Early Engagement of Safety & Mission Assurance Expertise Using Systems Engineering Tools: A Risk-Based Approach to Early Identification of Safety and Assurance Requirements

Scott Darpel, Sean Beckman

NASA John H. Glenn Research Center, 21000 Brookpark Rd, Cleveland, Oh 44135, Email:
scott.e.darpel@nasa.gov, sean.m.beckman@nasa.gov

ABSTRACT

Decades of systems engineering practice have demonstrated that the earlier the identification of requirements occurs, the lower the chance that costly redesigns will needed later in the project life cycle. A better understanding of all requirements can also improve the likelihood of a design's success. Significant effort has been put into developing tools and practices that facilitate requirements determination, including those that are part of the model-based systems engineering (MBSE) paradigm. These efforts have yielded improvements in requirements definition, but have thus far focused on a design's performance needs. The identification of safety & mission assurance (S&MA) related requirements, in comparison, can occur after preliminary designs are already established, yielding forced redesigns. Engaging S&MA expertise at an earlier stage, facilitated by the use of MBSE tools, and focused on actual project risk, can yield the same type of design life cycle improvements that have been realized in technical and performance requirements.

1. THE "HIDDEN FACTORY" OF REQUIREMENTS/DESIGN REWORK

Within the process improvement profession, a lot of time is dedicated to unearthing what is called the "hidden factory". This is a term to describe the myriad of steps in a process that evolve to deal with defects or other unplanned outcomes. These steps represent a drain on, or redirection of, valuable resources. They are often taken for granted, but do not add any value to the product. One example of a hidden factory would be the lost luggage department of an airline, with the defect addressed being a piece of lost luggage. No airline set out to design the need to deal with lost luggage into their original baggage handling process, as they did not intend to lose any pieces. And yet, all airlines have that counter at airports to do just that. Over time, these hidden drains on resources can creep into any process, even product development, where unplanned changes can be considered a defect.

Any product development team, whether in the aerospace, automotive, or consumer goods industries, can relate a simple fact: the later in the life cycle a change is made, the higher the impact to cost, schedule, and likely performance or success. Many such changes are the result of late identification of, or modification to, a product requirement. The more complex a system to be developed is, the higher the likelihood that such a miss or modification occurs. Just as with lost luggage, these unplanned changes are something that teams need to spend time addressing, pulling resources away from the true design effort, or increasing cost and schedule. Figure 1 illustrates the "hidden factory" steps that result from requirements "defects" in a the early steps of a typical NASA design life cycle.

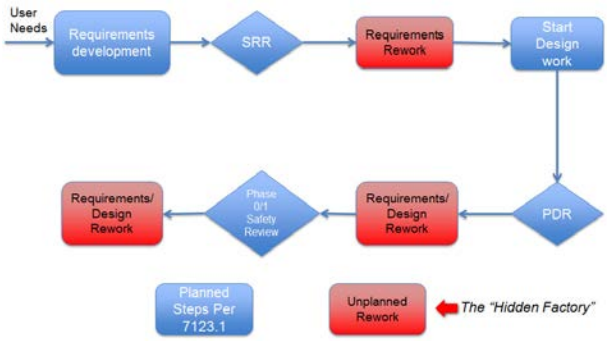

Figure 1: The "Hidden Factory" of requirements/design rework within the NASA design life cycle.

A significant amount of effort has gone into improving the process of capturing requirements within product development, such as that within systems engineering. A great deal of emphasis within systems engineering is focused on the identification, development, and management of project requirements. In his paper, "Systems engineering return on investment", Eric Honour cites the potential payback of 7 to 1 on project cost savings vs. investment in systems engineering efforts[1], much of which is due to this focus.

Systems engineering has evolved both as a discipline, and as a set of tools and practices that facilitate the kind of payback discussed by Honour. The "V" development

cycle depicted in Figure 2 illustrates both the relative timing and interaction of all the key life cycle activities, including requirements development and management. This development of requirements begins with the translation of customer and stakeholder needs during concept development.

