spare part fails; it goes up whenever a spare part returns from the repair center.

turnaround times fit with the lognormal distribution, in most cases.

- The location parameter γ may be used to express the minimum required *TAT*, which is usually greater than zero.
- The heavy tail of the lognormal distribution captures the risk of unexpected supply chain/repair cycle jams.
- Usually, the majority of turnaround times concentrate around the mode value of the data.
- The analyst may estimate the parameters of the three-parameter lognormal distribution from historical data. The data fitting process[8] is relatively easy, and most statistics software packages support it.
- It is relatively easy to generate a pseudorandom variable from a three-parameter lognormal distribution and then build a simulation process. If X is normally distributed with mean μ and standard deviation σ, then $Y = \gamma + e^X$ follows a three-parameter lognormal distribution with location parameter γ, scale parameter μ, and shape parameter σ.

8 A cost-free tool for data fitting to a three-parameter lognormal distribution is available at *http://demonstrations.wolfram.com/FittingDataToALognormalDistribution/*

Expedition Through the Model's Attributes

The model's kernel is an algorithm that generates pseudorandom times to failure and turnaround times for the critical spare part, according to the distributions parameters selected by the user. Based on the user's choices, a Monte-Carlo simulation routine generates "paths" for the remaining operational spare parts, through the period being under examination. The density of these paths enables probabilistic projections for the system availability.

The Monte-Carlo simulation is a problem solving technique used to approximate the probability of certain outcomes by running multiple trial runs (scenarios), using pseudorandom variables. This technique can be applied to estimate integrals or mean values. For example, the following integral:

$$\mu = \int_0^1 g(x)dx,$$

Equation 13

is written as:

$$E[g(U)] = \int_{-\infty}^{+\infty} g(x) f_U(x)dx,$$

Equation 14

Where U is uniformly distributed on (0, 1) with PDF: $f_U(x) = 1$. If a simulation process generates a large pseudorandom sample of $g(U_i)$ the sample average can be used as an estimator for the quantity μ:

$$\hat{\mu} = \frac{1}{n}\sum_{i=1}^{n} g(U_i) \xrightarrow[n\to+\infty]{} E[g(U)].$$

Equation 15

The model's menu includes a seed controller that "locks" the pseudorandom generation process. The menu also allows choosing the number of simulation iterations (scenarios) for the spare parts. The higher the number of iterations, the more reliable the simulation outcome but the more time-consuming the simulation process.

The model requires the following inputs:

- System operating period under examination (in months).
- The critical spare part inventory, in the beginning of the operating period.
- The system inventory in the beginning of the operating period.

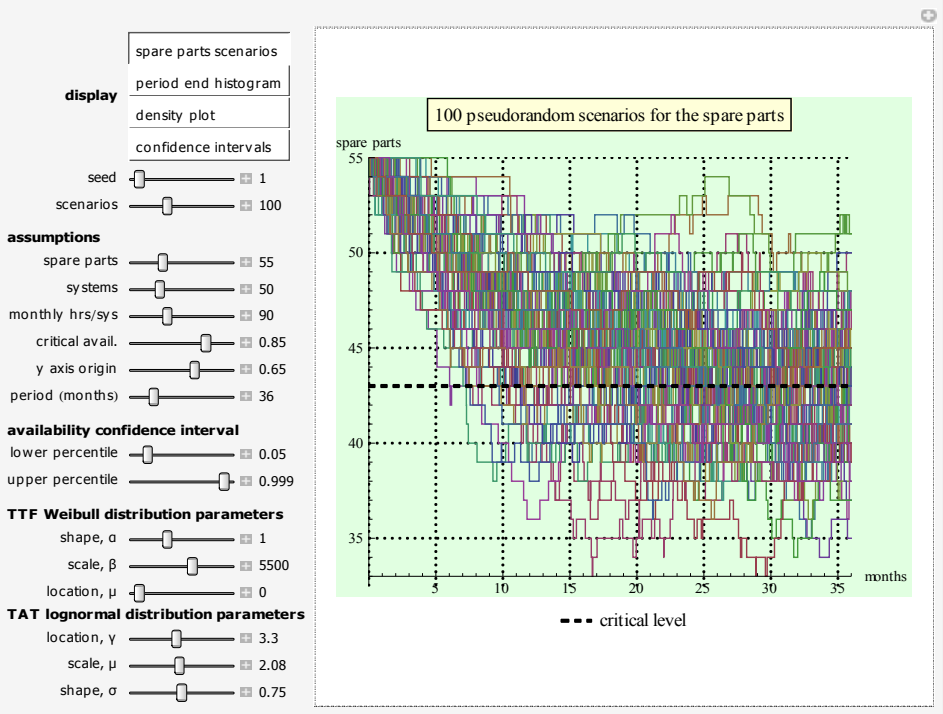


Figure II – The "spare parts" display selection illustrates the pseudorandom scenarios generated by the kernel. The "seed" slider re-generates pseudorandom scenarios. The higher the number of scenarios (simulated experiment trials), the more reliable the simulation outcome and the more time-consuming the simulation process. The horizontal dashed line shows the required number of operational spare parts that correspond to the system's "critical availability" selected by the user.

- The minimum acceptable (critical) availability level for the system, calculated as in formula (1).
- The average monthly system *OPTEMPO* (in flight hours per month).
- The Weibull distribution parameters α, β, μ for the critical spare part *TTF* (in flight hours).
- The lognormal distribution parameters γ, μ, σ for the critical spare part *TAT* (in months).

The following example enlightens the reader on the features of the stochastic model, demonstrates its projection capabilities and explains how it can be used as a decision supporting tool:

The DoD is ready to sign a contract for the procurement of 50 new aircraft. The DoD needs to determine the inventory of a critical spare part "A". Each aircraft is planned to fly 90 hours per month. The contractor reports that the Weibull distribution parameters for the spare part TTF (in flight hours) are: α=1, β=5500, μ=0. In case of failure, the spare part TAT (in months) will follow a lognormal distribution with parameters: γ=3.3, μ=2.08, σ=0.75, according to historical data for similar spare parts.

The stochastic model may provide valuable help to an analyst that seeks quick answers to complex queries, like:

1. What is the expectation that the aircraft availability will be higher than 85% after 3 years of operation, if the spare part *A* inventory is 55?
2. At the 95% confidence level, what is the expectation for the worst aircraft availability during the first 3 years of operation, if the spare part *A* inventory is 55? When is this expected to happen?
3. Provide an 80% confidence interval for the aircraft availability through the first 3 years of operation, if the spare part *A* inventory is 55.
4. What should be the spare part *A* inventory, so that the aircraft availability will stay above 85% during the first 3 years of operation, at the 95% confidence level?
5. If the objective is to maintain the aircraft availability above 85% at the 95% confidence level during the first 3 years of operation, provide alternative options, keeping the spare part *A* inventory at 55.

To answer the first query, the "period end histogram" display is selected. The table of the histogram shows that it is approximately 60% probable that the aircraft availability will be at least 85% at the end of the 3rd year of operation. This is equivalent to the probability that at least 43 spare parts *A* will be operational at that time.

The density of the aircraft availability during the whole 3-year period can be illustrated both in 3-D and 2-D, using the "density plot" display (Figure 4 on the following page).

To answer the second query, the "lower percentile" selection has to be set at 0.05, while the display selection is set to "confidence intervals." At the 95% confidence level, the diagram shows that the worst case for the aircraft availability is expected to be approximately 75%, not earlier than 30 months of operation.

To answer the third query, the 80% confidence interval for the aircraft availability through the 3-year period has to be constructed. This can be done by selecting the "lower percentile" at 0.10 and the "upper percentile" at 0.90.

To answer the fourth query, the initial inventory of the spare part *A* has to increase, so that the red line hits minimum at 85%, instead of 75%. As shown in the next Figure, this happens when the "spare parts" slider is set at 60.

FIGURE IV – The "density plot" display selection illustrates the density of the available aircraft through the selected period (36 months). This display offers a vivid and holistic view to the analyst.

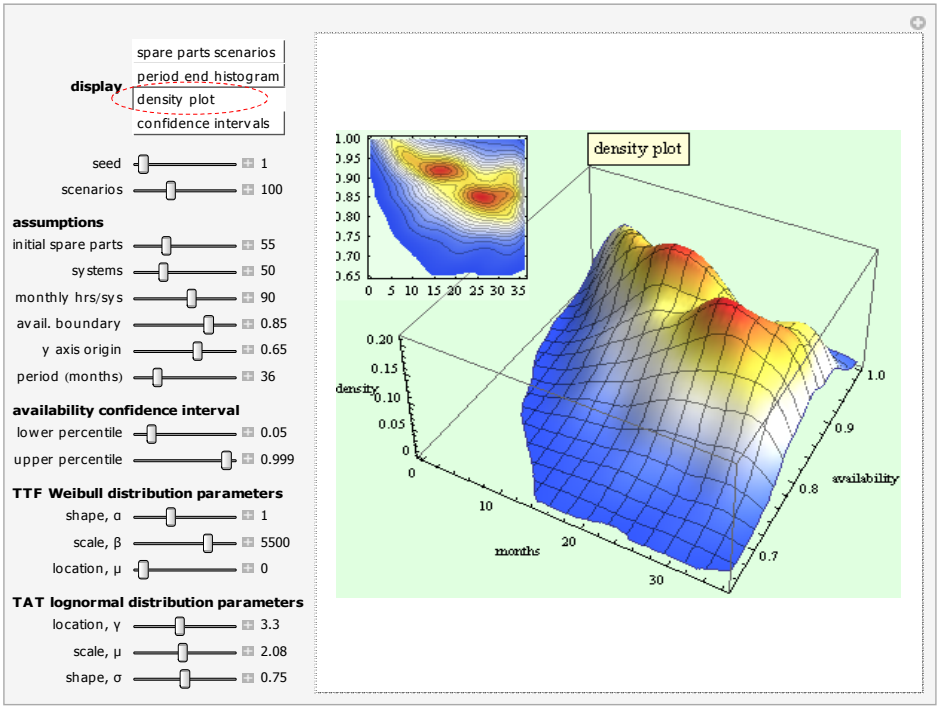


FIGURE V – The dark blue area (above the red line) shows where the aircraft availability is expected at the 95% confidence level. The light blue area (below the red line) corresponds to the 5% worst case scenarios for the aircraft availability. The red line hits minimum at approximately 75%.

