The Journal of Reliability, Maintainability, and Supportability in Systems Engineering

Summer 2018

Table of Contents Summer 2018

Editor's Note

John Blyler

Quotes of Interest in this issue:

- *"As component engineering has progressively advanced … to encompass a robust element of reliability, a paradigm shift has occurred in how complex systems fail."*
- *"…Certain defects, not removed through pre burn-in statistical screening, will become enhanced through the accelerated aging…"*
- *Two consumer sectors still at the early stage of digitalization are the avionics and automotive spaces, in part due to stringent safety, reliability and certification requirements.*
- *"…these products could be modified to perform below expectations or even fail, as well as to facilitate state or corporate espionage…"*

This issue of the RMS Journal offers something for everyone, from system-related failure prevention techniques and component process reliability improvements to digital threads-twins in reliability mandated markets and challenges inherent in our global supply chain.

We start with a look at advancements in risk modeling for complex systems. A new approach is offered based on a Time Based Failure Flow Evaluator (TBFFE), which is needed to account for, "variable probabilities in initiating events over the duration of a system's operation." Such an approach addresses the way that today's complex systems fail in contrast to traditionally well-understood component reliability and failures.

For those who must focus on component reliability, we have a detailed case study for tantalum capacitors in mission critical applications. The existing process to develop and qualify these components raises questions

whether Weibull still represents the best fit for today's near zero-defect applications. An improved approach is used to deal with certain deficiencies, in particular, early life failures and the potentially damaging application of excessive voltage in tantalum capacitors. This paper will discuss modifications to the existing burn-in process, techniques for DC leakage screening, and improvements in process monitoring.

The next article shifts from component reliability testing and manufacturing processes to the ongoing system-level digitalization of both the manufacturing and design processes. The concepts of a digital thread and twin are defined in the context of both the physical and virtual systems. The hope is that by understanding these basic concepts and examples of digitization that the activity of "engineering" will be brought back into system modeling and even systems engineering.

Our final offering considers the challenges faced by our global supply chain management (SCM) system. After a definition of terms, this paper discusses the increases in software supply chain attacks related to developing technologies such as fifth generation (5G) mobile network technology and the Internet of Things (IoT).

I hope you find this issue to be both interesting and educational. As always, please don't hesitate to share your comments and potential future articles with me via the email below. Cheers!

—John

Risk Modeling of Variable Probability External Initiating Events in a Functional Modeling Paradigm

Jose Dempere
Nikolaos Papakonstantinou
Bryan O'Halloran
Douglas L. Van Bossuyt
(Corresponding Author)

Summary & Conclusions

As component engineering has progressively advanced over the past 20 years to encompass a robust element of reliability, a paradigm shift has occurred in how complex systems fail. While failures used to be dominated by 'component failures,' failures are now governed by other factors such as environmental factors, integration capability, design quality, system complexity, built-in testability, etc. Of these factors, environmental factors are some of the most difficult to predict and assess. While test regimes typically encompass environmental factors, significant design changes to the system to mitigate any potential failures is not likely to occur due to the cost. The early stages of the systems engineering design process offer significant opportunity to evaluate and mitigate risks due to environmental factors.

Systems that are expected to operate in a dynamic and changing environment have significant challenges for assessing environmental factors. For example, external failure initiating event probabilities may change with respect to time, and new discovered external initiating events may also be expected to have varying probabilities of occurrence with respect to time. While some industry standard methods such as Probabilistic Risk Assessment (PRA) [3] and Failure Modes and Effects Analysis (FMEA) [4] can partially address a time-dependent external initiating event probability, current methods of analyzing system failure risk during conceptual system design cannot.

We have developed the Time Based Failure Flow Evaluator (TBFFE) to address the need for a risk analysis tool that can account for variable probabilities in initiating events over the duration of a system's operation.

This method builds upon the Function Based Engineering Design (FBED) [19] method of functional modeling and the Function Failure Identification and Propagation (FFIP) [9] failure analysis method that is compatible with FBED. Through the development of TBFFE, we have found that the method can provide significant insights into a design that is to be used in an environment with variable probability external initiating events. We present a case study of the conceptual design of a nuclear power plant's spent fuel pool experiencing a variety of external initiating events that vary in probability based upon the time of year. The case study illustrates the capability of TBFFE by identifying how seasonally variable initiating event occurrences can impact the probability of failure on a monthly timescale that otherwise would not be seen on a yearly timescale. Changing the design helps to reduce the impact that time-varying initiating events have on the monthly risk of system failure.

1 Background

There are several methods required to understand TBFFE and its background; one commonality all of those methods have is that they do not easily model failure probability shifts caused by time-based initiating event probabilities. This section reviews related methods and demonstrates the novelty of the TBFFE method presented in this paper.

1.1 Functional Modeling

Functional modeling connects a series of inputs, outputs, flows, and functions together that transform the inputs into outputs [19]. This tool is useful for modeling systems at a variety of fidelities. A common functional modeling implementation is FBED [19]; we use FBED as the basis for our method. Functional modeling's robustness makes it a useful tool for many kinds of systems modeling [12, 13, 14]. However, functional modeling is not useful for the stated goal of this method because it does not model failure.

1.2 Function Failure Design Method

The Function Failure Design Method (FFDM) is the groundwork upon which TBFFE is built [7]. Within FFDM, all functions are given a list of potential failures, and the probability of that failure is then cataloged for every function in the functional model. Next, the probability of a functional model failing can be calculated in much the same way as a failure is calculated in PRA—via cutset development and calculation. The limitation of FFDM is that there is no way to modify a risk's chance of occurring over time without creating a new functional model.

1.3 Function Failure Identification and Propagation

FFIP is an extension of the functional modeling theory underlying FFDM [9]. Instead of utilizing a table to quantify the possible failures, FFIP analysis iterates through failures of possible functions and follows the failure flow until it exits the system as an output. This method allows for a user to see how a failure state transmits across a complex system and whether or not it ultimately poses a major risk to the system. While the addition of flows adds the concept of failure propagation to a system modeled using functional modeling, FFIP does not include time-based failure probabilities.

1.4 Related Functional Model-Based Methods

There are various authors in multiple fields that have attempted to address the subject of applying time-variable risk analysis, but few of them have addressed functional modeling. For instance, Hutcheson et. al. fit failure modes to functions during prototypes through a time-informed lens [7]. While Hutcheson's method creates a certain amount of flexibility for modeling various stages of a mission when a system may be in different configurations, the method does not encapsulate different rates of change [6]. Another related method is a semi-functional nonparametric

analysis by Aneiros-Perez that attempts to use a series of past values as predictors for later behavior [1]. This method does not match the needs of functional modeling because its nonparametric analysis methods are well beyond the scope of a basic functional model or FFDM methods. Dynamic risk assessment techniques, such as those described by Siu, are applicable to multiple engineering systems, but they lack a functional framework and focus instead on the use of PRA and similar systems [15].

The final related method discussed here was developed by Woltjer et. al. and presents a functional analysis meant to react to shifting airplane conditions [19]. However, there are issues with this method because it does not account for multiple potential failure conditions and uses velocity components to resolve a time-based issue so that planes enter in the right order to a flight pattern rather than utilizing time to modify the failure velocity. In essence, Woltjer et. al.'s analysis method is, much like Hutcheson's, meant to change dynamically with time rather than take into account time from a risk analysis perspective so that probabilistic risk of failure may be determined.

1.5 Probabilistic Risk Assessment

PRA is a method that exists outside of the functional flow modeling methods that have been discussed so far. PRA usually is implemented at the component level rather than the functional level [6]. The focus of the PRA method is to create a series of cutsets based on initiating events to create a series of potential failure pathways and their associated probabilities.

PRA's use in nuclear power plants has resulted in its modification to deal with time-dependent issues unique to that specific use case [11]. In particular, the exploration of core damage frequency as a surrogate measure to reach particular safety goals is of interest when discussing time-varying risk mitigation methods. This method focuses on whether or not changes to a reactor are allowed by evaluating the frequency of reactor core damage.

1.6 Related Physics-of-Failure and Parametric Analysis Methods

Despite the limitations of the previously discussed methods, engineers do have various tools to evaluate time-dependent failure probabilities in a variety of contexts—however, the usefulness of these methods to an engineering team analyzing time-varying external initiating events is debatable. One such discipline is physics-of-failure mathematics. Physics-of-failure mathematics represents the identification and analysis of the physical causes for the failure of a particular component and then modeling the resulting data to develop a probability density function along a system's lifetime [8]. While this approach is useful for looking at the probabilities of failure that happen within any particular component, the approach does not contain a methodology for design teams to act on the data. It is primarily a statistical method, not a design method.

Another methodology used to determine risk of failure is parametric analysis which is a statistical technique used when the unknown parameters of a particular component's longevity are populated with random values and a distribution is made of the resultant variables. This approach has many implementations, and has been integrated both in PRA analysis as well as in time-dependent probabilities of failure [5, 2]. However, there are certain issues with this approach—parametric analyses require the population of a data set to be developed through a tool such as Monte Carlo analysis, which can lead to a high computational expense when the methodology is applied to a more complex functional framework.

2 Methodology

TBFFE is a risk quantification method used to analyze complex, cyber physical systems during systems engineering design. This method focuses primarily in early systems engineering design where systems have the opportunity for significant configuration changes with minimal cost (both monetary and

development time). The goal of this method is to inform the system designer and systems engineer on predominate risks that may be realized during the system's life cycle, and thus, the method systematically analyzes all known or foreseeable risks to the system.

The results of TBFFE can be used to enhance a system design by reducing its risk of failure. The type of results produced by TBFFE include the systems' functional risk, which combines failure probability with the loss in functional health, tied to an initiating event. The results are presented across time (e.g., per month in the following case study) to represent heightened risk during specific time periods. An example of solutions to an unacceptable risk could include a design configuration change where the failure propagation has a behavior that renders the system less susceptible to the specific initiating events being analyzed.

A key difference from other risk methods surveyed earlier in this paper is that TBFFE uses discrete time-based failure probabilities with short time scales to more accurately model the external initiating events caused by natural environmental cycles and related factors. Typical failure probabilities are modeled on an annual basis; however, we analyze failure probabilities either monthly (as in the case study), daily, or even hourly. The discretization depends on the fidelity of the data used to build the probability values. For example, when assessing the risk of failures due to storms, failure probabilities would depend on the occurrence of storms in the local environment. If data is recorded in storms per month, the discretized failure probabilities will be monthly.

TBFFE is a process-oriented methodology that has several well-defined steps. These steps are meant to guide a design team from a basic functional model to a complete time-dependent representation of all potential points of failure that can affect a system.

2.1 Step 1: Functional Model Creation

The first step is to create a functional model based on the initial system architecture. The initial system architecture is usually a body of work developed by the system design team or a system architect and ranges across design requirements, sketches, blueprints, flowcharts, reliability block diagrams, as well as piping and instrumentation diagrams. In the absence of such existing work, an experienced system design team might instead opt to generate a native FBED [8] from scratch based on the desired system inputs and outputs given to the team.

2.2 Step 2: Initiating Event Identification

After creating a functional model, the team must note potential initiating events that may cause a failure. Finding initiating events in TBFFE is similar to the method used in PRA. For TBFFE the, designers are encouraged to consider external and internal initiating events. External events are those which originate outside the system, such as weather or debris. After compiling a list of external events, designers then go through the system and identify potential internal initiating events, such as mechanical wear, fire, internal flooding, or an electrical bus failure.

2.3 Step 3: Time-Dependent Initiating Event Identification

After developing a list of initiating events, the design team then classifies each event as time-dependent or independent. Those events which are based on seasonal phenomena, weather events, or events of variable strength such as storms are considered time-dependent.

For each time-dependent initiating event, there must be a particular profile to how the probability of the initiating event occurring increases or decreases over the course of a year (or other time increment that is normally analyzed across for the specific system in question). Each initiating event should be analyzed for how the probability of the initiating event occurring increases or decreases. A practitioner can choose to model certain initiating events either through a continuous function or through a discretized, step-wise function. Contin-

uous functions best serve events like storms where there is an identifiable period of peak intensity followed by a gradual drop-off. Typically, a systems design team is limited by the discretization of available data. For instance, engineers may have access to thorough meteorological data for their region that covers several days, or they may only know that storms occur more frequently over a particular range of months out of the year. Another important aspect to cover is how a system's probability of failure is affected by long-term or short-term forecasts. As an example, the engineering team may know that a seasonally-affected failure is only possible during certain hours of the day (such as the position of the sun affecting certain sensors only certain months of the year). As a rule of thumb, systems design teams are encouraged to account for short-term forecasts if they represent a change in probability greater than a standard deviation from their given probability of risk. Changes of less than one standard deviation will likely be inconsequential as compared to other factors within the risk analysis during the conceptual design process such as design, model, and data uncertainty. The result of the data acquired by the engineers will be similar to a Bayesian statistical model, but dependent on time.

