WEBINAR

Implementing Requirements Management for ISO 21434

Jama software®

Adrian Rolufs

DIRECTOR OF SOLUTIONS

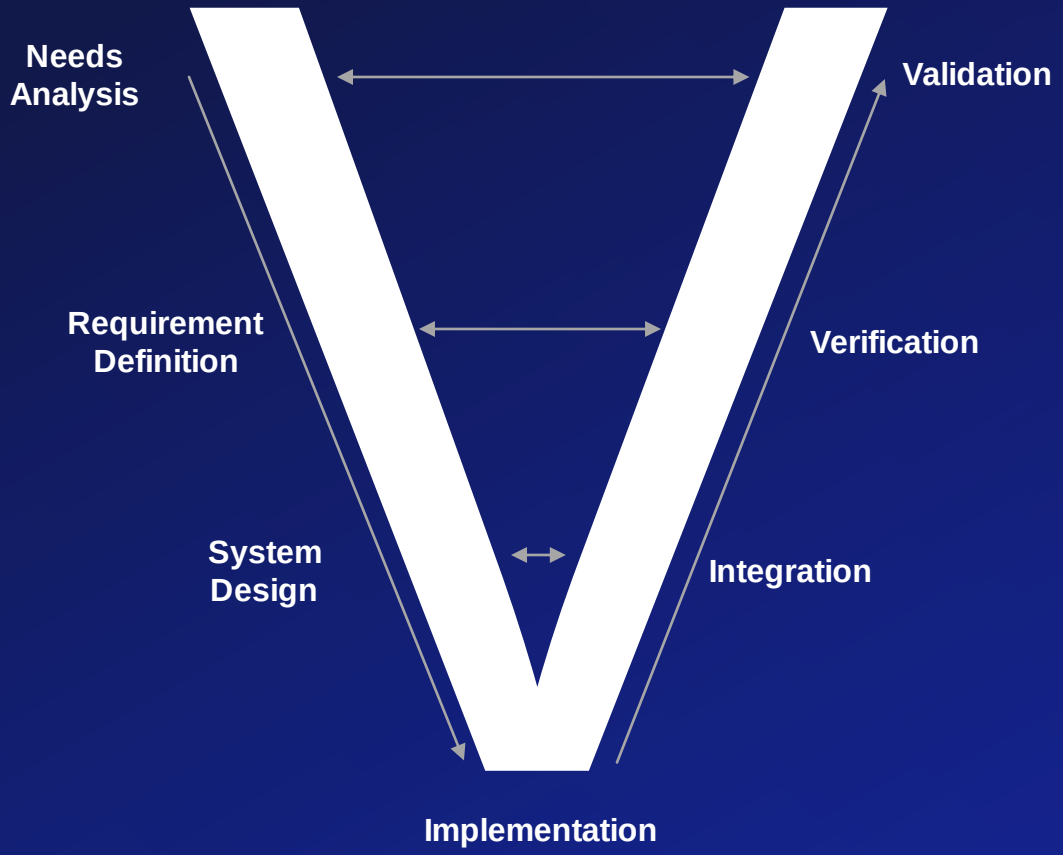
Jama Software

Agenda

- Overview of ISO 21434 impact to requirements management
- Similarities between requirements for functional safety and cybersecurity
- Updating an example requirements management data model for cybersecurity requirements
- Proposal for implementing a TARA in a requirements management database

Jama Software

PROVIDES…



FOR…

5 of the TOP 10	Global Semiconductor Companies
6 of the TOP 10	Electric Vehicle (EV) Startups in the World
6 of the LEADING 10	Global Semiconductor Companies Powering Autonomous Vehicle (AV) Production
3 of the TOP 8	Electric car manufacturers in the world
3 of the TOP 10	Automotive Manufacturers in the world

Jama powers the leading market innovators to build great products.

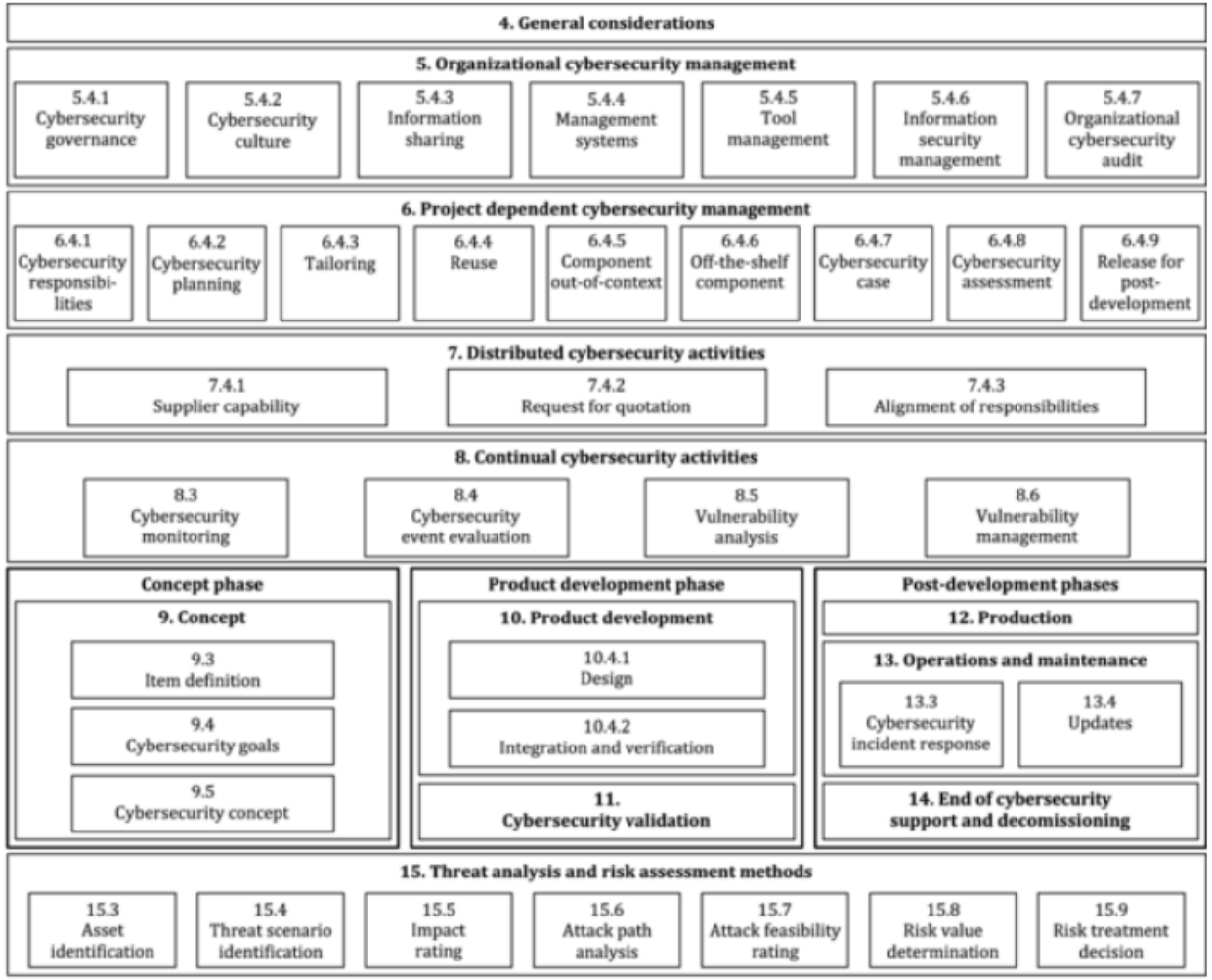
ISO 21434

Impact to Requirements Management

ISO 21434

IMPACT TO REQUIREMENTS MANAGEMENT

- ISO SAE 21434 "**Road vehicles — Cybersecurity engineering**" focuses on cybersecurity risks in the design and development of car electronics.
- The standard specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.
- Supports the implementation of a Cybersecurity Management System (CSMS)

