

DEKRA DIGITAL

Training ISO/SAE 21434



Distributed CS Activities

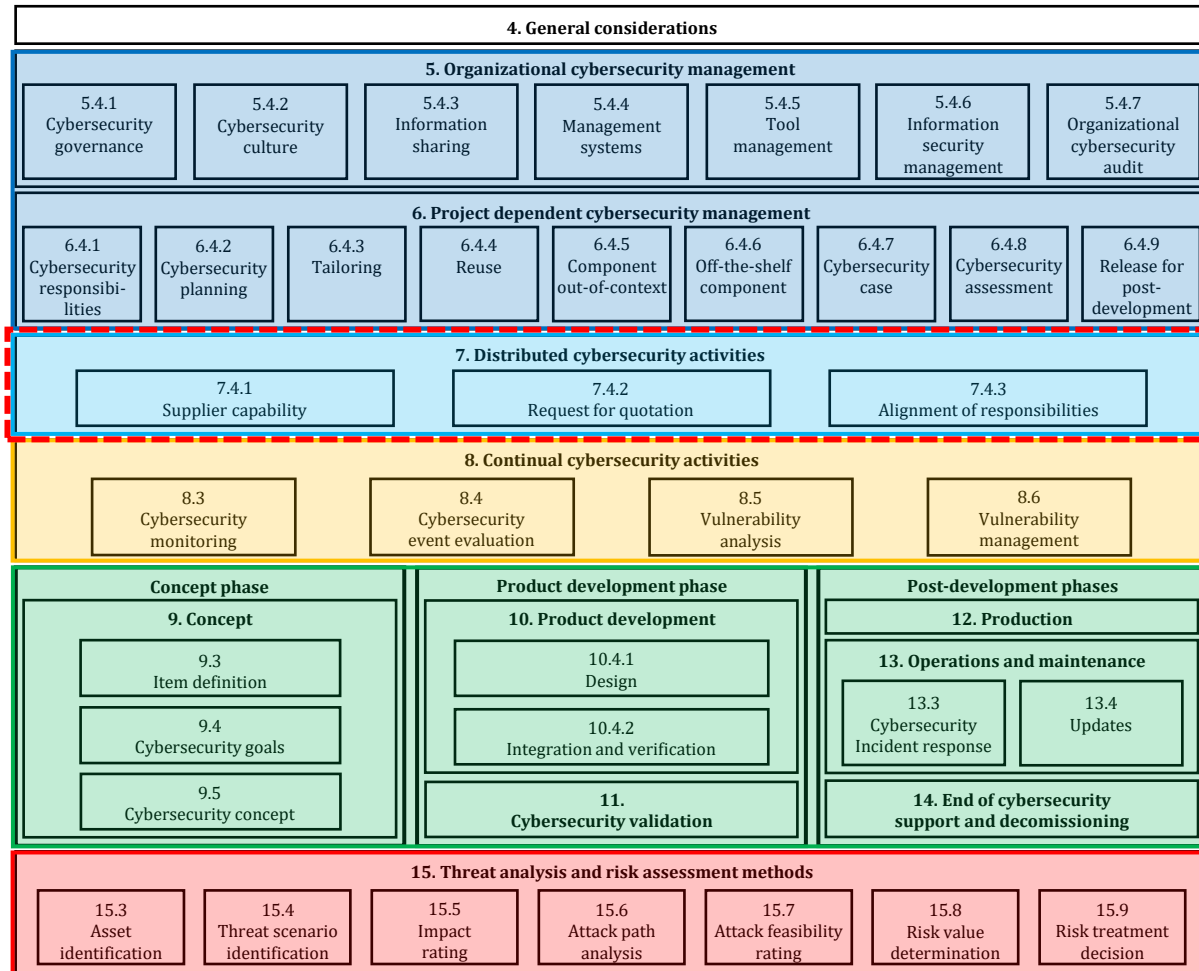
CONTENT

- 1. Introduction**
- 2. Supplier Capability**
- 3. Request for Quotation**
- 4. Cybersecurity Interface Agreement (CIA)**
- 5. Summary**



1. INTRODUCTION

Structure of ISO/SAE 21434



Overall & project specific management processes (similar to ISO 26262)

- Management systems
- Policies
- Preparation for assessment

Distributed CS activities

- Define interfaces between customer, supplier, third parties.