In the TBFFE method, the design team is presumed to have existing probability of failure (per year or unit of time used for the particular system) as well as more discrete and detailed data for initiating events. The existing probability of failure divided by the unit of time for the overlay data is the baseline probability. If a design team has a yearly probability of failure by storm, and monthly values for frequency of storms in their region, then the design team will divide the yearly probability by twelve. The probability data that the design team has will then resolve itself into a function that shows frequency over time. In the case of the storm example, the systems design team will be able to chart the per-month frequency of storms over the year. As a verification step, the overlay data can be scaled such that, when combined, its value equals the existing yearly frequency of occurrence of the initiating event.

Step 4: Analyze Failure Propagation in the System

Once the various initiating events have been given a time-dependent profile, a probability of failure for each function within the model can be constructed. Both time-dependent and time-independent initiating events represent causes of failure that can map to particular functions. The systems design team can assign various causes of failure to individual functions. A function's probability of failure is the OR probability of any particular event occurring. By calculating the function's probability of failure at each time step, the design team develops a time-dependent failure profile for each function. Doing this for all functions allows the design team to have a FFIP model that the team can look at through a temporal lens, which allows the team to identify peak risks for particular functions.

Step 5: Design Iteration or Retrofit the System

By analyzing the various probabilities of failure present at particular time steps, the design team can begin to optimize the system design from a risk-of-failure perspective. Starting with functions crucial to the system's operation, the designers can look at local maxima of failure probabilities for a given function. Functions that exhibit the highest risk across any period of time can then be marked as at-risk. By identifying the initiating event or events responsible for this heightened state of risk, systems designers can focus on mitigating the probability of those initiating events happening, potentially by including specific functions or components that are used specifically in times of heightened risk. Starting with the highest risk functions, designers can continue to mitigate risks within the constraints of time, complexity, cost, etc. Once optimizations are complete, they can then iterate through the previous step to compare how their design has improved.

3 Case Study

In this section, we present a case study that demonstrates TBFFE and its capabilities. A representative example was created of the potential applications in a nuclear power context specifically for this paper. Note that we have intentionally fictionalized probability data and plant design, and explicitly do not recommend using the results of this case study in a real-world application. The case study is demonstrative of the method and is intentionally not directly applicable to a specific nuclear power plant. In this example, a new nuclear power plant somewhere on the East coast of the United States is being designed. The engineers are working on designing a spent fuel pool where spent fuel rods will be housed until the rods are cool enough for dry cask storage and disposal. Consequently, the fuel pool's main purpose is to cycle hot water to a system of heat exchangers to continuously maintain the temperature of the water in the pool at acceptable levels. The region the plant is being constructed in is prone to stormy weather, as well as seasonal algae blooms. The plant is planned to have one internal loop of water exchanging heat to the ocean. The design team decides to utilize TBFFE to anticipate and mitigate time-variant risks due to these unique conditions.

3.1 Step 1: Functional Model Creation

The systems engineering team first creates a functional model (see Figure 1) using the FBED functional modeling method. This functional model represents the baseline design prior to any iteration or redesign. At this stage, the team has already decided that they wanted to include multiple redundant systems; three sets of motors that power three sets of pumps that move the water in the primary pool, and three different heat exchangers are available to remove heat from the pool and route the heat to the ocean. The pumps are designed to begin operation one after the other, in the event of failure, while the heat exchangers are designed such that any one of the heat exchangers can transfer heat efficiently enough to keep the system

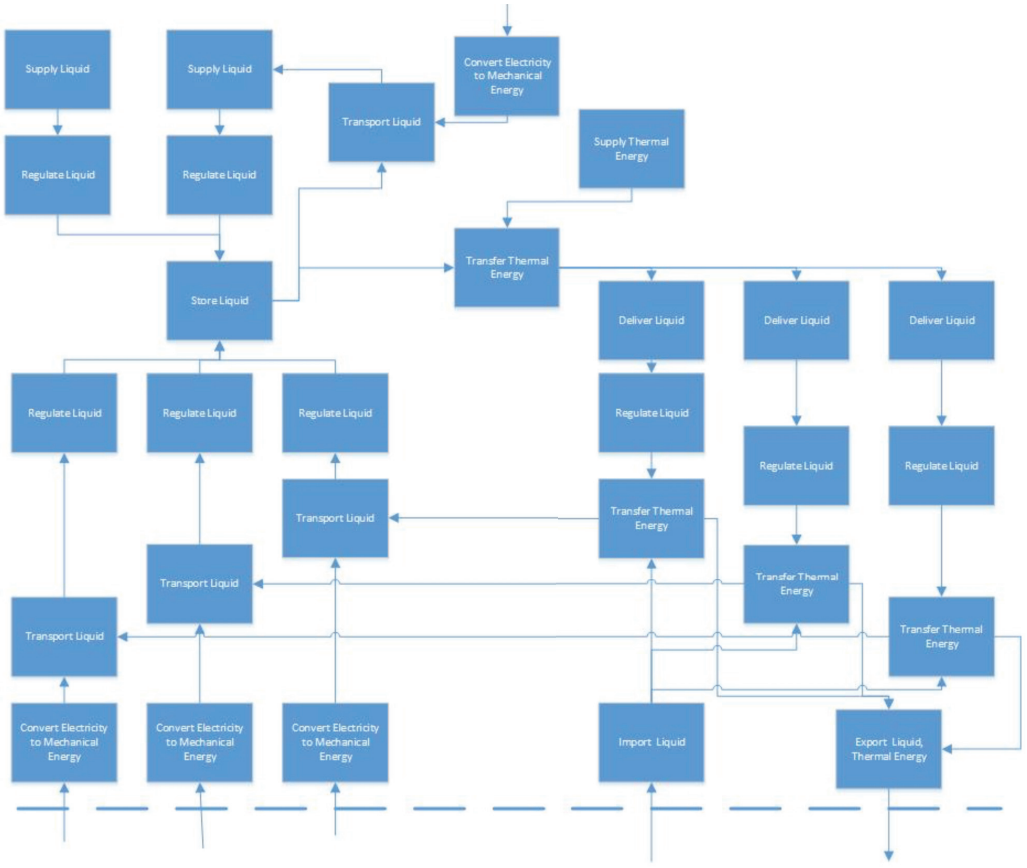


Figure 1. Functional model of a spent fuel pool.

operating nominally.

Initiating Event	Prob/Year
IE_MechanicalFailureCondenser	0.003
IE_Algae	0.004
IE_MechanicalFailureValve	0.001
IE_MechanicalFailurePump	0.005
IE_MechanicalFailureMotor	0.002
IE_Storm1	0.003
IE_MechanicalFailureValve	0.001
IE_MechanicalFailurePipe	0.003
IE_Storm2	0.002
IE_MechanicalFailureTank	0.0005

Table 1. List of initiating events for spent fuel pool used in the case study. Note that items that are italicized are time variant in their probabilities. The initiating events are presented here as an averaged yearly probability statistic. See Tables 2 and 3 for further details on these events.

3.2 Step 2: Initiating Event Identification

Once the functional model is complete, the systems engineers next consider potential initiating events and research the probabilities of occurrence until the systems engineers have a list of initiating events they feel is complete (see Table 1). The systems engineers first identify external failures like electrical storms shorting out motors or algae blooms clogging up the intake ocean water to the heat exchangers. Next identified are the internal failures such as mechanical wear within the machines.

3.3 Step 3: Time-Dependent Initiating Event Identification

Once the systems design team has a list of potential initiating events, the team can go through each initiating event and classify them as either time-variant or time-invariant. The team quickly recognized that algae blooms, electrical failures due to storms affecting the pumps, and heat exchanger failures due to storms affecting the intake of secondary water as significant initiating events that have a time-varying probability of occurrence. The reason for this is simple: both algae blooms and storms are events that occur seasonally, with significant change in event frequency occurring depending on the month.

Having identified which initiating events are time-dependent, the team next determines what data is available to better characterize the identified initiating events from a time basis. At this point, the team has finished researching initiating events and are able to use yearly probabilities of occurrence for all of the initiating events, as well as on-demand failure probabilities for all components. To acquire more detailed information on the behavior of the spent fuel cooling pool system, the team realizes that a monthly time step is appropriate for the external initiating event analysis. For storms, the systems engineering team determines the monthly number of storms that have historically occurred in the area where the nuclear reactor and its spent fuel cooling pool will be built. On the other hand, when researching the propagation of the algae the design team knows to be problematic, the team is restricted to data from marine biologists that forecast algae blooms to be most prevalent in the months of July to October and otherwise not present in the area. Knowing this, the design team creates a set of Boolean values corresponding to each month. Knowing the yearly probability of failure for the heat exchangers being installed for the spent fuel cooling pool due to storms and algae (as well as pumps failing due to storms), the team is able to develop the information found in Tables 2 and 3 to calculate the monthly probability of each initiating event occurring. Specifically, the annual failure rate for algae is evenly distributed across the months of May to October. Similarly, the annual failure rate for storms is proportionately distributed across the year based on the number of storms in each month (Storm for January: 0.03 x 10/526 = 5.7E–05 fails/month).

3.4 Step 4: Analyze Failure Propagation in the System

The team then generates cutsets based on the functional model of what possible failures could

occur based on the propagation of certain components failing when called upon to function. Table 4 shows the yearly probabilities of failure for ten generated example cutsets. Of the ten cutsets, four involve time-variant initiating events. Table 5 is then generated to track the monthly probabilities of failure. Tables 4 and 5 are generated based on the probability of the component failures required to cause the system to fail.

Available Monthly Frequencies

Month	Storm	Algae
1	10	0
2	5	0
3	7	0
4	12	0
5	22	1
6	35	1
7	77	1
8	110	1
9	96	1
10	80	1
11	50	0
12	22	0

Table 2. Monthly frequency values for storms as well as yes/no values for algae presence in the oceans. This data is utilized by the engineering team to produced scaled monthly probabilities, shown in Table 3.

Monthly Probabilities (probability of failure per month)

Month	Storm	Algae
1	5.7E-05	0
2	2.85E-05	0
3	3.99E-05	0
4	6.84E-05	0
5	0.000125	0.000667
6	0.0002	0.000667
7	0.000439	0.000667
8	0.000627	0.000667
9	0.000548	0.000667
10	0.000456	0.000667
11	0.000285	0
12	0.000125	0
Total	**0.003**	**0.004**

Table 3. Monthly Initiating Event Probabilities of Occurrence.

3.5 Step 5: Design Iteration or Retrofit the System

Based on analyzing the available data, the design team notices some statistically significant spikes in the probability of failure. For example, the team discovers from the cutsets that the probability of heat exchanger failure due to storms is highest in August, as is the probability of an electrical failure. Consequently, the team realizes that the system could be redesigned to mitigate the risk of failure during those months. For example, the team may decide that from July to October, the system could use a cooling pond rather than directly using the ocean to prevent both algae blooms and flotsam created by storms from clogging up the heat exchangers. Similarly, the design team realizes that backup generators could be kept on hot standby during the high risk months to lessen the risk of an outage caused by electrical storms. Beyond these specific seasonal improvements, the team also notices that an emergency cooling water pipe could be implemented that goes from the water tanks to the secondary loop to ensure that heat removal can continue in the case of an inlet water pipe clog. From there, the team is able to

Available Monthly Frequencies

Cutset No.	Prob (freq)/ year	Cutset
1	4.00E-03	IE_Algae, Import Liquid, Transfer Thermal Energy, Transfer Thermal Energy, Transfer Thermal Energy, Export Liquid/Thermal Energy
2	3.00E-09	IE_Storm1, Transfer Thermal Energy Transfer Thermal Energy, Transfer Thermal Energy, Export Liquid/Thermal Energy
3	1.80E-08	IE_Storm2, Convert Mechanical Energy to Electrical Energy, Transport Liquid, Regulate Liquid, Transport Liquid, Regulate Liquid, Transport Liquid, Regulate Liquid, Store Liquid, Transfer Thermal Energy
4	3.20E-08	IE_MechanicalFailureMotor, Convert Mechanical Energy to Electricity, Convert Mechanical Energy to Electricity, Convert Mechanical Energy to Electricity, Transport Liquid, Transport Liquid, Transport Liquid, Store Liquid, Transfer Thermal Energy
5	6.00E-08	IE_MechanicalFailurePump, Transport Liquid, Regulate Liquid, Convert Mechanical Energy to Electricity, Transport Liquid, Regulate Liquid, Transport Liquid, Regulate Liquid, Store Liquid, Transfer Thermal Energy
6	1.60E-08	IE_MechanicalFailureValve, Regulate Liquid, Convert Mechanical Energy to Electricity, Transport Liquid, Regulate Liquid, Convert Mechanical Energy to Electricity, Transport Liquid, Regulate Liquid, Store Liquid, Transfer Thermal Energy
7	1.00E-09	IE_MechanicalFailureValve, Regulate Liquid, Deliver Liquid, Transfer Thermal Energy, Deliver Liquid, Transfer Thermal Energy, Transfer Thermal Energy
8	3.00E-09	IE_MechanicalFailurePipe, Deliver Liquid, Transfer Thermal Energy, Deliver Liquid, Transfer Thermal Energy, Deliver Liquid, Transfer Thermal Energy
9	6.00E-09	IE_MechanicalFailureExchangers, Transfer Thermal Energy, Regulate Liquid, Deliver Liquid, Transfer Thermal Energy, Deliver Liquid, Transfer Thermal Energy
10	6.00E-09	IE_Storm1, Transfer Thermal Energy, Deliver Liquid, Transfer Thermal Energy, Regulate Liquid, Deliver Liquid, Transfer Thermal Energy

Table 4. Cutsets for yearly failure probabilities.