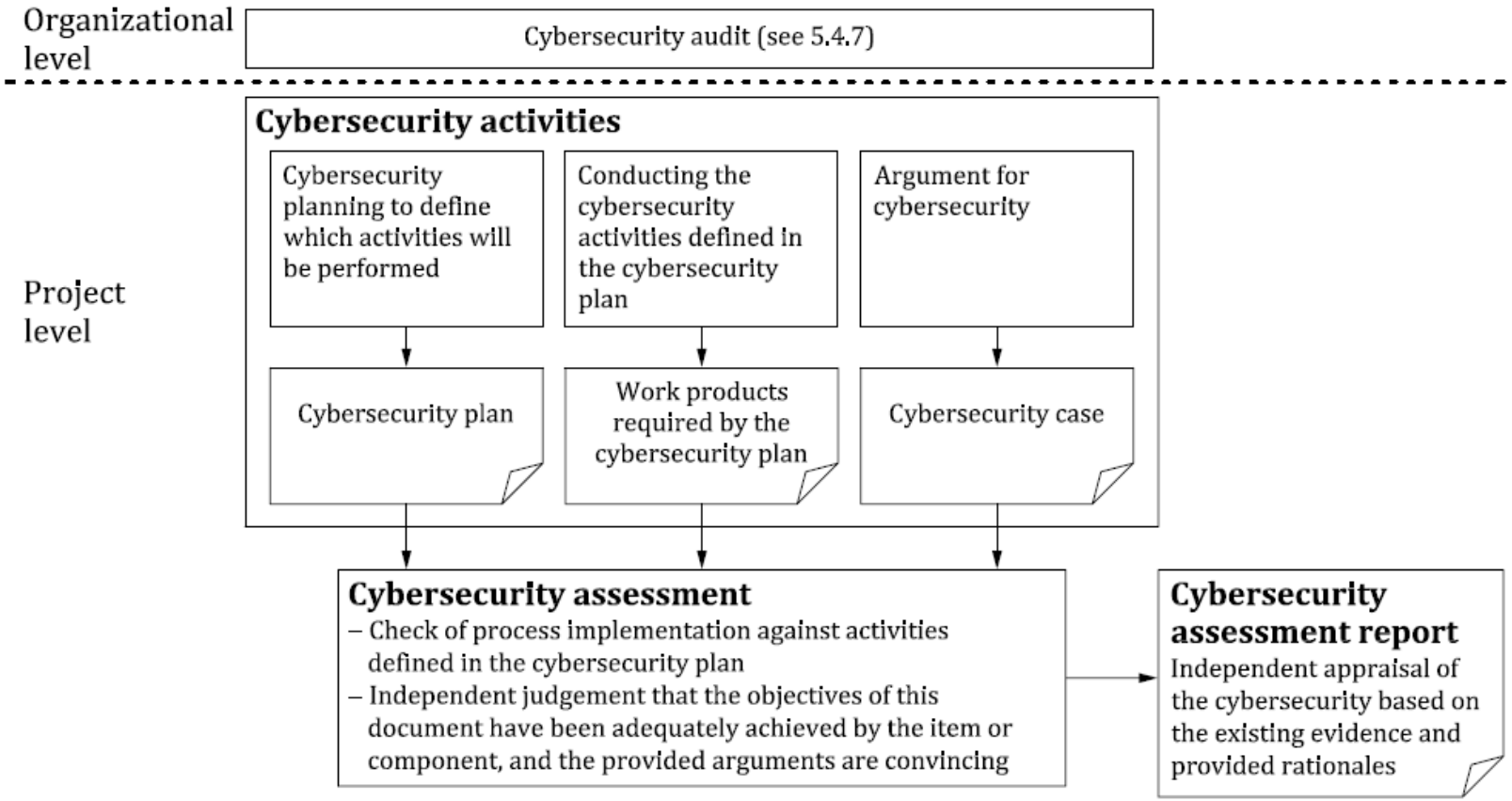


Organization and Project Level

CLAUSE 5,6 IMPACT TO REQUIREMENTS MANAGEMENT

New work products to develop, review and manage

- Plans
- Cases

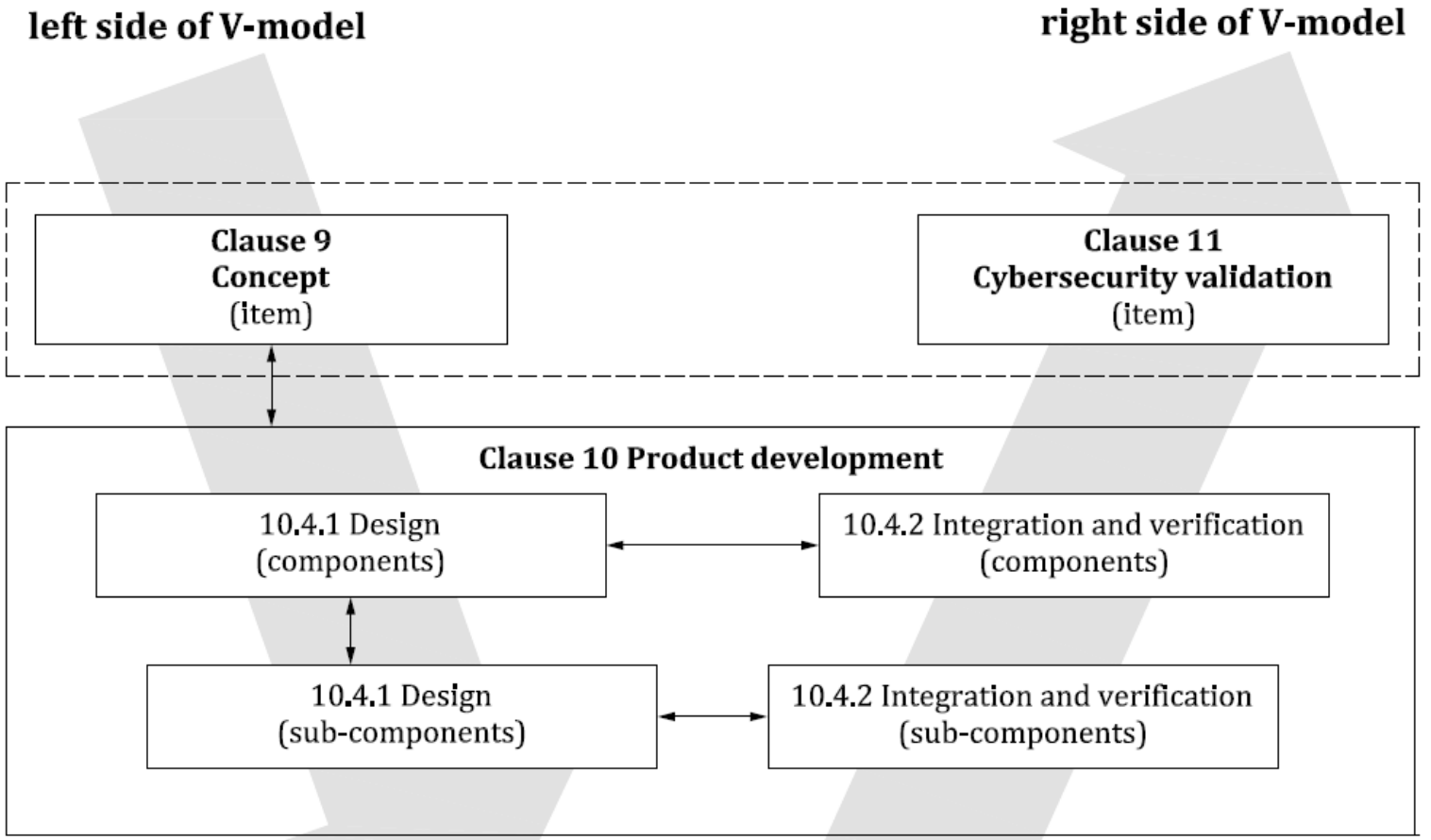


Product Development Phase Support

CLAUSE 9,10,11 IMPACT TO REQUIREMENTS MANAGEMENT

New work products to develop, review and manage

- Requirements
- Design
- V&V



ISO 21434

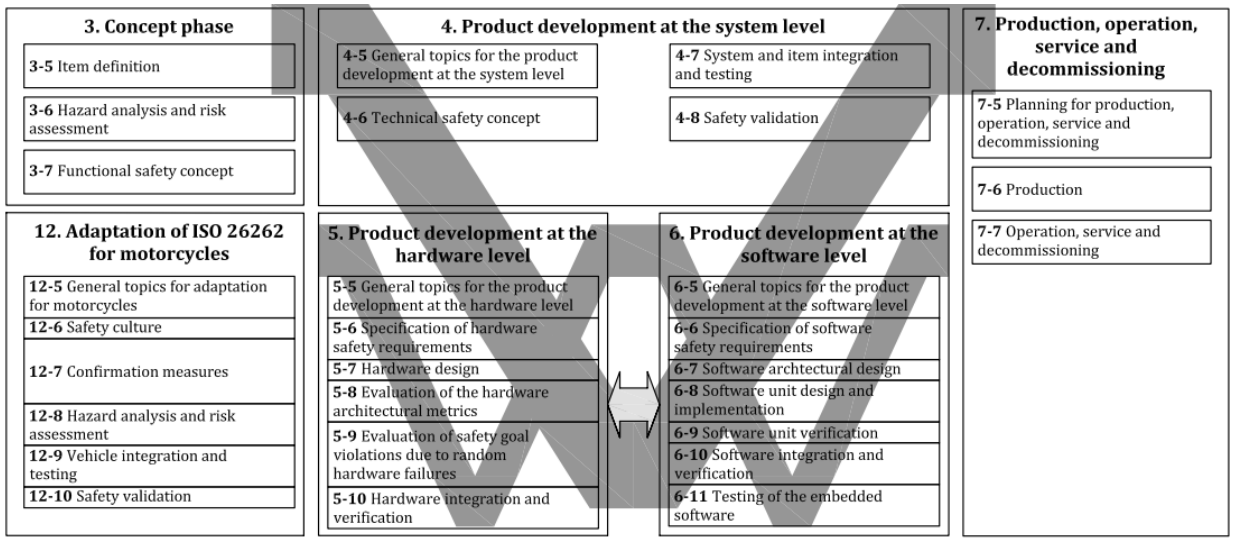
ISO 21434 vs. ISO 26262

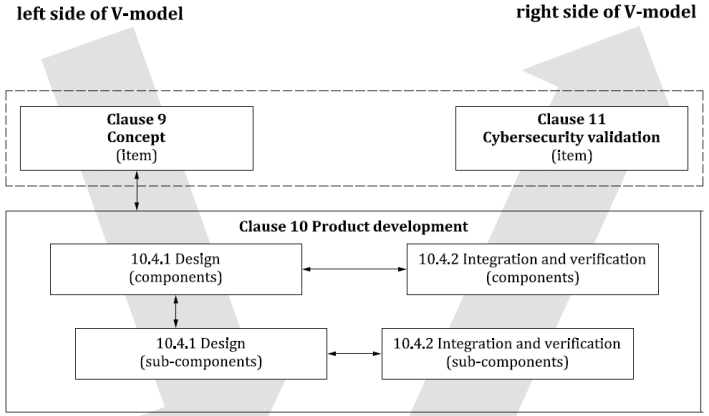
ISO 26262 vs ISO 21434

REQUIREMENTS MANAGEMENT

Both ISO 26262 and ISO 21434

- Analyze an item (system) and derive additional requirements
- Define a V-model focused on managing and verifying those requirements
- Cover product development at the concept, system, hardware, and software levels