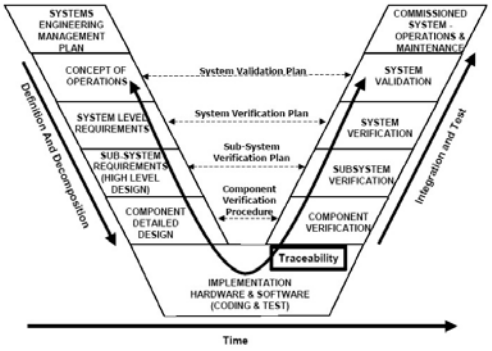

Figure 2: The Systems Engineering "V" approach to project life cycle [2].

It is during the concept development phase where projects begin to capture what is often referred to as the "voice of the customer" (VOC), which can be stated in terms of performance needs, goals, or objectives (NGOs). Teams translate these NGOs into requirements that are actionable, and are able to be verified. This VOC effort exists in product development in all industries, and has inspired the development of such practices as Design for Six Sigma, Concurrent Engineering, Concept Engineering, and Pugh Concept Selection. Within the aerospace and defense industry, this tends to be part of a stage-gate design philosophy capped with some sort of requirements review. Development projects within NASA most often follow the systems engineering practices and reviews specified in NPR 7123.1, "NASA Systems Engineering Practices and Requirements".

2. MODEL BASED SYSTEMS ENGINEERING

While the concepts of, and practices for systems engineering, including the "V" approach, have been implemented to some degree for decades, the recent efforts surrounding the Model Based Systems Engineering (MBSE) movement has provided a significant set of new tools which has greatly improved the effectiveness of the translation of VOC into requirements. These tools allow teams to model and simulate systems at early stages, before committing to any specific hardware architectures or choices.

MBSE makes use of the Systems Modeling Language (SysML) as a means of creating a representation of the system under development. SysML is an offshoot of the Universal Modeling Language (UML) that was developed in the 90's to help software engineers create a representation of the software system that was to be developed. UML is managed by the Object Management Group [3] and has been accepted by the International Organization for Standardization (ISO) as a modelling standard. The overlap and extensions of each set is shown in Figure 3. Both SysML and UML allow teams to represent how their systems should behave and interact with those who are using them.

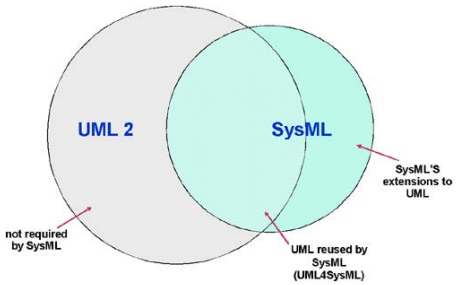

Figure 3: Overlap between UML & SysML tools

Within SysML, there are two main categories of diagrams that allow teams to represent the system: behavior diagrams and structure diagrams (see Figure 4). Early on, it is the set of behavior diagrams that have become valuable in the VOC to requirements translation process. Activity, sequence, state-machine, and use case diagrams give teams a way to represent what the system to be developed is supposed to do, per the NGOs of their customers and stakeholders. For the purposes of this paper, the Activity and Use Case diagrams will be explored further for their utility in improving the engagement of S&MA expertise.

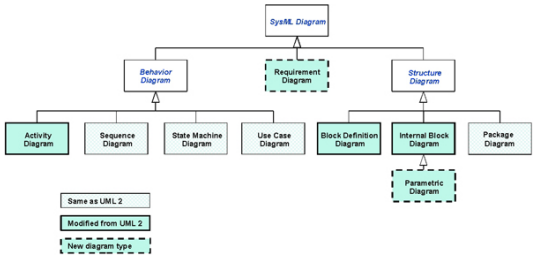

Figure 4: The 9 Diagrams of SysML

Activity diagrams help teams represent a process a given system is to perform. Any one system may be comprised of a number of activities, based on what the end-user needs are. These diagrams can be thought of as the modelling equivalent of a process map or

operational concept. Lenny Delligatti, author of *SysML Distilled*, describes them as “a dynamic view of the system the expresses sequences of behaviors and event occurrences over time” [4]. They detail what steps are to be taken, and in what order.

