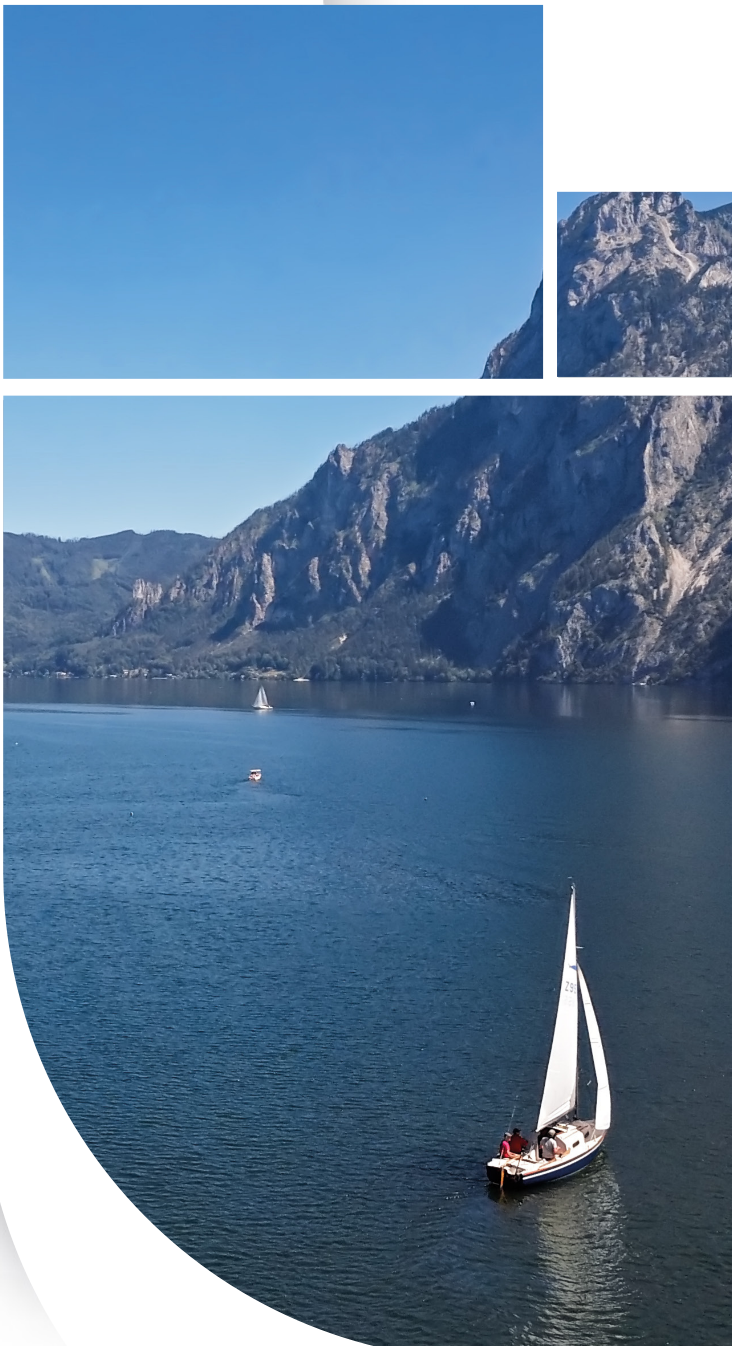
The Future of Systems Engineering

Exploring MBSE Trends in Research and Industry

MBSE Summit 2023 Report

MBSE Summit 2023



LieberLieber

JKU
JOHANNES KEPLER
UNIVERSITÄT LINZ

MBSE Summit 2023

Model-Based Systems Engineering is becoming increasingly important. From design to execution, complex systems should be supported with human-comprehensible and machine-readable models. In this context, the second MBSE Summit was held in Traunkirchen on June 5 and 6, 2023. More than 80 national and international experts and interested parties from science, research, technology, and industry met to discuss current trends and open challenges. The summit started with keynotes from standardization, research, and industry and was followed by intensive discussions in small breakout sessions on different MBSE focal points. It became clear that implementing model-based systems engineering from safety to standards to process quality is essential. Still, often, benefits have to be explained more intuitively, and the exchange between users needs to be intensified through training and discussions.