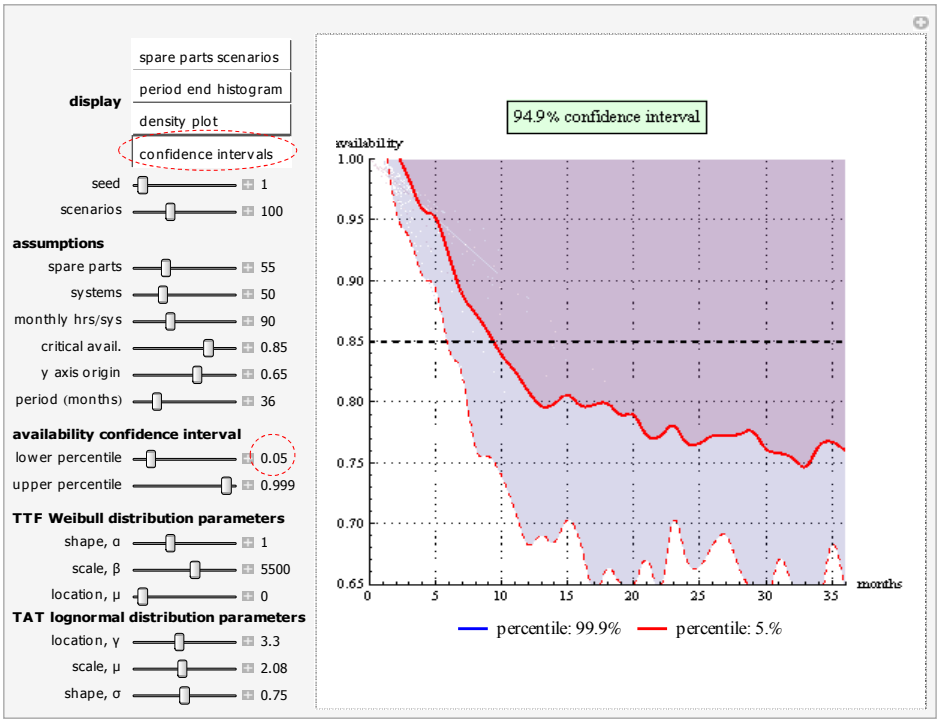


FIGURE VI – The dark blue area illustrates the 80% confidence interval for the aircraft availability during the 3-year period.

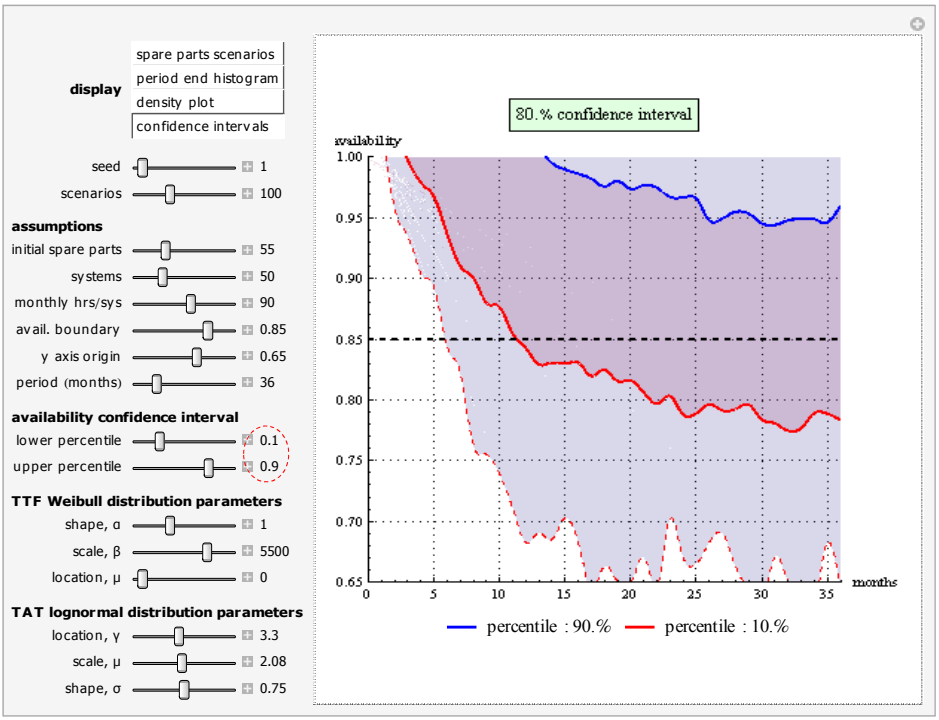
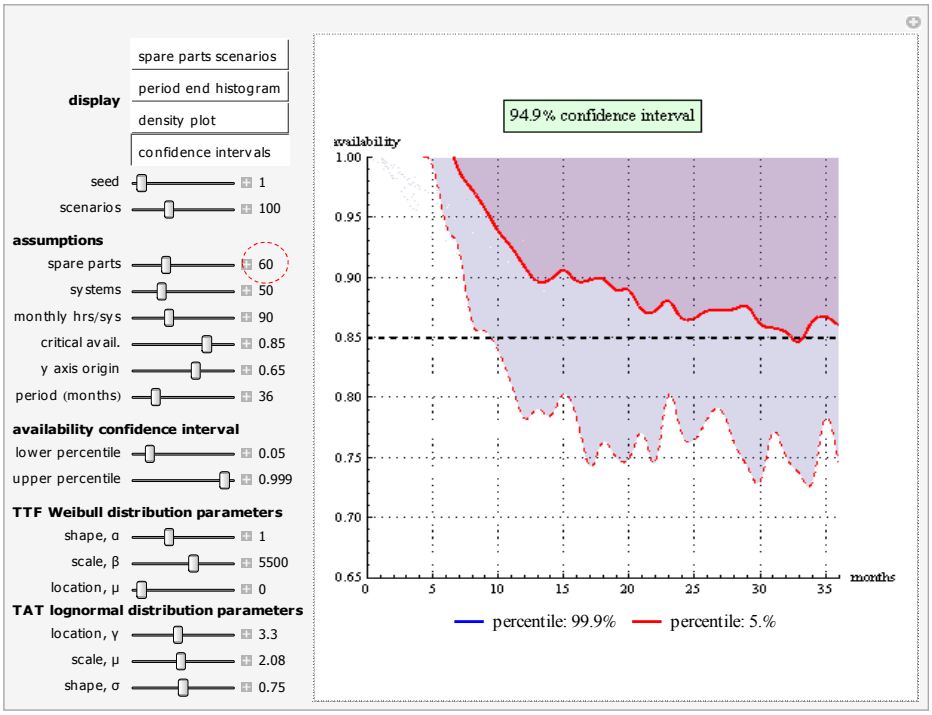


FIGURE VII – At the 95% confidence level, if the spare part *A* inventory is 60, the aircraft availability will be higher than 85% during the first 3 years of operation.



Evaluation of Alternatives

Having the objective:

"Maintain the aircraft availability higher than 85% at the 95% confidence level during the first 3 years of operation, keeping the spare part A inventory at 55," to answer the fifth query, the analyst may seek for options other than the procurement of additional spare parts:

Alternative 1: Reduce OPTEMPO

The objective is reached if the monthly *OPTEMPO* per aircraft decreases to 55. In practice, "Alternative 1" may require more hours of pilots training in simulators and/or transferring operational workload to other units. This alternative will become attractive if it is less costly than the procurement of 5 additional spare parts *A*.

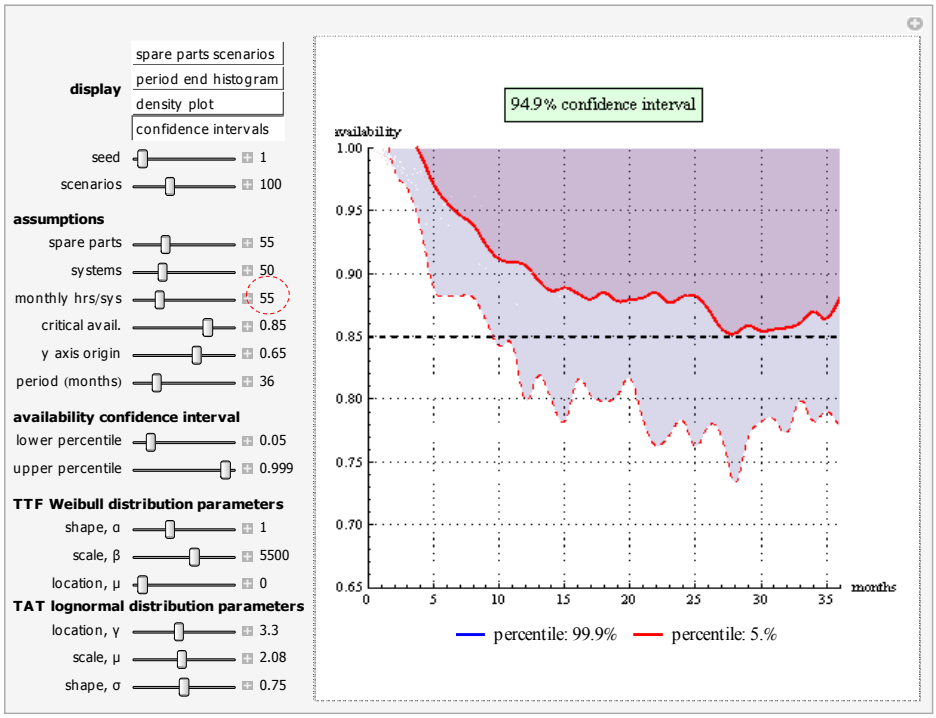


Figure VIII – To reach the objective with "Alternative 1", the monthly *OPTEMPO* has to be trimmed down to 55 flight hours per aircraft.

Alternative 2: Improve reliability

The objective may be reached if the spare part reliability improves. There are infinite options to examine, selecting different combinations for the Weibull parameters. For example, the objective may be achieved if the Weibull parameter β (scale) will increase from 5500 to 8800, which corresponds to a 60% increase in the spare part's *MTTF* (Notice that the shape parameter α is set to 1, which is the case of exponential distribution). In practice, "Alternative 2" may be translated into a *MTTF* guarantee term in the contract, the implementation of engineering changes, or the procurement of a more reliable spare part *B* instead of *A*. "Alternative 2" will become attractive if it is less costly than the procurement of 5 additional spare parts *A*.

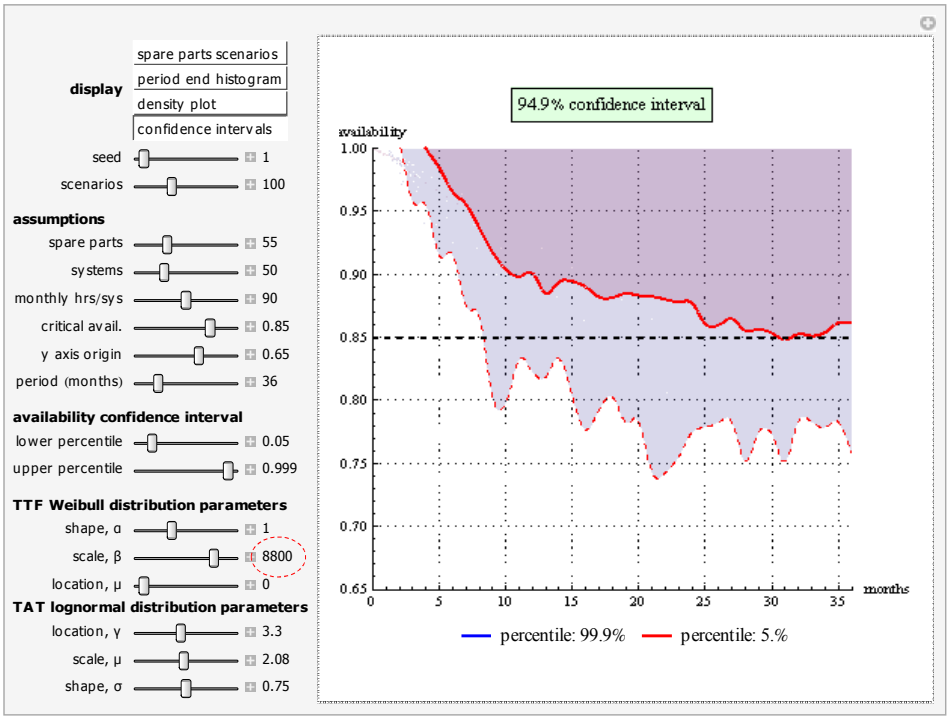


Figure IX – To reach the objective with "Alternative 2", the Weibull scale parameter has to increase to 8800.