Continuous CS activities

- Requirements for continuous monitoring of CS relevant information
- Framework for analysis and management of vulnerabilities

Concept, development and post-development

- Add-on of CS relevant activities during concept and development
- Establishment of CS goals and requirements
- TARA and vulnerability analysis during development
- Consideration of post-development requirements (during or after production, decommissioning ...)
- Definition of post-development processes (production, incident response, update)

TARA (Threat Analysis and Risk Assessment)

- Describes the steps to perform a robust risk analysis on the system
- Complex process to be performed multiple times and for multiple assets

What are Distributed Cybersecurity Activities?

To develop, produce, and maintain a cyber secure product, CS activities must be performed not only by the OEM, but also by the supply chain. This affects all business partners (including companies within the OEM) involved in the product lifecycle

This means

- When a cyber attack occurs on a product installed in a vehicle, there is a concern that information about the vehicle owner, driver, or OEM may be compromised
- Therefore, comprehensive distributed activities and responsibilities are required to prevent the risk of data loss and to jointly develop a cyber secure product

Objectives

- Manage distributed cybersecurity activities
- Define interactions, responsibilities, and dependencies of customers and suppliers for CS activities

2. SUPPLIER CAPABILITY

Supplier Capability

Supplier capability evaluation is a formal process that assesses a potential supplier's capacity to comply with ISO/SAE 21434 or another national or international cybersecurity engineering standard

Key Requirements - Supplier Capability

- Establish processes for evaluation
- Check prior adoption of cybersecurity standards by suppliers
- Suppliers can provide supporting information to demonstrate their capabilities
 - CS assessment report, quality management report
(e.g., CSMS certification acc. to ISO/SAE 21434, VDA ACSMS)
- Evidence of vulnerability management
- Continuous CS activities, risk management practices, etc.

3. REQUEST FOR QUOTATION

Request for Quotation

A request for quotation is a business process in which an OEM requests a quote from a potential supplier for a specific project, task, or service

Key Requirements - Request for Quotation

A request for quotation should include:

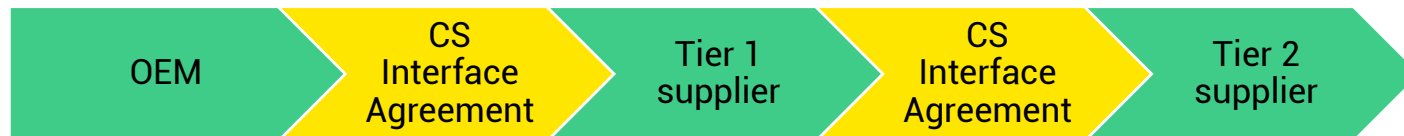
- Formal request to follow ISO/SAE 21434 standard, if applicable
- CS requirements for which the supplier is quoting (e.g. requirements related to information sharing)
- Supplier's CS responsibilities

4. CYBERSECURITY INTERFACE AGREEMENT (CIA)

Cybersecurity Interface Agreement (CIA)