Cutset 1

Month	Monthly Probability
1	0
2	0
3	0
4	0
5	6.67E-04
6	6.67E-04
7	6.67E-04
8	6.67E-04
9	6.67E-04
10	6.67E-04
11	0
12	0
Yearly Probability	**4.00E-03**

Table 5. Monthly probability of algae bloom creating a failure event as described in Cutset 1.

create new, lowered monthly probability profiles and iterate further through the system design to achieve a desired risk profile for the system.

4 Results & Discussion

To better demonstrate the full capabilities of the TBFFE method when applied to iterative design, the authors of this paper developed a tool based on a Universal Modeling Language (UML) [10] backend that does the work of generating cutsets automatically based on the functional model and using the TBFFE method. By implementing functional modeling in UML, defining critical functions that cannot be interrupted, and providing a per-month list of the probability of initiating events, the tool runs through all cutsets that result in the failure of the system and then calculates the overall risk of

failure applied on the given timescale. This tool enables designers to use TBFFE even in scenarios that involve rapid iteration. In the spent fuel pool case study, the critical function was defined as the transfer of heat out of the water in the spent fuel pool. Figure 2 shows the resultant UML functional model, and Figure 3 shows the results of the overall risk analysis.

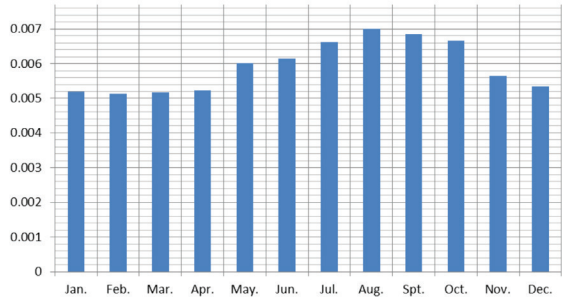


Figure 2. TBFFE Tool Implementation.

From these results, it is possible to see how the resolution in the risk of failure afforded by creating monthly probabilities is useful to systems design teams. Risk profiles can spike depending on the month; however, sometimes yearly probabilities are all that is available to an engineering team in databases for nuclear power plant failure events, and seasonal occurrences like storms or algae blooms are often unique to a region. The systems design team is best served by fitting local data to yearly probabilities that might be otherwise useful to their facility.

By utilizing the UML-based tool, iterative designs can be performed as described in the previous section. Cutsets have been generated (similar to those found in Table 4 – the baseline design cutsets) on a modified functional model from the months of July to October that uses a cooling pond as a cooling water intake source. Based on this model, the peak of risk of system failure is reduced significantly—the probability of a failure is reduced by 10% in August, and consistent decreases along similar months are observed. Figure 4 displays the new set of probabilities—the new risk profile is significantly flatter, and showcases potential avenues that the design team can take to improve the risk profile of their fuel pool.

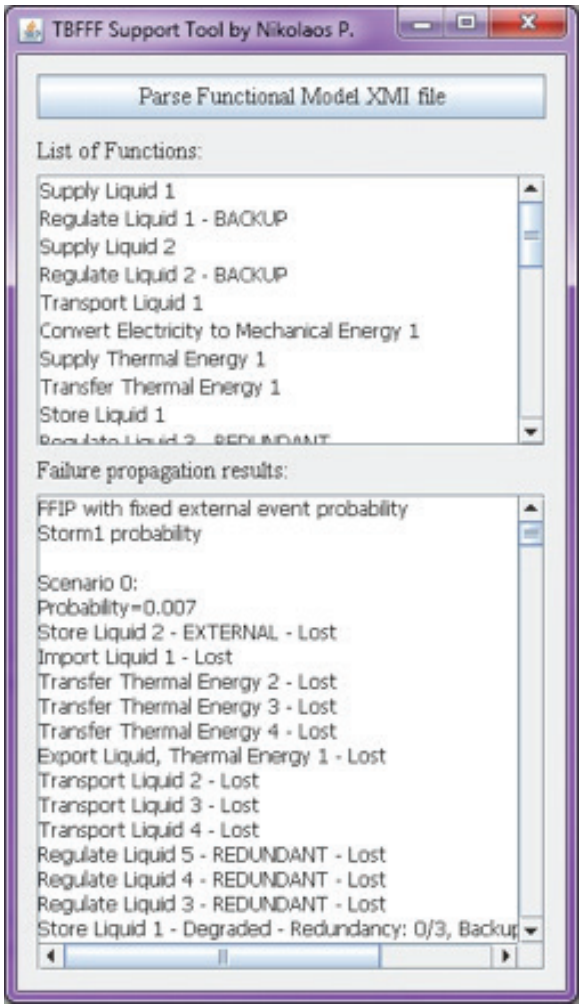


Figure 3. Probability of System Failure per Month.

From these results, the design team can note new avenues of development—increased risk of system failure occurs in May consistent with the heightened risk of the storm initiating event. The design team can then focus on mitigating that form of system failure by creating redundancies in the power supply such as waterproofing the motor system as well as potentially investigating redundant backup generators. The

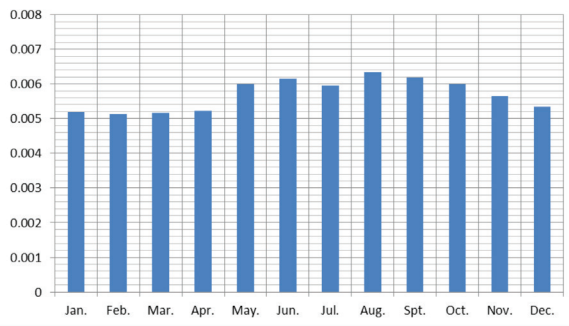


Figure 4. Probability of System Failure per Month After Iterative Design Using Insights Gained from TBFFE.

team may also run more TBFFE iterations and generate a new risk assessment based on the previously mentioned system design improvements with the aim of creating a very flat risk profile throughout the year. The iterative design potential is the main draw of TBFFE, permitting systems engineering teams, systems designers, and systems architects to rapidly identify and mitigate areas of concern for their systems that would go unnoticed without access to time-based failure evaluation methods.

The main benefit of time-dependent analysis of risk of system failure is that increased granularity of failure probabilities with respect to time over which the probabilities are analyzed allows engineers to mitigate risk in a more optimal way, thereby focusing on spending resources in times of heightened system failure risk. TBFFE allows practitioners to bring together risk data that operates on non-uniform timescales to create overall profiles of risk that provide insight which otherwise would be obscured by the commonly used yearly timescales of PRA and other risk analysis techniques.

One limitation of the TBFFE method is the need for more granular initiating event data as an input to the method. TBFFE is useful when the design team already knows that the system is going to be impacted by time-variant initiating events – in the example of the spent fuel cooling pool, the designers already knew that algae and storms had been problems in previous nuclear reactors and were able to account for this within their design by using the TBFFE method. TBFFE is a method best suited to characterizing known information with greater granularity—unknowns are harder for the system to deal with and frequently can be as opaque to the design team as they would be had they only used a method such as FFIP or PRA. An extension of this limitation is that TBFFE requires the design team to bring in data beyond what they might get from existing engineering databases to create distinct probability of occurrence data for initiating events. Depending on the initiating event, this may require assumptions on the part of the design team that possibly will not be borne out by reality.

By understanding these weaknesses, it becomes clear that TBFFE is best suited to those scenarios where designers wish to integrate data that is specific to their use case into a larger framework of existing probabilities in their system analysis. Examples include specific scenarios such as nuclear reactors or spacecraft, where there is a plurality of information available to an engineering team but where the details born of location or purpose are unique to a particular project.

References

1. German Aneiros-Perez and Philippe Vieu. Nonparametric time series prediction: A semi functional partial linear modeling. Journal of Multivariate Analysis, 99(5):834{857, 2008.
2. Corwin L Atwood. Parametric estimation of time-dependent failure rates for probabilistic risk assessment. Reliability engineering & system safety, 37(3):181{194, 1992.
3. US Nuclear Regulatory Commission et al. Regulatory Guide 1.174: An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant-specific Changes to the Licensing Basis. US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, 2002.
4. Warren Gilchrist. Modelling failure modes and effects analysis. International Journal of Quality & Reliability Management, 10(5), 1993.
5. PL Hall and JE Strutt. Probabilistic physics-of-failure models for component reliabilities using Monte carol simulation and weibull analysis: a parametric study. Reliability Engineering & System Safety, 80(3):233{242, 2003.
6. Julie Hirtz, Robert B Stone, Daniel A McAdams, Simon Szykman, and Kristin L Wood. A functional basis for engineering

design: reconciling and evolving previous efforts. Research in engineering Design, 13(2):65{82, 2002.

7. Ryan S Hutcheson, Daniel A McAdams, Robert B Stone, and Irem Y Tumer. A function-based methodology for analyzing critical events. In ASME 2006 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, pages 1193{1204. American Society of Mechanical Engineers, 2006.
8. K Kimseng, M Hoit, N Tiwari, and M Pecht. Physics-of-failure assessment of a cruise control module. Microelectronics Reliability, 39(10):1423{1444, 1999.
9. Tolga Kurtoglu and Irem Y Tumer. FFIP: A framework for early assessment of functional failures in complex systems. In The International Conference on Engineering Design, ICED, volume 7, 2007.
10. Craig Larman and UML Applying. Patterns: An introduction to object-oriented analysis and design and iterative development. 2004.
11. Nuclear Regulatory Commission et al. Severe accident risks: an assessment for five us nuclear power plants. Technical report, Nuclear Regulatory Commission, 1991.
12. Bryan M O'Halloran, Nikolaos Papakonstantinou, and Douglas L Van Bossuyt. Modeling of function failure propagation across uncoupled systems. In 2015 Annual Reliability and Maintainability Symposium (RAMS), pages 1{6. IEEE, 2015.
13. Bryan M O'Halloran, Nikolaos Papakonstantinou, and Douglas L Van Bossuyt. Cable routing modeling in early system design to prevent cable failure propagation events. In 2016 Annual Reliability and Maintainability Symposium (RAMS), pages 1{6. IEEE, 2016.
14. Nikolaos Papakonstantinou, Markus Porthin, M O'Halloran, and L Van Bossuyt. A model-driven approach for incorporating human reliability analysis in early emergency operating procedure development. In 2016 Annual Reliability and Maintainability Symposium (RAMS), pages 1{6. IEEE, 2016.
15. N Siu. Risk assessment for dynamic systems: an overview. Reliability Engineering & System Safety, 43(1):43{73, 1994.
16. Michael Stamatelatos. Probabilistic risk assessment: What is it and why is it worth performing it? NASA Office of Safety and Mission Assurance, 4(05):00, 2000.
17. R.B. Stone, I.Y. Tumer, and M. Van Wie. The function-failure design method. Journal of Mechanical Design, 127(3):397{407, 2005.
18. Robert B Stone and Kristin L Wood. Development of a functional basis for design. Journal of Mechanical design, 122(4):359{370, 2000.
19. Rogier Woltjer and Erik Hollnagel. Functional modeling for risk assessment of automation in a changing air traffic management environment. In Proceedings of the 4th International Conference Working on Safety, volume 30, 2008.

Reaching the Highest Reliability for Tantalum Capacitors

James Bates
Marc Beaulieu
Michael Miller
Joseph Paulus

Weibull reliability assessment has been used for characterization of tantalum capacitors for many decades driven by MIL standards. Over time major improvements have been made in process, material, testing, equipment and other process control.

Is Weibull still the best fit for today's technology and Hi-Rel applications?

A new approach is needed since the current Weibull grading to assure reliability has deficiencies, in particular, the need for early life failures and the potentially damaging application of excessive voltage during the burn-in in an effort to maximize the Weibull acceleration factor.

This paper will discuss modifications to the existing burn-in process, techniques for DC leakage screening, and improvements in process monitoring. These modifications improve the consistency of the resultant product DC leakage as well as eliminating the potential for field-induced dielectric damage. The result: tantalum capacitors that deliver the best performance in zero failure tolerance applications.