Alternative 3: Reduce TAT

The objective may be reached if the spare part's *TAT* will reduce. There are infinite options to examine, selecting different combinations for the lognormal parameters. For example, the objective may be achieved if the lognormal parameter γ (location) decreases from 3.3 to 2.5 and the parameter μ (scale) from 2.08 to 1.5. In practice, this can be achieved by accelerating the logistic procedures and diminishing await times. This alternative will become attractive if it is less costly than the procurement of 5 additional spare parts *A*.

Epilogue

The stochastic model for availability projections enables the examination of a wide variety of parameter combinations that affect the system availability through its operational life. An analyst may use this tool to perform cost-benefit analysis, project future level of availability, determine the effective utilization of the resources provided, minimize stock, and support decision making. ●

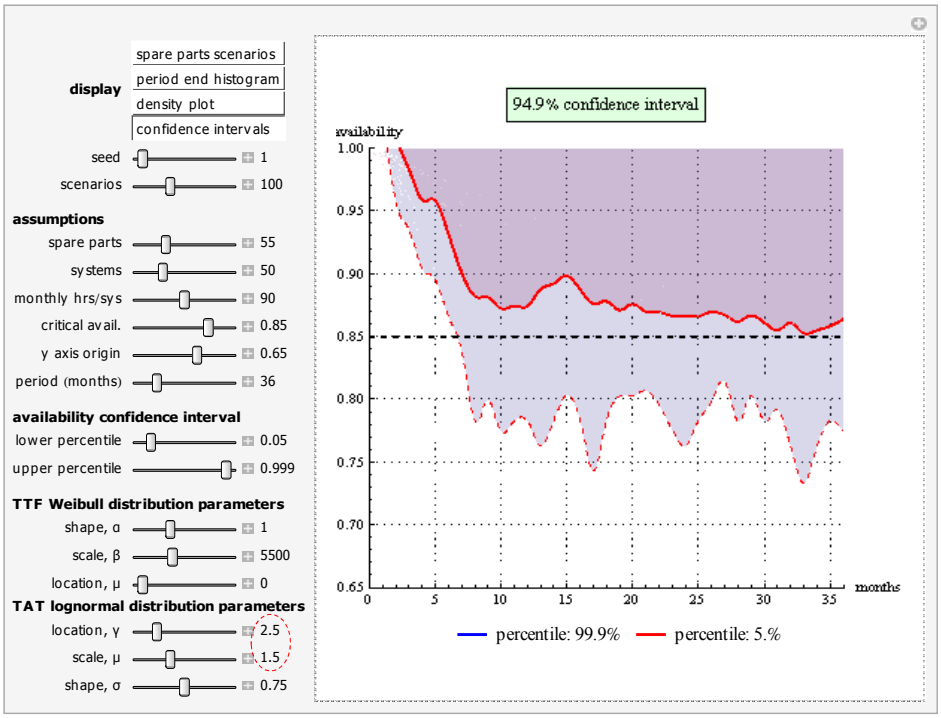


FIGURE X – To reach the objective with "Alternative 3", the lognormal parameters have to change.

References

1. R. Aristizabal, "Estimating the Parameters of the Three-Parameter Lognormal Distribution," 2012, *FIU Electronic Theses and Dissertations*, Paper 575 http://digitalcommons.fiu.edu/etd/575
2. Michail Bozoudis, "Fitting Times-To-Failure to a Weibull Distribution," 2015, *Wolfram Demonstrations Project*. http://demonstrations.wolfram.com/FittingTimesToFailureToAWeibullDistribution/
3. Michail Bozoudis, "Fitting Data to a Lognormal Distribution," 2015, *Wolfram Demonstrations Project*. http://demonstrations.wolfram.com/FittingDataToALognormalDistribution/
4. Michail Bozoudis, "System Availability," 2015, Wolfram Demonstrations Project, http://demonstrations.wolfram.com/SystemAvailability/
5. "Operation of the Joint Capabilities Integration and Development System," 2007, CJCSM 3170.01C, http://everyspec.com/DoD/DOD-General/download.php?spec=CJCSM_3170.01C.00000624.pdf
6. "Aviation Critical Safety Item Management Handbook," 2011, JAGG http://www.aviation.dla.mil/UserWeb/AviationEngineering/EngineeringSupport/Documents/AviationCSIHandbook.pdf
7. "Critical Safety Items (CSI)," 2013, DCMA-INST-303 http://www.dcma.mil/policy/303/DCMA-INST-303.pdf
8. "Cost Estimating and Assessment Guide," 2009, GAO-09-3SP http://www.gao.gov/new.items/d093sp.pdf
9. «Life Data Analysis Reference», 2014, ReliaSoft Corporation. http://www.synthesisplatform.net/references/Life_Data_Analysis_Reference.pdf

SecurityFusion Resolved: Dynamically Converging Cyber and Physical Infrastructures into a Single, Integrated, and Interoperable, Common Operating Picture

DR. CHRISTOPHER V. FEUDO

Introduction

It is becoming apparent that governments and industry can no longer afford to view the protection of physical assets and electronic assets as different domains independent of one another, requiring different approaches and organizations to assure appropriate protection. Technologies are converging in significant ways that now call into question the validity of these "stovepipe" practices. This paper discusses the significance of this phenomenon and offers an approach.

Current events strongly demonstrate the criticality of optimizing emerging technologies to protect our Critical Infrastructure(s). Such events include the attacks at the Office of Personnel Management (OPM) which compromised the personal information of up to 32 million individuals and the leaking of classified National Security Agency information [affecting whole sovereign nations] by NSA contractor Edward Snowden. Utilizing the strategic objectives of the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets efforts as underpinnings, considerations for protecting our Critical Infrastructures would include:

- Pre-empting potential threats.
- Identifying and assuring the protection of those infrastructures and assets we deem most critical. N.B., The infrastructure and key assets are comprised of resource cyber networks that are used to conduct day-to-day business and the physical infrastructure (facilities) that house the equipment and personnel. These assets, if lost or disrupted, could adversely affect our economy or endanger our well-being.
- Providing timely warning and assuring the protection of those infrastructures and assets that face a specific, imminent threat.
- Assuring the protection of other infrastructures and assets that may become targets over time by pursuing specific initiatives.
- Enabling a collaborative, corroborative, and correlative environment across local, state and federal governments (to include industry) and providing a comprehensive end-to-end virtual mission platform solution set to protect Critical Infrastructures in alignment with the National Strategy for Homeland Security.

Historically, not only have these infrastructures been separate and mostly unrelated, but the cyber/logical aspect of it totally isolated and segmented. This stovepiping approach has lead to communication gaps and inefficiency and an overall lack of situational awareness. In order to combat terrorism, natural disasters, vandalism and espionage effectively and achieve Critical Infrastructure Protection, the physical and cyber business infrastructure must be secured and monitored for maximum uptime and comprehensive, holistic end-to-end security. The focus must be on transitioning from the reactive to the preventive to the pre-emptive mode, through a highly flexible integrated relational real-time analytical architecture, monitored, managed and controlled by a virtual mission platform—locally,

remotely or through a managed service.

Investments in biometric and token technologies have blurred the lines between physical and logical identification and authentication. Further, the automation of systems controls and Supervisory Control and Data Acquisition (SCADA) infrastructures and their management through the use of electronic networks and the Internet have effectively eliminated the deference between physical controls and electronic information—both now vulnerable to unauthorized access and tampering from literally anywhere around the globe, as we have seen with the directed Stuxnet attacks against Iran's nuclear facilities—destroying nuclear centrifuges. Even legacy analog communications systems are now evolving into digital formats exposing them to the same vulnerabilities and risks as other forms of electronic data.

Integrating sensor intelligence and physical infrastructure status into existing cyber monitoring platforms leverages existing investments in monitoring systems for cyber infrastructure by correlating data from the physical environment that surrounds and protects the cyber equipment. This integration and convergence, SecurityFusion, allows you to view the real time status of the critical infrastructures of a distributed enterprise on a single map of any regional, state, national or global scale. When you have a comprehensive view of your distributed enterprise's physical and cyber environment, you have achieved a much higher level of overall situational awareness and can dramatically improve your ability to respond to any event—it can help operationalize security and privacy into its organization's business processes to achieve compliance and mission success. Strategic integration of these technologies empowers decision-makers with the real-time data require to pre-empt, prevent, detect and mitigate a real-time distributed attack on their entire enterprise; i.e., decision-makers are provided automated and integrated analysis, monitoring, management and the control of it all.

It is essential to have a pulse of the physical and cyber systems dynamically at all times and to deliver a clear picture of all monitored elements within and across all critical infrastructures—the *total* critical infrastructure, see Figure 1[1], not just network or physical aspects. This is the only viable solution set that can provide the capability to evaluate all the potential variables that may contribute to their infrastructure's vulnerabilities.

Approach

Recognizing the holistic nature of physical and cyber security, a holistic approach towards managing risk is strongly endorsed. As illustrated by Figure 2 (following page), an integrated approach for developing a successful Critical Infrastructure Protection (CIP) Strategy via the Agile Security Framework is offered.

This Agile Security Framework articulates an organization's mission vision from a risk management perspective through the identification and classification of its assets according to degrees of mission criticality, the definition of policies and standards that reflect that vision which are multi-focused through the prisms of security, privacy, business continuity and overall risk management. You then work through the infrastructure to bring it into compliance with that vision, taking into account both internal and external issues around entitlement and permissions, compliance management and certification to regulatory requirements. Finally, an integrated reporting framework is provided, that enables all, on a need-to-know basis, access to the information necessary to assure effective, preemptive risk management.

This approach is structured as separate or interacting capabilities that are defined by government documents.