Use Case diagrams represent how the system and its activities interact with users, also called actors. These diagrams allow teams to depict and model how these actors, including things like the environment the system is to be used in, “touch” the system. Use of activity and use case diagrams, along with MBSE in general, has improved the effectiveness of requirements identification and definition, in terms of the performance requirements for a desired system but has not eliminated the need for re-design on many projects

3. CURRENT PARADIGM FOR S&MA ENGAGEMENT & REQUIREMENTS IDENTIFICATION

Within projects following the stage-gate design process described in in NPR 7123.1, a project’s requirements are reviewed at the System Requirements Review (SRR) stage, but this, again, focuses on the performance requirements. Figure 5 shows the design milestone reviews from NPR 7123.1 and typical safety reviews, superimposed onto the systems engineering “V” paradigm.

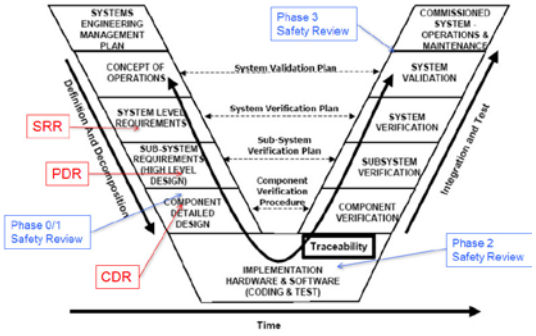

Figure 5: Systems engineering "V" paradigm with NPR 7123.1 and typical safety reviews superimposed. PDR is Preliminary Design Review; CDR is Critical Design Review

With the exception of some risk management focusing on performance NGOs, it is not until after a preliminary design is in hand that significant S&MA expertise is brought to bear on the project. Typically, the preliminary hazards assessment (PHA) is performed based on the preliminary design. Indeed, the first safety review is most often held after the preliminary design review (PDR), and can result in the need to redesign the system to address required safety features. The worst case scenario of waiting until this point in the design life cycle could be a complete abandonment of the preliminary design or concept if it is not possible to address or include required factors of safety or hazard controls. Figure 6 superimposes typical S&MA engagement on the same “V” paradigm.

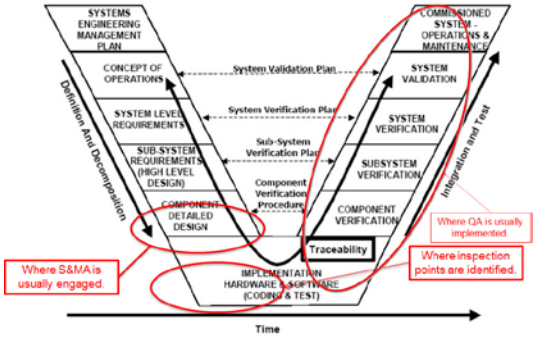

Figure 6: "V" paradigm with typical S&MA engagement

Although the S&MA community contains a rich mixture of expertise that can be thought of as another stakeholder in the system, it is often treated with skepticism in terms of adding value to a project. This is primarily due to a large set of requirements being added late in the life cycle that may or may not be associated with actual project risks. By delaying S&MA engagement, projects can arrive at a point that selection of an alternate concept is infeasible from a cost or budget standpoint, requiring concessions to function or performance to incorporate required safety or hazard controls.

A new paradigm, one that includes early engagement of S&MA expertise following a risk-based approach to the application of appropriate requirements and practices, can lead to a reduction in redesign efforts. The question considered was how to effectively implement such a paradigm shift, such that S&MA requirements can be both identified earlier, and provide real value to project success. Looking to the success of MBSE efforts can be used as an inspiration for such a shift.

