WHITEPAPER

How to Manage Cybersecurity in Jama Connect® for Automotive and Semiconductor Industries

Learn how automotive and semiconductor teams use requirements management tools to support meeting ISO/SAE 21434 while increasing visibility, collaboration, and review-cycle efficiency.

Written by Kevin Dibble and Jama Software

Introduction

Security threats such as malware, ransomware, and data breaches impact many industries, but with expanded connectivity in the automotive and semiconductor sectors, increased urgency exists to safeguard against fast-evolving risks.

Research shows that 91% of vehicles are connected, and that number is expected to rise to 96% by 2030. With more automobiles and semiconductor devices being connected, attack surfaces (cybersecurity vulnerabilities) are expanding quickly, and the ISO/SAE 21434 standard aims to understand and safeguard against potential threats.

However, managing a cybersecurity case within the standard requires many steps, and cross-team visibility and collaboration are often challenging. As a result, some teams are turning to requirements management tools to help improve visibility and increase transparency in review cycles.

If you haven't used a formal requirements management tool before, understanding the benefits, advantages, and how it works helps determine if it's right for your team.

91%

Research shows that **91% of vehicles** are connected, and that number is expected to rise to 96% by 2030.

Why manage a cybersecurity case in a requirements management tool?

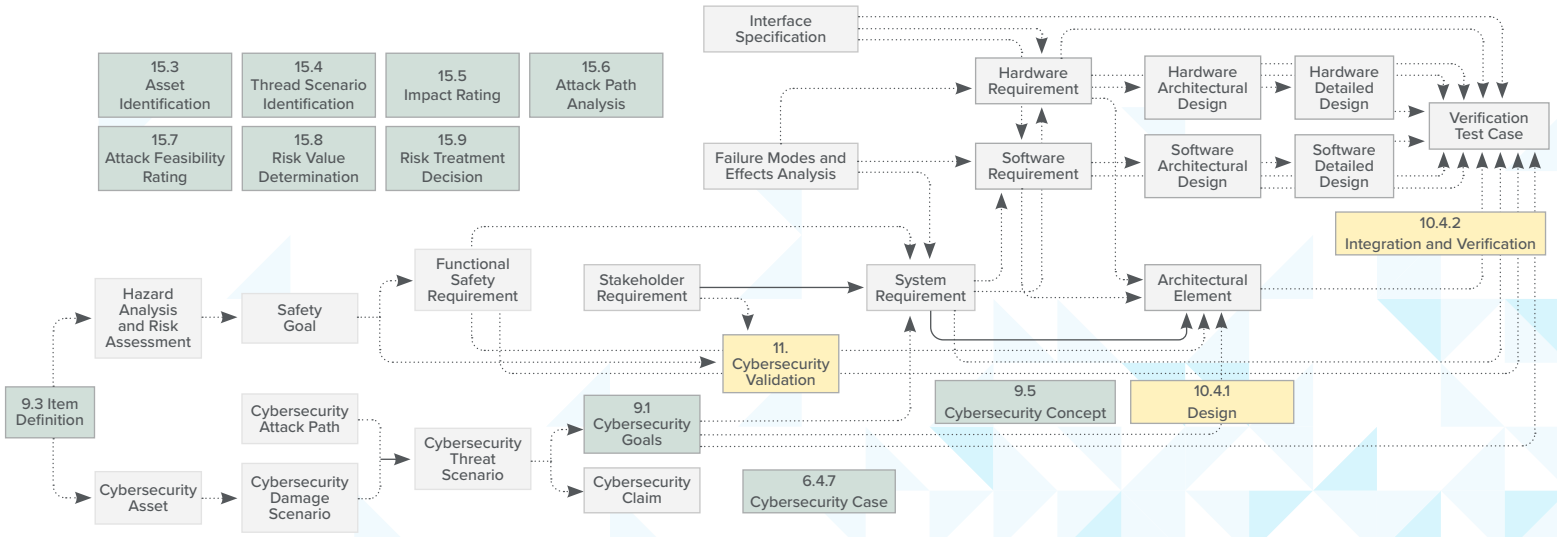
Creating a cybersecurity case for ISO/SAE 21434 is a complex process with many moving parts. Using a requirements management tool has many benefits, including improved traceability, easier collaboration, and improved functionality for reviews.

Here are several ways a tool can help.