1 Developed in concert with implementer IMCI, 590 Herndon Pkwy, Suite 300 Herndon, VA (703) 467-2999.

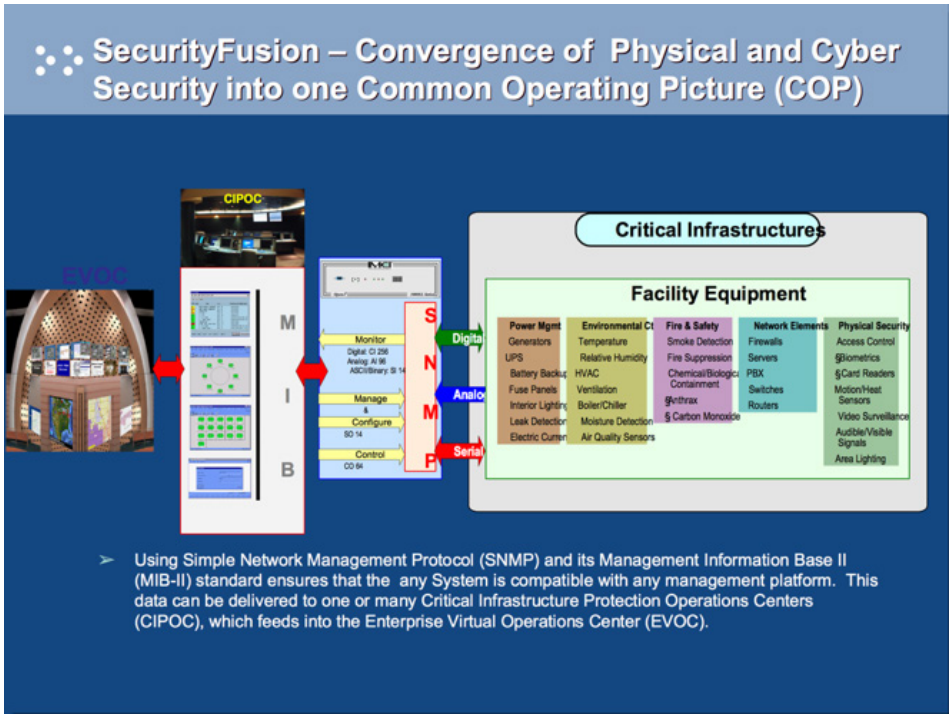


Figure 1 – Total Critical Infrastructure

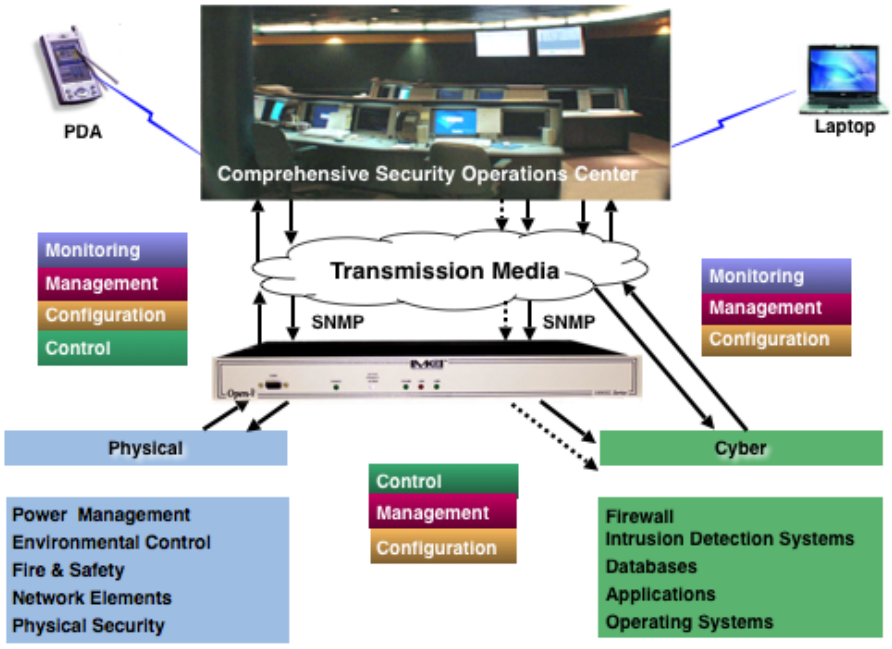


Figure II – Total Convergence

These capabilities constitute a complete life cycle of Homeland Security/Critical Infrastructure Protection activities. Specific methodologies are incorporated, in conjunction with industry standard best practices, for the Homeland Security/Critical Infrastructure Protection (CIP) and Information Technology (IT). Security teams within most federal agencies are currently focused on implementing FIPS 201[2] plans for initial deployment of the physical and logical access controls required to comply with HSPD-12[3] mandates. Any perception that an agency has what they need in place for a converged approach to physical and logical access security, when implementation has been completed, is wrong. Implementing FIPS 201 requirements is only a step toward this convergence. However, additional elements need to be considered, as described within this article.

This approach allows for introduction of new technical approaches, new management practices, and the use of proven solutions for security issues. Whether one, several, or all of the services are used, any Homeland Security/Critical Infrastructure Protection requested task can be analyzed and approached within the process. The use of this methodology allows you to customize the approach to your specific needs.

Through the application of its Relational and Integrated Pre-emptive Analysis methodologies, anticipatory intelligence and pre-emptive measure recommendations can be provided to help you better protect your assets—unique traffic analysis capabilities that are focused beyond typical statistical or relational analysis norms to associate dissimilar or unrelated incidents are integrated into Indicator Profiles. These Indicator Profiles isolate patterns from related events, illuminating subtle attacker's actions to weaken or defeat network security perimeters; this includes isolating insider threats. Integrating indicator profiles with client vulnerability profile data and threat profile data extends analytical capabilities sufficiently to predict future attacks against specific clients or forecast attack trends across any number of critical technologies or critical infrastructures. Trend profiling, ideally, supports consortium security supported industry types.

The crux of this approach is to continuously monitor the threat agent environment. Analysis of motive and intent, resulting in "trends" or "tendencies," identified by Indicator Profiles; e.g., information collected from open and closed sources; new technologies and techniques, and proprietary data—form the basis for the identification of relevant trends. These trends, combined with an understanding of the threat agents themselves, provide a basis for identification of threats.

Finally, it is the correlation of the client Indicator Profiles with the threats and knowledge of the client's network topology and technologies that will enable you to determine where new vulnerabilities to your infrastructure may have occurred and where future potential vulnerabilities may be developing.

What is needed is a Comprehensive Security Operations Center (CSOC) which provides federal and commercial clients a holistic approach to continuous computer network security support through predefined or specific-tailored services. The approach is to transition the focus from incident response to incident prevention, and provide real time integrated multi-disciplined analytical capabilities and services into a single intrusion prevention analytical architecture. This strategy allows for a quick response to flagged incidents and for preempting potential threats and follow-on attacks.

The most effective mechanism for protecting critical infrastructure is first

2 *http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf*

3 *http://www.dhs.gov/homeland-security-presidential-directive-12*

to use tools that capture and integrate information about physical and cyber security, and then correlates seemingly independent events, to:

- Isolate and report on root causes
- Improve times of response and notification
- Automate control and management processes
- Identify changes, disruptions and inconsistencies in processes or environments
- Manage the entire process with the same system and skill set

What is needed to accomplish this is an intelligent data collection methodology comprising people, software and remote hardware unit(s). Features include a sophisticated open architecture of receptors and emitters, a suite of software that interprets and relays critical information to one or multiple control centers and displays that provide informational messages that are simple to manage and act upon. It includes:

- Units for data collection, device management, Local Event Correlation™ and the viewing of integrated event(s).
- Software to monitor, manage, control and report on the connected system elements.
- CIP Services for cost-effective remote monitoring, management and control of the total Critical Infrastructure—all SNMP management systems—and
- The personnel to run and manage it; e.g., Tech Support, Monitoring, Incident Response, Forensic(s) and Analysis Teams.

Through its receptors, the system acquires data in any form—digital inputs (such as power distribution units), analog inputs (such as air quality sensors), or serial inputs (such as digital cross-connect switches)—then translates the data into a form compliant with the de facto standard protocol for network management (SNMP). It transmits the data across any transportation medium: telephone lines, Ethernet-based LANs, WANs, or wireless media including both land-based and satellite. The unit provides a unique capability for the Local Event Correlation of the data coming from physical security systems, power management systems, environmental systems, fire systems, network elements, and IT systems from any monitored site, providing reliable guaranteed delivery of each warning message to multiple destinations simultaneously. Through its emitters, which is able to initiate and manage state changes of remote or local devices. If one center is out of service, any one of the redundant centers is capable of immediate full monitoring and management. The management center can override any of the automated actions or reconfigure the system for different alarm or sensor combinations or resulting actions. It is also possible to establish a portable device (such as a laptop or PDA) as a remote monitoring station with limited or full mobile visibility, management, and control.

This flexible, modular and customizable methodology provides a roadmap to achieve the goal of developing Homeland Security/Critical Infrastructure Protection plans. Integrated into these processes are more than 50 templates and report skeletons to develop the solution.

With the emphasis on partnering, whole security methodology is built around working with clients to tackle their individual needs, within a framework that will help ensure all applicable issues are addressed—thus accelerating the implementation of enterprise-wide security solutions.

Methodology

Development of the appropriate policies, standards/processes and procedures for a CIP approach is realized when the first three phases of the following five-phased strategy are complete; Phase 4 and 5 provide the approach to successfully protecting these infrastructures as well as integrating the physical and logical security controls across these infrastructures.

Phase I – Identification: The emphasis is to identify assets requiring protection and quantify their value to the organization. Critical assets are identified by looking at all aspects of the enterprise, including cyber assets such as networks, data, software and hardware, and non-cyber organizational assets such as people, business processes, facilities and equipment. Skilled professionals/consultants, analyzing the various asset categories will determine points of failure mitigation strategies, and define risk reduction activities, which can be incorporated into the planning aspects of Phase II.

Phase II – Planning: In this phase, a foundation of planning, e.g., mitigation of vulnerabilities and for response and recovery in the event of a security incident or service disruption, is created. Mitigation plans will include real-time Monitoring, Pre-emptive activities, Incident Response, Disaster Recovery, Crisis Management, Resumption and Reconstitution Plans, Emergency Operations and Command Center Plans. The focus will be: monitoring, virtual management and control of critical infrastructures locally, remotely or through a managed service, along with a wide variety of asset specific mitigation plans tailored to individual threats, vulnerabilities and risks within the enterprise.

Phase III – Education and Awareness: Working closely across the enterprise, education, training and testing of

the plans developed in Phase II is executed. These efforts are aimed at raising enterprise-wide awareness. Phase III includes a robust security awareness and training curriculum to provide an integrated and customized training program developed as part of the overall approach. Tabletop exercises and functional drills can be utilized for testing the various plans. Involving representatives from across the enterprise in these exercises will act to validate the approaches and continue to raise awareness. Many of the plans will have specific procedures that will require testing prior to implementation. As weaknesses in the procedures are identified through testing, modifications can be immediately incorporated into the documented processes prior to full-scale rollout and activation.

Phase IV – Implementation: This phase constitutes the execution of mitigation strategies and the activation of specific plans that support response and recovery. Mitigation strategies are applied to minimize and protect against ongoing threats, prevent failures and support potential recovery activities. Installation of Intrusion Prevention Systems (IPS) (to identify malicious activity, log information about this activity, attempt to block/stop it, and report it), and of network firewalls to reduce the risk of intruders prevent computer viruses from infiltrating the network, the identification, setup and testing of an alternate site to support business operations, and/or the implementation of a comprehensive backup plan to support systems recovery are just examples of mitigation strategies.