4. INTEGRATING S&MA TOOLS INTO MODEL BASED SYSTEMS ENGINEERING, CURENT EFFORTS

The advantages of modeling behaviors and interactions using MBSE methods has been recognized by a growing number of S&MA leaders. As far back as 2004, there have been efforts to examine how the S&MA expertise

might either benefit from, participate in, or enhance the model development. Initially, these efforts have focused on the application of such S&MA domain tools as PRA, FMEA, or reliability analysis within a MBSE-type concept model. Or, within a similarly focused, early-life cycle model that could be used to enhance requirements identification and definition.

In his paper "*Integrating Failure Modes and Effects with the System Requirements Analysis*", Dr. Ronald Carson, introduces the concept of *functional failures* to allow analysts to identify potential system failures while the requirements are still being formulated and assigned to a piece of the functional architecture [5]. In essence, the proposed method has requirements analysts assign failure modes to functions that are modelled within the SE tool, thereby getting a jump on the failure modes and effects analysis that might yield insight into additional potential requirements. While this represents a significant step forward in early risk-informed requirements, some project and engineering leads may avoid the implied formality of a tool like FMEA. In 2014, Hecht, Dimpfl, and Pinchak examined the ability to auto-generate an FMEA from SysML models [6]. Again, a powerful step towards earlier S&MA consideration and potential requirements, but still focused on a potentially limited audience, current practitioners of FMEA.

In 2015, John Evans (NASA HQ), Steven Cornford (JPL), and Martin Feather (JPL) published a white paper and article through the NASA Office of Safety & Mission Assurance (OSMA) examining the concept of Model-Based Mission Assurance (MBMA) and its potential to enhance reliability and maintainability analysis during concept development [7]. The article surveys the landscape of efforts like Carson's, and determined the need to *"clearly and unambiguously establish the roles of uncertainty and risk in the system model"*. The goal has been to identify how to incorporate such tools as Probabilistic Risk Analysis (PRA) and Continuous Risk Management (CRM) earlier into the project life cycle.

5. CREATING A MORE INCLUSIVE FRAMEWORK FOR S&MA ENGAGEMENT DURING CONCEPT DEVELOPMENT

The efforts described, as well as many others, will go a long way to improving the quality of the models used to assist with requirements identification and definition. They have, in large part, focused on the specifics of tool interaction, such as in how one software tool used in the development of a reliability and maintainability (R&M) model can interact with those doing system functional modeling. What is also needed, however, is a way to actively engage the overall S&MA expertise and improve the value-proposition of using such tools, but without the specifics often involved in the software packages. The question under consideration is how to engage people with expertise in S&MA domains without the often complicating factor of software tool specifics. Referring back to Evans et al, what role can S&MA expertise play in concept and early stage model development?

When teams set out to create an Activity or Use Case diagram, one of the most effective methods may be considered one of the most old-fashioned: live and in person. Since the early days of their use, the creation of process maps is best done using a team approach, including those people impacted or served by the process. Developing an Activity Diagram, where a desired system process is going to be represented is no different. The more care given to having the correct expertise at the activity, including S&MA, will yield a better, more accurate depiction and model.

When constructing an activity diagram to depict a desired behavior for the system, the team starts by listing those steps it believes are the proper ones to execute, in their relative order. By taking the additional step of asking "is there anything hazardous about this step", "how can this step go wrong or fail", and "is there any kind of risk associated with performing this step" the team may identify unconsidered steps or conditions. This represents a risk-aware view of the concept under development. It forces the team to consider not just how they want a system to behave, but the ways by which it may fail to do so, or create hazards for the users. Not only is this a useful method by which to prevent redesigns later in the life cycle, it can also cause team members to think about and question the robustness of the activities. S&MA personnel often have a very deep understanding of typical system failure modes and can facilitate this type of discussion. Engaging S&MA expertise during the development of activity diagrams will help teams to consider whether certain safety or assurance requirements may result in a better concept.