Background: Tantalum Capacitor Reliability

It has been well established that the presence of impurities in the tantalum anode create disruptions in the Ta2O5 dielectric. These disruptions, in addition to those created by other manufacturing-induced defects, can result in elevated leakage current, parametric leakage instability, or catastrophic dielectric breakdown. The occurrence of these non-homogenous defects can be reduced through material and process controls, and practically eliminated with the implementation of appropriate testing regimens.

After the elimination of the non-homogenous defect portion of the population, there still remain a number of homogenous defects, parametrically represented by leakage current and phenomenologically represented by electron traps [1]. The robustness of the dielectric can be characterized as either a resistance to catastrophic dielectric failure or as parametric leakage stability. Both characterizations can be modeled, at least initially, using the thermochemical model championed by McPherson and corroborated by Teverovsky [2,3]. A key conclusion from the thermochemical model is the potential susceptibility of the Ta2O5 dielectric to time-dependent dielectric breakdown, potentially accelerated by an inappropriate application of burn-in voltage.

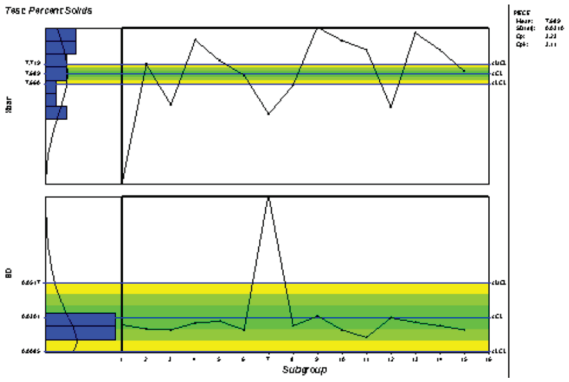
The need to control both manufacturing-induced defects and those defects intrinsic to the capacitor population is addressed with the Q-Process, incorporating the following elements:

- Process Monitoring: 3D Control Charts
- 125°C, Voltage-Optimized Burn-In
- Statistical Screening at Various Temperatures, Pre/Post Burn-In
- Enhanced Inline Reflow Conditioning
- Maverick Lot Identification
- Product Level Designator

Process Monitoring: 3D Control Charts

The reduction of non-homogenous defects through material and process control requires accurate monitoring of relevant processing, in particular the identification of special cause events. Traditional SPC charts fail to accurately characterize normal process variability since they are incorrectly based on within-batch variability instead of batch-to-batch variability.

Traditional SPC charts incorrectly use the within-batch sigma (based off the centerline on the sigma chart) in the control limit calculations in the batch-to-batch chart (the X-bar chart). This typically results in the pattern illustrated in Chart 1:



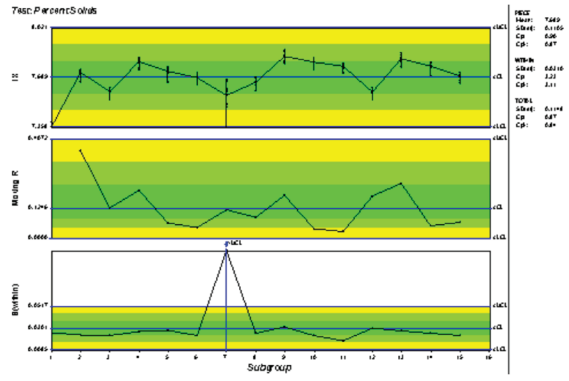
The calculated control limits on the X-bar chart are not representative of the plot points. In this example, the control limits are very tight. This clearly indicates that the within-batch variability is much smaller than the batch-to-batch variability. If these charts are used to control the process, the operators and engineers are simply chasing normal process variation and can't focus on special cause events because the majority of batches are "out of control."

Implementing 3D Control Charts

Using two charts to track the variability provides a more accurate representation of the true process variation:

- moving-range chart for batch-to-batch variability
- sigma chart for the within-batch variability

AVX now uses the centerline of the batch-to-batch moving-range chart in the calculations for the batch-to-batch X-bar chart. (Chart 2) shows the same data with the additional moving-range chart and the correct control limits on the X-bar chart. The top chart is now treated as an individuals chart—IX.



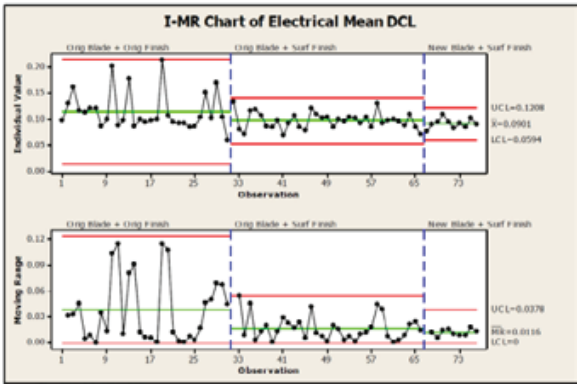
The Moving R chart displays the batch-to-batch variability and the S (within) chart displays the within-batch variability. Control limits on the top chart are based off the Moving R centerline.

The vertical lines on the IX chart's plot points represent the within-batch variability. Note that the within-batch variability of batch #7 is much higher than the others. This variability is limited to within the batch and does not show up as a special cause on the IX chart or the Moving R chart.

In the manufacture of tantalum capacitors there are many cases where both within subgroup and between subgroup sources of variability need to be monitored. Once the appropriate control charts are implemented on the manufacturing floor, both production and engineering can focus on special cause events. These special cause events are the key drivers for continuous improvement. Once a special cause event is identified, then root cause investigations can begin. Each root cause investigation identifies areas where either the process can be optimized or product or process enhancements can take place. Examples of some of these product/process enhancements while developing the Q-Process:

1. Tighter Anode Pressing Control
2. SPC Monitored and Controlled Sintering
3. MES-Controlled and SPC-Monitored Formation Equipment
4. MES-Controlled MnO2 Deposition Systems
5. Saw Optimization
6. Individual Part Stability Testing

The result of these improvements include but are not limited to tighter and lower DCL performance with less special cause variation (chart 3).



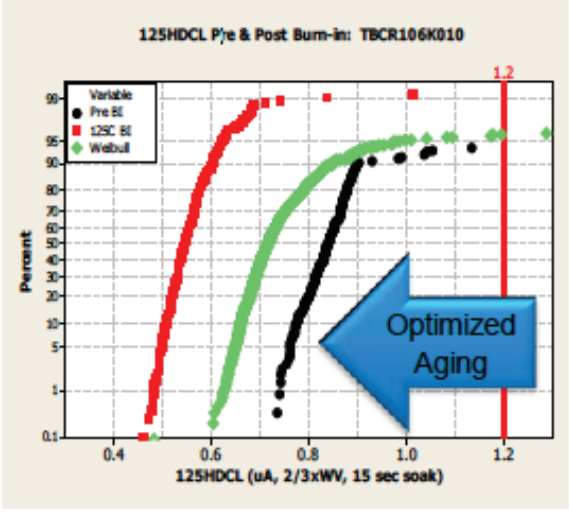
Optimized Burn-in

The burn-in process accomplishes two primary functions through the accelerated aging process induced by applied temperature and voltage:

- Component healing and defect isolation
- Destabilization of "maverick" defects

Certain defects, not removed through pre burn-in statistical screening, will become enhanced through the accelerated aging, that response characterized by a significant parametric increase in DC leakage. These previously undetected defects will now exhibit DC leakage uncharacteristic of the rest of the component population and can then be removed by post burn-in statistical screening.

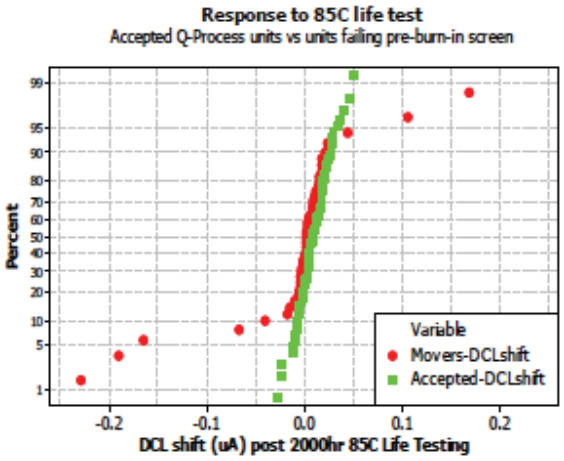
Intrinsic, homogenous defects, such as oxygen vacancies, minor dielectric disruptions, or nanoscale mechanical damage, can be repaired during the burn-in process through solid-state anodic oxidation [4] or electrically isolated through the irreversible reduction of conductive MnO2 to insulating Mn2O3 [5]. These healing processes require the application of voltage and are accelerated by both increased voltage and temperature. One of the key elements of the Q-Process is the successful optimization of applied voltage, temperature, and burn-in duration such that the burn-in process activates these healing processes without inducing localized dielectric breakdown as described by the McPherson thermochemical model. Chart 4 demonstrates the parametric shift in DC leakage resulting from



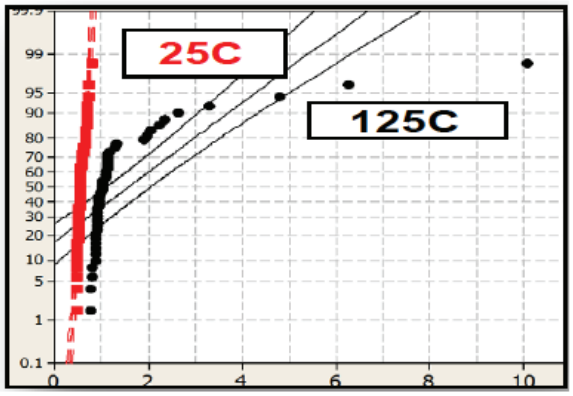
a burn-in process. The DC leakage of the optimized burn-in process exhibits significantly lower overall DC leakage, but the DC leakage of the maverick parts has been enhanced, improving the effectiveness of the statistical screening.

Statistical Screening, Pre/Post 125°C Burn-In Enhanced Inline Reflow Conditioning

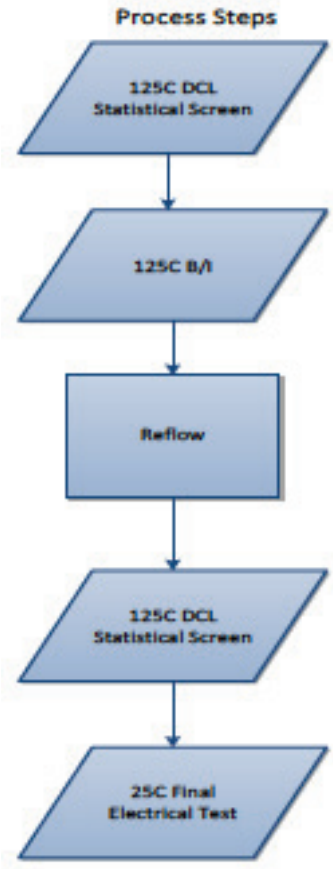
Another key component of the Q-Process is the elimination of inhomogeneous defects prior to the burn-in process. Due to the healing process induced during burn-in, it is possible for units within the population that may have defects uncharacteristic of the remainder of the population to "move" into the DCL distribution representing "good" units. AVX has determined that a portion of these units that "move" could be potentially unstable on long-term life test. Utilization of a statistical screening prior to 125°C burn-in eliminates the possibility of including this small quantity of potentially parametrically unstable capacitors (units in red).



In addition to the 125°C burn-in, AVX applies an optimized reflow that stresses the component at the appropriate level to induce mechanically weak components to undergo a parametric shift that can be subsequently detected at post burn-in statistical screening. The ability to detect the induced parametric shift can also be enhanced through elevated temperature screening. Chart 6 demonstrates individual part variations detected during 125°C testing that would normally be undetected during room temperature testing.

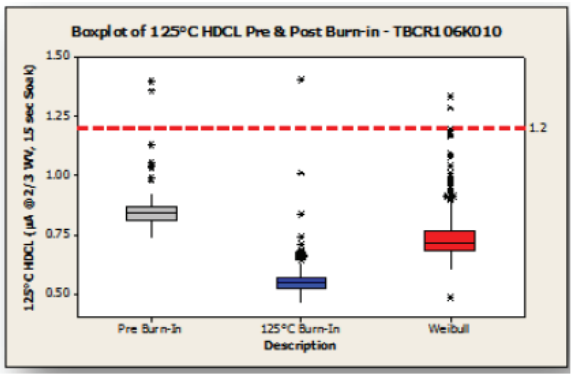


The combination of appropriate burn-in, reflow, and pre/post burn-in statistical screening yields the Q-Process flow, shown in Chart 7:

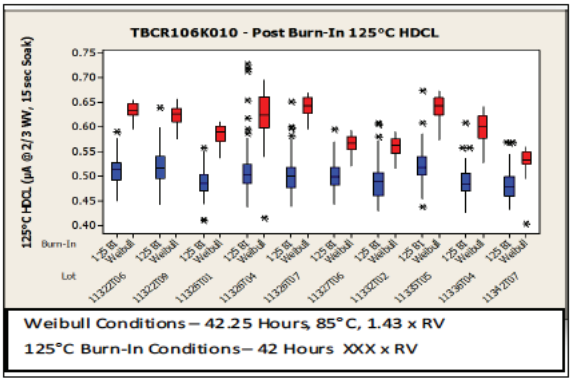


The Q-Process has repeatedly demonstrated an improvement in overall DCL relative to the conventional 85°C, voltage accelerated burn-in affiliated with Weibull. An interval plot (Chart 8) of pre burn-in DCL, post 125°C burn-In

DCL, and post 85°C burn-in DCL demonstrates this improvement.