Activation of a specific plan is based on an event or disruption. At that time, delivery services will shift focus from planning and mitigation to response, recovery, and resumption of normal business. This delivery strategy is consistent with the intent of HSPD-74 (Homeland Security Presidential Directive No. 7), issued by U.S. President George W. Bush in December, 2003 to update policies intended to protect the country from terrorist attacks. This directive superseded the earlier PDD-635 (Presidential Decision Directive No. 63), which was issued by President Clinton in May of 1998. This directive ensures critical infrastructure protection and homeland security. It also supports both the PDD 67 6focus on Continuity of Operations (COOP) and the anti-terrorism emphasis of PDD 397 and PDD 628.

With policies and processes in place, the approach to Homeland Security and Critical Infrastructure Protection focuses on a comprehensive, trusted solution. This solution will utilize National Security, Economic Security and Network and Information Protection strategies to protect and restore physical and cyber-based critical infrastructures. These strategies minimize the consequences of natural, technological and man-made disruptions of service. Core strategy components—determining risks and vulnerabilities, developing policies, processes, and procedures to ensure data integrity, secure communications, facilities and resources, Security, privacy and risk management services—enable government organizations and critical infrastructure components to achieve greater overall information systems security.

A comprehensive life-cycle approach, applied in the implementation phase, includes security-aware applications, security policies and disaster recovery and business continuity plans. Services include assessments, design development and implementation of security architectures, secure networks and intranets—including firewalls and virtual private network (VPN) technologies, capacity and workload planning and modeling, biometrics, and Smart Cards. Additional functionalities to be provided or integrated would include vulnerability scans, penetration testing, intrusion detection/preventive/pre-emptive analysis and security monitoring. Management support would be provided through virtual mission platform management, control and incident handling, token authentication, access control/identity management, and certification and authentication. New state-of-the-art-technologies will be evaluated, test, and considered as part of an overall solution to better provide optimum service. Secure Voice over Internet Protocol (VoIP), electronic risk management and content monitoring solutions will enable companies to guard against information disclosures that originate within any organization.

Phase V – Monitoring and Management: Integrated into all aspects of the Education and Awareness, and the Implementation Phases is a monitoring and virtual management program. Monitoring activities include a consistent review of instrumented assets, including the intrusion detection/prevention or security audit data. Monitoring is trended to incident analysis, which gives data to first responders. Managing the entire enterprise from a virtual mission platform plan will provide decision makers with the capabilities of managing the enterprise from their laptops/desktops or mobile devices. Metrics are developed for response times, given criticality of the resources, and responders are trained to

4 *http://www.dhs.gov/homeland-security-presidential-directive-7*

5 *encyclopedia2.thefreedictionary.com/PDD-63*

6 *http://www.fema.gov/pdf/library/fpc67.pdf*

7 *http://www.terrorism.com/documents/Legacy/PDD/PDD-39%20U_S_%20Policy%20on%20Counterterrorism.htm*

8 *http://www.iwar.org.uk/cip/resources/pdd63/pdd63-article.htm*

reduce cycle times for responses. Performance metrics will ensure the controls put in place remain effective and efficient. In the event of an incident or disruption, the actual execution of the response and recovery plans will be the true test of their effectiveness. It is critical to monitor these activities and use the valuable lessons learned as input to CIP program improvements. With real-time monitoring and detection of electronic risks, companies across various industries and government agencies now have the demonstrable proof they need to show they are in continuous compliance.

Summary

SecurityFusion is all about trust, and responsibility—convergence inherently breeds more vulnerability, if the environment is not adequately addressed. The convergence of the cyber and physical ambit is crucial for CIP security resolution and extends to any organization's awareness of potential security operational and management exposures. Cyber and physical infrastructures are increasingly dynamically coupled through integrated and interoperable common operating environments. Developing and implementing a robust strategy to ensure the security of the country's critical infrastructure and key assets requires a comprehensive assessment of facilities to identify vulnerabilities, whose impact can then be reduced or mitigated with customer focus innovative, proven and rational engineering measures.

Leveraging unique capabilities, global experience and effective strategies better enables our government's monitoring, pre-emption, detection, preparation, prevention, protection, management, control, response and recovery from physical and cyber attacks against the government, its citizens, national interests and its critical infrastructure.

Advantages of this Approach

This solution offers unique rewards:

- Effective and efficient convergence of cyber and physical infrastructure activities into a single, dynamic, and integrated Common Operating Picture.
- Robust and proven methodology, processes, and tools to isolate and defeat adversaries. Based on the attack patterns they exhibit and the trails of evidence they leave at the scene, adversaries unknowingly leave clues that are identified by analytical capabilities. The analytical processes and visualization tools are used to filter thousands of events and proactively hunt down obvious intruders attacking firewalls and more importantly, subtle intruders who have already hacked in and are hiding on private networks.
- Anytime, anywhere access: Web-based virtual command center, which can be accessed from any standard browser. It can reside on your local infrastructure or is available through a hosted platform.
- A comprehensive solution that protects past and future investments by incorporating any vendor's devices, using existing transmission media, operating on all management platforms and integrating physical and cyber input and output.
- Local Event Correlation™ capabilities to allow for coordinated reporting and management of events and responses, and the ability to initiate actions to mitigate risk with or without connection to the control center.
- Capability to monitor, manage, control, configure and update CIP devices and facilities, both locally and remotely, from multiple locations, eliminating the need for redundant recovery mechanisms and reducing the need for physical site visits.
- Secure, encrypted information protected by internal battery backup, with authentication call-back security protecting remote access.
- Common language translation of information to one control center, reducing staffing and training needs.
- Rapid deployment and ease of use. ●

Mechanical Accelerated Life Tests

FRANK STRAKA

Introduction

This article will discuss extrapolating accelerated life test results to normal operating conditions using statistical analysis. The study will look at a bracket that is used in an exercise cross trainer that has stresses generated on it when a person is operating the equipment.

Although the prediction will use a precise model, in actual use, there is considerable variability in usage of a single product. There are multiple users with different weights and operate the equipment at different speed and loading conditions. In addition the 1,500 hours will also vary based on the club where the equipment is used. When developing the baseline model for the prediction, one takes into the factor that a 350 lb. user will not operate the equipment at maximum speed. In addition, there will be multiple users that operate the equipment over the year. Therefore we established that an 85% profile user should be the baseline for estimating reliability.

User weight is an 85% profile person which is 235 lb. As a note, the worst case user weight is 350 lb.

Durability requirement is 37,500,000 cycles based on:

- The bracket is subjected to an average 5,000 cycles per hour
- The bracket has an average yearly usage of 1,500 hours of use
- The product is intended to last 5 years.

For the 85% profile in this case, we are considering the general population, but if the product is to be used by a professional football team, the 85% profile would be different. In establishing this baseline model to use, it is important to consider what the goal of the prediction.

The goal in this presentation is to evaluate whether the product will be suitable for a providing a R90 and R99 at C50, C70, and C90 confidence intervals for a life of 5 years.

Samples of bracket will be tested to failure under two test accelerated test loads and at an increase cycle rate with time to failure being monitored and recorded.

The time to failure data will be analysis by the Weibull distribution to determine its probability of failure at specific cycle time at each loading condition. Its horizontal scale will be used to plot cycles to failure and its vertical axis will provide the probability of expected failures at a various load. This will be done for each fatigue force.

The slope of each load force should be similar to verify that the same failure mode is being accelerated.

The 70% and 95% confidence intervals will be plotted and the results will be extrapolated to draw a stress versus cycles to failure to show how the results vary from the extrapolated from the Weibull curve fit. The curve developed at the accelerated loads will be extrapolated to 235 lb. to determine the number of cycles that would be applicable under normal usage.

Figure I - Test Termination

In addition, the effects of the confidence limits will be explored. Figure 1 illustrates the failure mode of the bracket. The test was terminated at the signs of a crack rather than waiting until the sample broke. The test method is shown in Figure 2.

Results

Load Level	Time to Failure, Cycles
1,100 lb.	103,000 113,000 233,000 132,000 142,000
900 lb.	484,000 651,000 396,000 552,000 688,000 461,000

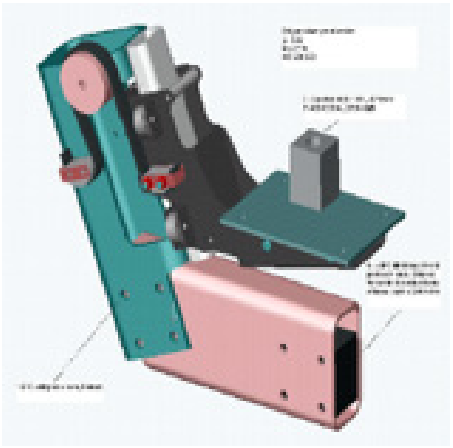


Figure II

Figure III
The basic Weibull plots show similar slopes indicating similar failure modes.

