2024 DevOps Tec. x SIEMENS POLARION

How to integrate ASPICE, Cybersecurity and Functional safety into your process architecture

Kevin Huang , May 17th 2024

DEKRA Kevin Huang

合辦單位： DEKRA SIEMENS 敦新科技 DAWNING TECHNOLOGY INC.

Kevin Huang 黃浩鈿

Qualifications:

- DEKRA Functional Safety Assessor (under **Dakks** accreditation)
- DEKRA Professional Functional Safety Engineer Automotive Lecturer
- DEKRA Professional Functional Safety Engineer Process-Industry Lecturer
- DEKRA Professional Cyber-Security Engineer Automotive Lecturer
- intacs Principal Assessor for Automotive SPICE
- VDA QMC ACS Expert in Automotive Cyber Security Management System Audits Lecturer
- VDA Automotive Software Essentials Lecturer

Experience:

- International projects among Germany, Netherland, Sweden, Belgium, US, Japan, Korea, China, Taiwan, Malaysia, Singapore, Thailand area
- Training of Functional Safety and Automotive SPICE at international OEMs and Suppliers over **1,000** employees
- Assessment, Consultancy, Workshops, Training on **Functional Safety/ Automotive SPICE**, **as client below:**

DAIMLER
HONDA
BAIC
HAITEC
inalfa
Continental
ABB
Schneider Electric
Foxconn
WNC
HIWIN.
ITRI
MEDIATEK
REALTEK
intel
tobii
ASE GROUP
KOSO
SPIL
LITEON
USI
DELTA
CMC
SAIC
HARMAN
Punch powertrain
MAGNA
英業達 inventec
VISION
AUO
PEGATRON
UTAC
GARMIN
TTE
LCKT
E-LEAD
INNOLUX
faurecia inspiring mobility
FocalTech
SOC
ESMT
JETOPTO

SOTIF (ISO 21448:2022) 預期功能安全

目錄概要

Outline

01 Trend of automotive

02 Automotive Security Motivation

03 Automotive Security Challenges

04 Introduction to Automotives Security Standards And UNECE Regulation

05 What is ASPICE

06 Understanding ASPICE for Cybersecurity

07 ASPICE for Cybersecurity vs. ISO/SAE 21434

08 ISO 26262 vs. ISO/SAE 21434

01

Trend of Automotive

Trend of Automotive?

Automotive industry products **must comply with a variety of technical standards**, depending on their purpose. These products should also comply with fundamental standards, such as quality, process, safety, and cybersecurity.

Standard	Definition	Automotive Field
A-SPICE	是汽車產業的軟體流程改進和能力評定標準，目前盛行於車廠對供應商進行 軟件開發過程評估。	SW Process
ISO 26262	功能安全面對的是汽車自己的系統，主要是對內的，要解決的是自己內在系統失效和隨機失效	Functional Safety
ISO 21448	預期功能安全則是應汽車智慧化趨勢而生，彌補了功能安全在AI領域、自動駕駛領域的不足，覆蓋了自動駕駛等級L1-5。它更多面對的是性能失效、系統預期功能不足和人員誤操作。這就開始向外延伸，更多地涉及到汽車與環境的交互，汽車和駕駛操作人員的交互	Safety Of The Intended Functionality
ISO/SAE 21434	網路安全則不是因“系統”而生，而是因“人”而生，面向的是來自於外部環境、外來惡意者甚至內在惡意者的威脅（Threat），加強的手段有全狀態防火牆、對稱非對稱加密、金鑰管理和入侵防禦和檢測系統等	Cybersecurity

Trend of Automotive?

In 2021, the National Highway and Traffic Safety Administration essentially reopened a 2017 investigation into the continuing and numerous fire incidents involving electric vehicles. Amongst other aspects, the investigation will include the roles of battery management systems, operating systems, system diagnostics, failure prognostics, cybersecurity and overall intervention; all of which are driven by software.

Subsequently, the marketplace has changed significantly. Insurance underwriters have noted the risks of functional safety and cybersecurity

"The Product Liability Insurance market has climbed significantly in the past few years. "Due to a lack of historical data on many of these providers of electric and/or autonomous systems and software, underwriters cannot easily extrapolate as to the risk of insuring a company."

"Safe Software"

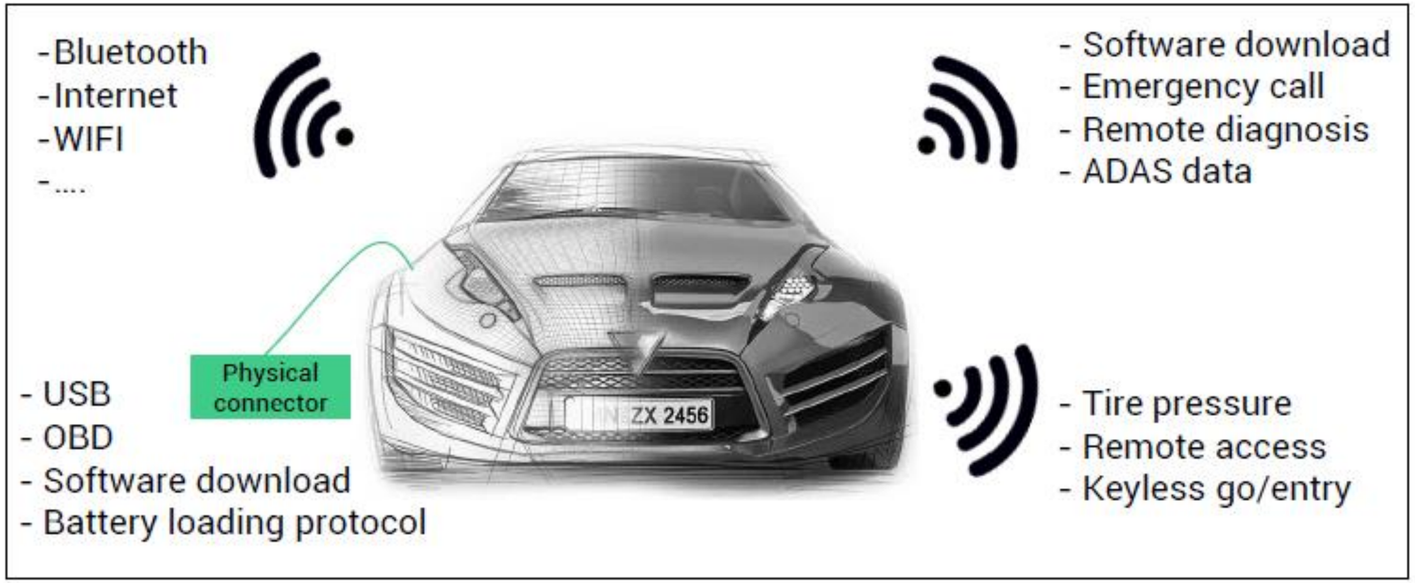
- What is your **functional safety level** ?
- What is your **Automotive SPICE capability** ?
- What is your **cybersecurity level** ?

02

Automotive Security Motivation

Connected Vehicles

Vehicles are getting more and more connected to the world by different communication channels



Vehicle systems need:

- Secured access by authorized parties
- Secured data for driver assistance or autonomous driving systems
- Data integrity
- Protection against misuse or manipulation

Safety and Security Correlation in Automotive

Safety protects humans and environment from the machines, and security protects machines from maliciously acting humans

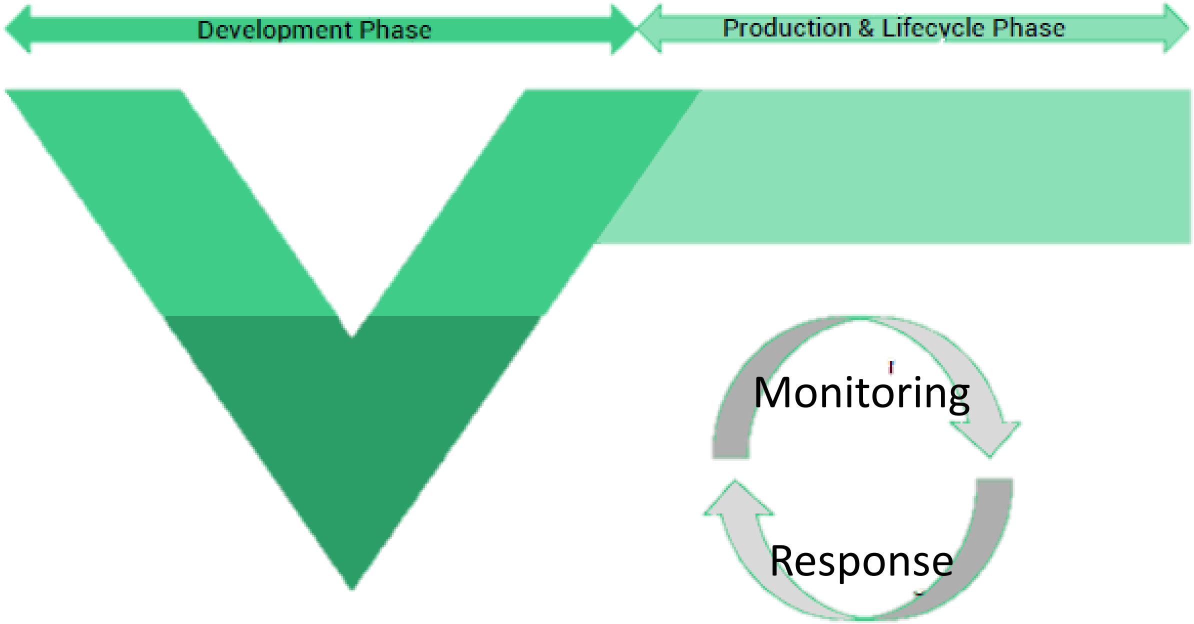
- A **cyber attack** on the car's safety functions may result in the change of control parameters or the deactivation of some sensor signals.
- **Human safety** may be put at risk.
- As a result, **cybersecurity and functional safety must be considered in parallel**.