This improvement in post burn-in DCL was also shown to be repeatable across multiple lots (Chart 9 – red: Weibull, blue: Q-Process):



The effectiveness of the Q-process is best illustrated through life testing. AVX utilizes both 85°C (rated voltage) and 125°C (⅔ rated voltage) for life testing.

Chart 10 represents ~100 components, sampled from 10 production lots and tested at 125°C. The black line represents the post life test results of approximately 1000 Q-Process components compared to approximately 170 traditionally burned-in components. It is easy to see that the 85°C accelerated voltage parts contain 2 units that fail through life testing. The Q-Process parts have 5 times amount of parts on test with zero failures to the specified DC leakage limit (0.225µA).

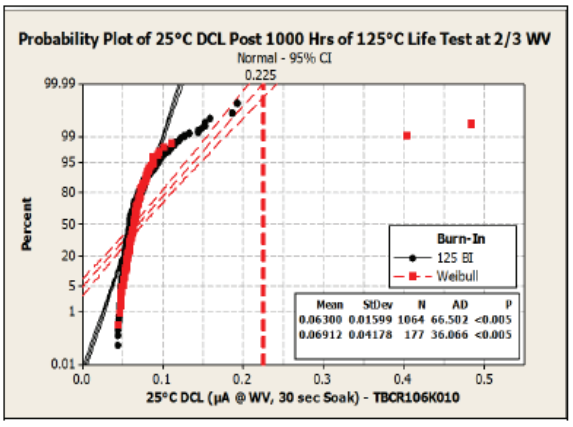
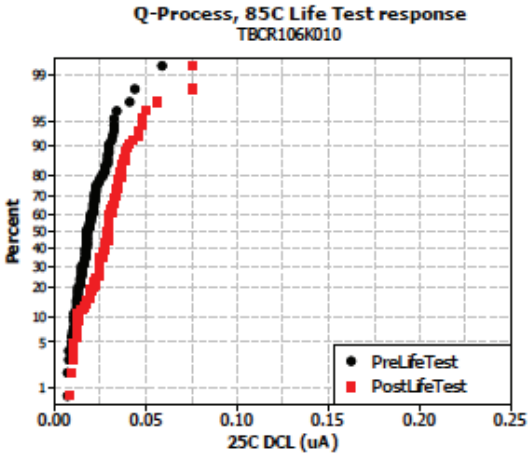
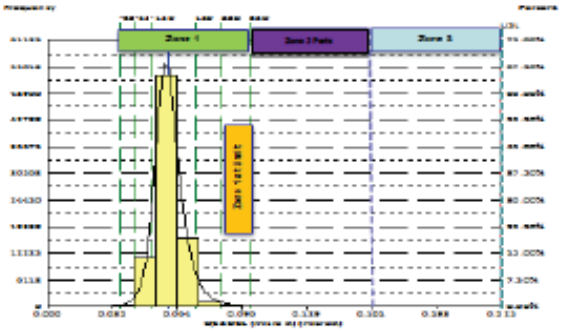


Chart 11 represents the 85°C (rated voltage) life testing of 10 components, sampled from the same 10 Q-Process production lots. As is evidenced by the chart, the post 2000hr life testing DC leakage exhibits a negligible shift.



Evaluation of AVX Statistical Algorithm

In order to evaluate the effectiveness of the AVX statistical algorithm segregation, individual unit life testing was performed. Individual pieces with marginal or anomalous performance through 125°C burn-in were captured, categorized, and submitted to 85°C life testing. Specific characterization is identified in each life test group. The grouping is specified in the 25°C DC leakage histogram below.



The 85°C life testing response, based upon grouping, is shown in charts 13a and 13b. The grouping is as follows:

1. 0 highest units for 125HDCL (post burn-in), but still within 3σ limit All units are stable, indicating relative effectiveness of 3σ limit and the Q-Process: Good (zone 1 at limit)
2. Units from entire 10-lot population that exceeded the 3σ limit but were within the hard cut limit, although the majority of the units are stable through 85°C life test, this population is likely to contain unstable units, as demonstrated by the 3 failed units. This supports that traditional hard cut limits do not effectively remove parts that have reliability issues: Marginal units (zone 2)
3. Good units (zone 1)

The pre-life test DCL is shown in black in Chart 13a.

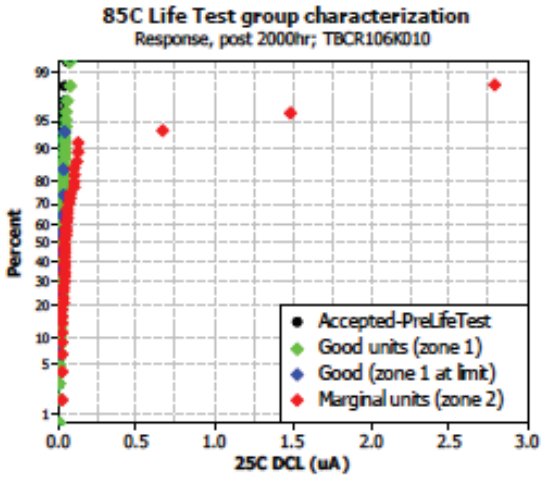
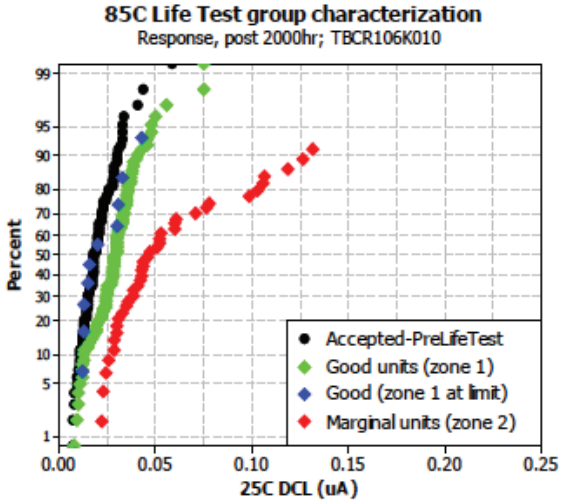
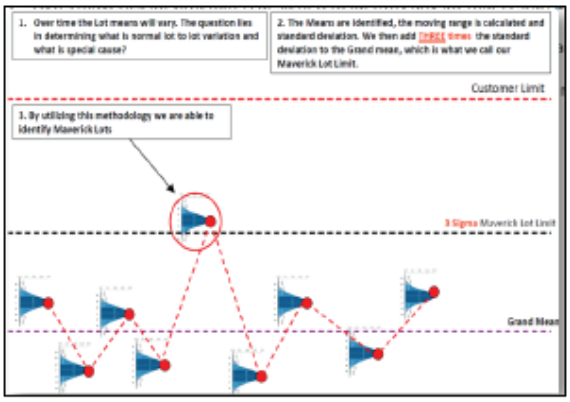


Chart 13b shows the same DCL distributions, but scaled to an appropriate component DCL limit.



Maverick Lot Program

AVX's maverick lot program is designed to identify any lot that is statistically different than previously supplied lots. This program insures that the lots produced are statistically the same as the originally qualified design. The maverick lot program is a key driver of continuous improvement projects at AVX. This program utilizes the 3D chart format discussed earlier in this paper. A visual representation of this program is shown in chart 14.



Product Level Designator/AVX Lot Acceptance Testing

Due to the removal of the early time failures prior to burn in, it is not possible to calculate a failure rate with the traditional Weibull model. It is now necessary to replace the Weibull grading system with one that can accurately predict the lots reliability performance. Weibull never took into consideration the effects of multi side reflowing of surface mount parts onto substrates into its calculation. This is a flaw in the current system and is a source of customer frustration when building product. The Product Level Designator is a demonstrated failure rate. What is unique about this system is before any calculation is performed, a simulated production routine is completed on a sample from the population, which includes double-sided reflow. Once that is completed a calculation is done based on the performance of the sample through simulated production. See Example 1

In order to calculate a product level designator for lot several assumptions and factors are

made in the creation of the formula

1. The Equivalent Component Hours is based upon the MIL-HBK-217 model for solid tantalum capacitors
2. Test Temperature Acceleration Factor is based upon the Arrhenius model. The temperatures are in degree Kelvin.
3. Activation Energy (1.08eV to 1.15eV) [6]
4. Boltzman Constant = 8.63E-5 eV/°K
5. Test Voltage Acceleration Factor is Test Voltage divided by the Rated Voltage, cubed
6. The total component hours at test temperature is multiplied by the Test Temperature Acceleration Factor and the Test Voltage Acceleration Factor to get the Equivalent Component Hours used in calculating the failure rate.
7. Failure Rate predictions are based on Chi-Squared distribution, the Degrees of Freedom in the use of the Chi-Squared Distribution is the number of failures plus 1 multiplied by 2
8. Application Voltage Acceleration Factor is Application Voltage divided by the Rated Voltage, cubed
9. The calculated failure rate is multiplied by the Application Voltage Acceleration Factor to get the final Failure Rate

Inputs	10-volt Part
Rated Voltage	10
Qty Tested	30
Hours Tested	6
TestTemp C	125
Test Voltage	6.6
Number Failures	0
Confidence Level	90
Application Temp C	25
Application Voltage	5
Activation Energy of Tantalum Cap (eV)	1.08

Example 1

Outputs	
Component Hours (Equivalent at Application Temp)	1,978,593
Component Years (Equivalent at Application Temp)	225.71
Test Acceleration Factor (Temperature)	38,234.21
Test Acceleration Factor (Voltage)	0.287496
Application Acceleration Factor (Voltage)	0.1250
Failure Rate (% failures per 1000 hours)	0.007273
MTBF (Mean Time Between Failures) (Hours)	1,374,867
Application Temp C	25
Application Voltage	5
Activation Energy of Tantalum Cap (eV)	1.08

This model allows for a standard calculation to be made based on actual application temperature and voltage. What is unique about this model is that it is very flexible. The model can be used to calculate application specific failure rate as well as mean time between failures at various confidence intervals. This is simply done by changing the input variables and since these are "live" inputs the model recalculates these numbers based on the new information.

Conclusion

The Q-Process actively motivates and exercises the known failure mechanisms for DC leakage, and then identifies non-normal parts and removes them from the population. The portions of the Q-Process implemented to date have demonstrated an order of magnitude reduction in customer line fallout. AVX is pursuing implementation of the full Q-Process for all of our high reliability surface-mount solid tantalum capacitors.

References

1. R. Ramprasad, Phys. Stat. Sol. (b) 239, No. 1, 59-70 (2003)
2. J.W. McPherson et al., IEEE Transactions on Electron Devices, Vol 50, No. 8, August 2003
3. A. Teverosky, IEEE Transactions on Device and Materials Reliability, Vol 9, No. 2, June 2009
4. D.M. Smyth, Journal of the Electrochemical Society, Vol 113, No. 1, January 1966
5. J.S. Wiley and H.T. Knight, Journal of the Electrochemical Society, Vol 111, No. 6, June 1964
6. J.L. Paulsen, "Reliability Characterization of Tantalum Capacitors with MnO2 Counter-Electrode", CARTS, 2006

Threading Together the Twins in a Contextually Relevant Digital World

John Blyler

The emergence and usefulness of digital continuity, twins and threads, is a direct result of the ongoing process of digitizing the physical world.

Digitization of the Manufacturing World

Digitization is the conversion of the physical world to a digital equivalent. It represents the convergence of the real and the virtual worlds. This conversion has been accelerated with the emergence of the sensor and data rich markets known as the Industrial Internet-of-Things (IIOT). When focusing exclusively on manufacturing and production processes, the IIOT becomes part of the Industry 4.0 evolution (see Figure 1).