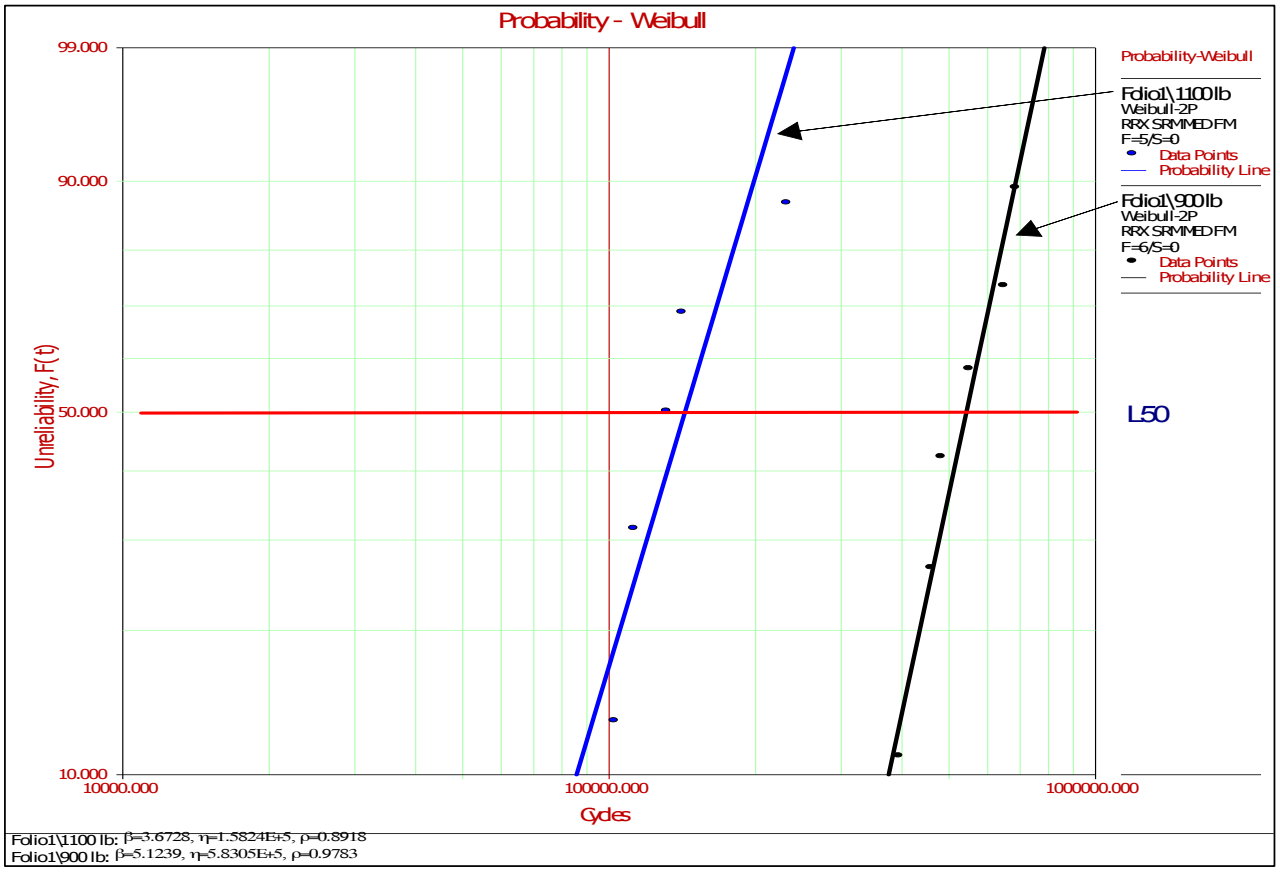


FIGURE IV
Weibull plots at 70% confidence.

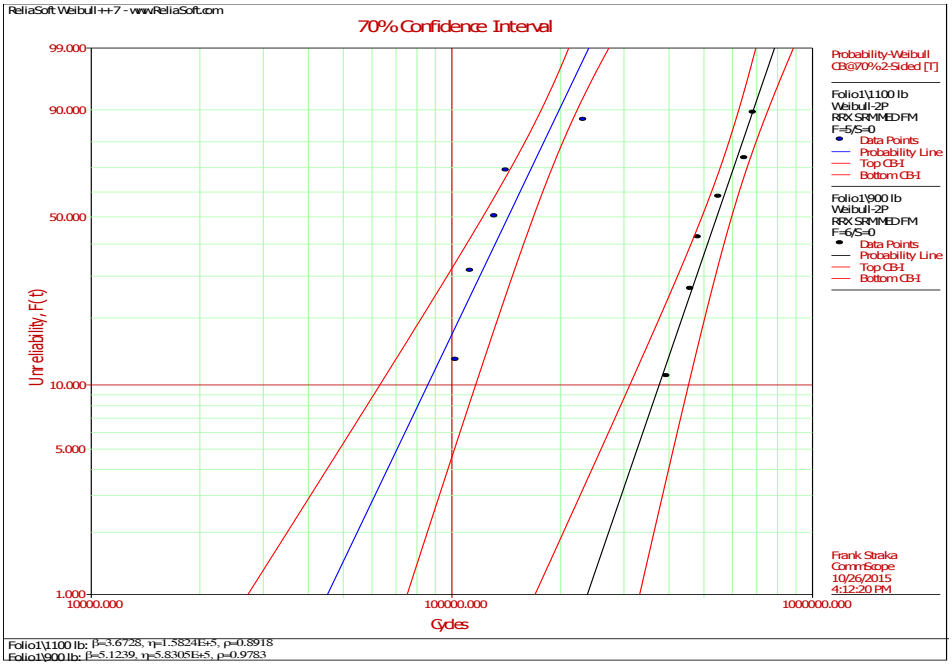
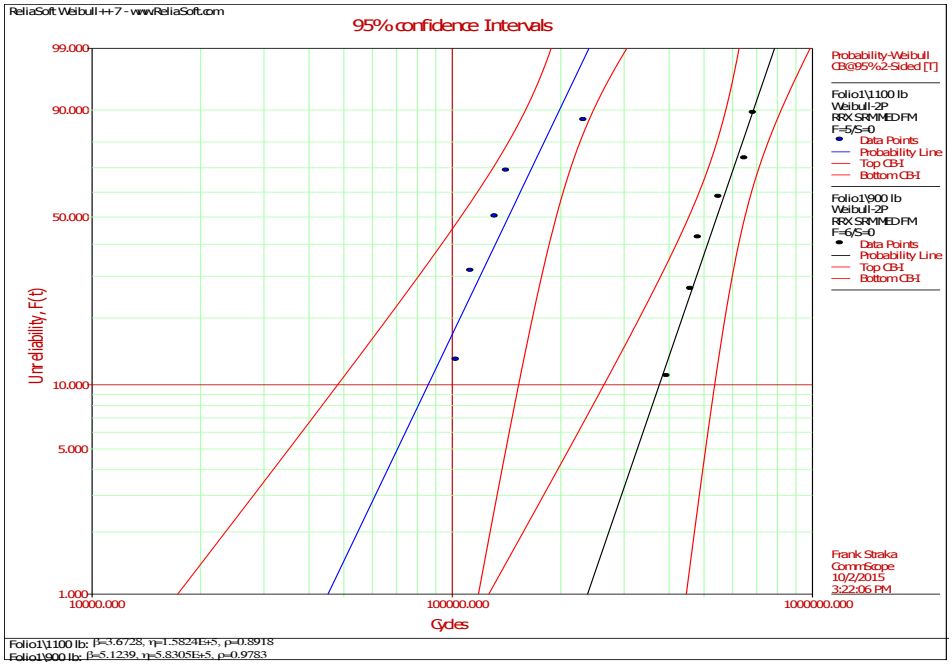


FIGURE V
Weibull plots at 95% confidence.



Note: Although one data point falls outside the confidence boundary and possibly may indicate another potential failure mechanism in the lower confidence intervals. Since it is no statistically significant at 95%, I have treated it as part of the same distribution for all confidence intervals although the failure mode is worth exploring.

From the plots, the following information (see Tables 2, 3 and 4) for the unreliability (L) for the number of cycles to failure at a given L can be documented.

L	Median Rank Regression (MRR)	
	1,100 lb.	900 lb.
	C501100	C50900
50	144,639	545,130
10	86,468	379,248
5	71,150	329,438
1	45,147	236,760

Table II

L	C70 Interval			
	1,100 lb.		900 lb.	
	C70L1100	C70U1100	C70L900	C70U900
50	123,612	170,154	497,100	604,200
10	63,500	117,737	315,470	458,395
5	48,967	102,274	261,000	415,820
1	27,283	75,519	172,007	333,026

Table III

L	C95 Interval			
	1,100 lb.		900 lb.	
	C95L1100	C95U1100	C95L900	C95U900
50	106,800	195,880	455,919	651,798
10	47,659	152,688	265,275	539,258
5	35,382	137,014	213,610	508,072
1	17,218	118,376	127,700	446,149

Table IV

From each of the previous tables, the cycles versus user weight was plotted to develop the appropriate graphs to illustrate this relationship. These are shown in Fig. 6 and 7.

Summary

The graphs show that the parts easily achieve the objectives at L1 or L1 criteria of 37,500,000 cycles.

As observed from the charts, the lower and upper confidence curves cross providing an ambiguous statistical meaning. Some thoughts on this:

1. The small number of samples used in testing which results in wide statistical confidence limits. This is observed for the C70 or C95 confidence intervals. It could have also resulted in the lines diverging.
2. The power law curve fit than will subject to nuances of the fit.

Generally this may not be known since the minimum life is the interest of testing and a statistical confidence limit is used to determine the minimum life. In these cases, the upper life is not considered. An improvement in prediction could be made with a larger quantity sample along with using a third force level to provide a better curve fit. This shows that one needs to proceed with caution when extrapolating results. ●

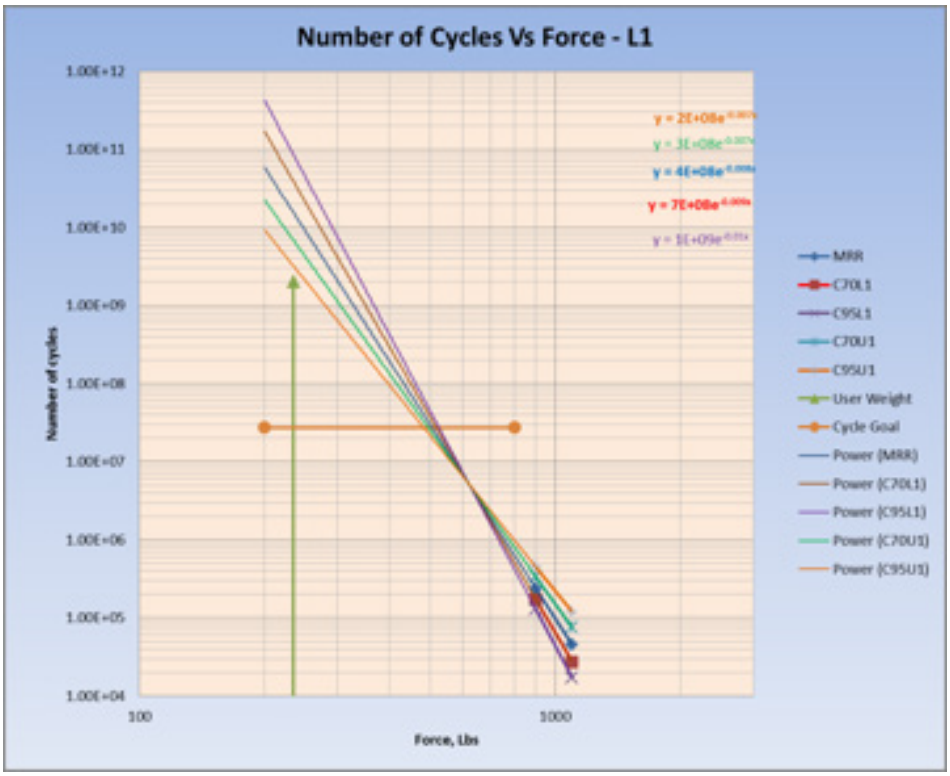


FIGURE VI

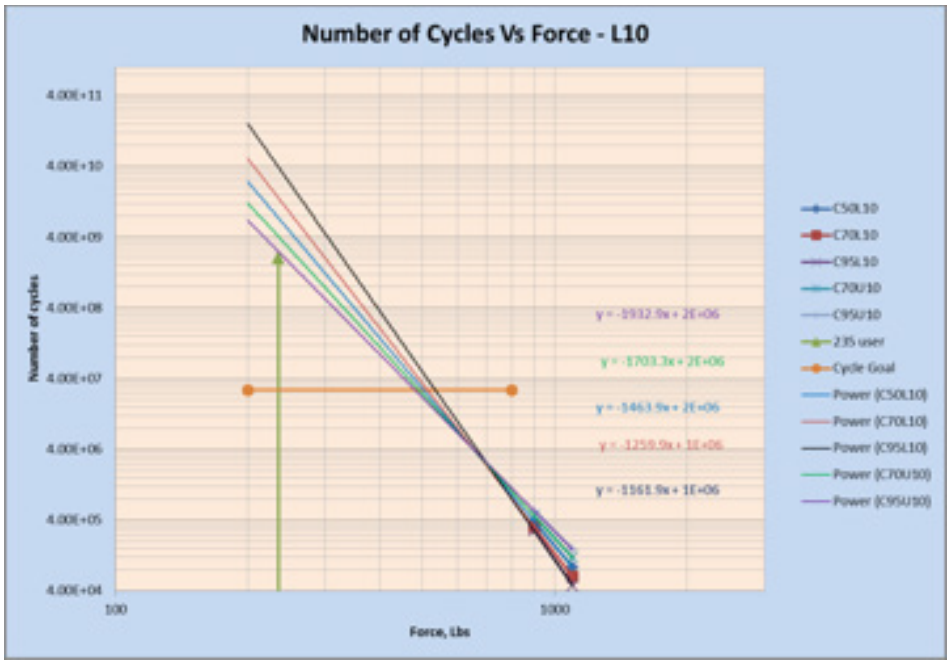


FIGURE VII

Design Failure Modes, Effects, and Criticality Analysis (D-FMECA) Process Explained