03

Automotive Security Challenges

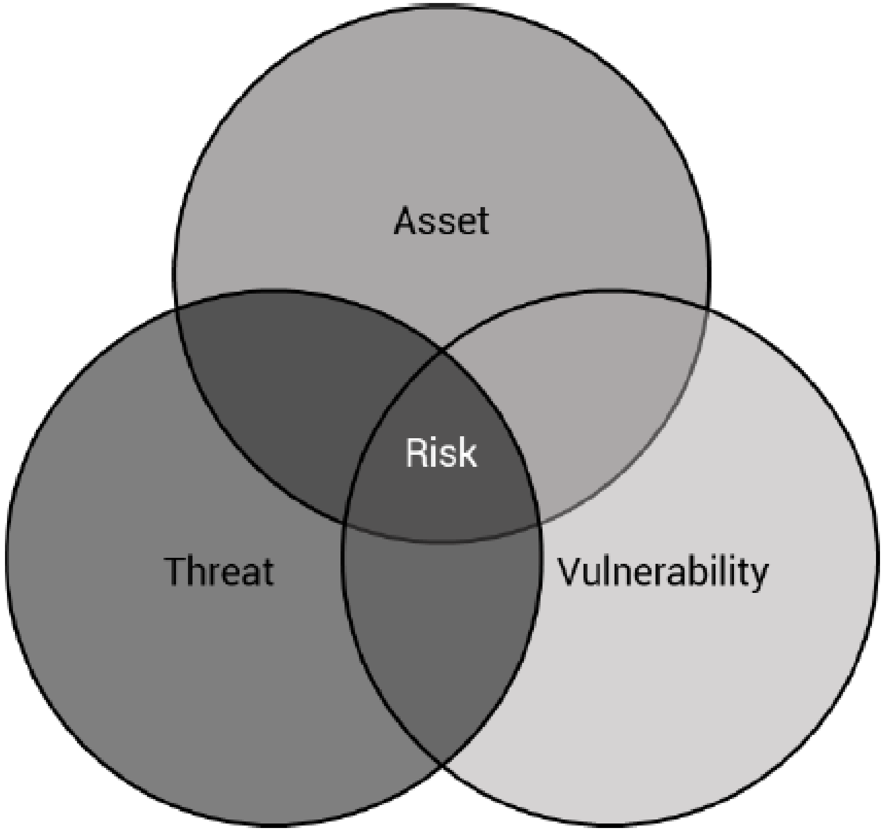
Cybersecurity Cannot be Guaranteed!

- Principle of risk minimization
- “Secure" technologies
- Additional protective measures
- Cybersecurity test strategy penetration testing, vulnerability scan, fuzzing
- "Mature organization" for development, production, operation, maintenance and repair
- Continuous market and product monitoring, incident detection and response
- Extended V-model



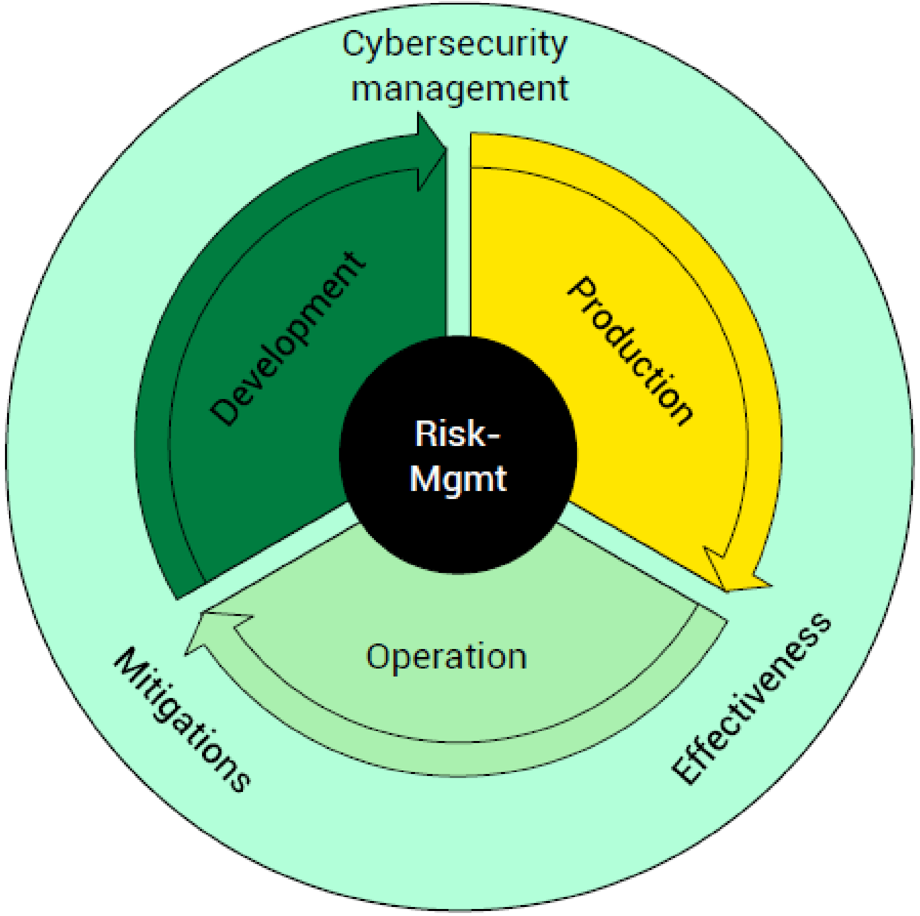
Risk Based Approach

- Identification of assets
- Identification of threats and attack paths
- Analysis of vulnerabilities
- Risk determination



Cybersecurity Management

- Manage risks and change of risks
- Define mitigations to minimize risks
- Observe the remaining risks by monitoring product and environment
- Detect and identify new threats / new vulnerabilities
- Define countermeasures to reduce risks
- Implement & test CS solutions
- Rollout CS solutions into the products
- Cyclic process, valid for the whole product life cycle



04

Introduction to Automotives Security Standards And UNECE Regulation

Drivers for Automotive CS Unification since ~2015

- SAE -Society of Automotive Engineers
- NHTSA -National Highway Traffic Safety Administration
- ENISA -European Union Agency for Network and Information Security
- European Commission -Cybersecurity Act
- ISO International Standardization Organization
- ISO/SAE 21434 “Road vehicles -Cybersecurity engineering”
- ISO/DIS 24089 “Road vehicles -Software update engineering”
- ISO/PAS 5112 “Road vehicles -Guidelines for auditing cybersecurity engineering”
- UN World Forum for Vehicle Regulation, Task Force on Cybersecurity and OTA
- Regulation UN ECE R155 “Cybersecurity”
- Regulation UN ECE R156 “Software update” (including Over-The-Air, OTA)
- VDA-QMC Redbook -Auditing a CSMS

UNECE R155: Cybersecurity and Cybersecurity Management System

Regulation for the OEM

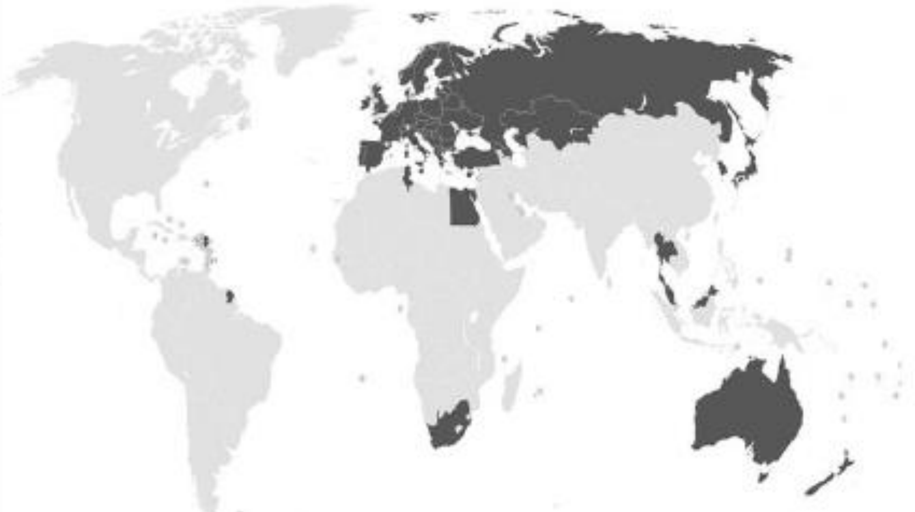
- Concerned are vehicles of categories M, N, O (if equipped with at least one ECU), L6 and L7 if equipped with ADAS level 3 or higher.

Part 1:

- Each OEM must establish and maintain a Cyber Security Management System (CSMS)
- for organizational processes, responsibilities, and governance
- to treat risk from cyber threats to vehicles andto protect vehicles from cyber attacks
- which includes complete lifecycle of a car
- and which must be certified as a precondition for futuretype approval.