MBSE Summit is organised for you by LieberLieber & Johannes Kepler University Linz (JKU)

#SECURITY #MBSE

#STANDARDS #SYSMLV2

#RESEARCH

LieberLieber

JKU JOHANNES KEPLER UNIVERSITÄT LINZ

Keynotes

Ed Seidewitz: Building a major modeling language standard: Reflections on how we got to SysML v2 and where we are going

Ed Seidewitz (Model Driven Solutions, OMG) presented the new version of SysML v2 in its current status. It was shown why this new version is necessary and which new functionalities are made possible by this standard. For example, SysML v2 will use not only graphical but also textual notation, and there will be a standard API and exchange format based on JSON so that interoperability and project exchange will be possible. There are also reference implementations in parallel with the development. However, the overall implementation of v2 is more complicated and complex than v1, but it is proving possible.

Judith Michael: Modeling – the Swiss Army Knife of Engineering Methods

Dr. Judith Michael (Software Engineering, RWTH Aachen) lighted the relevance and necessity of modeling in today's modern and complex systems. There is a wide range of possible applications for system models, and research results from the Cluster of Excellence IoP, for example, prove this. The Cluster of Excellence is researching how this versatility of system models can be used and promoted in the system life cycle.

Models can be used well for documentation; they facilitate the understanding of complex interrelationships and make it possible to reduce this complexity. In addition, the models created can be used for various other purposes. For example, it is possible to use engineering models made during system design for the systematic and efficient definition of larger parts of a digital twin.

Tobias Gawron-Deutsch: Feature-based development – Applied MBSE in the context of overall vehicle development

Dr. Tobias Gawron-Deutsch (Robert Bosch AG) explained the application of MBSE in the automotive industry. It was pointed out that there must be a paradigm shift from a document-based to a modeling-based integrated world. Concerning development and application in the automotive sector, he showed the advantages of considering the development steps on a feature basis. This allows components to be developed individually for an overall concept. It is essential to consider the chain of effects "required" to "execute" the feature. There are shared requirements that do not have to be fulfilled by just one feature. These must be considered and validated for all features. The MBSE approach prevents features from becoming isolated silos.

Breakout Sessions

The most important results

MBSE and the Agile Mindset – Guarantees for Successful System Development in the Age of Complexity

Introduced, moderated and summarised by: Stephan Roth, oose Innovative Informatik eG, Hamburg, Germany

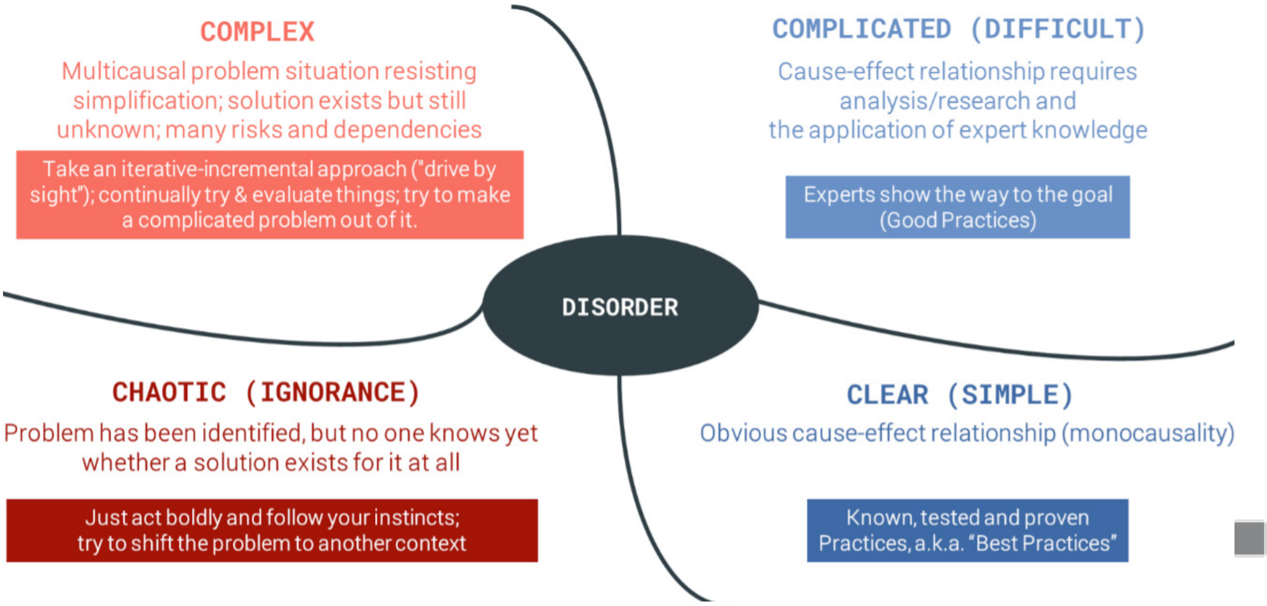
When people talk about the discipline of Model-Based Systems Engineering (MBSE), they often describe it as an approach to dealing with complexity. But what exactly do we mean when we use the term complexity? And which kind of complexity is intended?