1. Improved collaboration between OEMs and tier 1 and 2 suppliers. A requirements management tool, such as Jama Connect®, supports requirements interchange format (ReqIF), which can be used for bidirectional communication of requirements, item definitions, and more. Using the tool, you can support improved collaboration workflows.

2. Provides "trace as you go" visibility. You don't want traceability to be an afterthought handled by your requirements engineer at the end of the project, especially when that project is complex. A purpose-built requirements management tool, like Jama Connect, allows you to create requirements tracing to parent requirements, design blocks for requirements allocation, and more. It supports a trace-as-you-go methodology.

A cybersecurity case is a structured argument supported by the evidence of work products to detail why risks found within the Threat Analysis and Risk Assessment (TARA) are reasonable.



3. Access impact analysis to handle midstream project changes more effectively. Jama Connect provides access to an impact analysis, a powerful capability supporting the trace-as-you-go approach. Running an impact analysis as project changes happen midstream allows for greater understanding and visibility.

4. Automatically generate test coverage reports. With Jama Connect, you can allocate requirements to design blocks or interconnect the requirements management system to design tools. Using tools like Design Architect provides powerful analytics and test coverage reports that are automatically generated.

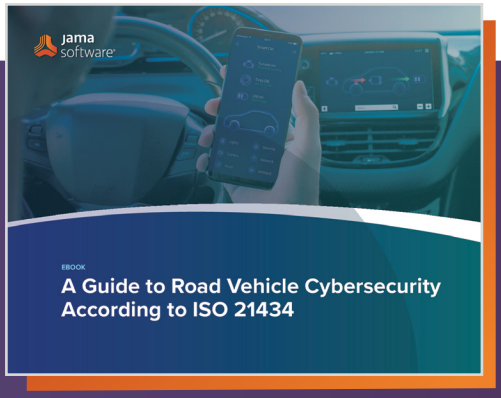
5. Connect tools and avoid disjointed tooling challenges. Disconnected tools are often a source of visibility issues. Jama Connect links disparate tools and offers a "toolchain view" for more seamless tool functioning and visibility, like with the Design Architect example above.

6. View exactly where you're at in a project in real time. As you move through the management of a case, it's important to see where you are in the process so you can stay on track. Jama Connect can provide analytics that clearly indicate where you're at in a project, including allocated requirements, tests that have been covered, and more.

EBOOK

A purpose-built requirements management tool can significantly improve traceability and collaboration and streamline reviews when managing your ISO 21434 cybersecurity case. Learn more by reading our eBook, *"A Guide to Road Vehicle Cybersecurity According to ISO 21434"*