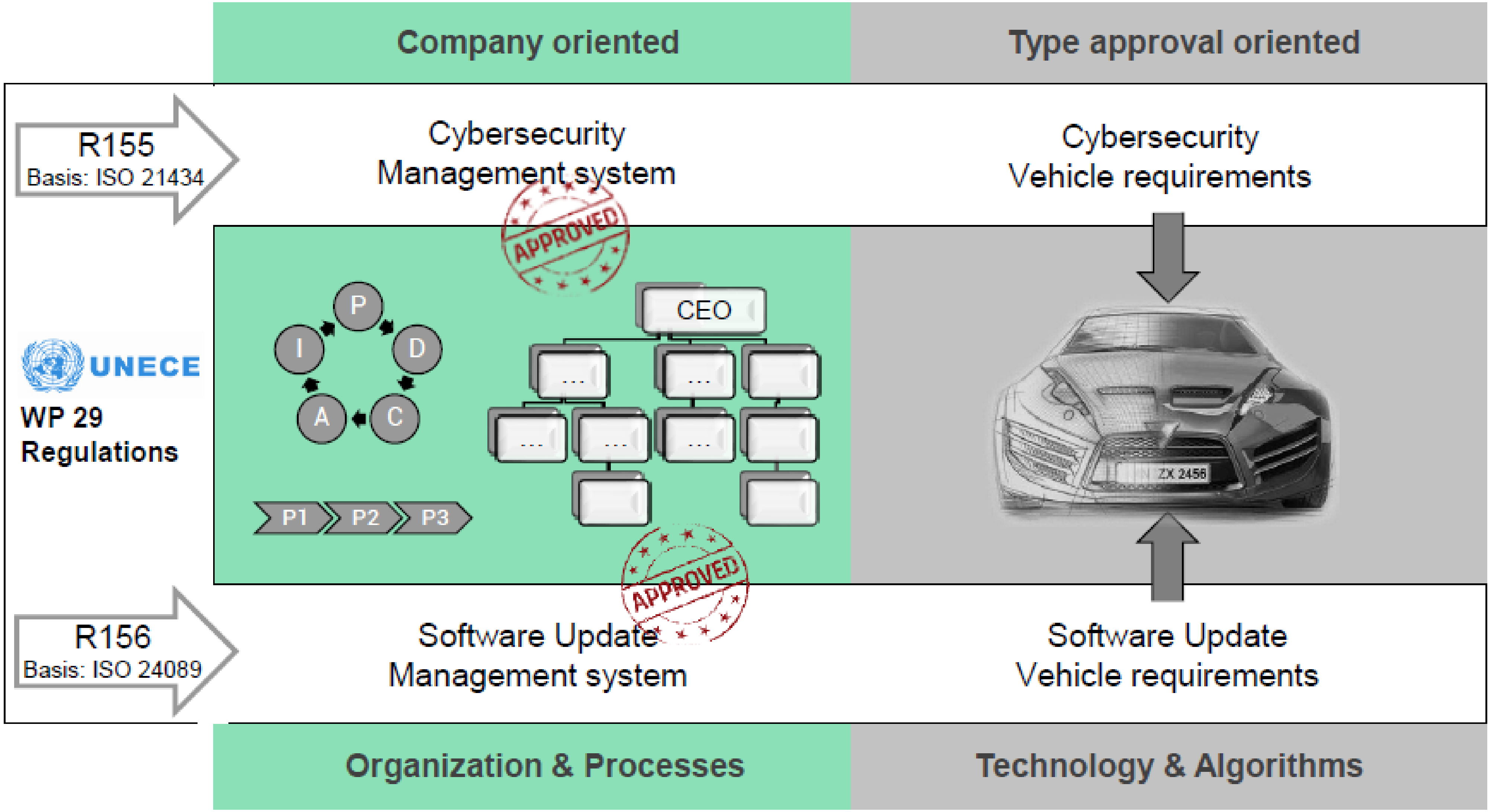
Part 2:

- Each OEM must identify vehicle technology-related risks and to protect the vehicle against them.
- This must be demonstrated at type approval.



UNECE world forum for vehicle regulations WP29Contracted countries (Dark)