Use case diagrams can be thought of in much the same way. As stated earlier, these diagrams depict how users, or actors, interact with the system. For example, a "crew member" may interact with the activity called "enter mode". In the early concept development stage, there will not be a specific manner by which this interaction

occurs, only that it does. Still, the team can consider what the different ways this interaction can go wrong are. This could include “crew member enters the wrong mode”, or “system executes the wrong mode”. Both of these items represent a risk to the system not behaving as required. Teams might consider adding activities for the system to verify that the proper mode is being selected. While this simplified example may appear to be common sense, something addressed through good design, it may not be identified until after a first set of software or sample hardware is delivered.

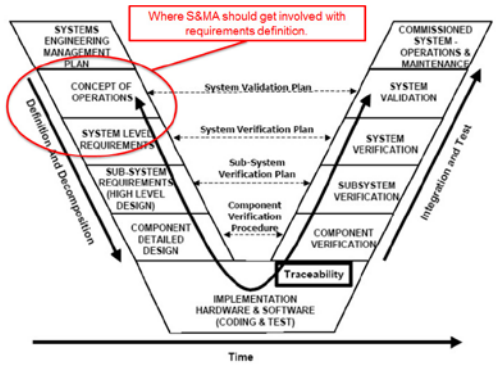

Figure 7: ""V" with Earlier S&MA Engagement

The objective is to draw S&MA expertise earlier into the concept development and requirements identification steps, as seen in Figure 7. Using it in the development of activity or use case diagrams, or similar early system behavior determination, allows the team to:

- Identify potential hazards and their requisite levels of control
- Identify a larger pool of potential risks that can help with concept trade studies
- Identify good practices early that could limit consequences or reduce the likelihood for performance risks

S&MA personnel, typically being those charged with the later development of safety data packages and reviews, are often keenly aware of what different carriers or programs may require for hazards of any type. For example, by understanding very early that a certain fluid is required for an experiment, teams can make an informed choice about controls that may be required due to toxicity levels.

For the purposes of concept exploration, the notional example of a human powered delivery system is considered. A team is tasked with developing a new delivery system that will increase the company’s range, while adhering to a 30-minute cycle time. The following use case and activity diagrams can be considered an example of the typical output from such effort, following traditional flows without early S&MA engagement.

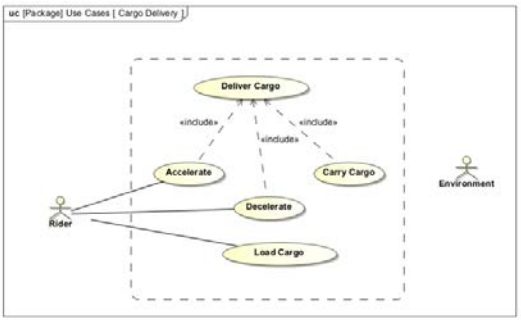

Figure 8: Typical use case diagram for example delivery system

From the use case depicted in Figure 8, the team has identified two potential actors: the “rider”, being the human in the human-powered system, and the environment. The specific use case shows what activities the “rider” interacts with. In this case, the rider must load cargo, accelerate and decelerate.

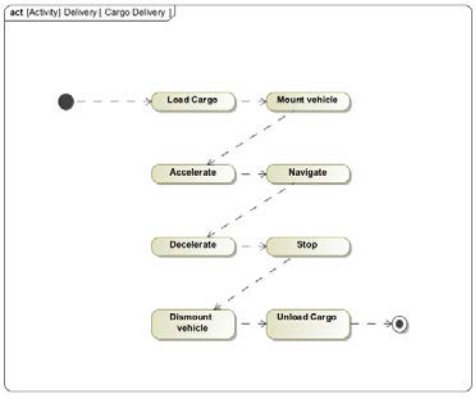

Figure 9: Typical activity diagram for example delivery system

In the activity diagram in Figure 9, the team has captured what was felt to be a primary process, starting with load cargo, and completing with unload cargo.

After going through the exercise of creating the use case and activity diagrams, the team could have come up with a set of performance requirements, such as those listed in Figure 10.