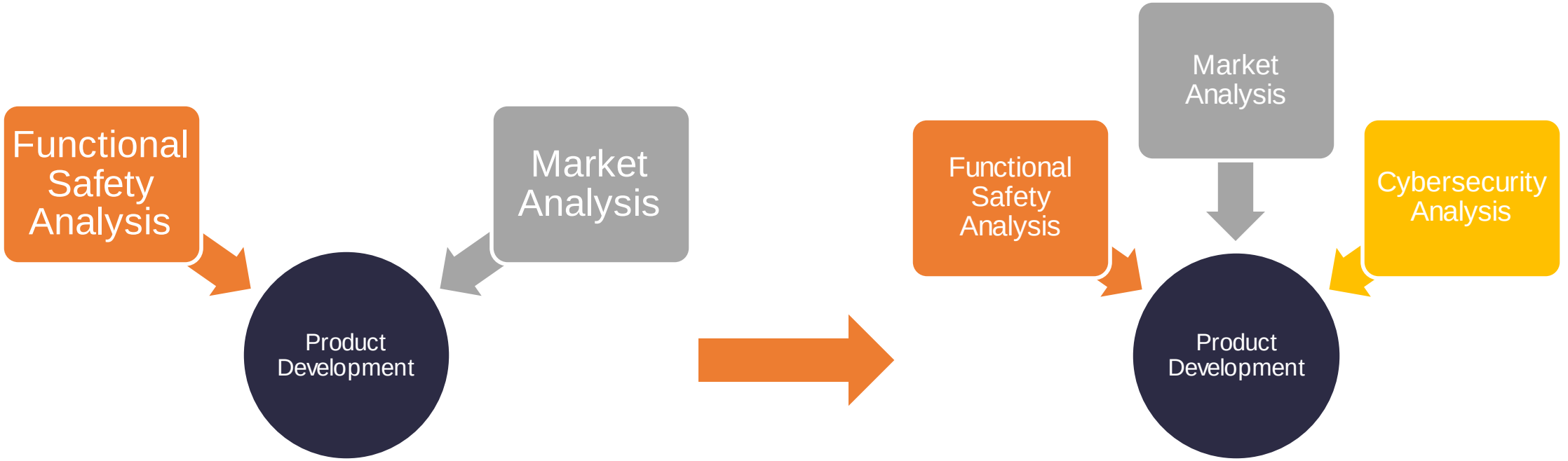


ISO 21434

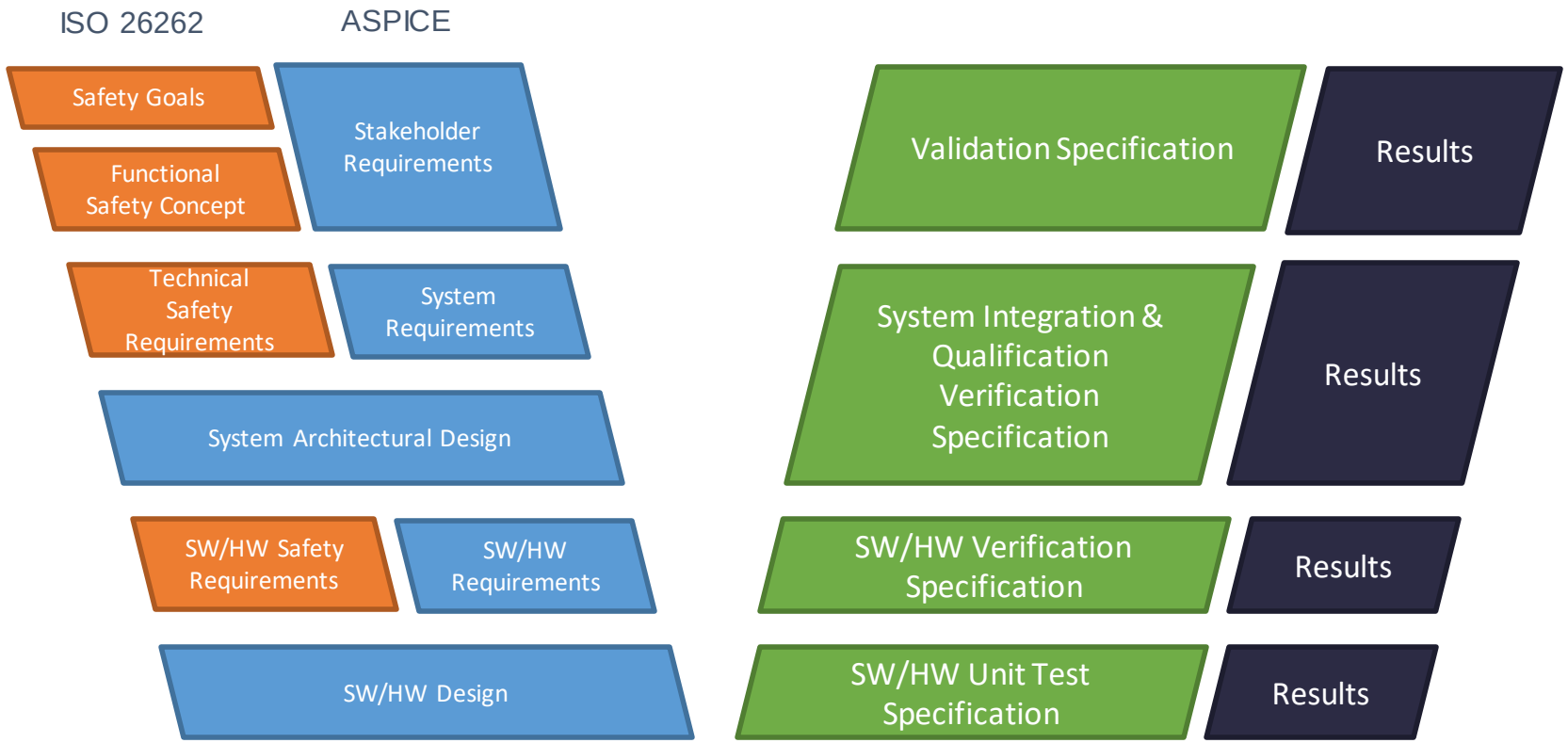
Updating your data model

Adding Cybersecurity

A NEW INPUT TO PRODUCT DEVELOPMENT

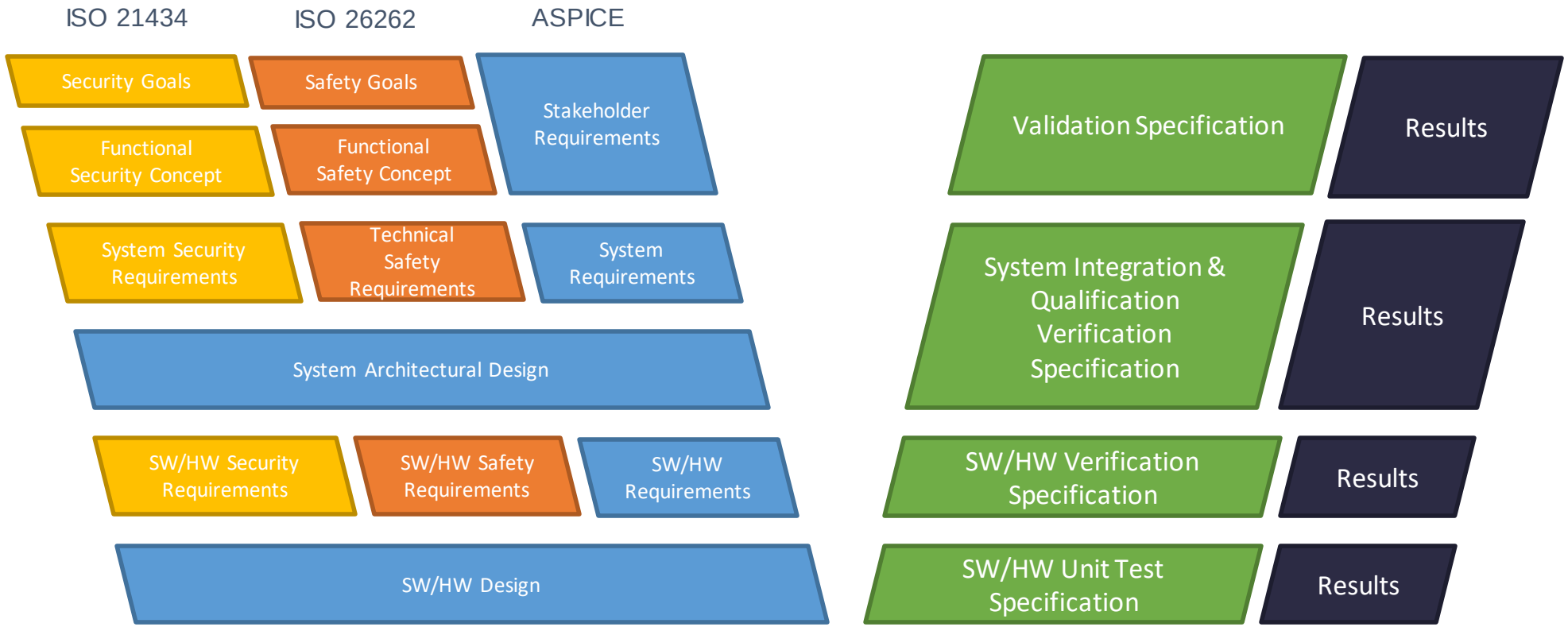


Product Development without ISO 21434



Reviews | Configuration Management Plan | Change Management Plan | Project Management Plan | Document Management Plan | Confidence in the Use of Software Tools Documentation | Supplier Management

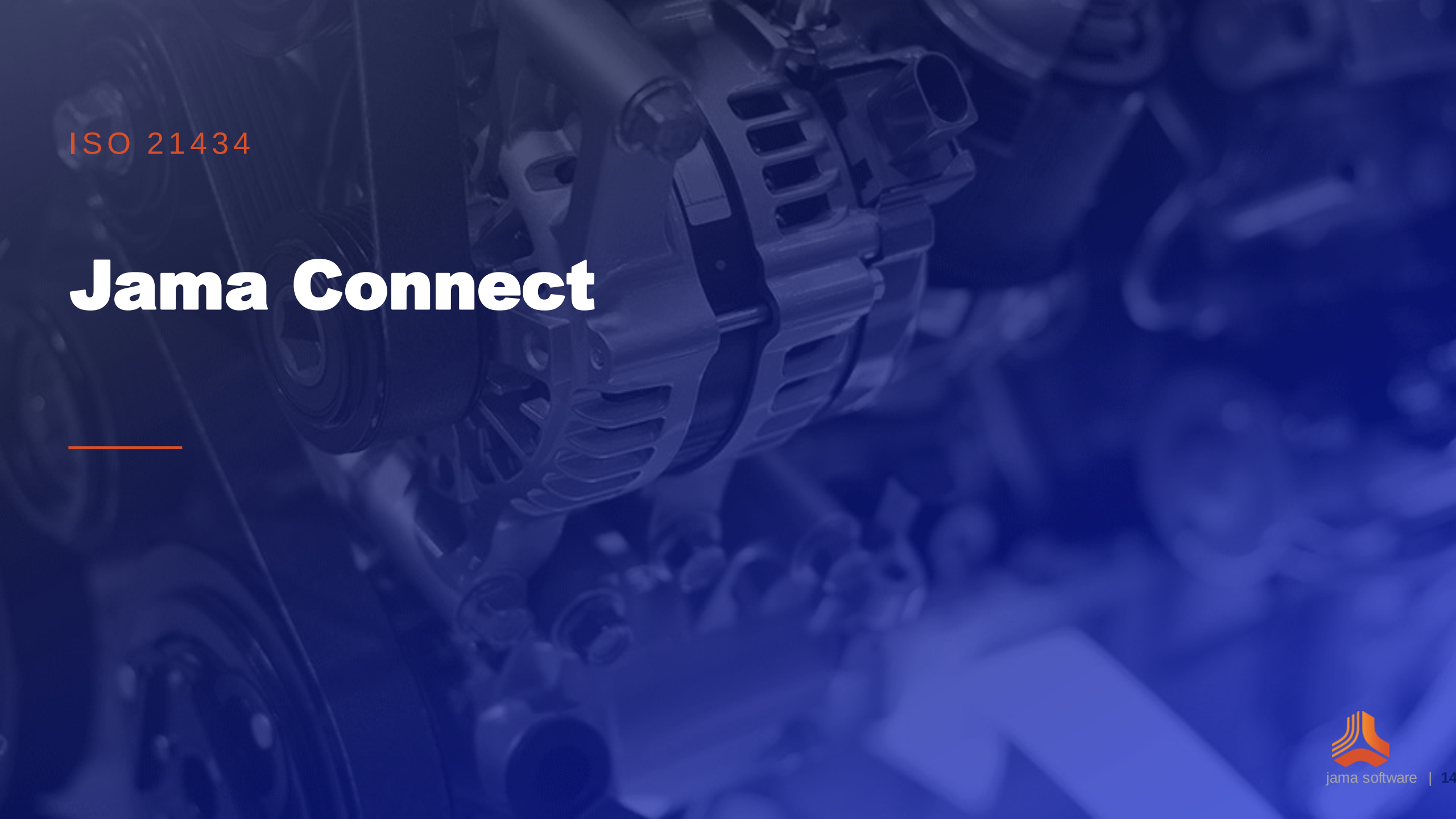
Product Development adding ISO 21434



Reviews | Configuration Management Plan | Change Management Plan | Project Management Plan | Document Management Plan | Confidence in the Use of Software Tools Documentation | Supplier Management