UNECE R156: Software Update and Software Update Management



Company oriented

Type approval oriented

R155
Basis: ISO 21434

Cybersecurity
Management system

Cybersecurity
Vehicle requirements

UNECE
WP 29
Regulations

R156
Basis: ISO 24089

Software Update
Management system

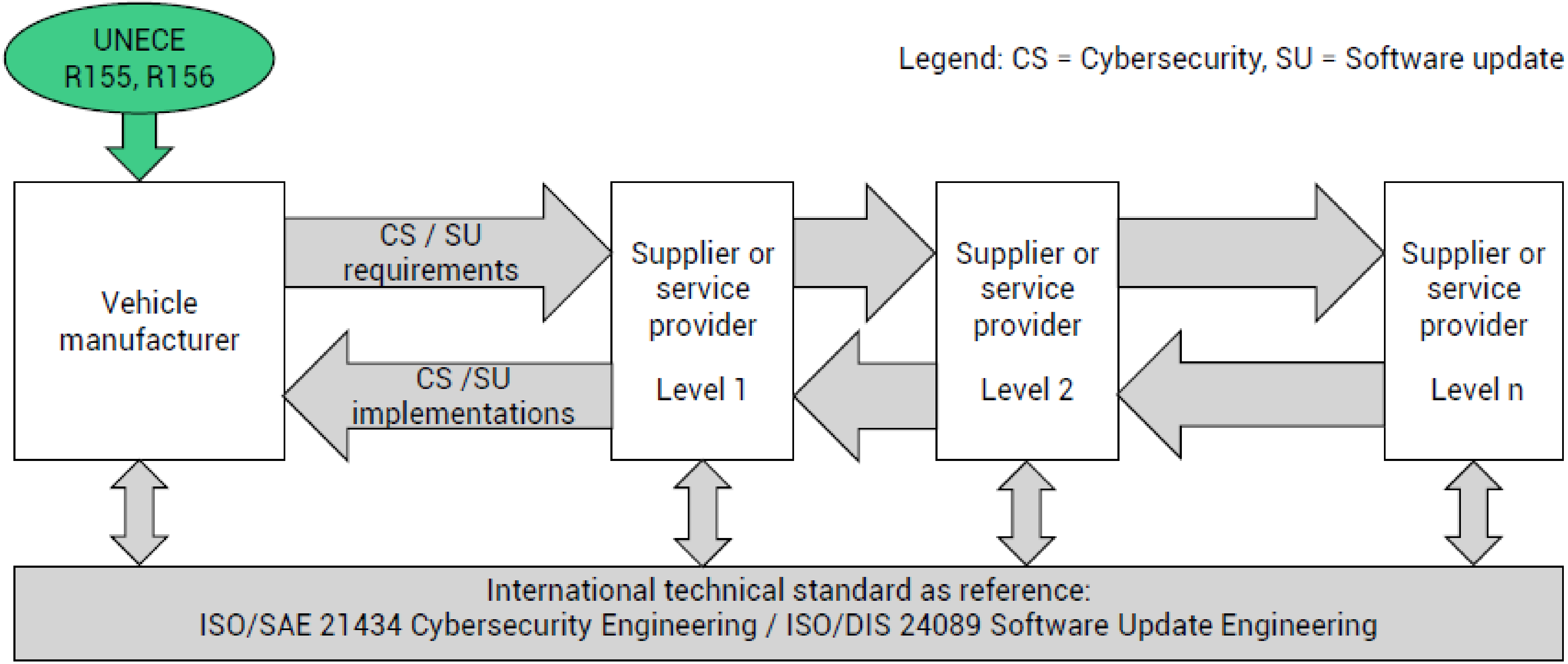
Software Update
Vehicle requirements

Organization & Processes

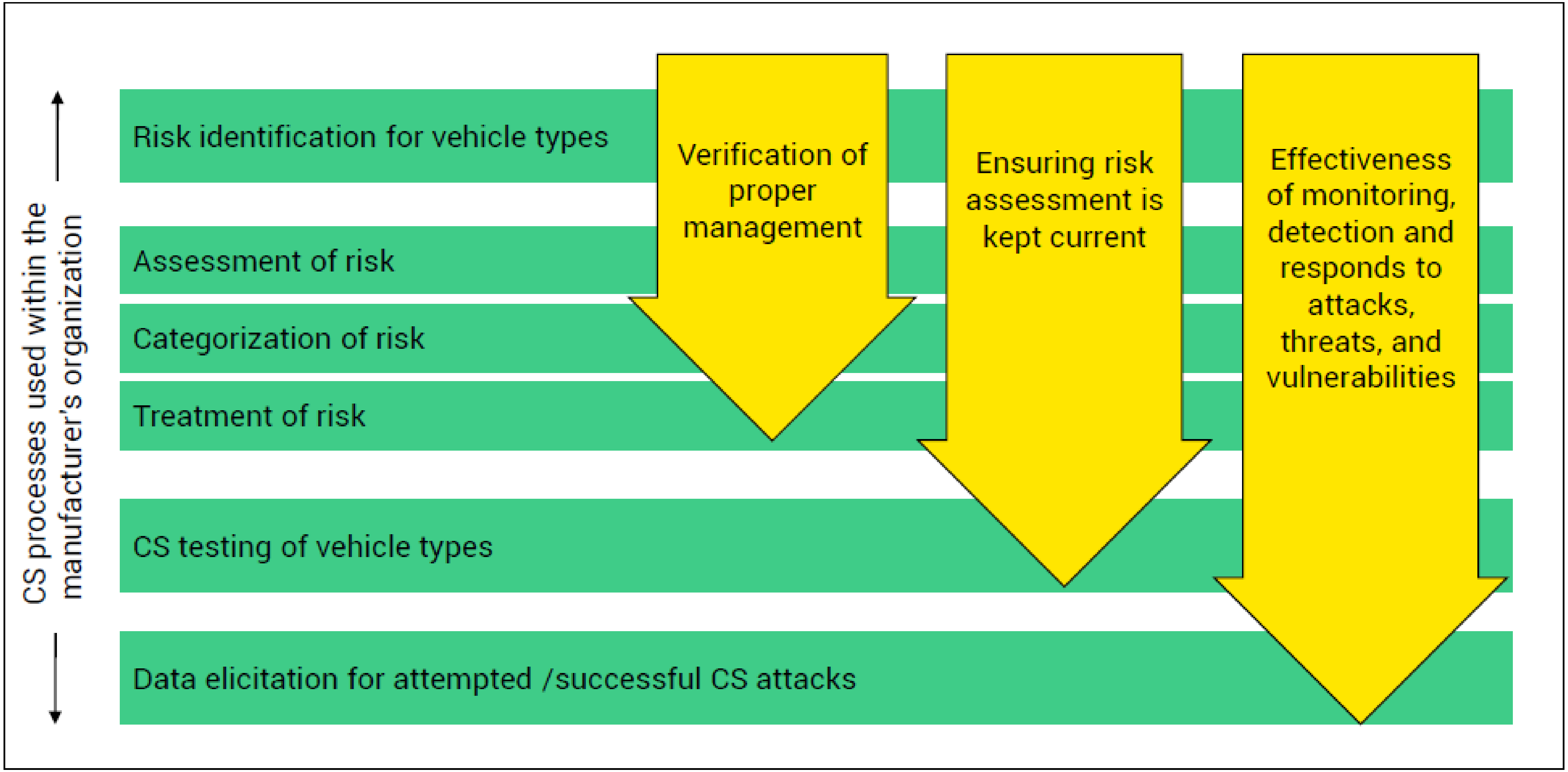
Technology & Algorithms

Role of Suppliers and Service Providers

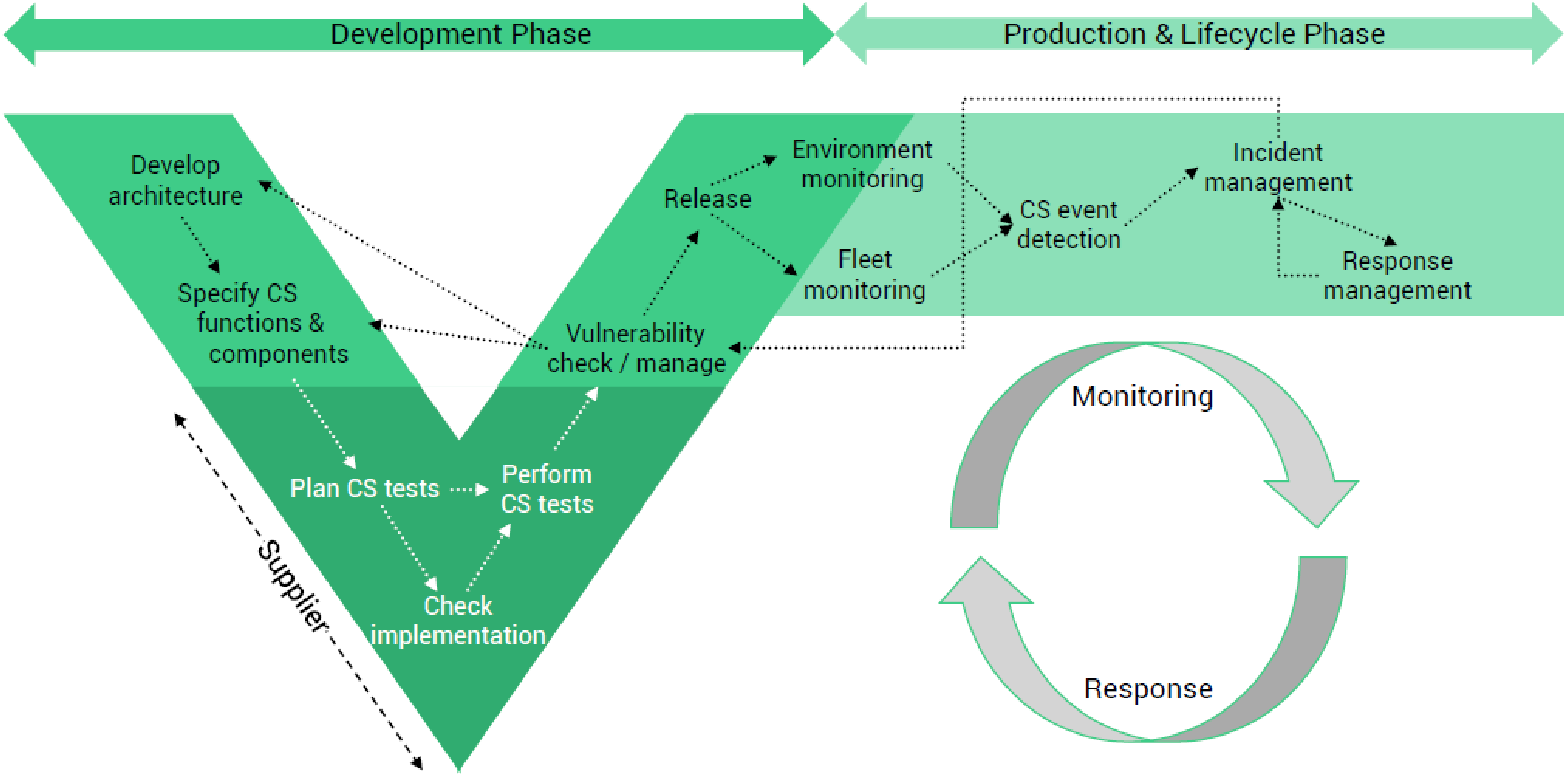
OEMs may require their suppliers to meet all the UNECE regulatory requirements by demonstrating compliance with national/international standard frameworks, which can then be used to demonstrate compliance with the WP.29


UNECE
R155, R156
Legend: CS = Cybersecurity, SU = Software update
Vehicle manufacturer
CS / SU requirements
CS /SU implementations
Supplier or service provider Level 1
Supplier or service provider Level 2
Supplier or service provider Level n
International technical standard as reference:
ISO/SAE 21434 Cybersecurity Engineering / ISO/DIS 24089 Software Update Engineering

Part 1 of R155: CSMS


CS processes used within the manufacturer's organization
Risk identification for vehicle types
Assessment of risk
Categorization of risk
Treatment of risk
CS testing of vehicle types
Data elicitation for attempted /successful CS attacks
Verification of proper management
Ensuring risk assessment is kept current
Effectiveness of monitoring, detection and responds to attacks, threats, and vulnerabilities

Part 1 of R155: CSMS Example of OEM CS Processes



Part 2 of R155: CS for a Vehicle Type

For vehicle type approval the vehicle manufacturer (OEM) …

- Shall have a valid certification of his CSMS (July 2024 at the latest)
- Shall identify and manage supplier-related CS risks for the vehicle type
- Shall perform an exhaustive risk assessment for the vehicle type and manage all the identified risks appropriately:
  - ✓ Including individual elements of the vehicle types and their interactions
  - ✓ Including interactions with any external systems (external communication)
  - ✓ Considering a given list of known threats & mitigations (see “Annex 5”) as well as any other relevant risk
  - ✓ Must protect the vehicle type against all identified risks under consideration of the list of all known mitigations (see “Annex 5”)

R155 Requirements Summary

Requirements for CSMS

- CSMS applies all lifecycle phases of a vehicle
- OEM demonstrates process capability within CSMS
- Ability of the OEM to detect and resolve cybersecurity issues and continuous monitoring for all vehicles
- Manage dependencies with suppliers and third party

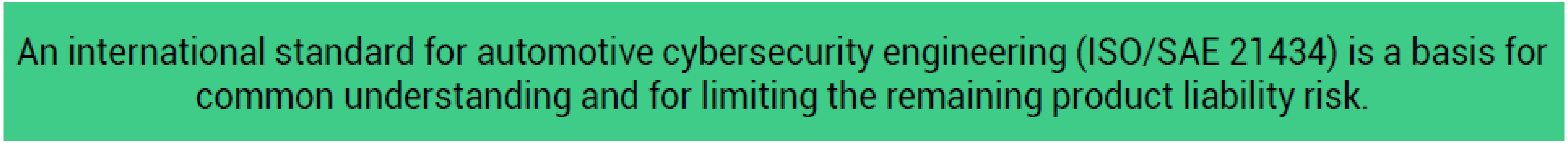
Requirements for vehicle type

- Managing supplier related risks for the vehicle type approved
- Extensive risk assessment on individual elements of vehicle types
- Appropriate security controls against common attack vectors
- Sufficient testing and verification of effectiveness of security measures
- Process to report outcome of monitoring activities

ISO/SAE 21434

Managing the complexity of cybersecurity requires a common understanding of the following:

- Security engineering
- Clear responsibilities
- Comparable approaches for risk determination and corresponding mitigations
- Similar processes with a high degree of maturity by all parties involved



An international standard for automotive cybersecurity engineering (ISO/SAE 21434) is a basis for common understanding and for limiting the remaining product liability risk.

UNECE Regulation vs. ISO Standard

UNECE: Harmonization of vehicle regulations

- National authorities create laws based on the UNECE documents
- Fulfillment mandatory, by law

ISO: Standardization committee

- Technical reference, basis for common understanding
- “State of Technology” = insurance concerning product liability
- Recommended, but not mandatory
- OEMs force fulfillment in the supply chain

05

What is ASPICE ?

What is ASPICE?

- In 2005 the industry-specific standard Automotive SPICE (**Software Process Improvement and Capability Determination),** derived from the ISO 15504 International Standard for software process assessments, was published by the Special Interest Group Automotive
- Objective: Improvement of SW-Product Quality
- SW-Product Quality

What is ASPICE?