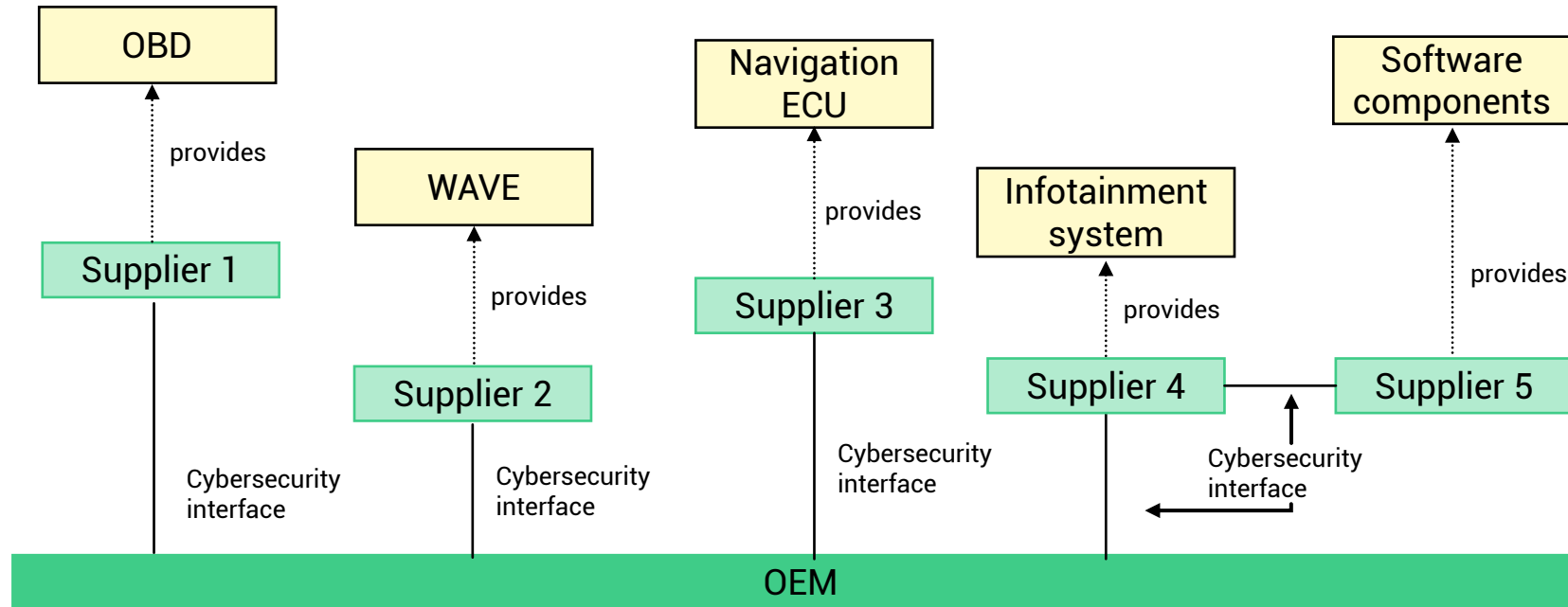
The Cybersecurity Interface Agreement (CIA) is an important document that ensures the successful planning and execution of distributed cybersecurity activities

- It is intended as a record of what is expected of each party and should define the exact way distributed CS activities will be conducted
- It describes the information and the work products to be shared between OEM and supplier and documents responsibilities
- It must be mutually agreed upon between OEM and supplier prior to the start of the distributed CS activities
- The way the CIA is communicated is significant to avoid communication gaps between organizations involved in a distributed development



CIA – Nested Dependencies

Example



Example of RASIC Table for Distributed CS Activities

Phase	WP	Doc Ref.	Supplier					Customer					Level of confidentiality	Comments
			R	A	S	I	C	R	A	S	I	C		
Concept	Item Definition							X						
	TARA					X		X						
	CS Concept					X	X	X						
	Concept Verification				X			X						
Analysis	Vulnerability analysis		X	X							X			

5. SUMMARY

Summary

Key Takeaways


CS activities performed by an OEM and its suppliers should be specified in the CIA and must include

- Points of contact regarding cybersecurity at both the ends
- Identification of CS activities to be performed by both the parties
- Process definition in case of a CS issue
- Target milestones regarding CS activities
- Resolving conflicts and incidents through mutual agreement
- Responsibility sharing
- Definition of the end of CS support

Work Products

- [WP-07-01] Cybersecurity interface agreement

Training Overview ISO/SAE 21434



Part 1, Duration: 4hrs
Introduction
Organizational Management Activities
Project Dependent Management Activities
Distributed Cybersecurity Activities
Part 2, Duration: 4hrs
Threat Analysis and Risk Assessment Methods (TARA)
CS Related Topics and Case Study
Part 3, Duration: 4hrs
Continual Cybersecurity Activities
Concept
Product Development
Cybersecurity Validation
Part 4, Duration: 4hrs
Production
Operations and Maintenance
End of Cybersecurity Support and Decommissioning
Final Questions / Knowledge Test (if considered in this training)

* intermediate break to be decided by trainer and participants on an hourly basis

DEKRA DIGITAL

innovating safety

That's all of

DISTRIBUTED CYBERSECURITY ACTIVITIES

Thank you!