ISO 21434

Jama Connect



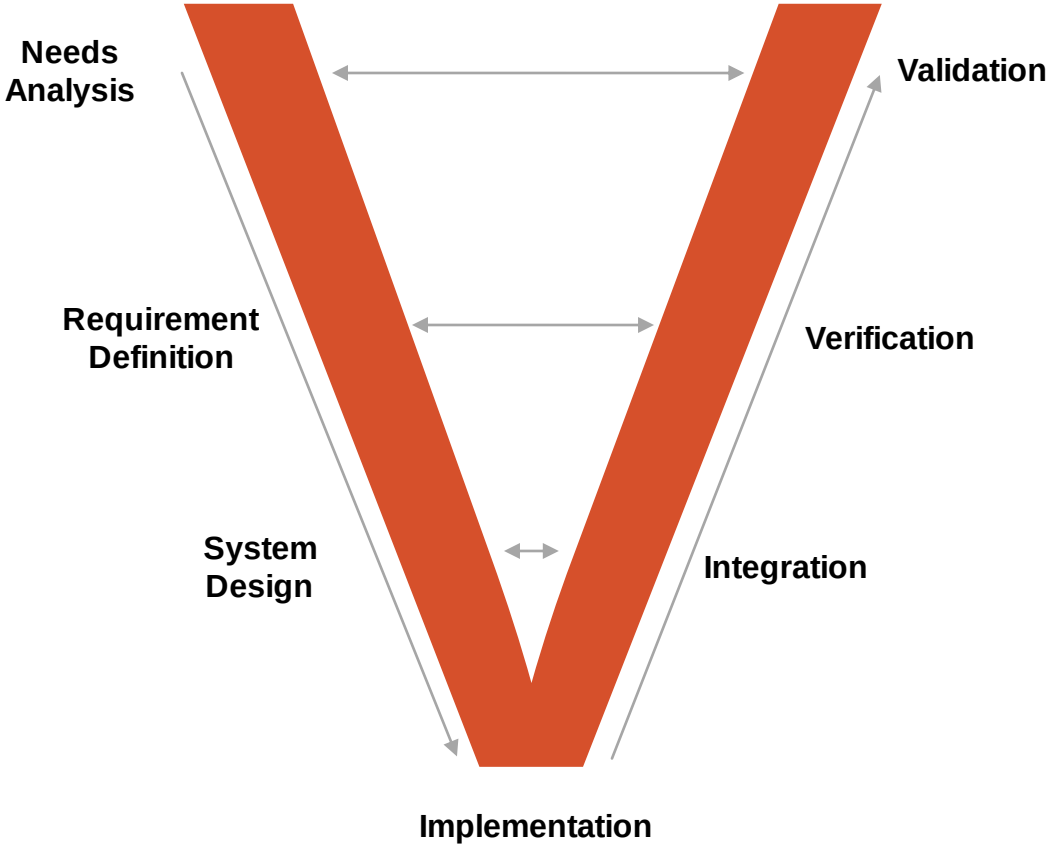
Best Practice | Traceability of Requirements from Definition to Validation

DELIVERS HIGHEST QUALITY, LOWEST COST, COMPLIANT PRODUCT DEVELOPMENT

Traceability

- Enables early identification of requirement deficiencies to minimize cost/time to correct. The cost multiple of identification post System Design grows quickly:
  - Integration (**16X** more expensive)
  - Verification (**40X** more expensive)
  - Validation (**110X** more expensive)

- Industry standards are based on live traceability principles to deliver quality engineering benefits.