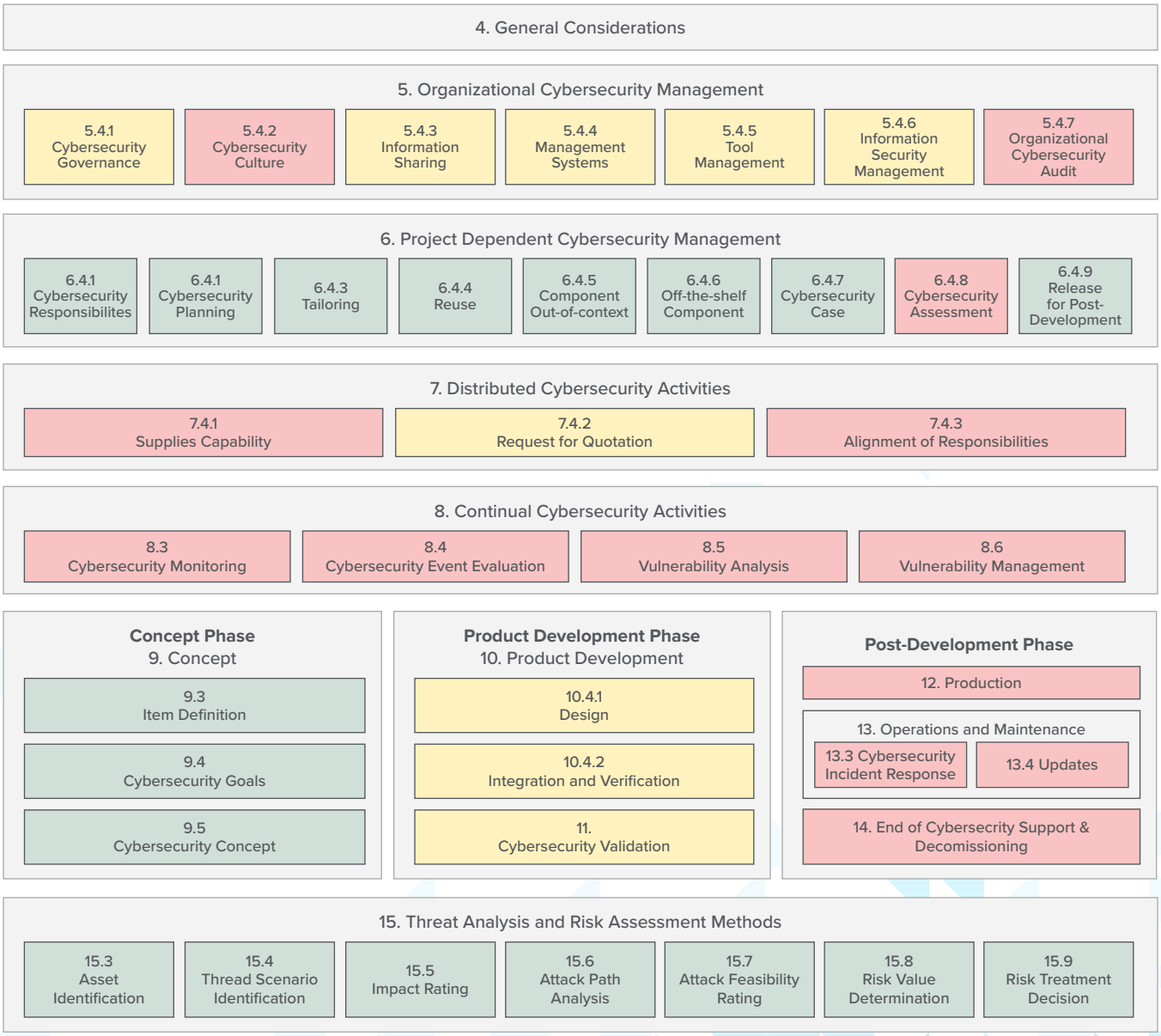
Download the eBook »



How does a requirements management tool fit with the ISO/SAE 21434 standard?

Traceability, collaboration, and improved review processes are all benefits of a purpose-built requirements management tool, but to understand how it works, it helps to have an example. In the details below, we've used the Jama Connect platform as an example to see how it works – from product-dependent cybersecurity management to threat analysis and risk assessment methods.

ISO/SAE 21434 is organized by clauses and subclauses, which are broken out below.



The right requirements management tool will enable your teams to optimize the development process in many of the above areas. Specifically, here's a breakdown of how the Jama Connect platform supports each of them, as indicated by the box's color.

Green. These areas are fully supported and recommended to be implemented in Jama Connect. For example, when viewing section 9 in the chart above under the "Concept" heading, Jama Connect supports the item definition, cybersecurity goals, and cybersecurity concept.

Yellow. These are optional and can be implemented in Jama Connect. For example, you'll see subclauses 5.4.3 "Information sharing" and 5.4.4. "Management systems" fall into this category.

Yellow-green. These are partially supported in the tool. In other words, Jama Connect can support some of the requirements but not all of them. As an example, 10.4.1 "Design" and 10.4.2 "Integration and verification" are included in this category.

Red boxes. These are not recommended for support in Jama Connect and are usually handled with an in-house tool instead—in that some are processes that expand throughout the organization, and some are activities or work products suited for alternative best-of-breed tools. The progression of these work products can, however, be brought back to Jama Connect to reflect status through the Cybersecurity case. An example is the areas under the "post-development phases, including 12 "Production" and 13 "Operations and maintenance."