SPICE

- Requirements, Rules, Guidelines and Instructions for Trainings, Certifiers and Assessors
- Working groups
- Support of Domains (e.g. Automotive)
- Verification of compliance (e.g. of Assessments)

Automotive SPICE ®

- Common steering committee of German Car manufacturers
- Working groups for definition of unique Standards for the Automotive Domain

- Certification of SPICE-Assessors
- Events for SPICE (e.g. SPICE Days)
- GATE4SPICE

European Certification & Qualification Association

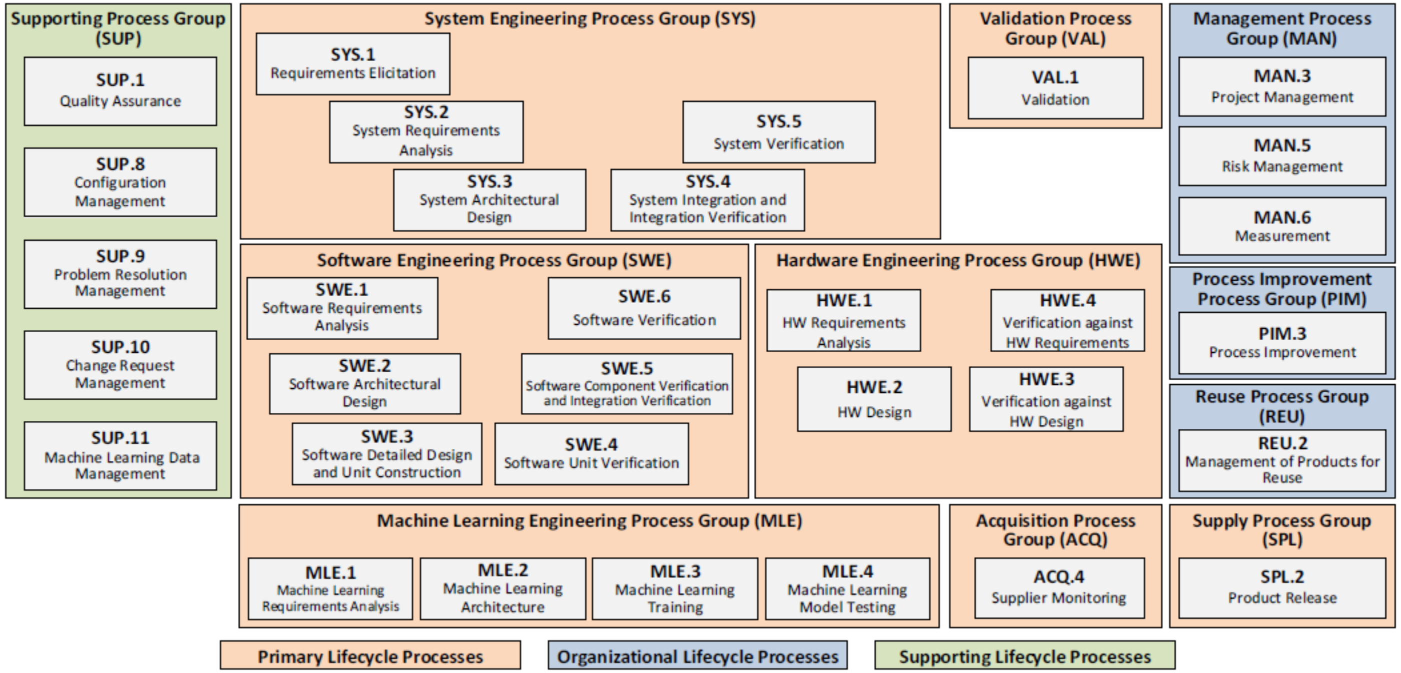
- Certification of Automotive SPICE ® - Assessor

- Trainings provider for SPICE and Automotive SPICE ®

- Competence network (Meetings, Workshops, etc.) of the Community
- Working groups

What is ASPICE?

- Collection of best practices to be applied in the development of electronic control units-based software systems *(Process Reference Model)*.
- Contains a set of methods to perform evaluation of processes fulfillment i.e., ASPICE Assessment *(Process Assessment Model)*
- OEMs demand supplier's process capability during RFQs
- OEM / ASPICE Assessments predominantly focus on 16 Key Processes. Define the capability level from Level 0 to 5.



Supporting Process Group (SUP)
- SUP.1 Quality Assurance
- SUP.8 Configuration Management
- SUP.9 Problem Resolution Management
- SUP.10 Change Request Management
- SUP.11 Machine Learning Data Management

System Engineering Process Group (SYS)
- SYS.1 Requirements Elicitation
- SYS.2 System Requirements Analysis
- SYS.3 System Architectural Design
- SYS.4 System Integration and Integration Verification
- SYS.5 System Verification

Validation Process Group (VAL)
- VAL.1 Validation

Management Process Group (MAN)
- MAN.3 Project Management
- MAN.5 Risk Management
- MAN.6 Measurement

Software Engineering Process Group (SWE)
- SWE.1 Software Requirements Analysis
- SWE.2 Software Architectural Design
- SWE.3 Software Detailed Design and Unit Construction
- SWE.4 Software Unit Verification
- SWE.5 Software Component Verification and Integration Verification
- SWE.6 Software Verification

Hardware Engineering Process Group (HWE)
- HWE.1 HW Requirements Analysis
- HWE.2 HW Design
- HWE.3 Verification against HW Design
- HWE.4 Verification against HW Requirements

Process Improvement Process Group (PIM)
- PIM.3 Process Improvement

Reuse Process Group (REU)
- REU.2 Management of Products for Reuse

Machine Learning Engineering Process Group (MLE)
- MLE.1 Machine Learning Requirements Analysis
- MLE.2 Machine Learning Architecture
- MLE.3 Machine Learning Training
- MLE.4 Machine Learning Model Testing

Acquisition Process Group (ACQ)
- ACQ.4 Supplier Monitoring

Supply Process Group (SPL)
- SPL.2 Product Release

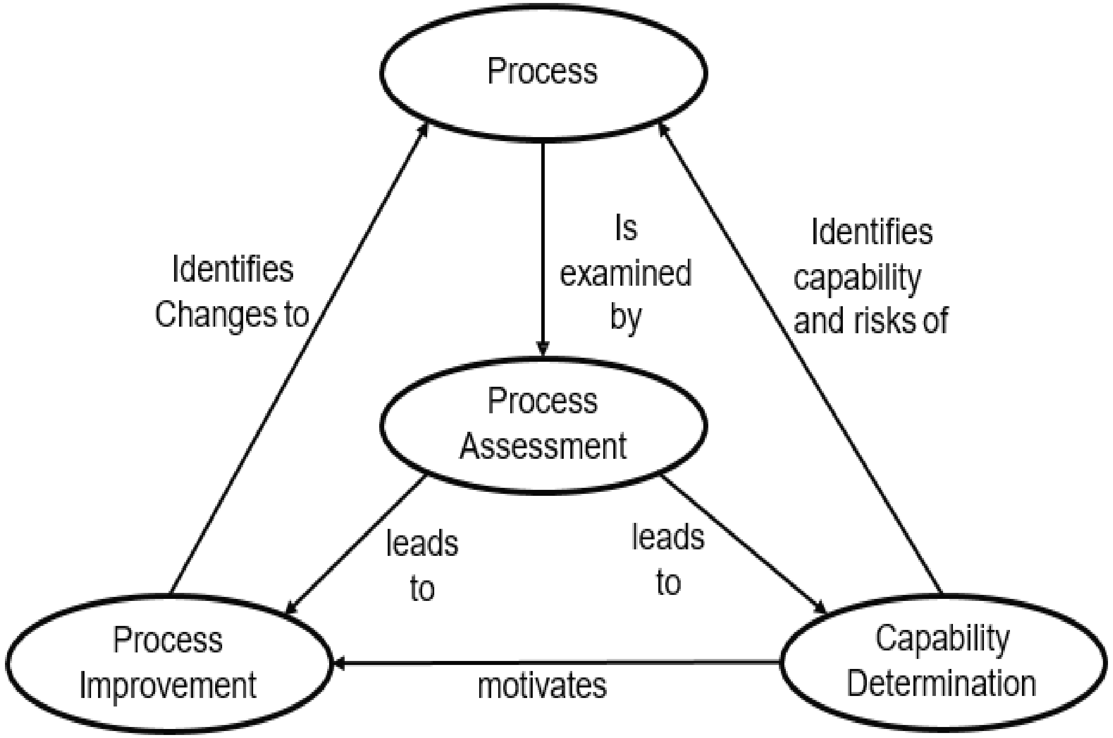
Primary Lifecycle Processes

Organizational Lifecycle Processes

Supporting Lifecycle Processes

ASPICE PRM & PAM

- Collection of best practices to be applied in the development of electronic control units-based software systems.
- Contains a set of methods to perform evaluation of processes fulfillment i.e., ASPICE Assessment.
- 16 Process Areas under VDA scope
- Derived from ISO/IEC 15504 by Automotive SIG.
- Is a trademark of Verband der Automobilindustrie e.V. (VDA).