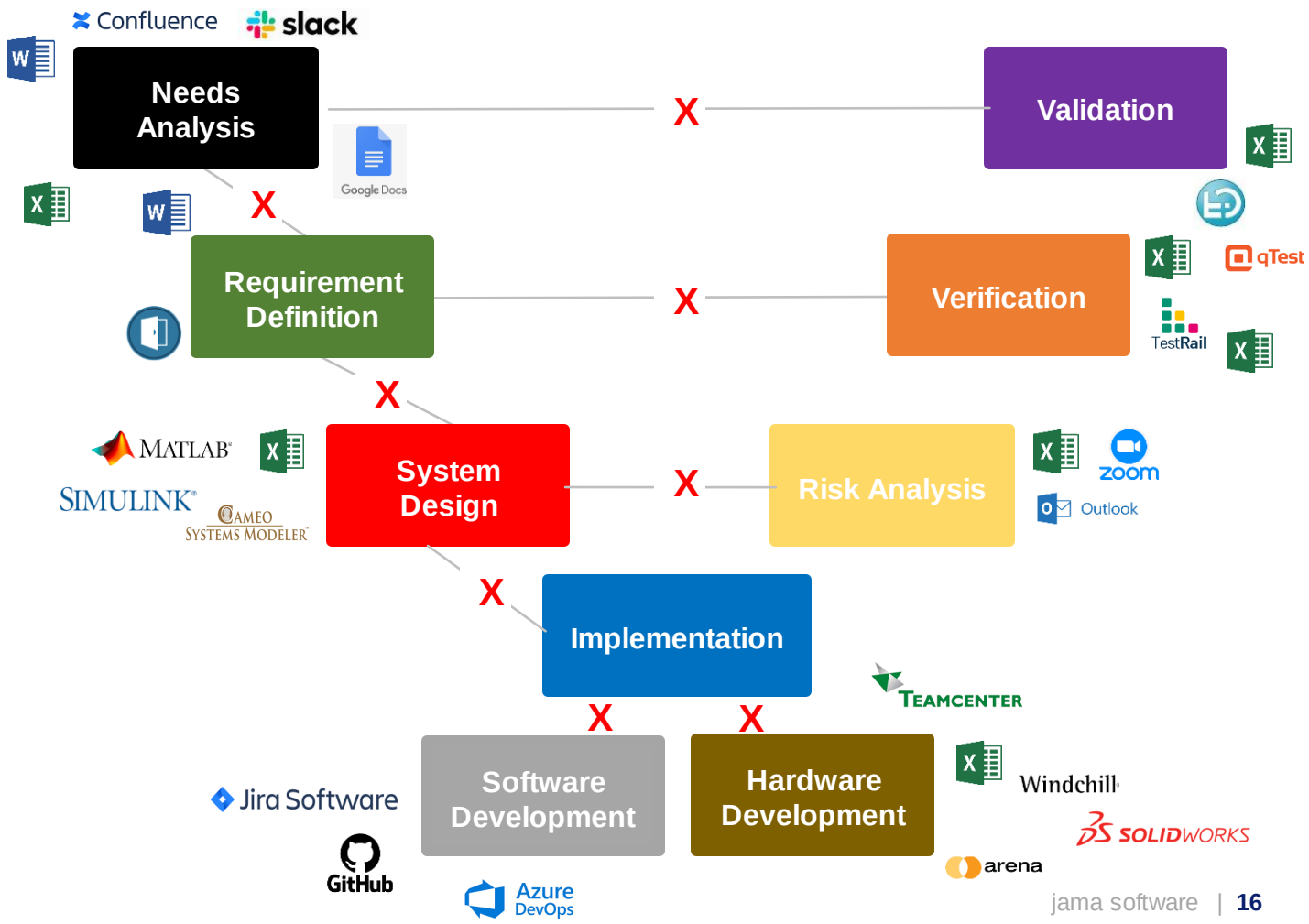
Source: : INCOSE, NIST, Report

Reality | V is Broken into Siloed Tools & Spreadsheets

#1 CAUSE OF NEGATIVE PRODUCT OUTCOMES

#1 Cause of Product Delays, Defects, Cost Overruns, Audit Failures, Product Failures

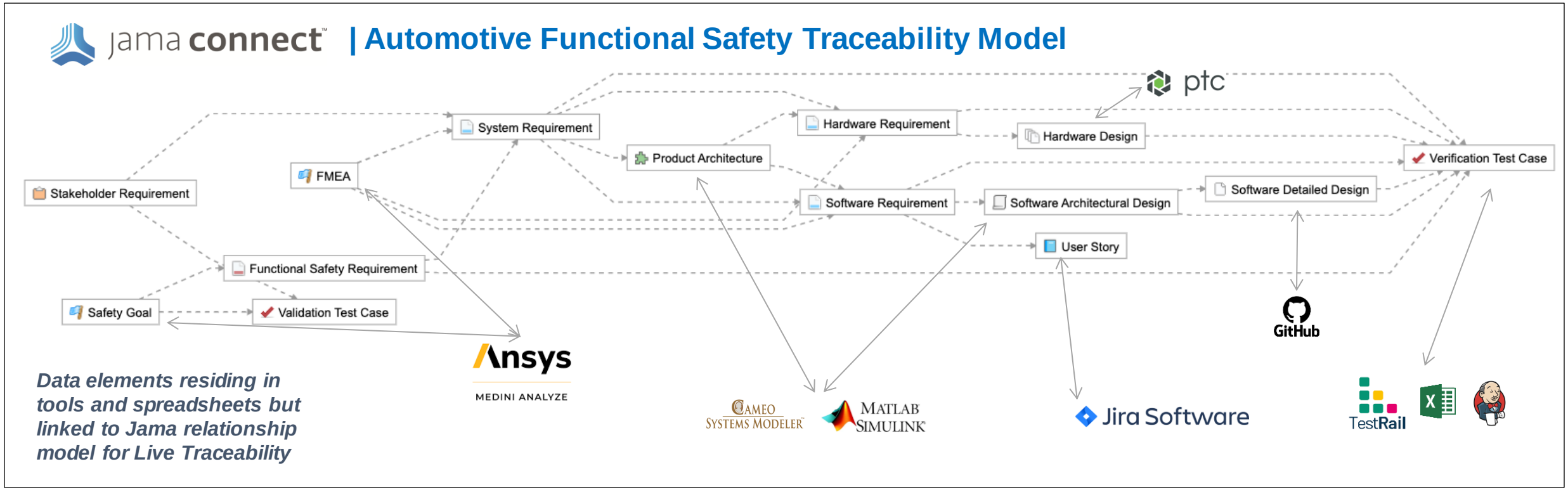
- Late identification of defects/coverage gaps due to lack of visibility through development process
- Lack of requirement coordination and change management between hardware/software
- Lack of ongoing risk assessment and change management