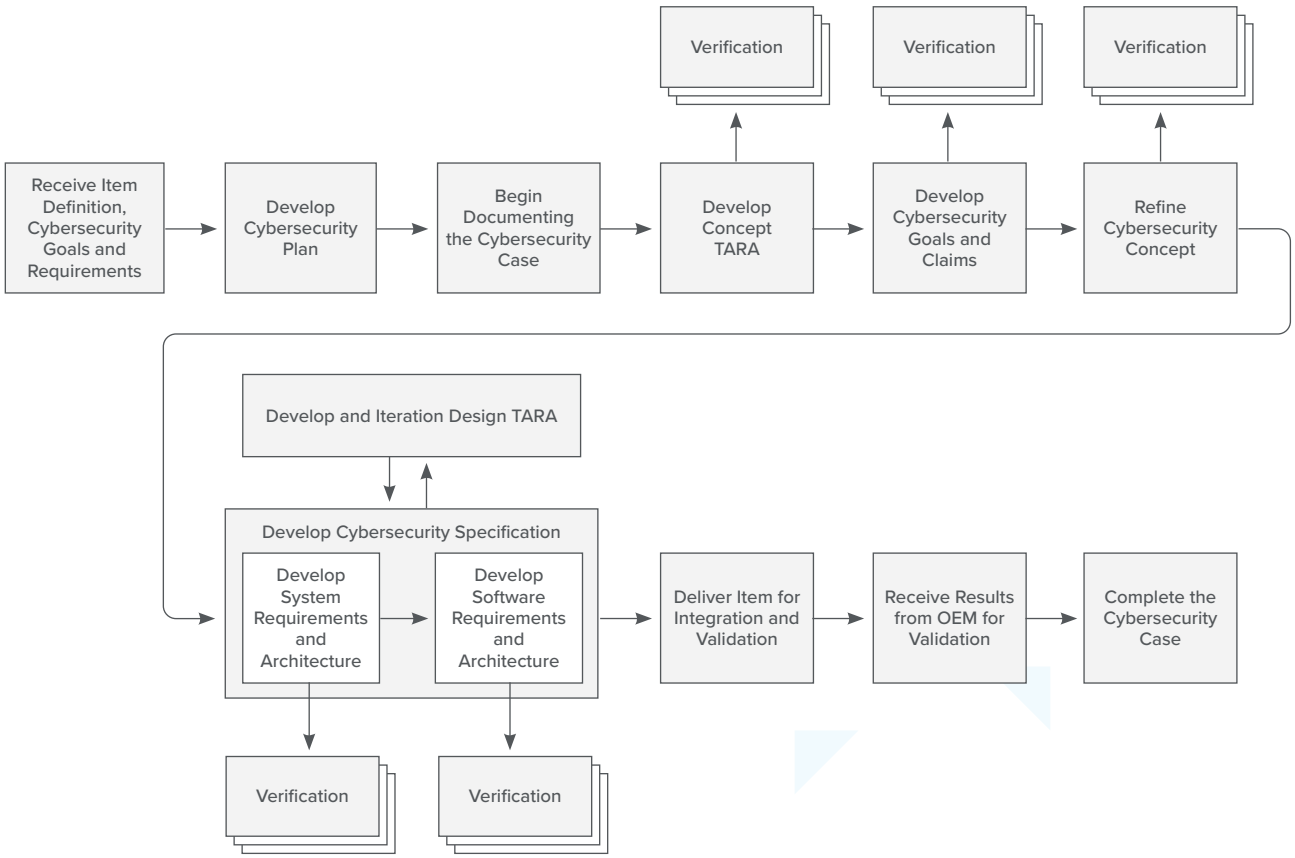
One of Jama Connect's most powerful capabilities is supporting the green and yellow categories through **document building** and **generation**. The tool supports the process of building and reviewing documentation with real time collaboration as well as creating documentation with a single click and no post processing.

Interested in learning about how AI can improve your products, systems, and software? Meet Jama Connect Advisor™, Jama Connect's natural language processing (NLP) tool, designed to improve requirement quality.

Watch this short video »

Understanding the tier 1 flow and how a requirements management tool supports your team

A requirements management tool supports you from receiving the item definition to completing the full cybersecurity case. There are eight steps in between, and we'll walk you through how Jama Connect helps during each of the eight steps.



1. Receive item definition, cybersecurity goals, and requirements

After receiving the item definition from your OEM, you can import the document into Jama Connect. Importing allows your team to review details in the context of cybersecurity, make comments, and note any required changes. Once everyone has settled on the item definition and next steps, your team can get to work on the artifacts required for cybersecurity.

2. Develop cybersecurity plan

The cybersecurity plan typically includes objectives, dependencies, and resources. You can organize all those important elements within Jama Connect, just as you would a traditional document, and Jama Connect has a template for doing that.

Additionally, you can comment against items and review the document as it's being created. You can also export the document, including referral links within the file, without having to leave the system.