#	Id	Name	Text
1	HPPDV1	Carry Capacity	The HPDV shall carry cargo of at least A m by B m by C m in dimension.
2	HPPDV2	Speed	The HPDV shall be capable of traveling at a speed of at least TBD kph.
3	HPPDV3	Acceleration	The HPDV shall be capable of accelerating at a rate of TBD kph/sec.
4	HPPDV4	Deceleration	The HPDV shall be capable of decelerating at a rate of TBD kph/sec.
5	HPPDV5	Maneuverability	The HPDV shall be maneuverable.
6	HPPDV6	Mass	The HPDV shall weigh no more than TBD kg.
7	HPPDV7	Size	The HPDV shall fit in an envelope no larger than X m by Y m by Z m.
8	HPPDV8	Cargo mass	The HPDB shall carry cargo of at least TBD kg in mass.

Figure 10: Example requirements derived from use case and activity diagrams.

User needs, as modelled through the diagrams, are translated into a requirements set. This initial set of requirements is reviewed at a System Requirements Review, or similar. Once this set of requirements passes review, work begins on the preliminary design, reviewed at the Preliminary Design Review (PDR). Typically, there are some concerns that require redesign as determined by reviewers. At times, this can require requirements re-work. After the PDR is passed, teams work on the initial safety reviews (Phase 0/1). This review can then lead to even more requirements rework.

If the team in the example, however, includes S&MA expertise during the development of the diagrams, expertise that can facilitate asking "what can go wrong with this step or interaction", it may determine that extra attention should be paid to the activity "load cargo". Additionally, the S&MA expertise involved with the development of the diagrams can help determine if there are any applicable regulations or laws that should considered.

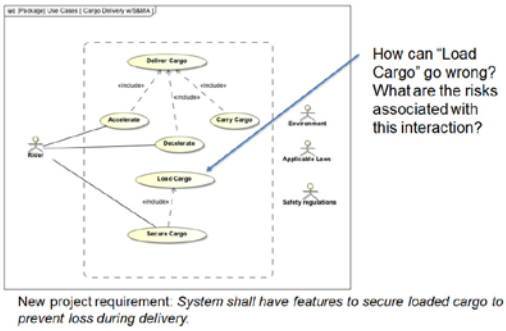

Figure 11: Enhanced use case with S&MA engagement

As an example, the city in which the company operates may have helmet ordinances which could prompt the team to include a requirement for helmet stowage. Per Figure 11, the team also determined that, as the cargo could be improperly loaded, a new requirement for a locking feature would be included. The team may even consider an operational requirement to ensure the cargo is locked in place. This, in turn, can lead to a requirement to ensure that the rider can inspect the condition.

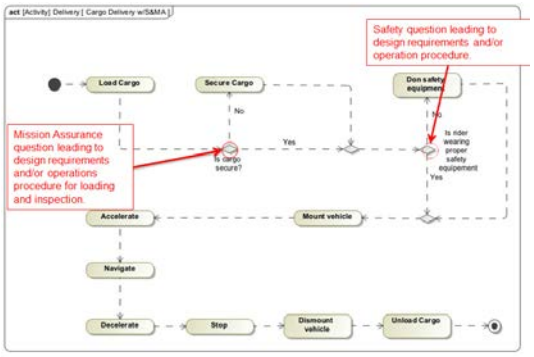

Figure 12: Enhanced activity diagram with S&MA engagement

Looking at the revised activity diagram in Figure 12, the team chose to depict the questions being asked as decision points in the activity flow. They could continue by examining each step on the activity diagram, determining if additional requirements can benefit the system, or reduce the risk associated with its success. This, in turn, may be just one of the activities they need to consider.

The proposed method focuses on personnel engagement in a software tool-neutral setting to bring more expertise into the early stages of determining what a system should do. There are a great many different tools on the market for creating MBSE models, as well as performing S&MA activities such as FMEA or PRA, with some organizations even creating in-house packages, as well. Teams should allow the process of development to determine the needs of software tool use and interaction, rather than having those tools dictate the process followed.