Source: INCOSE, NIST, NASA V&V

Live Traceability | Full Process Connected

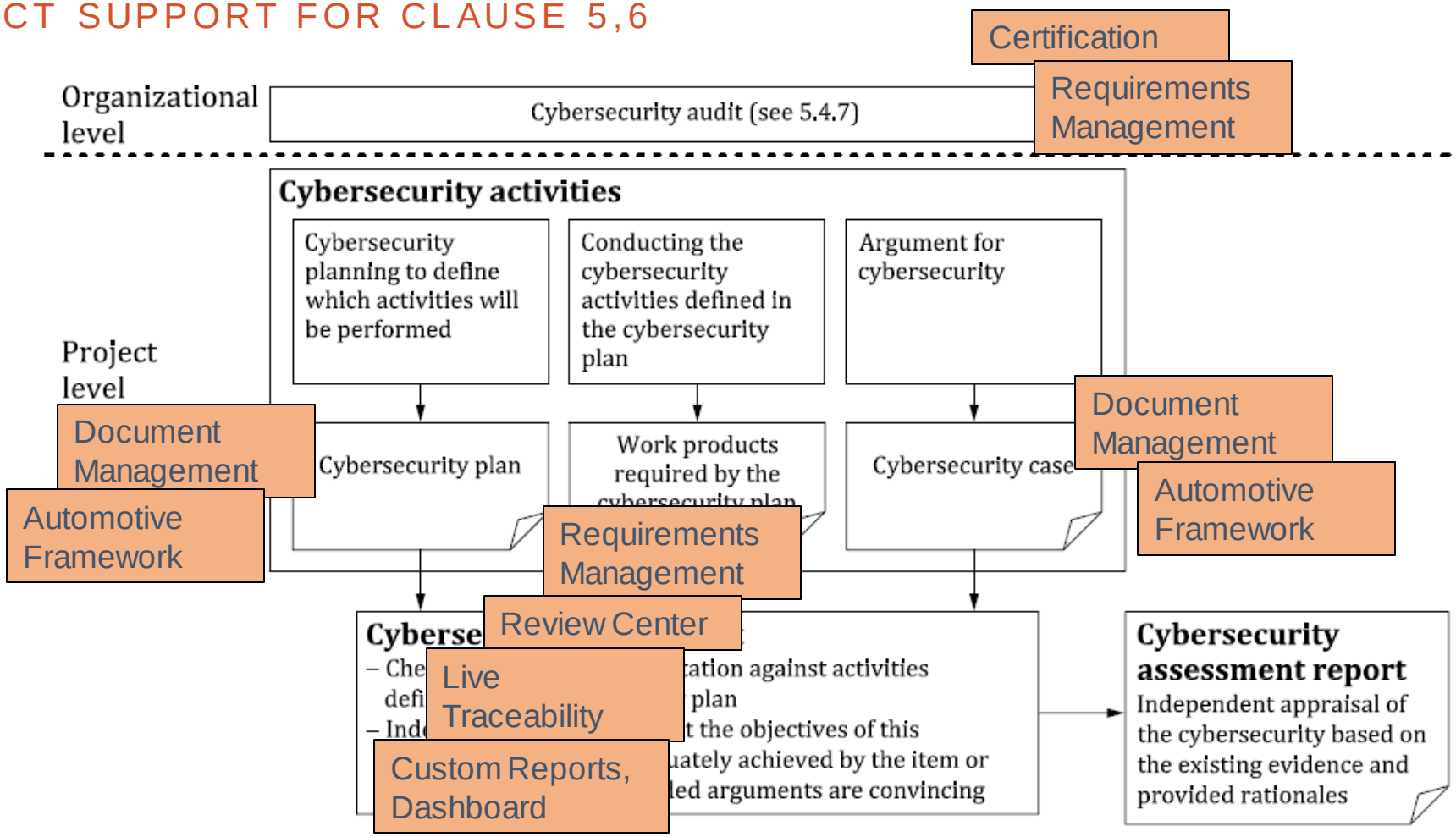
TRACEABILITY ENABLED FOR ASPICE, ISO 26262, ISO/PAS 21448



Critical, best-of-breed tools for traceability shown in this example. Competitive alternatives to those listed are also supported.