David ("Dave") Snowden, a Welsh management consultant and researcher in complexity science, invented the so-called Cynefin framework in 1999. Cynefin is a Welsh word meaning something like „habitat." The Cynefin framework can be used as an aid in decision-making (see Figure 1). It offers five decision-making contexts, a.k.a. "domains": clear, complicated, complex, chaotic, and a center of disorder (confusion).

As described earlier, challenges in systems engineering are often attributed to complexity (the upper left domain is depicted in Figure 1). So, according to the Cynefin framework, these would be multicausal problems resisting simplification. But is that always correct?

I'm sure people often say "complex" when they actually mean complicated. There are a lot of things in Systems Engineering that are just complicated. That means these problems can be solved with the knowledge of experts, e.g., researchers, scientists, and engineers. And, of course, in any systems engineering project, some things are easy ("clear") and can be addressed using best practices.

But when we talk about complexity, my thesis is that in every Systems Engineering project, we have two different kinds (dimensions) of complexity: The complexity of the System of Interest itself and the complexity of the operational environment (context) of the system to be developed.



COMPLEX

Multicausal problem situation resisting simplification; solution exists but still unknown; many risks and dependencies

Take an iterative-incremental approach ("drive by sight"); continually try & evaluate things; try to make a complicated problem out of it.

COMPLICATED (DIFFICULT)

Cause-effect relationship requires analysis/research and the application of expert knowledge

Experts show the way to the goal (Good Practices)

DISORDER

CHAOTIC (IGNORANCE)

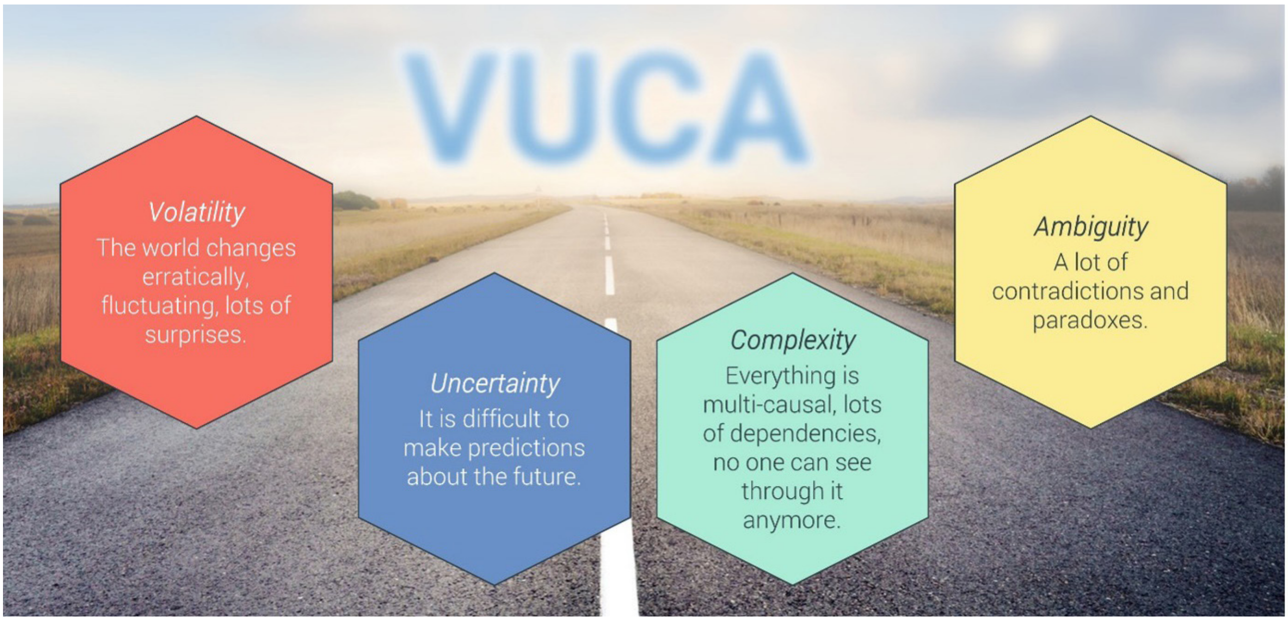
Problem has been identified, but no one knows yet whether a solution exists for it at all