LOUIS J. GULLO

Abstract

This article describes the FMEA, FMECA and the Design-FMECA (D-FMECA) process. It explains the purpose and goals of the D-FMECA, and reasons for performing D-FMECAs and depicts the three approaches—functional, hardware, and software—to perform D-FMECAs. A new term, Additive Risk Priority Number (APRN) is defined and discussed in terms of the value to the analyst as compared to other methods for prioritizing failure modes for corrective actions when performing D-FMECAs.

Acronyms

FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
D-FMEA	Design Failure Modes, Effects, and Criticality Analysis
P-FMEA	Process Failure Modes, Effects, and Criticality Analysis
LRU	Line Replaceable Unit
CCA	Circuit Card Assembly
FRACAS	Failure Reporting, Analysis and Corrective Action System
RPN	Risk Priority Number
ARPN	Additive Risk Priority Number
SE	Severity Effect
PFO	Probability of Failure Mode Occurrence
PD	Probability of Detection

1.0 Introduction

Failure Modes and Effects Analysis (FMEA) is a complex engineering analysis used to identify potential failure modes, failure causes, failure effects and problem areas affecting the system/product mission success, hardware and software reliability, maintainability, and safety. A FMEA provides a structured process for assessing failure modes and mitigating the effects of those failure modes through corrective actions. When the FMEA is performed on hardware and in collaboration with the electrical circuit designer or the mechanical design engineer, it is very useful to effect design improvements. This collaboration is especially valuable for uncovering and resolving single-point failure modes that have an unacceptably high probability of occurrence or a critically severe failure effect that could cause personnel injury or high system repair costs due to the loss of system functionality. Elimination of these single point failures is the primary concern of the analyst performing a FMEA. If elimination of a single point failure is not possible, then design changes should be incorporated to reduce the severity of the failure effects or minimize the probability of occurrence of the particular failure mode.

Failure Modes, Effects and Criticality Analysis (FMECA) is an analysis of system or product similar to the FMEA, but with the addition of a quantitative analysis to assess the criticality of each failure mode. A FMECA is very useful when applied to a design for assessing the failure mode criticalities, comparing each failure mode criticality to the others, and ranking them together; or for determining the criticality relative to a benchmark criticality or threshold level.

2.0 Design FMECA

One type of FMECA, commonly called a Design FMECA (D-FMECA) is an

analysis of the design of a system or product performance, considering what happens when or if a failure occurs. The goal of a Design FMECA is to identify and prevent design-related failures, and strive for zero single point failures. This type of FMECA is performed by examining assembly drawings, part datasheets, electrical schematics, and specifications. The design FMECA does not include analyses of manufacturing-related failures, workmanship or maintenance induced defects, or random isolated incidences related to variations in assembly or component supplier build processes.

Another type of FMECA is the Process FMECA. What is the difference between a Process FMECA and a Design FMECA? The Process FMECA is a FMECA that analyzes the failure modes and failure causes related to the product manufacturing or maintenance processes. The Design (D-FMECA) analyzes the failure modes and failure causes related to the system or product design. Since this article focuses on D-FMECAs, further mention of P-FMECAs will not be included. P-FMECA is briefly mentioned here only to inform the reader that FMECAs are used for other purposes besides product design analyses.

2.1 Purpose of the D-FMECA

The purpose of the D-FMECA is to analyze a system/product design, to determine the results or effects of the system or product failure modes on the system/product operation, and to classify each potential failure according to its severity, frequency of occurrence and detection method. Each identified failure mode will be classified with a number that is used in the design process to assign priorities to the failure modes for design corrective actions.

The goal of a design FMECA is to identify and prevent design-related failures, and strive for zero single point failures. Some examples of design-related failures are failures that are due to:

- Incorrect or ambiguous requirements;
- Incorrect implementation of the design in meeting requirements;
- Unspecified parameters in the design that should have been specified to ensure the design works correctly;
- Inherent design flaws that should have been found during design verification testing;
- High electrical or mechanical stress conditions which are beyond the strength of the design (e.g., conditions that exceed design derating guidelines or manufacturer's ratings);
- Design process weaknesses; and
- Pprobabilistic pattern failures and systematic failures that are random isolated incidences related to design weaknesses.

Probabilistic pattern failures and systematic failures that are random isolated incidences related to design weaknesses may need further discussion. Examples of these types of design failures are intermittent random failure events, such as race conditions related to static or dynamic hardware or software timing, or incorrect usage of shared data or global variables. These design-related failures include defects in the specification and requirements. One type of timing failure mode, the race condition, may be prevented with properly worded requirements, such as synchronizing timed events and controlling the application of processor interrupts which occur asynchronously. If functional timing requirements and interface requirements are properly specified, timing and race conditions can usually be eliminated.

The D-FMECA is a living document during the development of the product or system hardware and software design. The value of the FMECA is determined by the early identification of all critical and catastrophic subsystem or system failure modes so they can be eliminated or minimized through design improvements early in development prior to production and delivery to the customer. It is important to continually update the data contained in the D-FMECA with actual failure modes and effects data from testing and actual field applications to keep pace with the evolving design so it can be used effectively throughout the development and sustainment phases of the product or system life cycle. Furthermore, the results of a D-FMECA are valuable for logistics support analysis reports and other tasks that may be part of an Integrated Logistics Support plan.

2.2 Three Approaches to D-FMECA

There are three approaches to a Design FMECA (D-FMECA): a functional approach, hardware approach and a software approach:

1. In the functional approach, each item is analyzed by its required functions or operating modes, or the outputs that it generates [3]. The failure modes of a system are analyzed for specification and requirement ambiguities and defects that have a high potential for system faults due to a lack of fault tolerant design architecture. Functional block diagrams are created to illustrate the operation and interrelationships between functional entities of the system as defined in engineering data, specifications, or schematics. This diagram will provide a functional flow sequence for the system and lower level functional blocks. Since this FMECA approach is highly dependent on complete and accurate product or system level requirements for conducting a thorough analysis,

the functional FMECA may also be called a requirement(s) FMECA. This type of FMECA may also be called a System Design FMECA, or an Architecture FMECA, or a Top-Level FMECA.

2. In the hardware approach, all predictable potential failure modes are identified and described [3]. Each of the part/component level failure modes and failure mechanisms are analyzed to determine their effects at the next higher indenture level, and at the product/system level. Actual failure analysis data that identifies the physics of the failure mechanism are useful in providing realistic data to the FMECA in terms of applicable failure modes and failure effects. In different contexts the Hardware FMECA is called by many other names, such as Electrical Design FMECA, Mechanical Design FMECA, Piece Part FMECA, or Component Bottom-Up FMECA to name only a few.
3. In the software approach, software design functions are analyzed. The Software Design FMECA includes analyses of software components, configuration items, modules and blocks that are analyzed during code walk-throughs and code reviews to determine potential failure modes such as static and dynamic timing issues and race conditions caused by probabilistic failure mechanisms that could lead to system/product effects [3, 9, 10]. All software errors found will be classified as bugs, faults or failures. Faults are bugs that are not detectable at the system level. Failures are bugs that are detectable at the system level. If software functions are analyzed a software FMECA is very similar to a functional FMECA.

2.3 The Design FMECA Process

A D-FMECA should be started early in the design process, when the design specifications have been written, but before drawings, schematics, and parts lists are created. The Functional D-FMECA is the type of D-FMECA that is usually performed at this time. The Functional D-FMECA is done from the top level requirements down to the lower level requirements to ensure the design requirements will incorporate features to handle mission critical failure modes and mitigate their effects. Fault tolerant capabilities and system sparing are the most common architectural approaches to handle mission critical failure modes and mitigate their effects. The concept of redundancy is the easiest fault tolerance implementation, but it may also be the most costly. The cost of redundancy depends on how much of the redundant capability is applied in spare mode and how much provides additional active capability.

During the execution of a D-FMECA, the analyst must identify all the causes of failure for a particular failure mode. Failure modes include one or many failure symptoms. Failure symptoms are the characteristics of the failure that define the failure at different levels, such as physical, electrical, mechanical, molecular, or atomic. Failure symptoms are failure effects at higher levels in the system or product configuration. There are multiple one-to-many relationships in this analysis. Each failure identified (e.g., failure to meet specification or process), may have one or more failure modes. Each failure mode may have are one or more causes and one or more effects.

After the initial top-down functional D-FMECA, the next D-FMECA that may be performed is the hardware D-FMECA. The phase in design when a hardware D-FMECA may be performed is the prototype phase or critical design phase. The hardware D-FMECA is performed on newly designed hardware, such as systems, enclosures and boxes, Line-Replaceable-Units (LRUs) and Circuit Card Assemblies (CCA), and component or piece part levels. The hardware D-FMECA is typically implemented at the assembly or circuit card level, but may also be implemented at lower levels of hardware, such as modules and complex electrical or mechanical components, or higher levels of assembly such as system or sub-system levels. This hardware D-FMECA is performed when the drawings, schematics and parts lists are created, but prior to building production hardware.

2.4. LRU Level or CCA-Level D-FMECA

The failure modes of an LRU or CCA include component or piece part level failure modes and their failure causes. In this D-FMECA, all parts are analyzed, looking at part failure modes involving functions and bus interfaces, and failure modes on pins such as opens, shorts, and low impedances for analog devices, and stuck at one or stuck at zero states for digital devices. The FMECA traces the effects of failure modes up the system hierarchy to determine the next higher effects and the end effect on system performance. This type of D-FMECA uses inductive logic (a process of finding explanations) on a "bottom up" system analysis.

2.5. Design FMECA Verification

One should verify failure modes and failure causes in the FMECA using data from a Failure Reporting, Analysis and Corrective Action System (FRACAS). When test or field data is not available, the second choice is engineering analyses, failure mechanism modeling, durability analysis and models, or physics of failure models.