3. Begin documenting the cybersecurity case

The cybersecurity case is a structured argument supported by the evidence of work products to detail why risks found within the Threat Analysis and Risk Assessment (TARA) are reasonable. With Jama Connect, you can easily document that argument. You can also understand how work products are related to downstream reference documents and easily view the evidence and status of all moving parts, such as outstanding reviews.

4. Using Jama Connect to Develop concept TARA

Once you've defined the cybersecurity case, you can use Jama Connect to support work on the TARA. Several factors must be considered, and the tool can help with each and provide the appropriate work product, including:

- **Identify items.** Identify the cybersecurity assets against the item definitions.
- **Identify assets.** Relate downstream cybersecurity assets within the system.
- **Identify cybersecurity properties.** Associate cybersecurity properties with assets that would lead to damage scenarios.
- **Identify damage scenarios.** Record cybersecurity properties in the damage scenarios, including their relation to an item's functionality and any adverse consequences.
- **Determine impact rating for DS (SFOP).** Conduct a four-dimensional SFOP impact analysis for safety, financial, operational, and privacy metrics to help determine relevant impacts.
- **Identify threat scenarios.** Create downstream threat scenarios, which are potential causes of a compromise of the cybersecurity properties of one or more assets.
- **Identify attack paths.** Attack potential within the tool provides ratings that enable you to define feasibility.
- **Rate the feasibility of attack paths.** Define feasibility based on rating, which originates from a template that Jama Connect includes automatically.
- **Determine risk for threat scenarios.** More than one attack path can exist for a cybersecurity threat scenario. Within the tool, you can take the most feasible of the attack paths against the scenario and determine risk treatment options.
- **Establish cybersecurity goals and claims.** You can create a cybersecurity goal resulting from reducing the risk.
- **Develop a cybersecurity concept.** The tool houses all the elements needed to develop your cybersecurity concept, so you can easily pull it together within the system.
- **Develop cybersecurity specifications.** Easily tie back to cybersecurity specifications within the tool.

It's also important to note that you can navigate the entire process at a glance with Jama Connect. For example, you could conduct a trace view and view an item from cybersecurity assets, and from there, you could jump to the damage scenarios and add different types of impacts.

You could also go further downstream to view your threat analysis. Viewing everything at a glance gives you improved visibility into the whole picture.

5. Develop cybersecurity goal and claims

A cybersecurity goal can be created for any threat scenario needing risk reduction in a cybersecurity claim or threat scenario. Once goals are defined, you can define derived cybersecurity requirements and validate those with test cases within the tool.

Most of the time, the OEM will complete the validation of the goals but it's important to know that it can be done in the Jama Connect.

6. Refine cybersecurity concept

Once you've defined cybersecurity claims and goals, you can use the tool to work on the cybersecurity concept. The documentation and text have already been collected within the tool to support creation.

7. Develop and iterate design TARA

You can develop cybersecurity specifications, including development system requirements and architecture, and develop software requirements architecture and verification for both.

8. Deliver item for integration and validation and get results

Within the tool, you can also create a verification plan with validation. You can run items through a test plan, or multiple tests, by simply clicking the "test" option. As you complete this process, the tool will support you in working toward full verification against the cybersecurity goal and completing your cybersecurity case.