Just act boldly and follow your instincts; try to shift the problem to another context

CLEAR (SIMPLE)

Obvious cause-effect relationship (monocausality)

Known, tested and proven Practices, a.k.a. "Best Practices"


VUCA
Volatility
The world changes erratically, fluctuating, lots of surprises.
Uncertainty
It is difficult to make predictions about the future.
Complexity
Everything is multi-causal, lots of dependencies, no one can see through it anymore.
Ambiguity
A lot of contradictions and paradoxes.

Model-Based Systems Engineering (MBSE) is a very suitable and proven approach to deal with the complexity of the System of Interest itself. But what about the system‘s operational environment and the dynamics that prevail there, i.e., changing market conditions, volatile business goals, changing requirements, and ever-present surprises (for example, geopolitical disruptions, such as wars)? This is what today‘s VUCA world is all about. VUCA (see Figure 2) is an acronym for Volatile, Uncertain, Complex, and Ambiguous. The term "VUCA" was coined in 1987 to describe the volatility, uncertainty, complexity, and ambiguity of general conditions and situations.

My thesis is that MBSE can cope with the system‘s complexity very well but is not very helpful in addressing the complexity of its operational environment, the system's context, or its domain. For this purpose, we need something else: Agile!

In February 2001, 17 well-known software developers met in Snowbird (Utah) to formulate a kind of declaration of principles, a manifesto. It is roughly two pages long but changed the way of thinking about how to develop software significantly: The Manifesto for Agile Software Development (agilemanifesto.org). After some time, the values and guiding principles formulated therein could also be applied to system and product development in general. It doesn't define a process or methodology. It is about people and their collaboration! Ultimately, the Manifesto for Agile Software Development conveys an attitude, a mindset, that should enable those humans involved in a development project to respond appropriately to the constantly changing environment of the VUCA world.

So, my conclusion and thus thesis for the discussion in my breakout session at MBSE Summit 2023 was:

MBSE is not the silver bullet for all challenges in Systems Engineering. To address the complexity caused by the VUCA world, all people involved need an agile mindset, must internalize all the agile principles, and must act accordingly in addition to applying MBS.

MBSE Process and Quality Assurance Guidance

Introduced, moderated and summarised by: Christoph Mayr-Dorn, PhD, Senior Researcher, Institute for Software Systems Engineering, Johannes Kepler University, Linz, Austria
Stefan Klikovits, PhD, Senior Researcher, Institute for Business Informatics, Software Engineering, Johannes Kepler University, Linz, Austria

The session on MBSE process and quality assurance guidance consisted of participants with diverse backgrounds from academia, requirements engineers, system engineers, enablers/consultants, and tool vendors.

To obtain a common ground for discussion and the topic, a short explanation of the passive process engine approach and prototype demonstration was given in which participants experienced one possible mechanism in guiding engineers for fulfilling process and QA constraints. To this end, the prototype scenario showed how such constraints are checked based on engineering information in Azure Dev Ops Services to reason upon which process steps (as part of the user requirements to system requirement refinement process for compliance with Automotive Spice) were fulfilled. The demo then proceeded to show that upon following the guidance from the prototype to fix a violation in Azure DevOps Services, the constraint violation was immediately resolved, and the process status was updated.

The initial provocative question for the ensuing group discussion was, “Would engineers engage in activities to signal engineering process progress and quality assurance status if it was not mandated?” Most provocatively answered this: “Nobody does it if it is not mandated.”
During the discussion of the reason behind this, the value and importance of traceability were confirmed, for example, for bug finding or impact assessment. Process conformance was primarily identified to matter due to regulations, customer requests, project manager interests, and procurement. During the discussion in the context of MBSE, explicitly mentioned activities and situations that would significantly benefit from process conformance checking (and thus guidance support) are to ensure modeling follows a method to avoid fragmented models but achieve streamlined models and to support the synchronization of asynchronous SW/HW co-development.