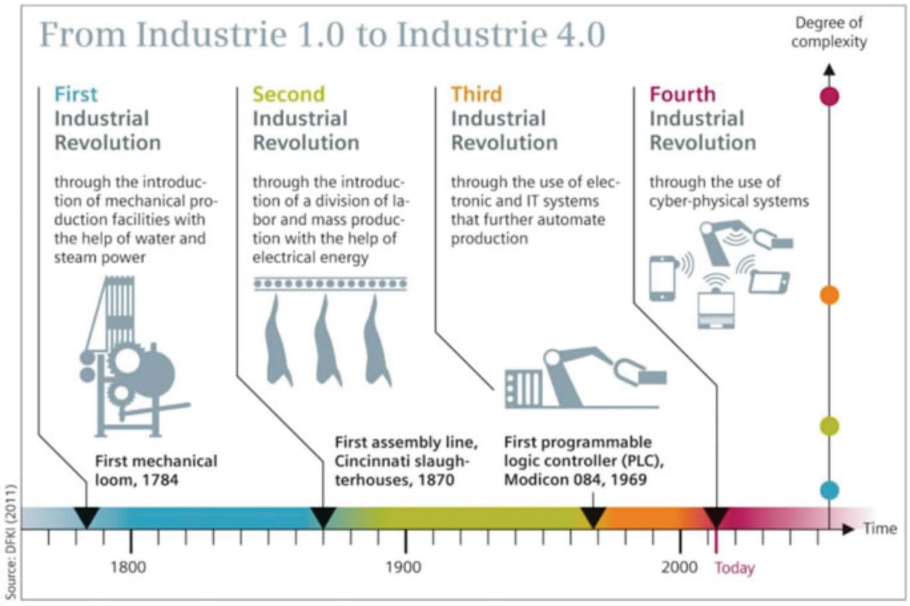


Figure 1. Timeline of Industrie 1.0 to Industrie 4.0. Graphic source: Courtesy of DFKI (2011)

The traditionally mechanical, pre-digital industry supply chains were very siloed (Reference 1). The evolution to today's Industry 4.0 required movement beyond siloes to deal with rising complexities and shrinking time-to-markets (TTM). The key to this evolution has been the digitalization of the physical to achieve smart connectivity between things and people throughout both the design and manufacturing process.

Two consumer sectors still at the early stage of digitalization are the avionics and automotive spaces, in part due to stringent safety, reliability and certification requirements. The avionic—really Aerospace and Defense (A&D)—market is used to long-cycles in both funding and product development. Recent surveys [Reference 2] have shown that only a scant 26% of aerospace companies do business with clients and suppliers in a digital, electronic manner.

Recently, market researcher Accenture has highlighted the drivers behind the digitalization of the A&D sector (Reference 3), which are indicative of other market segments grappling with digitization:

- Flat budgets
- Longer, more complex programs
- A shrinking talent pool of human capital
- Rising demand for products and services
- The explosion of big data, often used for predictive maintenance
- Operational cost optimization due to flat or shrinking budgets

Many of these same factors are drivers in the evolution of the Industrial Internet of Things (IIOT), but none more so than the application of data analytics. This is a natural result of the nature of the IIOT, namely, a system of connected and integrated electronic, electrical and mechanical physical assets that provide raw data for analysis and manufacturing process optimization.

The availability and ever growing amount of this data, in turn, has helped enable the early digital continuity in IIOT market vendors such as GE, Siemens, PTC, CSC, etc. But what does this mean in practical terms?

The Digital Trifecta: Threads, Twins and Continuity

Digitization is the process of converting almost anything into a digital format, e.g., books become e-books, analog music becomes MP3 bits and bytes, etc. Interestingly, the reverse of digitalization is also occurring as demonstrated by the 3D-printing of a completely digital electronic model.

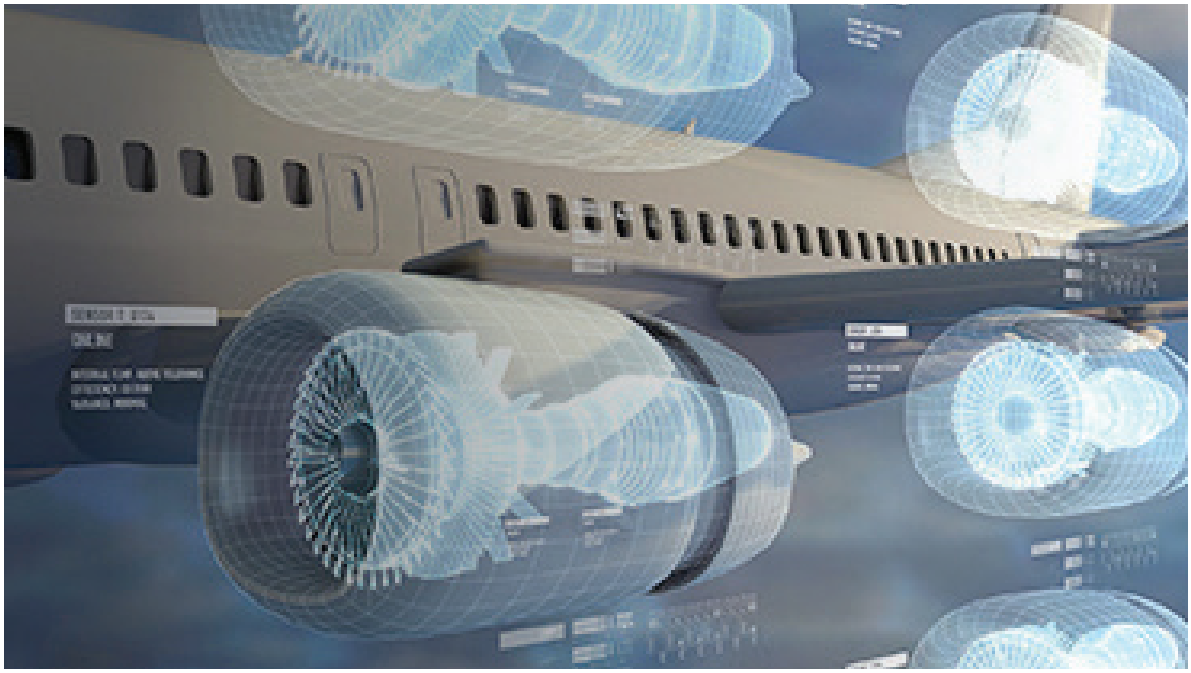


Figure 2: The Digital Twin is a real-time replica of specific aspects of the physical twin. (Image credit: General Electric)

Digitization is needed to turn a physical system into a digital replica or twin—at least to some degree (see Figure 2). This digital representation originated as a by-product of digital manufacturing trends whose purpose was to maintain and re-use digitized production information, e.g., machine settings, specifications, assembly-line configurations, etc. For the manufacturing process, the Digital Twin also incorporates Computer Integrated Manufacturing (CIM), production line equipment/robotics, and warehouse and material management. Computer-integrated manufacturing (CIM) refers to the use of computer-controlled machineries and automation systems in manufacturing products that combine both computer-aided design (CAD) and computer-aided manufacturing (CAM) technologies.

Over time and with improved simulation technology, the Digital Twin has expanded to include design activities. Today, Digital Twins comprise a near real-time digital image or software copy of a physical asset or process (see Figure 2). From a design perspective, a Digital Twin is a digital representation of a physical product such as an aircraft engine. Including CAD and related engineering information, it incorporates product specifications, geometry models, material properties and associated simulation information.

Digital Twin

Perhaps nowhere is the value of the Digital Twin more evident than in NASA operations. Once deployed, spacecraft are generally inaccessible for repairs. The only way to determine what is wrong with a spacecraft is from information gleaned from sensor systems and transmitted via telemetry technology. When manned missions encounter problems, simulators and Digital Twin databases can help pinpoint the problem, devise possible fixes, and test out repair actions on the ground.

To achieve maximum efficiency, a Digital Twin for the product development, manufacturing and even the entire supply chain will need to be created. This comprehensive goal is still a ways off except in product manufacturing, in which the Digital Twin idea comprises not only the product but also the factory, the equipment and the logistics systems.

Creating a Digital Twin that bridges manufacturing, design and every life cycle phase in-between requires lots of Digital Threads.

Digital Thread

The Digital Thread helps extends the Digital

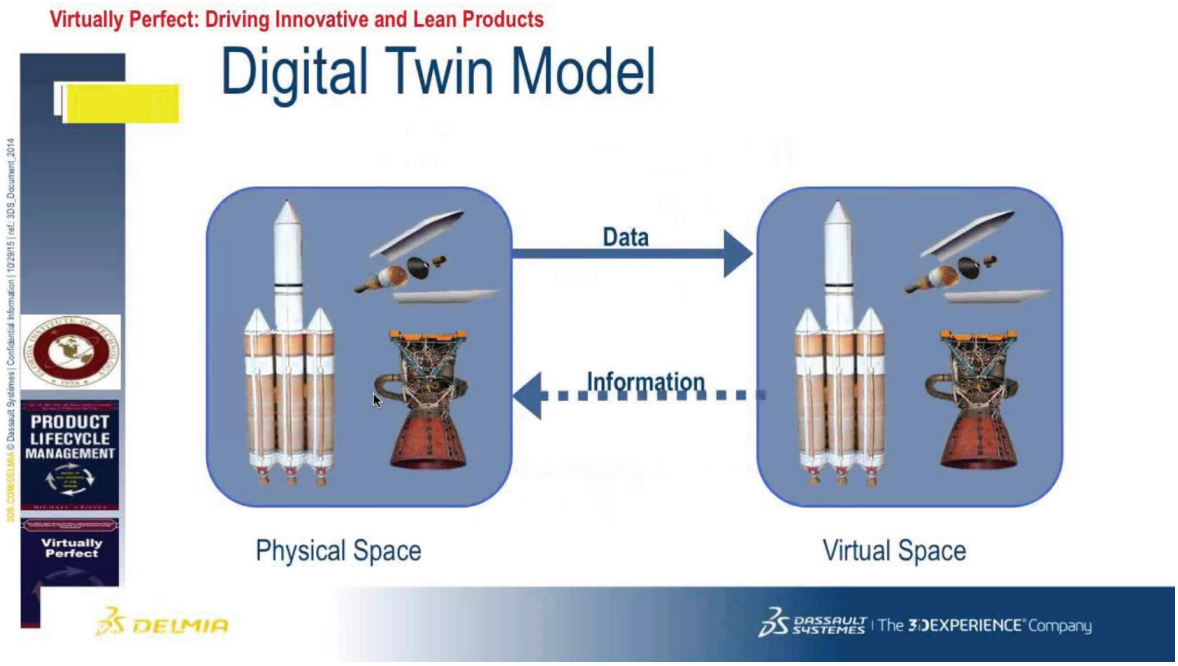


Figure 3. The Digital Twin consists of Digital Threads that connect data and information between the virtual and physical spaces. (Courtesy of Dr. Michael Grieves whitepaper, Delmia – Apriso)

Twin into a product's entire lifecycle, encompassing all data flows across initial architecture, design, engineering, performance, manufacturability and serviceability. It's a vital thread that runs through all the disciplines, domains and contexts with which a product/service interacts.

The Digital Thread is a framework that enables connected data flows and an integrated view of assets and systems across traditionally siloed elements in manufacturing (and design). The Digital Thread ensures connections between all of a product's digital assets–and their revisions over the lifecycle –including versions of BOMs, CAM databases, parts, software, electronics, CAD models, documents, requirements, process plans, and service manuals, etc.

It would be a mistake to imagine that the Digital Thread and twin are similar concepts. The former is data centric path that establishes a connected data flow for all pertinent product data throughout its lifecycle. Conversely, the Digital Twin enables the creation, building and testing of the product in a virtual environment (see Figure 3). By developing Digital Threads, design and product engineers can collaborate with manufacturing engineers to create a virtual, 3D model between the design and manufacturing environments.

If an unbroken, contextually consistent and streamlined flow of data, information and views can be established between the design environment and the manufacturing execution systems, then digital continuity can be achieved. Such digital continuity will allow the information to be updated and constantly available throughout the product's development lifecycle.

What Twins and Threads are Not!

It is only in recent years that the creation of a truly Digital Twin has been possible. As might be imagined, the digitization of a physical system requires massive amounts of data, computing power, storage, bandwidth and cost. These requirements have been met over the last several years thanks to ever more powerful yet cheaper electronics afforded by Moore's Law. (3)

A Digital Twin enables companies to understand not only the product as designed but also the system that built the product (manufacturing) and how the product is used in the field (operations and service). Understanding these aspects of the product help companies shrink time-to-market, improve operation, meet stringent safety requirements, reduce defects and more.

Some wonder if these benefits are worth the cost of creating a complete Digital Twin of a new product all at once. How is it even possible to capture every conceivable piece of information about the physical twin that must surely be necessary?

The latter point is an idealization, much like assuming all system-of-system (SOS) projects must start from scratch. Despite the impressive state of today's computing electronics, no computer system would be able to crunch all the numbers for an exact and complete digitalization of a physical product. Even if all the data could be processed, there would be no way to filter and analyze all the data in a timely manner.