6. SUMMARY

While there are a great many possibilities for bringing specific S&MA models and analyses into direct interaction with those models created during early-phase concept development (within MBSE), the first step is engaging the S&MA personnel and expertise earlier in the requirements definition phase. This can be accomplished by adding the additional considerations and personnel during the development of such MBSE products as the activity and use case diagrams, exploring the risks inherent in the concepts under development. Doing so, engaging S&MA expertise to facilitate the questions "what can go wrong" or "what is hazardous about this", can significantly reduce the need to perform redesign later the in the life cycle due to missed requirements. A team may also find they have an

advantage in creating initial sets of risks and hazards that can improve concept trades or design reviews. The ultimate evolution of Model-Based Mission Assurance will be the natural off shoot of this engagement, creating much more robust system models. Finally, the proposed paradigm reinforces a risk-aware or risk-informed process for the application of additional requirements, again, reducing the likelihood of redesigns later in the life cycle.

7. BIOGRAPHIES

Scott Darpel, MSIE
Program & Projects Assurance Division
Safety & Mission Assurance Directorate, NASA GRC

Scott Darpel earned a bachelor's and master's degrees in Industrial & Manufacturing Engineering from Cleveland State University. He has worked with organizations across many industries on process improvement, product development, systems engineering, and quality engineering. He has been a trainer for six sigma black belt, lean enterprise, set-up reduction and FMEA, and taught undergraduate and graduate level courses in statistical analysis, design of experiments, and quality management.

Mr. Darpel has served as the Chief S&MA Officer (CSO) for GRC's ISS Physical Sciences & Human Research Program, and as the Orion Multi-Purpose Crew Vehicle's external interface requirements manager. He is currently serving on the S&MA Team for NASA's Exploration Systems Development Division, focusing on cross-program risk and the secondary/co-manifested payloads safety review process. Scott is a member of the Cleveland-Northern Ohio chapter of INCOSE

Sean Beckman, CSEP
Quality Engineering and Assurance Branch
Program & Projects Assurance Division
Safety & Mission Assurance Directorate, NASA GRC

Sean Beckman received a Bachelor of Science degree in physics from the University of Akron and is pursuing a Master's of Science degree in Systems Engineering from Worcester Polytechnic Institute. He has spent over 15 years as a systems engineer working various projects for NASA, Boeing and DoD, including NASA GRC's Fluids and Combustion Facility, Orion and Altair spacecraft, the 747-8 aircraft, and the Army's Armored Multi-Purpose Vehicle. While specializing in requirements management he has taken on other systems engineering roles and tasks for these programs. Sean is now a quality assurance engineer at NASA's Glenn Research Center.

A member of the Cleveland-Northern Ohio chapter of INCOSE Sean is an advocate of Model Based Systems Engineering and continues studying SysML and ways it can be used for system development most recently looking at Model Based Mission Assurance (MBMA) in the NASA community. He currently holds an INCOSE Systems Engineering Professional certification.

Mr. Beckman and Mr. Darpel will be co-leading a NASA community of practice in Model-Based Mission Assurance.

8. REFERENCES

1. Honour, Eric, 2013, Systems engineering return on investment, PhD Thesis, University of South Australia. 12 p.

2. www.engineering.com/DesignSoftware/DesignSoftwareArticles/ArticleID/7352/Model-Based-System-Engineering--Beyond-Spreadsheets.aspx

3. http://www.omg.org

4. Delligatii, Lenny (2014). SysML Distilled: A Brief Guide to the Systems Modeling Language. Addison-Wesley, pp 89.

5. Carson, Ronald, Integrating Failure Modes and Effects with the System Requirements Analysis, 14th Annual International Symposium Proceedings, 2004, Boeing Integrated Defense Systems, Seattle, WA

6. M. Hecht, E.Dimpfl, J. Pinchak, "Automated Generation of Failure Modes and Effects analysis from SysML Models", 2014 IEEE International Symposium on Software Reliability Engineering Workshop (ISSREW). IEEE 2014.

7. http://sma.nasa.gov/news/articles/newsitem/2015/11/09/is-model-based-mission-assurance-the-future-of-nasa-sm