Along these lines, it was noted that traceability, respectively process activities, still results mainly in an asymmetric cost/benefit: the engineers need to invest the effort, and the benefit appears mainly at the level of team leaders, architects, or managers. Some ideas towards decreasing the perceived burden included training to maintain discipline (similar to trainers in sports demanding tiresome exercise to improve stamina and skill) and to increase motivation by raising awareness of the benefits (aiming to find intrinsic needs of developers/engineers). The question, then, is how to motivate quality and quality assurance in a company. From the beginning, gathering intrinsic motivation for a thorough quality assurance process in modelers is difficult. Usually, motivation is extrinsic, i.e., due to regulations or certification requirements, instructions from “above” (the team leader, company policy), or previous negative experiences (e.g., compare with data backups: “You start backing up data only after you lost some.”). From the tooling side, participants noted that engineers must obtain information on why violation of a constraint matters (criticality), that tooling should minimize the overhead of QA and process conformance, feedback needs to be timely/immediate, and that quality checks for models would be outstanding to have (beyond syntactic). This raises additional requirements on tools to allow access to fine-granular and frequent access to (model) changes at no performance penalty. This is a technical challenge and a question of the tool vendors‘ stance on making engineering data open for integration.

To conclude, a main takeaway from the discussion is that process and QA conformance is, to a significant degree, a human-centric challenge and a technical challenge. In this context, the goal of MBSE should or should not be the motivation of modelers to establish QA guidance but mainly to help users once the process is started.

Significance of Modeling in Fulfilling System Safety and Cybersecurity Goals in Modern Systems

Introduced, moderated and summarised by: Florian Wagner, msg Plaut Manufacturing
MSc Martin Eisenberg, Researcher, Institute for Business Informatics, Software Engineering, Johannes Kepler University, Linz, Austria

The session concerned methods and systematic approaches to developing systems concerning security and safety aspects, with model-based system development (i.e., MBSE) at its core. In this context, significant failure cases of the past and the overlaps in security and safety were discussed.

Although safety and security are distinguishable in their potential effects when neglected, they often have a common origin. The principles and practices used to ensure security and safety in systems share similar foundations and goals. Hence, measures taken that contribute to security often affect the safety aspects of a system and vice versa. They share the aim of risk mitigation and protection against intentional and unintentional harm. In security and safety considerations, a thorough risk assessment is necessary to identify potential risks and vulnerabilities. Systems are designed with measures to prevent incidents from occurring, and when they still happen, they are equipped with a strategy to handle them appropriately and minimize their impact. Furthermore, a reliable system presumes rigorous testing and validation, let alone proper use of instructions, as the human factor can denote a serious impact on both security and safety. Moreover, both are ongoing concerns throughout the system's lifecycle to accommodate threats and risks that evolve over time.

As technical systems become increasingly complex, the importance of addressing system safety and cybersecurity requirements grows. The rise in connectivity features has emerged as a critical driver for enhanced cybersecurity considerations. In cybersecurity, standards have been established to incorporate historical data from prior projects, threat databases, and experiential knowledge to identify and mitigate cybersecurity threats. However, a significant challenge arises when applying these measures to novel systems, as their efficacy may not be adequately ascertained. Put simply, the question arises about the source of historical data when one claims to work on innovative systems that have not yet been encountered. Consequently, ensuring the compatibility and appropriateness of such measures for emerging system types becomes a critical concern. A systematic approach that encompasses both safety and cybersecurity aspects is crucial. Following the importance of modeling as an effective method to fulfill system safety and cybersecurity goals in modern systems, providing an overview of its benefits and application shall be discussed.

To address the question of "What needs to be protected?" a systematic approach becomes essential. In many cases, system safety and cybersecurity measures can be mutually exclusive. However, there are instances where one measure can effectively fulfill both safety and cybersecurity goals. For example, a simple mechanical pressure relief valve can prevent a boiler from exploding, whether caused by malfunction or malicious intent. Compliance with programming guidelines, such as Misra-C, can reduce code weaknesses, benefiting safety and security.