The key to creating a Digital Twin is to start in one area first, presumably the area that is causing problems. As with the engineering of any problem source, the Digital Twin will involve simplifications and assumptions in order to be of value. It will not include every physical aspect of the system, only those aspects that are of interest and value to solve the problem.

To refine our earlier definition, the Digital Twin is really a virtualized representation of all the information needed to supplement existing engineering models and tools to solve a given problem. The creation of the Digital Twin must occur within the scope and context of a given challenge.

Similarly, context is critical for the Digital Thread, too.

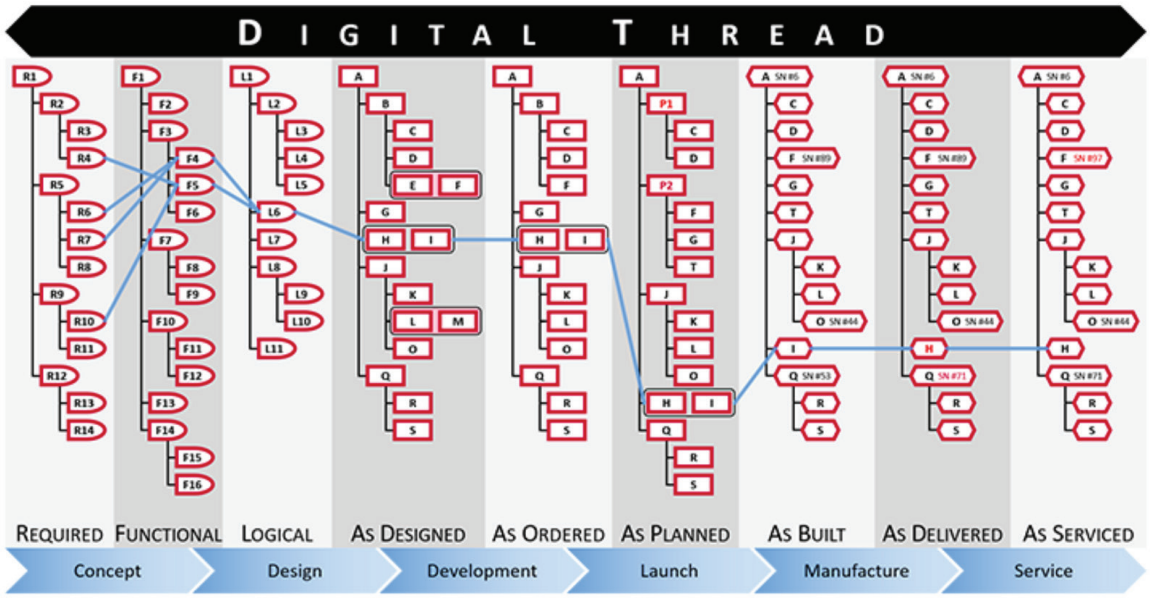


Figure 4. Flowing the Digital Thread. (Courtesy of the Aras Open PLM Community)

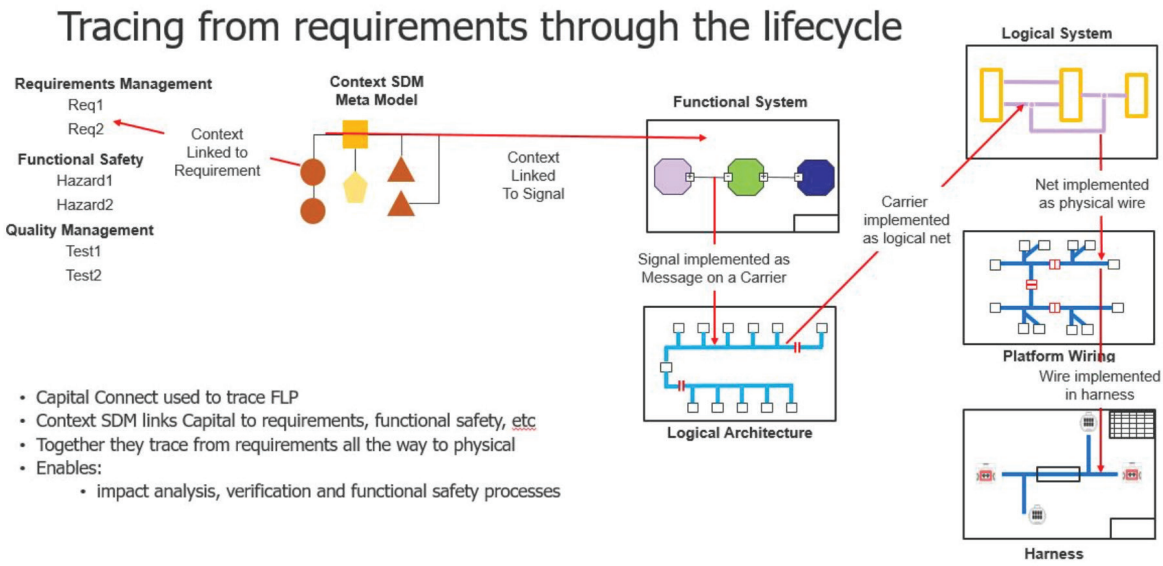


Figure 5. The Digital Thread in action, tracing requirements, functional, logical, and physical (RFLP) entities and relationships throughout the product lifecycle. (Courtesy of Mentor Graphics)

Context is Critical

The defining characteristic of the Digital Thread is the continuity of its connection throughout the product lifecycle. Looking at a representation of the Digital Thread (see Figure 4) is very much like looking at a diagram about requirements traceability (see Figure 5). But the Digital Thread is about more than just traceability, it's about the context and relationship of the connections between all of a product's digital assets and their revisions—BOMs, parts, software, electronics, CAD and CAM models, documents, requirements, process plans, and service manuals, etc.

The relationship aspect of the Digital Thread information addresses both the context and the dependency of the data. For the context, it might answer the question of how a given part is related to another and whether they are both part of the BOM. In terms of dependency, the Digital Thread must reflect how and when data for both parts is changing over time.

This is not to say that the Digital Thread is merely a collection of web links between different data points and subsystems. The threads

must be meaningful links between data and subsystems. Nor are these links just a parser-based interconnection of engineering to manufacturing processes or CAD to CAM tools. Instead, Digital Threads must provide the data connections and traceability from concept to end-of-life and across all involved disciplines including software, electronics, hardware, wiring harnesses (for cars and planes), requirements, etc.

In simpler terms, a Digital Thread (there may be more than one) provides traceability to the configuration of the Digital Twin.

Digitization of Systems Engineering

Some have said that the Digital Thread and its connection to the Digital Twin have put the engineering back into systems engineering. Another way of saying this—at least for the design activity—is that model-based technologies have enabled systems engineering in the digital world. Such digital collaboration enables information (digital) continuity across lifecycle processes (see Figure 6).

If done properly, weaving the Digital Thread will reinforce the basic tenants of system-of-systems (SOS) engineering especially the contextual flow of information. The starting point for the Digital Thread is typically early life-cycle model-based systems engineering (MBSE). This modeling serves as the foundation for all later cross-functional design. As a reminder, model-based systems engineering (MBSE) is the methodology that focuses on creating and integrating domain models as the primary means of information exchange between engineers, rather than on document-based information exchange.

In practice, using the results and insights gained from MBSE and Digital Threads enables early detection of failure modes in product simulations, which in turn lead to less design mistakes. Manufacturing can then link to the resulting Digital Twin to prepare all manner of production assets to build the actual product.

Using MBSE tools, engineers will be able to run system-wide and life-cycle long simulations of products for the Digital Twin to simulate hardware-software plants, products or services at the system level. In so doing, the hardware, software and content functions of the system can be more efficiently managed.

Practical Example

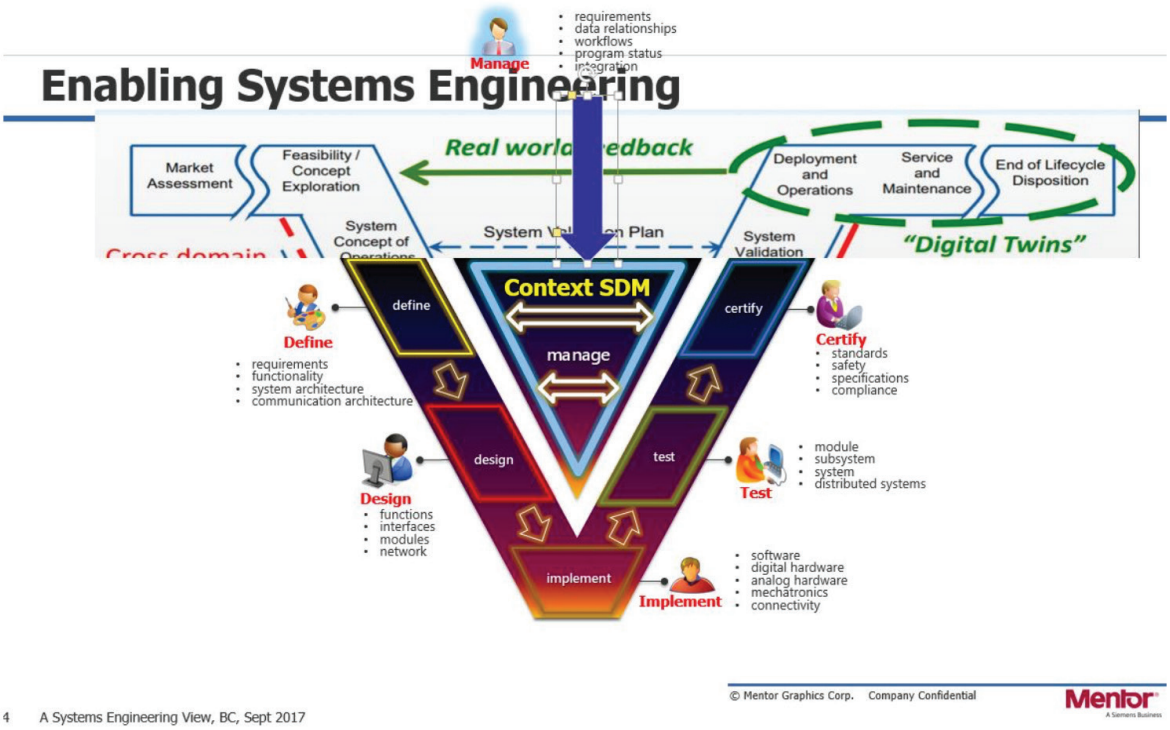


Figure 6. Digital Twins with their accompanying threads ensure digital continuity throughout a product's life cycle.

Consider the example of a Digital Twin for a transmission generator as part of a Siemens SIMOTICS general purpose factory motor (see Figure 7). Once available, the motor's Digital Twin provides up-to-date technical electrical and mechanical specifications, spare parts and operating instructions and more by simply scanning the data matrix code on the physical motor. But what was needed to create the Digital Twin of the generator portion of this motor?

As with any engineering project, one must first determine the requirements before developing an architectural and functional design, performing simulation and implementing the design in a physical system. The basis for this work comes from a variety of contextual sources and is conducted using a multi-tool environment (see Figure 8) that is tied together with at least one—Digital Thread. In the case of a generator, essential design issues would focus on power transmission requirements, voltage loss and static-dynamic system loads.

The result of the associated specifications and analysis work (see Figure 9) is a complete configuration that serves as the Digital Twin. Traceability of the data between the different models and associated engineering disciplines is provided by the Digital Thread. The MBSE ensures a high level of integrated interoperability and digital continuity.

Summary

Many cost, performance and production issues are driving the digitization of the physical world. To ensure digital continuity during this process, Digital Threads must be used to create a Digital Twin of the pertinent portions of the physical entity being designed and manufactured. Further, all of these activities must take place within the context of the system with both the physical and virtual worlds. Understanding the concepts and examples of digitization, Digital Threads, Digital Twins and continuity are needed to develop new products and bring the "engineering" back into systems engineering.

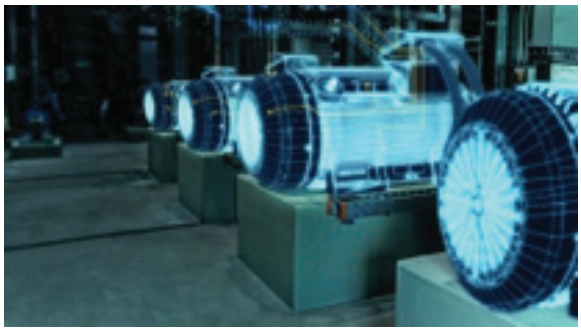


Figure 7. Digital Twin of a Siemens SIMOTICS general purpose industrial factory motor.