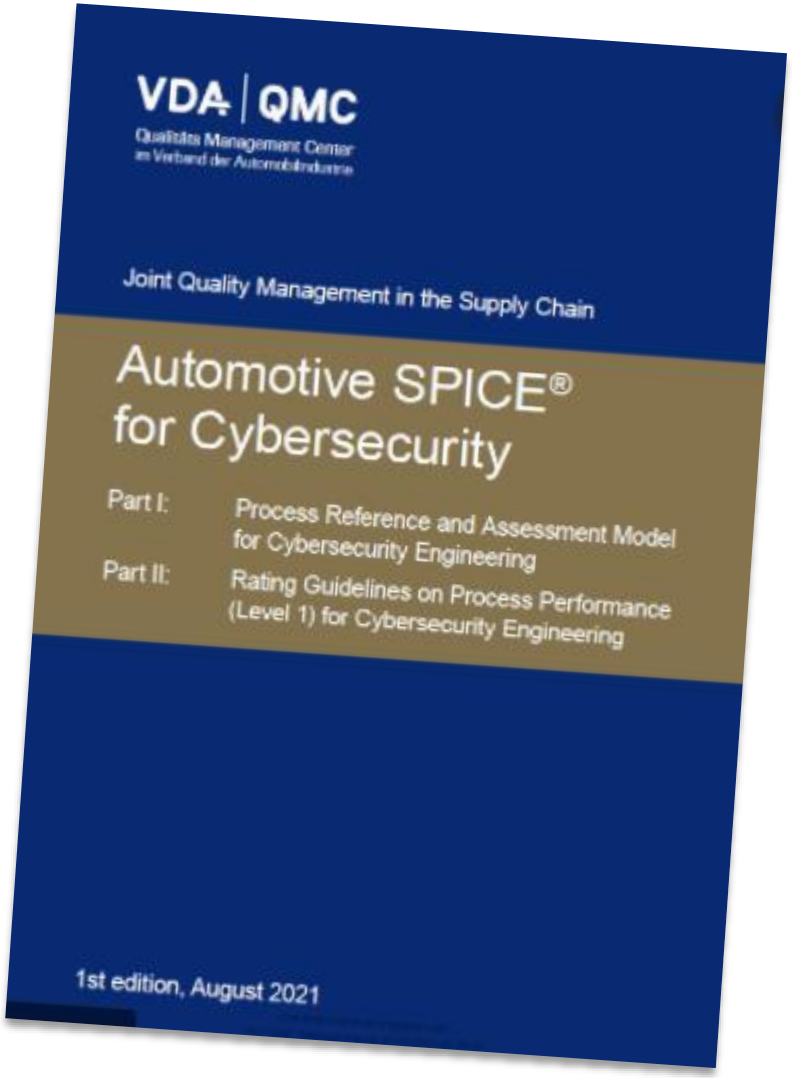
What is ASPICE?

- ASPICE is **not product standard**, i.e. the software is not validated.
- **No methods or tools** are specified or favored.
- ASPICE is not automatically a **process improvement,** but it can be a basis for it.
- ASPICE is also been used for assessments of **system processes** and **organizational maturity.**
- ASPICE provides a **procedure for process assessments.**

06

Understanding ASPICE for Cybersecurity

ASPICE for Cybersecurity



VDA | QMC

Qualitäts Management Center
im Verband der Automobilindustrie

Joint Quality Management in the Supply Chain

Automotive SPICE®
for Cybersecurity

Part I: Process Reference and Assessment Model for Cybersecurity Engineering

Part II: Rating Guidelines on Process Performance (Level 1) for Cybersecurity Engineering

1st edition, August 2021

Created to **support UNECE R155** using ASPICE as a proven assessment model.

To **identify process-related product risks** in Cybersecurity projects.

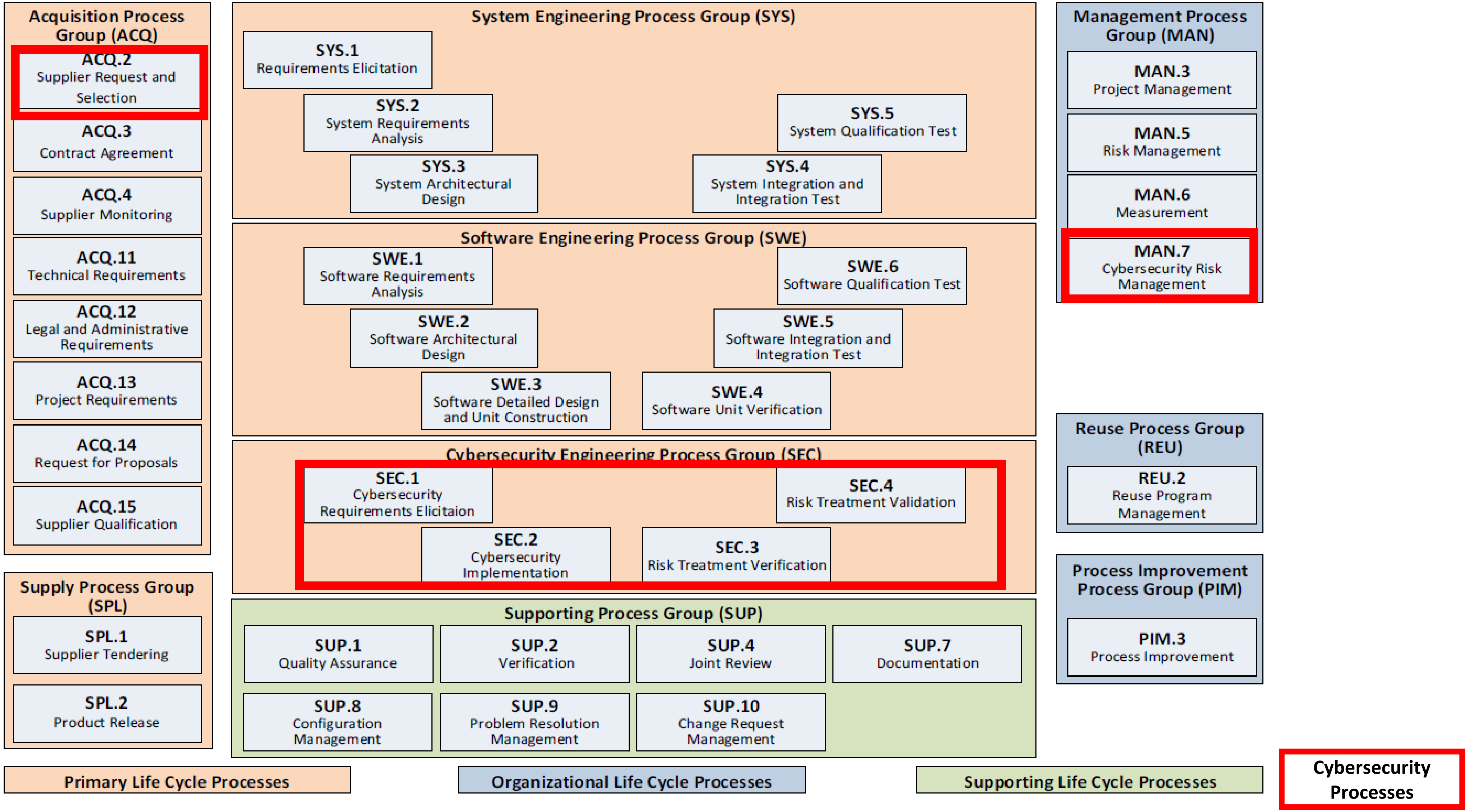
Additional 6 processes have been added specific to Cybersecurity.

Not all parts of ISO/SAE 21434 is covered**; only product development aspects are covered.**

Parts such as cybersecurity management, continuous cybersecurity management, distributed cybersecurity,
post development phases are not covered.

The above parts are subject to
cybersecurity management system audit (CSMS).

ASPICE for Cybersecurity Process Reference Model (PRM)



Acquisition Process Group (ACQ)

- ACQ.2 Supplier Request and Selection
- ACQ.3 Contract Agreement
- ACQ.4 Supplier Monitoring
- ACQ.11 Technical Requirements
- ACQ.12 Legal and Administrative Requirements
- ACQ.13 Project Requirements
- ACQ.14 Request for Proposals
- ACQ.15 Supplier Qualification

Supply Process Group (SPL)

- SPL.1 Supplier Tendering
- SPL.2 Product Release

System Engineering Process Group (SYS)

- SYS.1 Requirements Elicitation
- SYS.2 System Requirements Analysis
- SYS.3 System Architectural Design
- SYS.4 System Integration and Integration Test
- SYS.5 System Qualification Test

Software Engineering Process Group (SWE)

- SWE.1 Software Requirements Analysis
- SWE.2 Software Architectural Design
- SWE.3 Software Detailed Design and Unit Construction
- SWE.4 Software Unit Verification
- SWE.5 Software Integration and Integration Test
- SWE.6 Software Qualification Test

Cybersecurity Engineering Process Group (SEC)

- SEC.1 Cybersecurity Requirements Elicitaion
- SEC.2 Cybersecurity Implementation
- SEC.3 Risk Treatment Verification
- SEC.4 Risk Treatment Validation

Supporting Process Group (SUP)

- SUP.1 Quality Assurance
- SUP.2 Verification
- SUP.4 Joint Review
- SUP.7 Documentation
- SUP.8 Configuration Management
- SUP.9 Problem Resolution Management
- SUP.10 Change Request Management

Management Process Group (MAN)

- MAN.3 Project Management
- MAN.5 Risk Management
- MAN.6 Measurement
- MAN.7 Cybersecurity Risk Management

Reuse Process Group (REU)

- REU.2 Reuse Program Management

Process Improvement Process Group (PIM)