A warning against insufficient consideration of safety issues can be drawn from past events. The A320 Warsaw accident demonstrated the consequences of incorrect maintenance procedures and a lack of proper security protocols. The aircraft crashed, resulting in the loss of numerous lives, and has become a warning example for the aviation industry. An example of the importance of ensuring safety and security in space exploration is the Mars Polar Lander incident. A software error caused the spacecraft to shut down its engines prematurely, leading to a crash landing on Mars. The incident underscored the need for robust software development practices and rigorous hazard analysis in space missions.

In some scenarios, it may be challenging to determine whether an issue falls under safety or security. Consider the case of an autonomous vehicle that crashes due to biased data used for training a neural network. Is it a safety issue, a security issue, a data integrity issue, or a system availability issue? Such cases require finding solutions that transcend traditional boundaries. A common method capable of addressing multiple considerations, particularly system safety and cybersecurity, would be advantageous.

Modeling provides a comprehensive approach to addressing system safety and cybersecurity concerns. By meeting specific requirements, modeling offers numerous advantages for modern systems:

- Analysis for Multiple Purposes: Modeling allows for a holistic analysis that serves multiple objectives, reducing the need for separate assessments.
- Fewer Interfaces, Fewer Vulnerabilities: A well-designed model reduces the number of interfaces, minimizing potential vulnerabilities and improving overall system resilience.
- Enhanced Overview: Modeling provides a shared visual representation that offers a better understanding for all stakeholders involved.
- Integration of safety and security analyses within the system model
- Usability for Management and Engineering: Modeling allows abstraction across all levels of development, presenting not only technical factors but also encompassing broader aspects relevant to management and engineering perspectives.

What are the anticipated prerequisites for a comprehensive approach that identifies both safety hazards and cybersecurity threats while allowing for the systematic mapping of concerns about safety, security, mission, publicity, and finances to their corresponding assets? One notable analysis method that fulfills the requirements of a comprehensive approach is Systems-Theoretic Process Analysis (STPA). Developed at MIT under the guidance of Nancy Leveson, STPA is a hazard and risk analysis method based on systems theory. Its goal is to identify damage scenarios based on stakeholder concerns, which can be risks to human lives, financial loss, privacy breaches, and more. STPA can be applied across various industries and domains, focusing on compliance with system constraints rather than

solely preventing failures. To implement STPA effectively, the following steps must be followed:

1. Definition of Losses and Hazards: Identify losses, which include anything of value to be avoided, and hazards, which represent system states that can lead to losses in worst-case scenarios.
2. Definition of the Control Structure: Establish the logical and functional architecture of the system, determine feedback between system blocks, and define control commands (Control Actions) between blocks.
3. Identification of Unsafe Control Actions: Analyze and identify unsafe control actions in specific contexts.
4. Definition of Loss Scenarios: Determine the causal factors that lead to Unsafe Control Actions, thereby creating loss scenarios.

Example Loss Scenario: “ACC does not provide braking when the distance to the obstacle in front is too low due to incorrect distance information.”

- Functional Safety Analysis: Further analyze the possibility of erroneous distance data caused by sensor malfunction.
- Cybersecurity Analysis: Ensure the protection of distance data from manipulation.

In modern systems, modeling is crucial in fulfilling system safety and cybersecurity goals. Organizations can comprehensively address safety and security concerns by adopting a systematic approach and leveraging modeling techniques such as STPA. Modeling provides numerous benefits, including enhanced risk analysis, better decision-making, and a shared understanding among stakeholders. By embracing modeling, organizations can proactively tackle the complex challenges posed by system safety and cybersecurity, ultimately leading to safer and more secure systems in the digital era.

An additional advantage inherent in this approach lies in its enhanced efficiency, a quality of utmost significance given the prevailing scarcity of safety and cybersecurity experts vis-à-vis the growing demand. Standardizing analysis methods becomes imperative to foster seamless collaboration and facilitate comprehensive analyses spanning multiple organizations and tools. In this regard, the introduction of RAAML represents an initial stride toward achieving this objective. RAAML, developed by the Object Management Group (OMG), is a standardized modeling language for risk analysis and safety assessment.