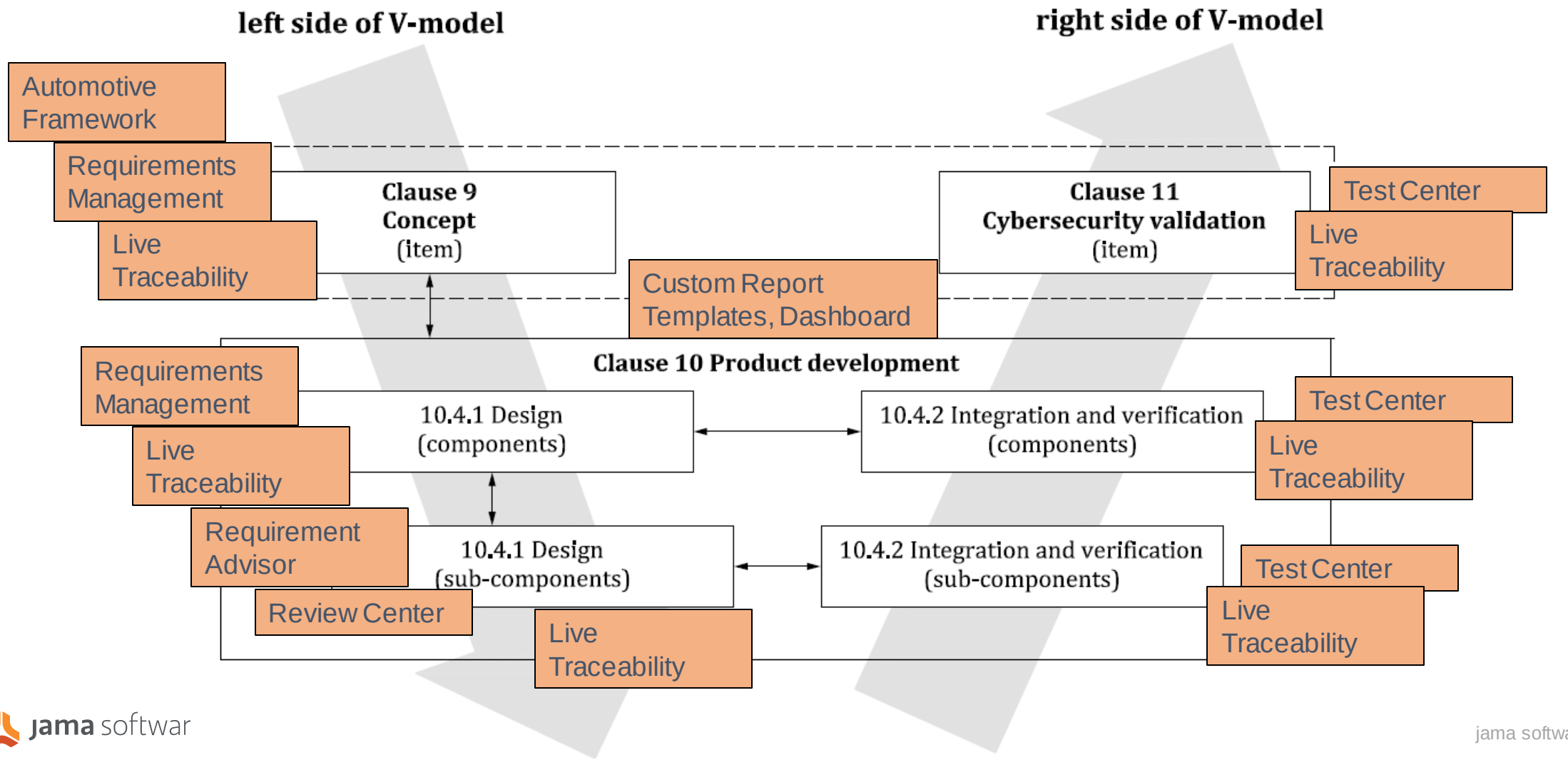
Organization and Project Level

JAMA CONNECT SUPPORT FOR CLAUSE 5,6



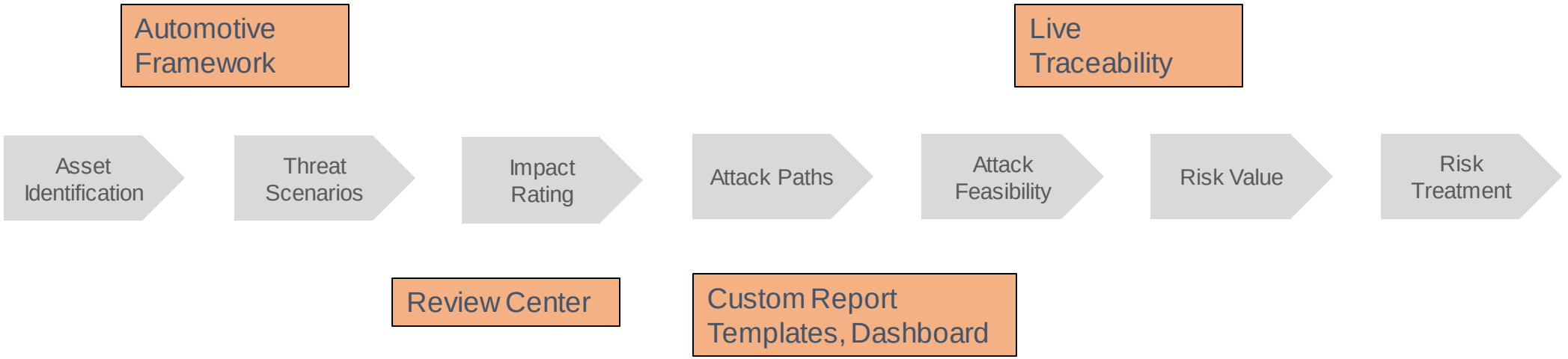
Product Development Phase Support

JAMA CONNECT SUPPORT FOR CLAUSE 9,10,11



Threat and Risk Analysis

JAMA CONNECT SUPPORT FOR CLAUSE 15



ISO 21434

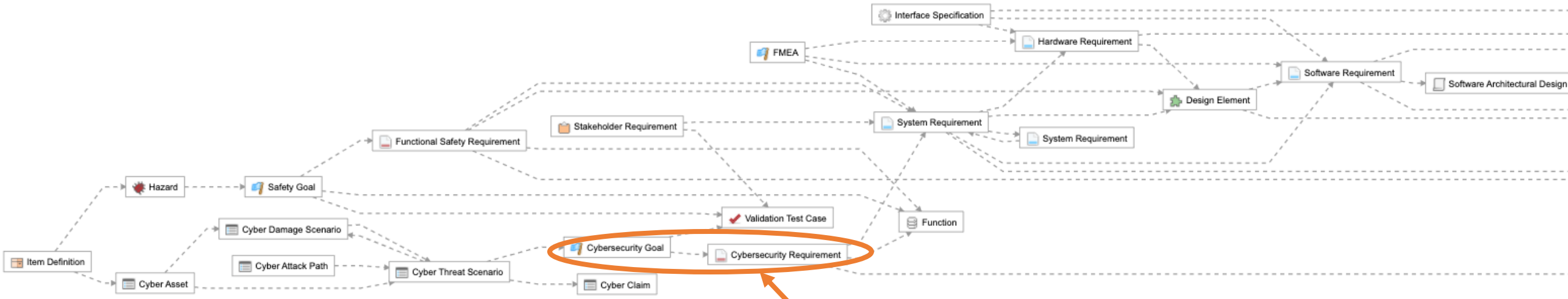
Case Study: Jama Connect Automotive Framework

Data Model Updates for ISO 21434 Requirements

PROJECT STRUCTURE

Data Model Updates for ISO 21434 Requirements

RELATIONSHIP MODEL



Added for ISO 21434 Requirements Management

Example Traceability in Jama

STAKEHOLDER, FUSA, AND CYBERSEC REQUIREMENTS

1 LEVEL UP — Filter items — Set columns Functional Safety Requirement (6), Stakeholder Requirement (3), Cybersecurity Requirement (2)			SOURCE ITEMS — Filter items — Set columns System Requirement (48), Folder (15)		
	Project ID	Description		Project ID	Description
				FuSa-SYSRQ-20	The system shall have an airbag control unit which monit…
	FuSa-SHRQ-10	The vehicle shall have visible dashboard notification of th…		FuSa-SYSRQ-21	The system shall not deploy when there are less than 10 l…
				FuSa-FLD-179	
				FuSa-FLD-183	
	FuSa-FSR-5	The system shall detect failure in seat sensors		FuSa-SYSRQ-27	The item shall be developed with two seat sensors locate…
	FuSa-FSR-5	The system shall detect failure in seat sensors		FuSa-SYSRQ-28	The output of the two seat sensors shall be compared so …
	FuSa-FSR-5	The system shall detect failure in seat sensors		FuSa-SYSRQ-29	The result of the signal from the arbitration unit shall be r…
	FuSa-FSR-5	The system shall detect failure in seat sensors		FuSa-SYSRQ-30	A watchdog running at 2 Khz shall be used by the ACU m…
				FuSa-FLD-184	
	FuSa-FSR-3	The system shall detect failure in speed sensors		FuSa-SYSRQ-31	Two independent means of sensing vehicle speed inform…
	FuSa-FSR-3	The system shall detect failure in speed sensors		FuSa-SYSRQ-32	The two speed signals shall be compared and if they diffe…
	FuSa-FSR-3	The system shall detect failure in speed sensors		FuSa-SYSRQ-33	When the ACU module recieves the speed sensor failure …
	FuSa-FSR-3	The system shall detect failure in speed sensors		FuSa-SYSRQ-34	A watchdog running at 2 Khz shall be used by the ACU m…
				FuSa-FLD-191	
	FuSa-CSRQ-1	Verify the received data if it is sent from valid entity.		FuSa-SYSRQ-51	The product shall use a 256 bit key to encrypt the receive…
	FuSa-CSRQ-1	Verify the received data if it is sent from valid entity.		FuSa-SYSRQ-52	The host shall provide a new key generation function.
	FuSa-CSRQ-2	Prevent unauthenticated entities from accessing to the ce…		FuSa-SYSRQ-53	The cellular modem shall require a token to initiate data tr…

ISO 21434

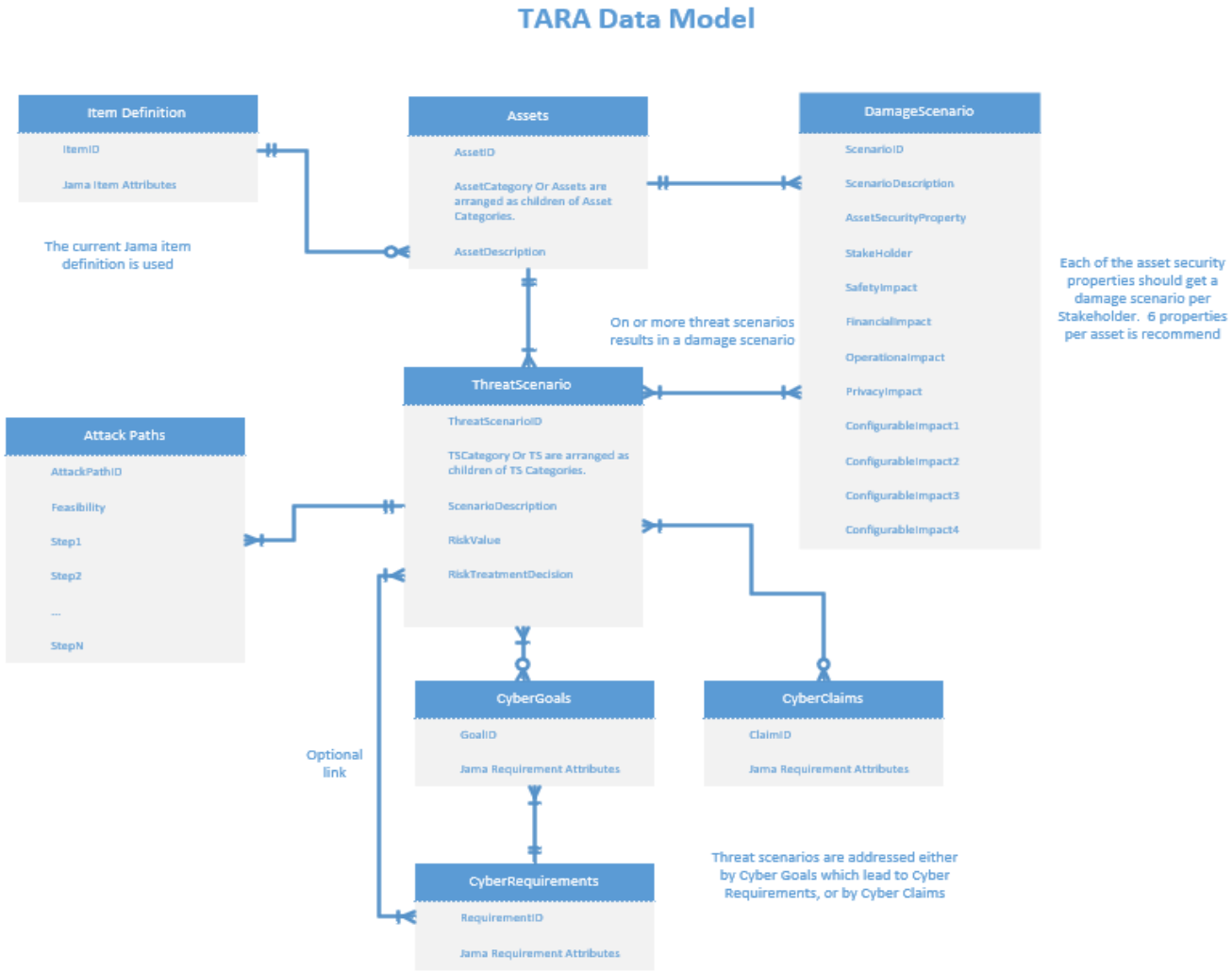
TARA in a RM Solution

Why Develop a TARA in an RM System?