- PIM.3 Process Improvement

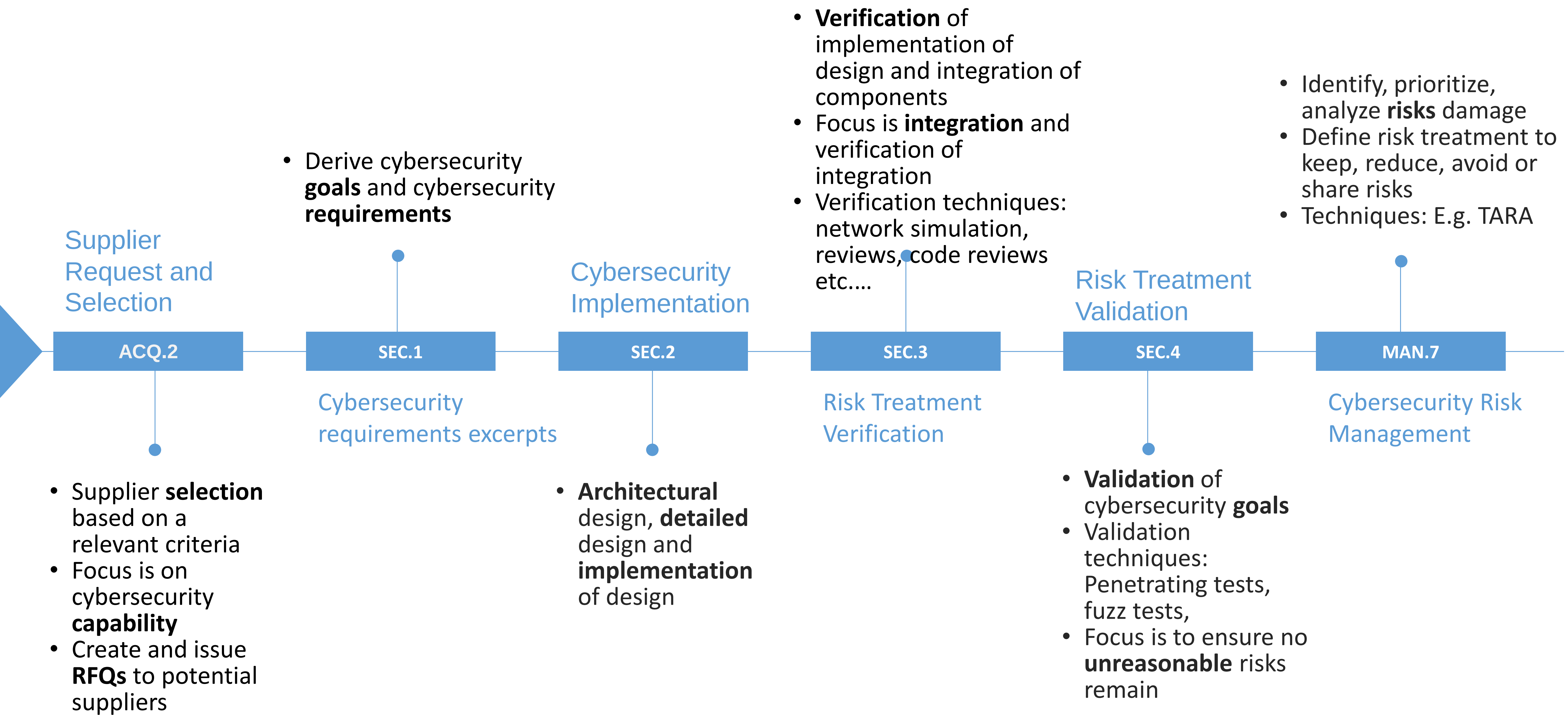
Primary Life Cycle Processes

Organizational Life Cycle Processes

Supporting Life Cycle Processes

Cybersecurity Processes

Brief intro to ASPICE for cybersecurity processes



ACQ.2 Supplier Request and Selection

- Supplier **selection** based on a relevant criteria
- Focus is on cybersecurity **capability**
- Create and issue **RFQs** to potential suppliers

SEC.1 Cybersecurity requirements excerpts

- Derive cybersecurity **goals** and cybersecurity **requirements**

SEC.2 Cybersecurity Implementation

- **Architectural** design, **detailed** design and **implementation** of design

SEC.3 Risk Treatment Verification

- **Verification** of implementation of design and integration of components
- Focus is **integration** and verification of integration
- Verification techniques: network simulation, reviews, code reviews etc.…

SEC.4 Risk Treatment Validation

- **Validation** of cybersecurity **goals**
- Validation techniques: Penetrating tests, fuzz tests,
- Focus is to ensure no **unreasonable** risks remain

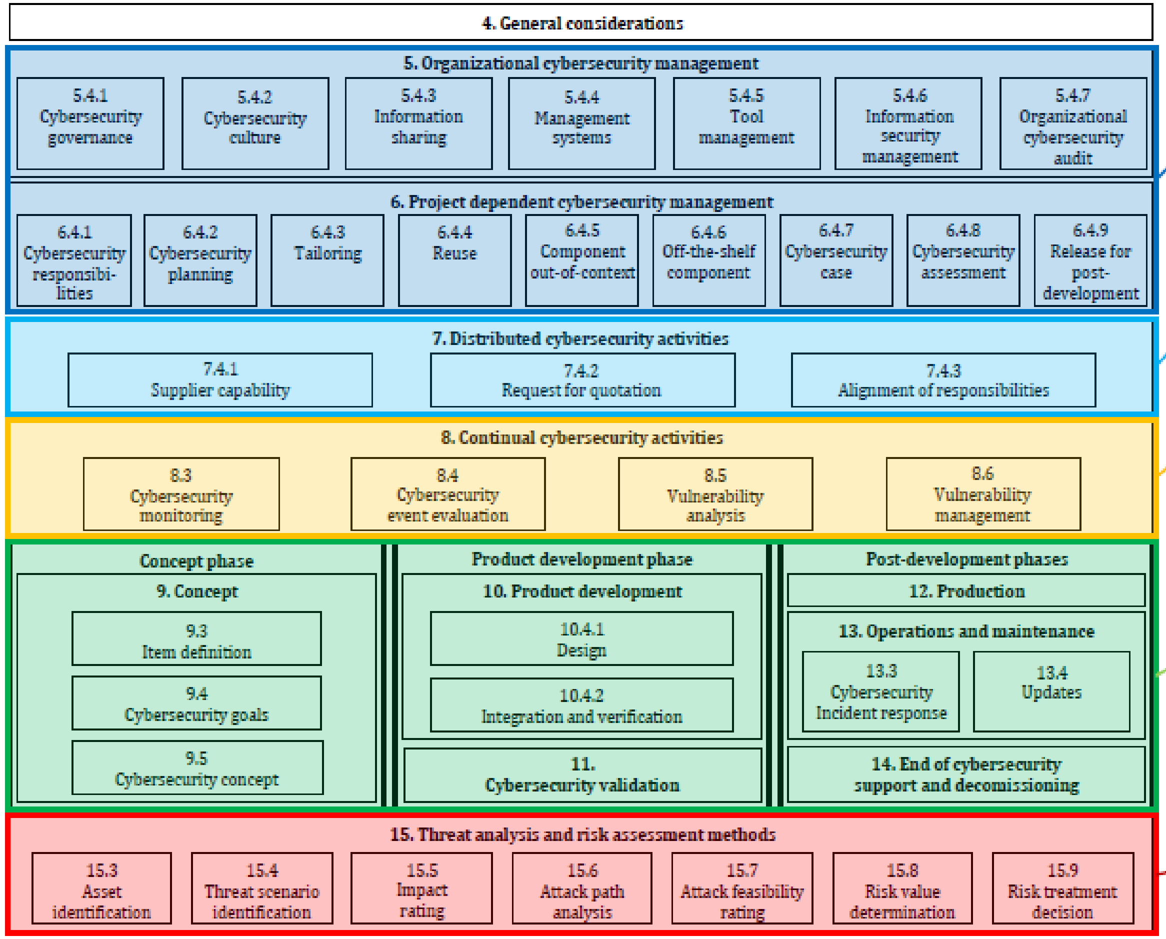
MAN.7 Cybersecurity Risk Management

- Identify, prioritize, analyze **risks** damage
- Define risk treatment to keep, reduce, avoid or share risks
- Techniques: E.g. TARA

07

ASPICE for Cybersecurity vs. ISO/SAE 21434

Structure of ISO/SAE 21434



4. General considerations

5. Organizational cybersecurity management

5.4.1 Cybersecurity governance
5.4.2 Cybersecurity culture
5.4.3 Information sharing
5.4.4 Management systems
5.4.5 Tool management
5.4.6 Information security management
5.4.7 Organizational cybersecurity audit

6. Project dependent cybersecurity management

6.4.1 Cybersecurity responsibi-lities
6.4.2 Cybersecurity planning
6.4.3 Tailoring
6.4.4 Reuse
6.4.5 Component out-of-context
6.4.6 Off-the-shelf component
6.4.7 Cybersecurity case
6.4.8 Cybersecurity assessment
6.4.9 Release for post-development

7. Distributed cybersecurity activities

7.4.1 Supplier capability
7.4.2 Request for quotation
7.4.3 Alignment of responsibilities

8. Continual cybersecurity activities

8.3 Cybersecurity monitoring
8.4 Cybersecurity event evaluation
8.5 Vulnerability analysis
8.6 Vulnerability management

Concept phase

9. Concept

9.3 Item definition
9.4 Cybersecurity goals
9.5 Cybersecurity concept

Product development phase

10. Product development

10.4.1 Design
10.4.2 Integration and verification

11. Cybersecurity validation

Post-development phases

12. Production

13. Operations and maintenance

13.3 Cybersecurity Incident response
13.4 Updates

14. End of cybersecurity support and decomissioning

15. Threat analysis and risk assessment methods

15.3 Asset identification
15.4 Threat scenario identification
15.5 Impact rating
15.6 Attack path analysis
15.7 Attack feasibility rating
15.8 Risk value determination
15.9 Risk treatment decision