All in all, security and safety are integral to systems engineering, ensuring the reliability and resilience of complex systems. STPA and FMEA are essential tools for identifying and mitigating hazards and risks. The A320 Warsaw accident and the Mars Polar Lander incident serve as reminders of the consequences of neglecting safety and security. With MBSE, principles of systems engineering, such as „security-by-design”, can be effectively integrated into the development process and the same facilitated with tool support like RAAML, and therefore, lead to more robust and secure systems. Moreover, the machine-readable nature of models facilitates seamless integration with analysis tools, making it easier to perform automated security and safety assessments. In turn, engineers can effectively identify and address potential hazards, assess risk levels, and develop targeted mitigation measures. MBSE further encourages collaboration and communication among multidisciplinary teams as models provide a common point of view and language. Therefore, they facilitate better understanding and decision-making throughout the development lifecycle, ensuring that all concerns of the stakeholders are adequately addressed. MBSE enhances the overall reliability, resilience, and safety of complex systems by supporting automation and promoting a proactive security approach and facilitates meeting the ever-growing demands of secure and safe technologies in an interconnected world.

The Power of Standards: Unleashing the Potential of MBSE

Introduced, moderated and summarised by: Daniel Siegl, LieberLieber Software
Sabine Sint, Researcher, Institute for Business Informatics, Software Engineering, Johannes Kepler University, Linz, Austria

In the standards session, we dealt with the topic of standardization. Why are standards relevant? How quickly are they implemented? Are they still up to date?

We identified some frustrations concerning standards committees. It isn‘t easy to get funding just for participating in standards. Therefore, there is a lack of contributors, but later, there are complaints about the lack of features in the standards. Standardization often requires not only a technical contribution but also “political” interventions and finding compromises. In other words, there is often a trade-off between user-friendliness and provider satisfaction, and ultimately, these compromises can dilute the actual vision. In addition, the standardization process can require a blueprint for everything very early on. This complicates the process of adding/changing/discarding features later on. Furthermore, the reasons for designing a standard are often not systematically recorded and published. The question then arises as to why things are the way they are.

The users of a standard must understand the business case to accept the norm.
Standards are usually difficult to read and interpret. They are also generally excessively long. This can lead to misinterpretation and the need for expensive training. It also often happens that users ignore rules and best practices. Furthermore, there is a lack of interoperability of “standardized” tools and models, making the practical application of a standard more complex, and best practices are often not explicitly standardized. Another complicating factor for applying a standard is that many have to be purchased at great expense and are, therefore, rarely used in education and training.

In addition to these problems, the general standardization process can also cause frustration. There is a lack of harmonization of standard parts developed by different groups, and errors can be overlooked. In general, the standardization schedule is quite long, so that results are only available late. However, a rushed specification can also mean it cannot be implemented. The work in the committees can feel opaque as attendance fluctuates, group members change, and, in some groups, there is a lack of professional management.
However, there are also possible solutions to the challenges mentioned. For example, public funding could be made available for standardization bodies so that more people become invol-

ved in standardization. This would also allow the group's expansion to be driven forward early. In addition, examples and reference implementations must be provided with the standards so that users can also understand the standards. It is also essential to provide non-trivial application examples.

Concerning the documentation of standards, besides the specification, which is often difficult to read, there should also be application documents and documents for the community.
In the standardization process, professional moderation of standardization groups should be considered. In addition, an iterative development approach should be used for standardization so that incremental development is supported. Sometimes, the best starting point is a minimum viable product!

MBSE Summit 2024

LieberLieber

JKU JOHANNES KEPLER UNIVERSITÄT LINZ

Would you like to attend the 3rd MBSE Summit in Traunkirchen? (June 10 and 11, 2024) Then register now, we look forward to seeing you:

MBSE Summit 2024 Registration

In 2024, our MBSE Summit will take place in Traunkirchen for the third time. From 10. - 11.6.2024 the MBSE community will once again meet to discuss the latest trends. We have already been able to secure three well-known experts for the keynotes:

- Univ.-Prof.in Dr.in Cristina Olaverri-Monreal, President IEEE Intelligent Transportation Systems Society and Head of the Chair for Sustainable Transport Logistics 4.0 at the Johannes Kepler University Linz
- Florian Beer, Chief Software Architect, Bosch
- Tim Weilkiens, Executive Board of oose Innovative Informatik eG

Imprint

Responsible
Dr. Konrad Wieland
LieberLieber Software GmbH

Prof. Manuel Wimmer
JKU Linz

Content
Sabine Sint, JKU/TU Wien
Rüdiger Maier, LieberLieber Software GmbH

Graphic Design
Florian Kalenda, LieberLieber Software GmbH

Graphics
LieberLieber Software GmbH, iStock, oose Innovative Informatik eG

Contact
welcome@lieberlieber.com