OVERVIEW

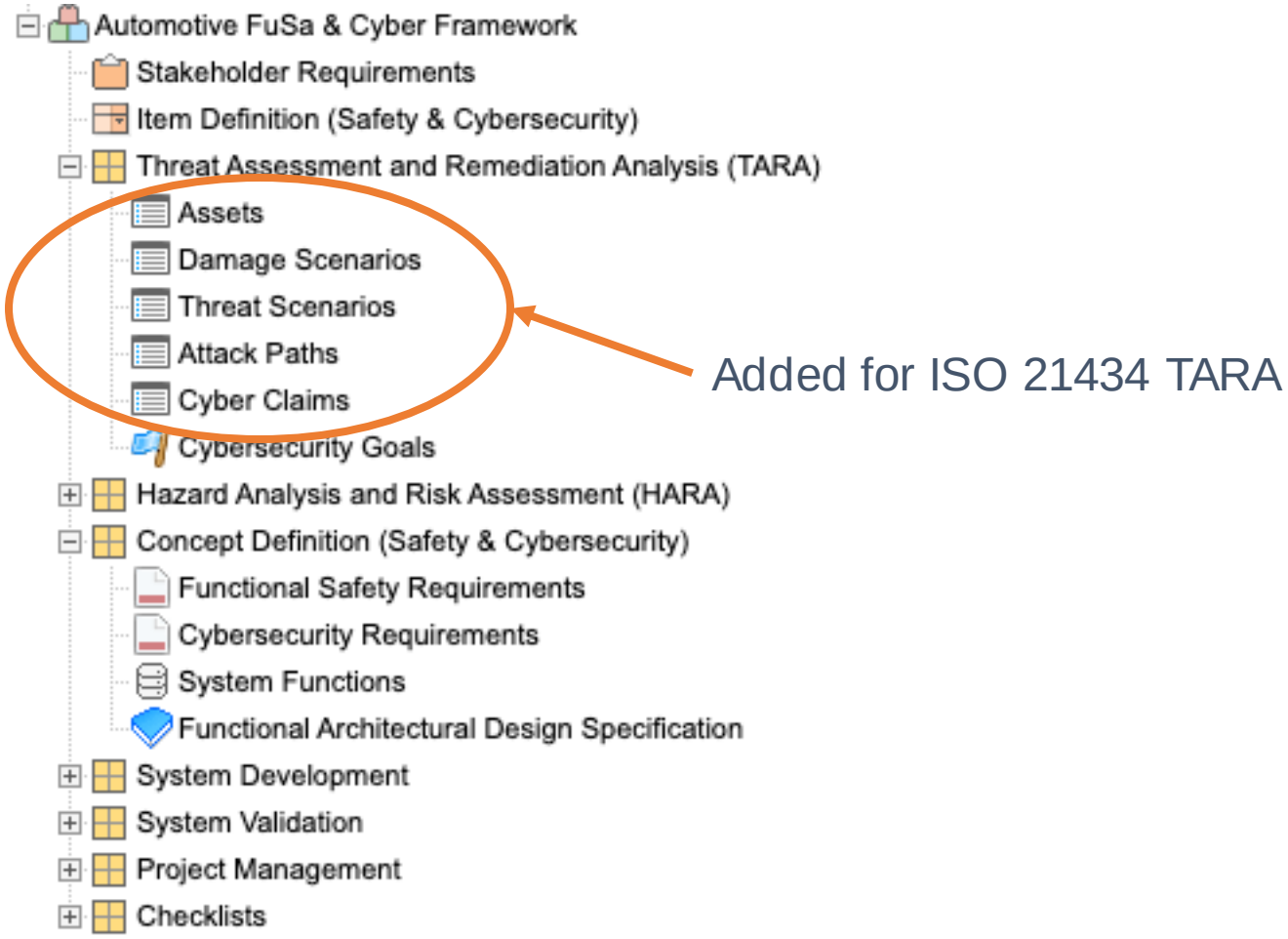
- While managing a complex TARA may be best done in dedicated tools, not all customers can afford the cost or learning curve of a dedicated tool.
- Startups and companies developing simpler products often rely on their requirements solution for managing non-requirements content

ISO 21434 TARA Data Model



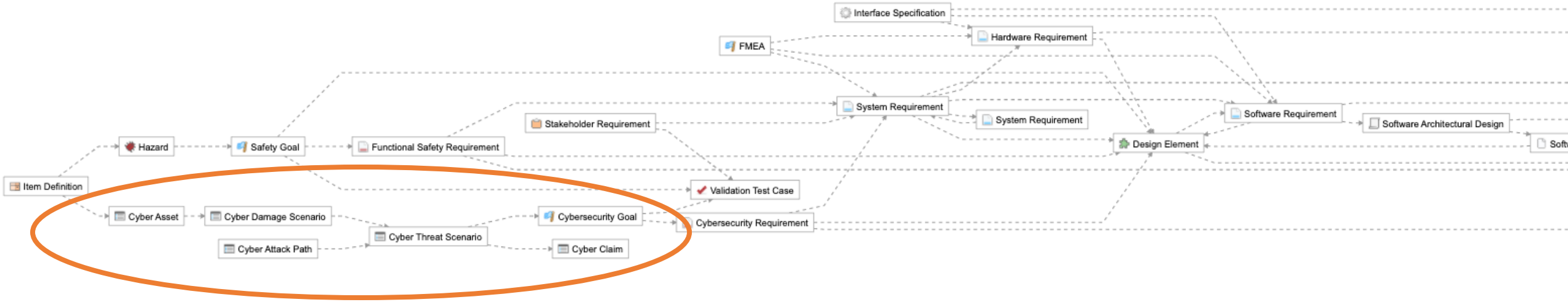
Data Model Updates for ISO 21434 Requirements

PROJECT STRUCTURE



Data Model Updates for ISO 21434 TARA

RELATIONSHIP MODEL



Example TARA in Jama

Damage Scenarios

Set • View details

Add | Trace view | Export

3 items

Project ID		Name	Stakeholder	Financial Impact	Safety Impact	Operational Impact	Privacy Impact	Impact Justification
FuSa-DAMAGE-1	0	Unintended headlamp's turn off during l…	Road User	Unassigned	1 - None	Moderate	Unassigned	Since the headlamp turns off when …
FuSa-DAMAGE-2	0	Unintended headlamp's turn off during ni…	Road User	Unassigned	S3	Unassigned	Unassigned	A crash against a street tree poses …
FuSa-DAMAGE-3	0	Unintended low beam of headlamp	Road User	Unassigned	S0	Moderate	Unassigned	Since the headlamp turns off when …

1 LEVEL UP — Filter items — Set columns

Cyber Attack Path (3), Cyber Damage Scenario (1)

Name	Attack Feasibility	Operational Imp…	Privacy Impact	Safety Impact
Unintended headl…		Unassigned	Unassigned	S3
Cellular Interface	High			
Bluetooth	Medium			
OBD2	Low			
Unintended headl…		Unassigned	Unassigned	S3

SOURCE ITEMS — Filter items — Set columns

Cyber Threat Scenario (2)

Description
Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power S…
Tampering of a signal sent by Body Control ECU leads to...

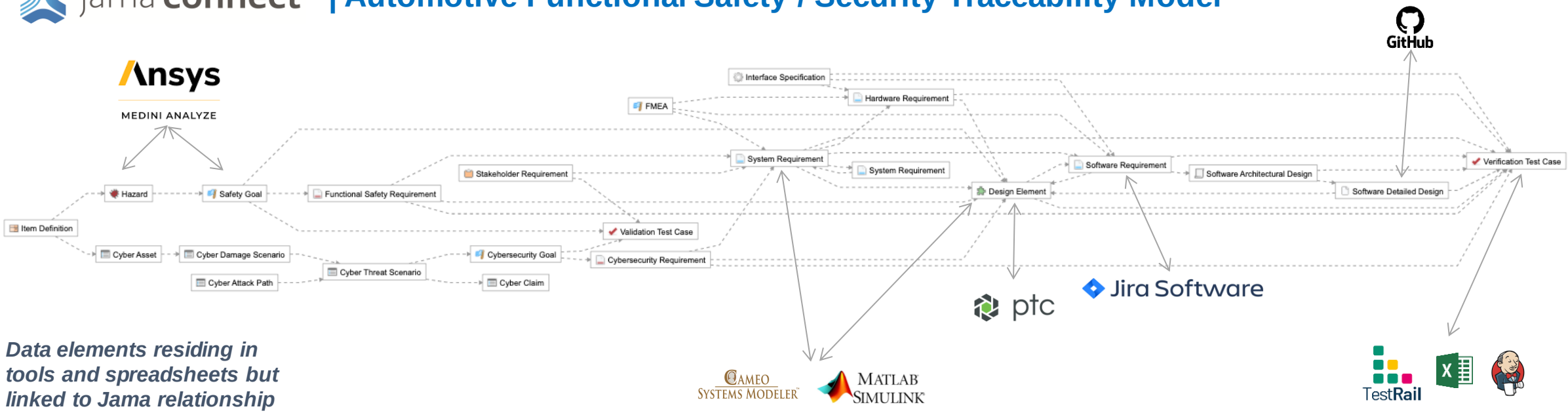
ISO 21434

New Automotive Framework

1. Live Traceability | Full Process Connected

TRACEABILITY ENABLED FOR ASPICE, ISO 26262, ISO/PAS 21448, ISO 21434

jama connect™ | Automotive Functional Safety / Security Traceability Model



Data elements residing in tools and spreadsheets but linked to Jama relationship model for Live Traceability

Critical, best-of-breed tools for traceability shown in this example. Competitive alternatives to those listed are also supported.

Thank You

jama software®