Failure mechanism models, and the like, exist for many failure modes and failure causes. The failure mechanisms for electronic assemblies over their life are often associated with fatigue, corrosion, diffusion, wear out, fracture, to name only a few of the many possible types of failure mechanisms. These can be identified through engineering physics modeling and analysis.

3.0 Additive Risk Priority Number (ARPN)

The industry and military procedures on FMECA offer several different ways of determining the criticality of a failure mode. The Risk Priority Number (RPN) has been used extensively in FMECAs performed by analysts in the automotive and aerospace industries. Several of the references provided in this article refer to the use of RPNs [1, 2, 3, 4]; however, the method of calculating the RPNs in these references is slightly different from the method discussed here. Both methods rank the severity of effect, probability of the failure mode occurrence, and the probability of detection of the failure on a numeric scale. However, the referenced RPN calculation multiplies these three terms whereas we add them here. We call this calculation of the risk priority number an Additive Risk Priority Number (ARPN) to distinguish it from the multiplicative RPN in the references. The additive methodology was chosen as a simpler approach to calculating criticality and priority compared to the multiplicative method.

The ARPN is the sum of the Severity of Effect (SE), the Probability of Failure mode Occurrence (PFO) and the Probability of Detection of the failure mode (PD):

$$ARPN = SE + PFO + PD$$

Each of the 3 terms is assigned a number between 0 and 3 as shown in Tables 1 to 3. Note that these scales also differ from those used in the multiplicative RPN which range from 1 to 10 [1, 2].

Table 1 describes the method for assigning the Severity of Effect (SE). A minimal effect is a severity that results in minor damage, such as a cracked component or a discolored printed wiring board. A moderate effect is a severity with more physical damage beyond a minimal effect, such as a burned component or printed wiring board. A hazardous effect is a severity that could result in personal injury and excessive physical damage, such as a failure mode that results in a persistent flame.

Category	Effect Severity
0	No Effect
1	Minimal Effect
2	Moderate Effect
3	Hazardous Effect

Table I

Table 2 describes the method for assigning the Probability of Failure mode Occurrence (PFO). Remote means the probability of occurrence of the failure mode is extremely small, i.e., in the lowest range of the failure probability distribution. Slight means the failure mode is in the low range of failure probabilities within the failure probability distribution, such as the bottom 10% – 20% of the total distribution. Moderate means a probability in the 50% range of the distribution and high means a probability at the high end of the distribution where the occurrence of failure is extremely likely in a short period of time after operation starts. Exact probabilities are not presented here since the values are relative to the type of design being analyzed. For instance, analysis of a microcircuit may refer to a failure mode with a remote probability in terms of a failure per billion hours, while a complex system may refer to a remote probability in terms of a failure per 10 years.

Category	Probability of Failure Occurrence
0	Remote Probability
1	Slight Probability
2	Moderate Probability
3	High Probability

Table II

Table 3 describes the method for assigning the Probability of Detection (PD). High probability means failure detection is very likely to occur in a short period of time with a probability on the high end of the distribution. Moderate means a probability in the 50% range of the distribution. The definitions for Slight and Remote probability are similar to the descriptions for the terms in Table 2.

Category	Probability of Detection
0	Remote Probability
1	Slight Probability
2	Moderate Probability
3	High Probability

Table III

Each identified failure mode will be classified with an ARPN. ARPNs assist the designer in prioritizing the failure modes and the associated causes of these failure modes. The ARPN is used in the design process to assign priorities for product design or design process corrective actions. The ARPN determines which failure causes should be fixed immediately and which can be deferred. Risk mitigation techniques are developed to correct the high

risk single point failures first, to offset the risks, to reduce the risks, or to eliminate the risks (also known as risk avoidance). The design improvements might be planned as scheduled system/product enhancements incorporated at a later date or incorporated immediately, if severity warrants it. An ARPN limit may be set to a predefined threshold, such as 6, on a scale of 0 to 9. ARPNs are calculated for each failure mode, and compared to the ARPN limit, and a design change decision is made based on scoring of failure modes, such as a failure mode with an ARPN > 6, on a scale of 0 to 9, must be eliminated, or, as a minimum, its effects reduced.

The ARPN number is used to rank the potential weaknesses so that the team can consider more effective actions to reduce the incidence of failure modes for critical and significant characteristics, reduce process variation and accordingly make the process more robust. Regardless of the ARPN number, special attention should be paid to failure modes with a high severity number. The threshold for the ARPN number could be assigned at 6, out of a possible 9 score, so that any failure mode scored between 7 and 9 will be corrected immediately with a design change. Moderate ARPN failure modes, such as 5 to 6, are planned corrections later in the program. ARPNs between 2 and 4 are included on a watch list for collection of further data to support the need for immediate or planned corrective actions. ARPNs of 0 and 1 require no action.

3.1 ARPN Ranking

A Pareto chart is the preferred method to illustrate results for ranking the design change priorities and to reveal the "low hanging fruit," which are those failure modes to focus on that warrant design investments to prevent further life cycle cost exposures. This ranking of ARPNs with associated failure modes and failure causes provides a method to organize and plan improvements to the design, process or test and ultimately to improve the system/product reliability.

4.0 Final Thoughts

There are two reasons for performing a FMECA: to improve the system design reliability through design changes, and to learn about the design for documenting how the design reacts to failures. Performing an FMECA by itself does not improve the reliability of the design. The reliability is only improved when design changes are implemented that avoid failure modes, minimize the probability of failure mode occurrences, lessen the severity of failure effects and/or alter the architecture to incorporate fault tolerance features which may include functionality and circuit redundancy, and/or increase the system or product capability and efficiency of the design to detect, isolate, and recover from failure modes.

To truly impact design for reliability, influencing designers to improve their design using the FMECA methods must occur. The FMECA analyst should conduct open dialogue sessions with the system/product designers and other stakeholders in the product. The analyst should act as a facilitator to brainstorm ideas and capture all thoughts without passing judgment. The analyst should be able to gain valuable design information and data from the sessions to properly complete the FMECA, maintain points of contact for peer reviews, visibility and follow-up actions, engage stakeholders and promote teamwork through use of collaborative tools. ●

References

1. SAE J1739 (July 1994) "Potential Failure Modes and Effects Analysis in Design (Design FMEA and Potential Failure Modes and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) Reference Manual," Society of Automotive Engineers (SAE) International.
2. FMEA-3 (July 2001) "Potential Failure Mode and Effects Analysis (FMEA Third Edition), Automotive Industry Action Group (AIAG).
3. SAE ARP5580 (July 2001) "Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications," SAE International, July 2001.
4. IEC 60812 (January 2006) "Analysis Techniques for System Reliability – Procedure for Failure Mode and Effects Analysis (FMEA)," International Electrotechnical Commission (IEC), January 2006
5. Stamatis, D. H. (1995) Failure Mode and Effect Analysis: FMEA from Theory to Execution, American Society of Quality (ASQ).
6. McDermott, R. E., Mikulak, R. J., Beauregard, M. R. (1996) The Basics of FMEA, Productivity Press.
7. MIL-STD-1629A (November 1980) Failure Modes Effects and Criticality Analysis (FMECA).
8. IEEE 1413.1-2002, (February 2003) IEEE Guideline for Selecting and Using Reliability Predictions Based on IEEE 1413.
9. Goddard, P. L. (January 2000) "Software FMEA Techniques," Proceedings of the Annual Reliability and Maintainability Symposium, pp. 118-123.
10. Ozarin, N. and Siracusa M. (January 2003) "A Process for Failure Modes and Effects Analysis of Computer Software," Proceedings of the Annual Reliability and Maintainability Symposium.
11. Gullo, L. and Raheja, S. "Design for Reliability," published by Wiley in 2012.

About this Issue's Authors

Michail Bozoudis serves as a Senior Engineer in the Hellenic Air Force, stationed in Athens, Greece. During his 23-year military career he held senior positions in the fields of maintenance, quality control, cost engineering, airworthiness, ILS, data analysis, and system life cycle management. He holds a B.Sc. in Aeronautical Engineering, a M.B.A. in Business Administration and a M.Sc. in Applied Statistics.

Dr. Christopher V. Feudo is the Program Director for the Nirvana Project, an innovative approach to protecting all data against all threats. He was previously, the President of the University of Fairfax, the only online 100% focused Cyber Security University. With more than 20 years of extensive experience in the CyberSecurity field, Chris has served as a participant and Chair in a number of Presidential sub-committees, an operational senior executive within DoD, Lockheed Martin, EDS/HP, Edgewater, and Secureant, an executive speaker and an author. Dr. Feudo is also a DAWIA certified Program Manager, co-patent holder, a recipient of the Vice President of the United States Hammer Award and the Vice Chief of Staff U.S. Army Medallion. Chris retired from the U.S. Army where he served as an Airborne, Ranger and Special Forces Officer. In 2006, Dr. Feudo was selected as one of four Presidential candidates for the position of Cyber Security and Telecommunications Assistant Secretary at the Department of Homeland Security. He is a graduate of Boston Latin High School, earned a B.S. in Engineering from West Point, a M.S. in Computer Science at the Naval Postgraduate School, and a Doctorate of Science in Computer Science from The George Washington University.

Frank Straka has been involved in the Quality & Reliability of products for over 25 years. This experience covers the testing and analysis of electronic hardware, software, and mechanical products to evaluate their performance and reliability. He has worked in RF design, RF filters, product safety, consumer electronics, commercial and consumer exercise equipment, and the telecommunications industries.

Mr. Straka's responsibilities have included: Reliability program management; Accelerated test methods for electronics, mechanical, and software systems; Reliability Growth; Root cause analysis and corrective action; DFMEA and PFMEA; Reliability predictions; Environmental testing; and statistical methods.

Mr. Straka has a Bachelor of Science degree in Electrical Engineering from the University of Illinois and a Master of Business Administration from Northwestern University.

Mr. Straka is ASQ certified as a Reliability Engineer, Quality Engineer, and Quality Auditor. He is certified as a six sigma black belt and is a registered professional engineer. He is currently employed as Reliability Manager for CommScope, a manufacture of telecommunication components for the mobile market.

Lou Gullo works for Raytheon Missile Systems, Engineering Product Support Directorate (EPSD), Reliability and System Safety Engineering Department, which is located in Tucson, AZ. He is a member of the technical staff leading an Prognostics and Health Management (PHM) research project and Software Reliability activities at Missile Systems. He has over 30 years of experience in military, space and commercial electronic systems programs. He previously worked for Raytheon Integrated Defense Systems, Honeywell, Texas Instruments, Flextronics, Tyco/Sensormatic, and the US Army. He is a retired US Army Lieutenant Colonel. Lou has a BS degree in Electrical Engineering from the University of Connecticut in 1980.

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

Editor-in-Chief: James Rodenkirch
Managing Editor: Russell A. Vacante, Ph.D.
Production Editor: Phillip 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, James Rodenkirch at rodenkirch_llc@msn.com for additional guidance.

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