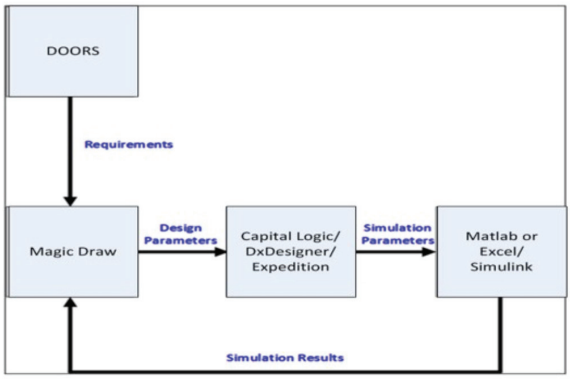


Figure 8. Requirements flow, architectural design and simulation in creation of the Digital Twin which will eventually be a physical generator subsystem within an industrial digital motor. (Courtesy of Mentor Graphics)

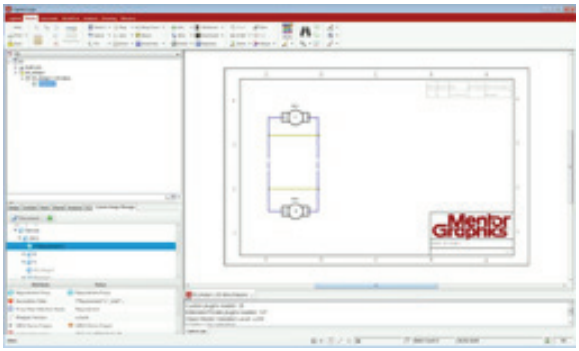


Figure 9. Specifications and design details form the data portion of the Digital Thread which can then be accurately modeled and manufactured.

References

1. Timeline of Industrie 1.0 to Industrie 4.0. Graphic source: Courtesy of DFKI (2011) https://wireless.electronicspecifier.com/iot-1/smoothing-the-path-towards-iot-and-industry-4-0
2. Stegkemper International Operations Excellence
3. Economist: Cloud Computing Prices Keep Falling

Supply Chain Risk Management (SCRM)

Katherine Pratt

Supply Chain Management (SCM) is defined as the process of planning, implementing, and controlling the efficient, effective flow and storage of goods, services, and related information, (such as software) from point of origin to point of consumption for the purpose of conforming to customer requirements. The core activities are customer service standards, transportation, inventory management and supply, plus information flow, order processing and transmittal.

Supply chains (SC) are typically used to transport goods from a source of supply to points of distribution or storage. There are four stages in a supply chain:

1. Supply network
2. Internal supply chain (i.e. manufacturing plants)
3. Distribution systems
4. End users

There are also four flows in a supply chain.

1. Material
2. Service
3. Information
4. Funds

e-Procurement links the supply network, the manufacturing plant, e-distribution links with the manufacturing plant, and the distribution network, while e-commerce links the distribution network and the end users.[1] At present, the U.S. federal government does not have a national strategy for supply chain risk management (SCRM) of commercial supply chain vulnerabilities in the U.S. federal information and communications technology (ICT).

1 "Supply Chain Management, Concepts, Techniques and Practices – Enhancing Value Through Collaboration" www.worldcibooks.com/business/6273.html

The standard risk planning strategy involves these steps:

1. **Identify Risk.** A team of SC experts should meet regularly to identify as many potential risks both before and after product production actually begins. Individual risk assignments should be made between the participants, to distribute the workload.
2. **Quantify Risk.** The SC team should agree to a method for quantifying the identified risks, such as Failure Mode and Effect Analysis (FMEA). This will enable the team to address the most critical risks first.
3. **Build Contingencies.** The team will develop strategies and prioritized actionable plans to address all delays, such as supplier delays, and or shipment delays at customs. Examples of contingencies can include backup third-party participants with pre-negotiated and agreed-upon contracts for replacement parts, due to unforeseen delays. Best practices would involve an on-sight plant visit to determine the working conditions, as well as to determine and quantify the SC risks and to help develop contingency plans.
4. **Address Cyber threats.** Virtual threats must be addressed as well as the physical ones. The National Institute of Standards and Technology (NIST) provides a cybersecurity framework consisting of standards, guidelines, and best practices to manage cybersecurity-related risks.[2]

The ICT supply chains are multi-tiered, webbed relationships rather than singular or linear ones. The supply chain threat to U.S. national security stems from products produced, manufactured, or assembled by entities that are owned, directed, or subsidized by national governments or entities known to pose a potential supply chain or intelligence threat to the U.S., including China. Currently, these products could be modified to perform below expectations or even fail, as well as to facilitate state or corporate espionage, or otherwise compromise the confidentiality, integrity, or availability of a federal information technology system.[3]

It is anticipated that software supply chain attacks will become more prevalent as the time required to breach these systems are decreasing, as well as developing technologies, such as fifth generation (5G) mobile network technology and the Internet of Things (IoT) provide exponentially increased avenues for attacks.

The IoT refers to a system of interrelated computing devices, mechanical and digital machines, objects, and living beings equipped with network connectivity that enables them to connect and exchange data. Growth in IoT connectivity, including the federal ICT networks, will provide an increased attack surface as new product designs continue to expand IoT usage, and further challenge ICT SCRM.

Ideally, we need policy strategies based upon forward planning, rather than one that is merely reactive. It will need to include software, cloud-based infrastructures, and hyper-converged products, as well as hardware. Strategies and policies will need to be crafted that address next generation technologies and the creation of new standards. Supplier SCRUM lifecycles need to be addressed from inception to demise, ensuring the SC relationship information is transparent for government oversight to mitigate risk exposures.

However, where are the Reliability, Maintainability and Supportability (RMS) metrics? How are ongoing effective planning, management and program support going to be measured and the program effectiveness to be evaluated without these types of important metrics?

The term "reliability" is often used as an overarching concept that includes availability and maintainability. Reliability in its purest form is more concerned with the probability of a failure occurring over a specified time interval, whereas availability is a measure of something being in a state (mission capable) ready to be tasked (i.e., available).

3 "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communication Technology" Tara Beeny, Senior Business Analyst, Interos Solutions, Inc.

2 NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

Maintainability is the parameter concerned with how the system in use can be restored after a failure, while also considering concepts like preventive maintenance and Built-In-Test (BIT), required maintainer skill level, and support equipment.

When dealing with the availability requirement, the maintainability requirement must also be invoked because some level of repair and restoration to a mission-capable state must be included. Clearly, logistics and logistic support strategies are also closely related and are dependent variables at play in the availability requirement. This takes the form of sparing strategies, maintainer training, maintenance manuals, and identification of required support equipment.

The linkage of Reliability, Availability, Maintainability (RAM) requirements and the dependencies associated with logistics support illustrates how the RAM requirements have a direct impact on sustainment and overall LCC. In simple terms, RAM requirements are considered the upper level, overarching requirements that are specified at the overall system level.

Software must be addressed in the overall RAM requirements for the system. The wear or accumulated stress mechanisms that characterize hardware failures do not cause software failures. Instead, software exhibits behaviors that operators "perceive" as a failure. It is critical that users, program offices, the test community, and contractors agree early as to what constitutes a software failure.

For example, software "malfunctions" often are recoverable with a reboot, and the time for reboot may be bounded before a software failure is declared. Another issue to consider is frequency of occurrence even if the software reboot recovers within the defined time window, as this will give an indication of software stability. User perception of what constitutes a software failure will likely be influenced by both the need to reboot and the frequency of "glitches" in the operating software.[4]

The relationship that commercial SCM has to military SCM can be described as highly compatible and supportive. This is not to say that they are equal in most respects. The goals, objectives and environment in which these two SCM systems operate are different and, in many cases, very unique. The military frequently provides the commercial SCM industry with advanced technologies such as the Internet and RFID, as well as, innovative total asset visibility and sense and respond concepts. Industry often then improves these technologies and concepts in a way that makes them more accurate, efficient and flexible. These commercial modifications often subsequently are adopted and re-incorporated into the DoD SCM system to better ensure the improved timely, accurate delivery of goods and services to the DoD's end user—the warfighter.

As compatible and supportive both SCM commercial and military applications currently are to each other, indications are that they have to become even more closely aligned. Issues such as Internet security, physical infrastructure maintenance and cost, lines of communication, and growing global economic and military competitiveness appear to be too socially challenging and technologically complex for either DoD or industry to address them separately as opposed to collectively. The cost to both the commercial and military SCM system is overwhelming. The decaying transportation infrastructure alone is costing the U.S. "$78 billion annually in lost time and fuel" and "by 2020, every major U.S. container port is projected to double the volume of cargo." The Urban Land Institute reports that the U.S. needs to invest $2 trillion to rebuild its mass, multi-facet transportation infrastructure.[5]

The time is now for the strategic planning and implementation of a single SCM system for hardware as well as software, that is designed and built to accommodate both commercial and military SCM requirements.[6]

5 "4 Reasons to be Excited about Sustainability" by Thomas Singer, 12-21-16

6 "Electricity Generation", by IER Institute for Energy Research

4 https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/integrated-logistics-support/reliability-availability-and-maintainability

About the Authors

Risk Modeling of Variable Probability External Initiating Events in a Functional Modeling Paradigm

Jose Dempere is a graduate research assistant at the Colorado School of Mines in the Van Bossuyt Research Group housed in the Department of Mechanical Engineering. His research focuses on system failure modeling using functional modeling techniques and risk analysis methods. Systems of interest include rockets and space missions, nuclear power plants, and energy systems. He holds a Bachelor of Science in Petroleum Engineering and a Master's of Science in Mechanical Engineering from the Colorado School of Mines.

Dr. Nikolaos Papakonstantinou has a diploma in Electrical & Computer Engineering from the University of Patras (Greece) and a doctorate degree in Information Technology in Automation from Aalto University (Finland). Currently he works as a senior scientist at VTT Technical Research Centre of Finland in the area of system modeling and simulations. He focuses on simulation, model and data driven approaches to system design, operation and safety assessment. Even before moving to VTT, as a post-doctoral researcher at Aalto University, he focused on simulation based safety assessment of complex systems using case studies from the nuclear power production industry. He managed the IFAPROBE project, part of the Finnish Research Programme on Nuclear Power Plant Safety and was the responsible teacher for the "Managing the product life cycle" master level course. His earlier research was in the area of automation software design, mainly targeting IEC61131 and IEC61499 based controllers, with applications on machine, batch and continuous process automation control.

Dr. Bryan O'Halloran is currently an Assistant Professor in the Systems Engineering (SE) department at the Naval Postgraduate School (NPS). Prior to joining NPS, he was a Senior Reliability and Systems Safety Engineer at Raytheon Missile Systems and the Lead Reliability and Safety Engineer for hypersonic missile programs. He holds a Bachelor of Science degree in Engineering Physics and a Master of Science and Doctorate of Philosophy in Mechanical Engineering from Oregon State University. His current research interests include risk, reliability, safety, and failure modeling in the early design of Complex, Cyber-Physical Systems (CCPSs). He is a member of the American Society of Mechanical Engineers (ASME) and the Institute of Electrical and Electronics Engineers (IEEE) and regularly attends the International Design Engineering Technical Conference (IDETC), the International Mechanical Engineering Congress and Exposition (IMECE), and the Reliability and Maintainability Symposium (RAMS).

Dr. Douglas L. Van Bossuyt is currently an Assistant Professor in the Systems Engineering Department at the Naval Postgraduate School (NPS). He holds a PhD in Mechanical Engineering, a Master's of Science in Mechanical Engineering, an Honors Bachelors of Science in Mechanical Engineering, and an Honors Bachelors of Arts in International Studies from Oregon State University. His research interests lay at the intersection of risk and failure analysis, systems engineering and design, manufacturing, and operation of complex systems such as defense systems, nuclear reactors, and aerospace systems. Dr. Van Bossuyt is a member of the American Society of Mechanical Engineers (ASME) and the Prognostics and Health Management Society (PHM Society), and regularly attends the International Design Engineering Technical Conference (IDETC), the PHM Society Conference, and the Reliability and Maintainability Symposium (RAMS).

Threading Together the Twins in a Contextually Relevant Digital World

John Blyler holds a BS degree in Engineering Physics from Oregon State University and an MS in EE from California State University, Northridge. He has co-authored several multi-edition text books on systems engineering, RF-Wireless design and hardware-software computer systems for Wiley, Elsevier and the IEEE, respectively. John is the founding advisor for Portland State University's online graduate program in systems engineering. He teaches online IOT and systems engineering courses at UC-Irvine. He spent many years leading hardware-software integration teams in commercial, industrial, and DOD electronic industries. Finally, he has served as editor-in-chief for a variety for technical semiconductor and embedded trade journal publications.

Supply Chain Risk Management (SCRM)

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

Colophon

The Journal of Reliability, Maintainability, & Supportability in Systems Engineering

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

Office of Publication: 9461 Shevlin Court, Nokesville, VA 20181
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.

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

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

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.

The Journal of Reliability, Maintainability, and Supportability in Systems Engineering

Summer 2018