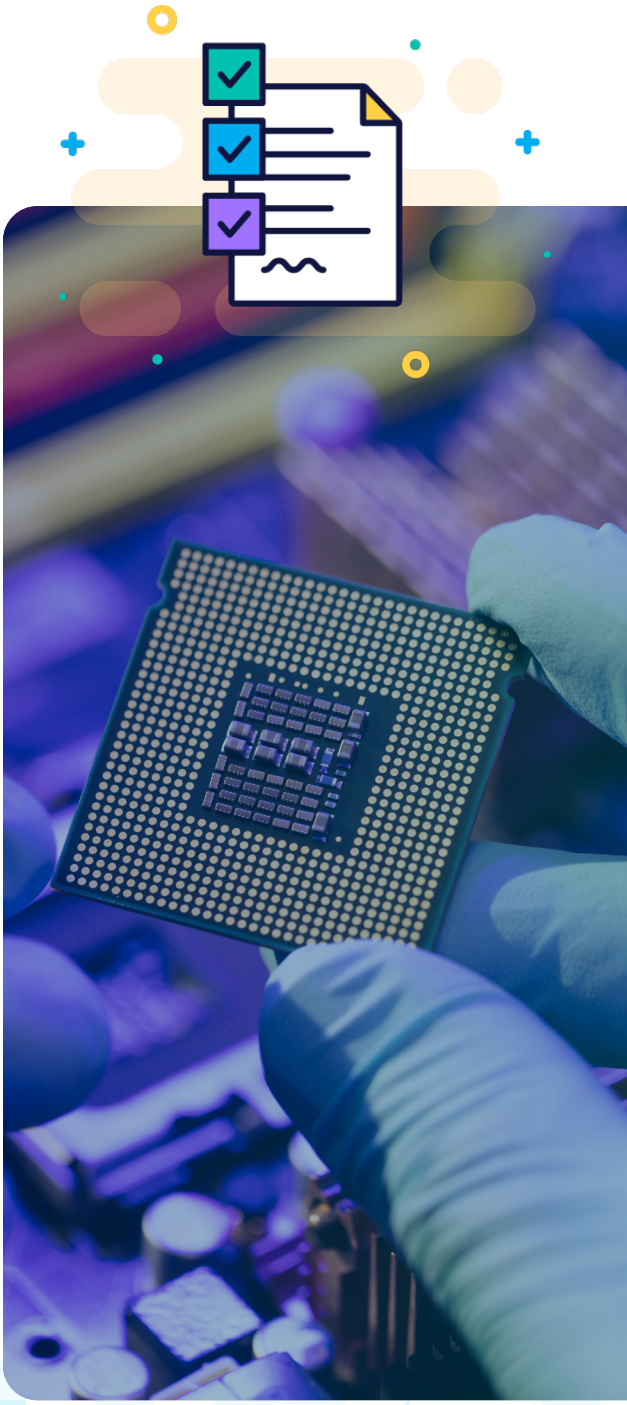
WEBINAR

See it in action! Watch our webinar to see how Jama Connect can help you effectively manage cybersecurity.

Watch the webinar »

Achieving flexibility and customization with a requirements management tool

Since every team's needs differ, having a customizable tool is important. Jama Connect allows a high level of flexibility, allowing you to customize based on your specific needs. Also, consider a tool's integration capabilities since you might want your output to flow into a product lifecycle management (PLM) tool. Jama Connect can integrate with many tools, including most PLM tools.



Live Traceability™ is also key, since the tool automatically tracks relationships and dependencies between various elements throughout the product development lifecycle. With Live Traceability, you can quickly understand the impact of changes on related artifacts, assess risk, and improve collaboration among cross-functional teams.

As automotive organizations move into the future, high-quality tools that support meeting cybersecurity-related standards will only grow more important. If you'd like to explore how requirements management tools like Jama Connect can help, our experts can support you in getting started with a free trial of the platform.

Connect with us here »

ABOUT THE AUTHOR

Kevin Dibble, President at Reinnovate Consulting

As a Engineering Consultant, Kevin Dibble helps companies primarily in the Automotive Industry improve their agile adoption and automotive compliance to ISO 26262, ASPICE, and ISO 21434 by leveraging the ASPICE model, the ISO 26262 and ISO 21434 standard, and Agile / Lean principles.

As an interim CTO and Go to Market expert, he helps companies, mainly startups, create and implement strategies to iteratively deliver innovate products based on Agile methods and state of the art targeted marketing.

Specialties: Agile Software Development, ASPICE, ISO 26262, ISO 21434, Model Driven Design, Artificial Intelligence, Machine Learning (ML), Natural Language Processing (NLP), Embedded Systems, 2D and 3D Graphics Technology, OpenGL, Marketing Technology, MultiVariant / MVT, A/B testing, Behavioral Targeting, Segmentation, Personalization, Lead Generation.

Jama Software® is focused on maximizing innovation success in multidisciplinary engineering organizations. Numerous firsts for humanity in fields such as fuel cells, electrification, space, software-defined vehicles, surgical robotics, and more all rely on Jama Connect® requirements management software to minimize the risk of defects, rework, cost overruns, and recalls. Using Jama Connect, engineering organizations can now intelligently manage the development process by leveraging Live Traceability™ across best-of-breed tools to measurably improve outcomes. Our rapidly growing customer base spans the automotive, medical device, life sciences, semiconductor, aerospace & defense, industrial manufacturing, consumer electronics, financial services, and insurance industries. To learn more, please visit us at jamasoftware.com.