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

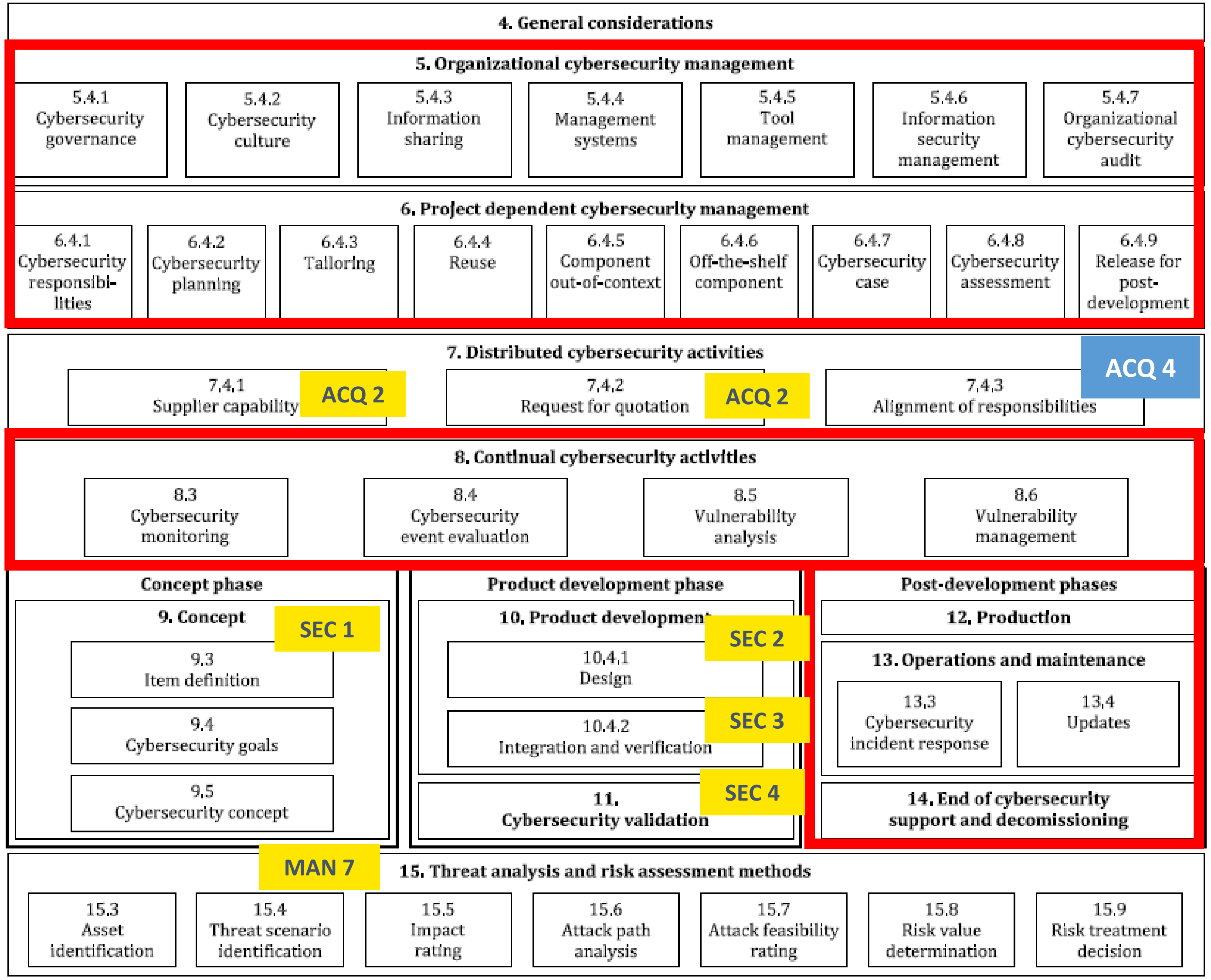
Concept, development and post-development

- 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

On top of ISO/SAE 21434



4. General considerations

5. Organizational cybersecurity management

5.4.1 Cybersecurity governance

5.4.2 Cybersecurity culture

5.4.3 Information sharing

5.4.4 Management systems

5.4.5 Tool management

5.4.6 Information security management

5.4.7 Organizational cybersecurity audit

6. Project dependent cybersecurity management

6.4.1 Cybersecurity responsibilities

6.4.2 Cybersecurity planning

6.4.3 Tailoring

6.4.4 Reuse

6.4.5 Component out-of-context

6.4.6 Off-the-shelf component

6.4.7 Cybersecurity case

6.4.8 Cybersecurity assessment

6.4.9 Release for post-development

7. Distributed cybersecurity activities

ACQ 4

7.4.1 Supplier capability

ACQ 2

7.4.2 Request for quotation

ACQ 2

7.4.3 Alignment of responsibilities

8. Continual cybersecurity activities

8.3 Cybersecurity monitoring

8.4 Cybersecurity event evaluation

8.5 Vulnerability analysis

8.6 Vulnerability management

Concept phase

9. Concept

SEC 1

9.3 Item definition

9.4 Cybersecurity goals

9.5 Cybersecurity concept

Product development phase

10. Product development

SEC 2

10.4.1 Design

SEC 3

10.4.2 Integration and verification

SEC 4

11. Cybersecurity validation

Post-development phases

12. Production

13. Operations and maintenance

13.3 Cybersecurity incident response

13.4 Updates

14. End of cybersecurity support and decomissioning

MAN 7

15. Threat analysis and risk assessment methods

15.3 Asset identification

15.4 Threat scenario identification

15.5 Impact rating

15.6 Attack path analysis

15.7 Attack feasibility rating

15.8 Risk value determination

15.9 Risk treatment decision

NOT in scope ASPICE for Cybersecurity PAM

ASPICE for Cybersecurity

ASPICE PAM 3.1

ACQ2. Supplier request and selection

ACQ.4 Supplier monitoring (PAM 3.1)

SEC.1 Cybersecurity requirements elicitation

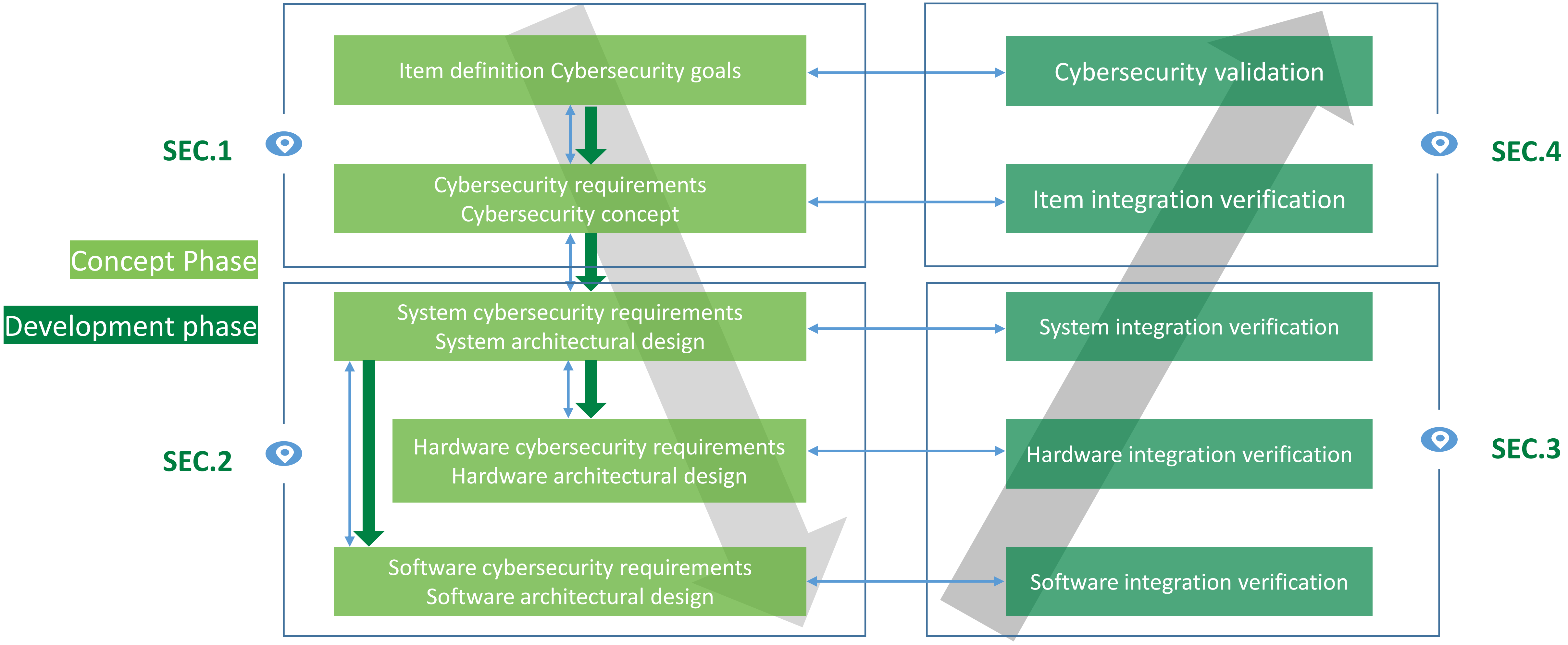
SEC.2 Cybersecurity implementation

SEC.3 Risk treatment verification

SEC.4 Risk treatment validation

MAN.7 Cybersecurity risk management

Mapping to V Cycle


Item definition Cybersecurity goals
Cybersecurity requirements
Cybersecurity concept
System cybersecurity requirements
System architectural design
Hardware cybersecurity requirements
Hardware architectural design
Software cybersecurity requirements
Software architectural design
Cybersecurity validation
Item integration verification
System integration verification
Hardware integration verification
Software integration verification
SEC.1
SEC.2
SEC.3
SEC.4
Concept Phase
Development phase

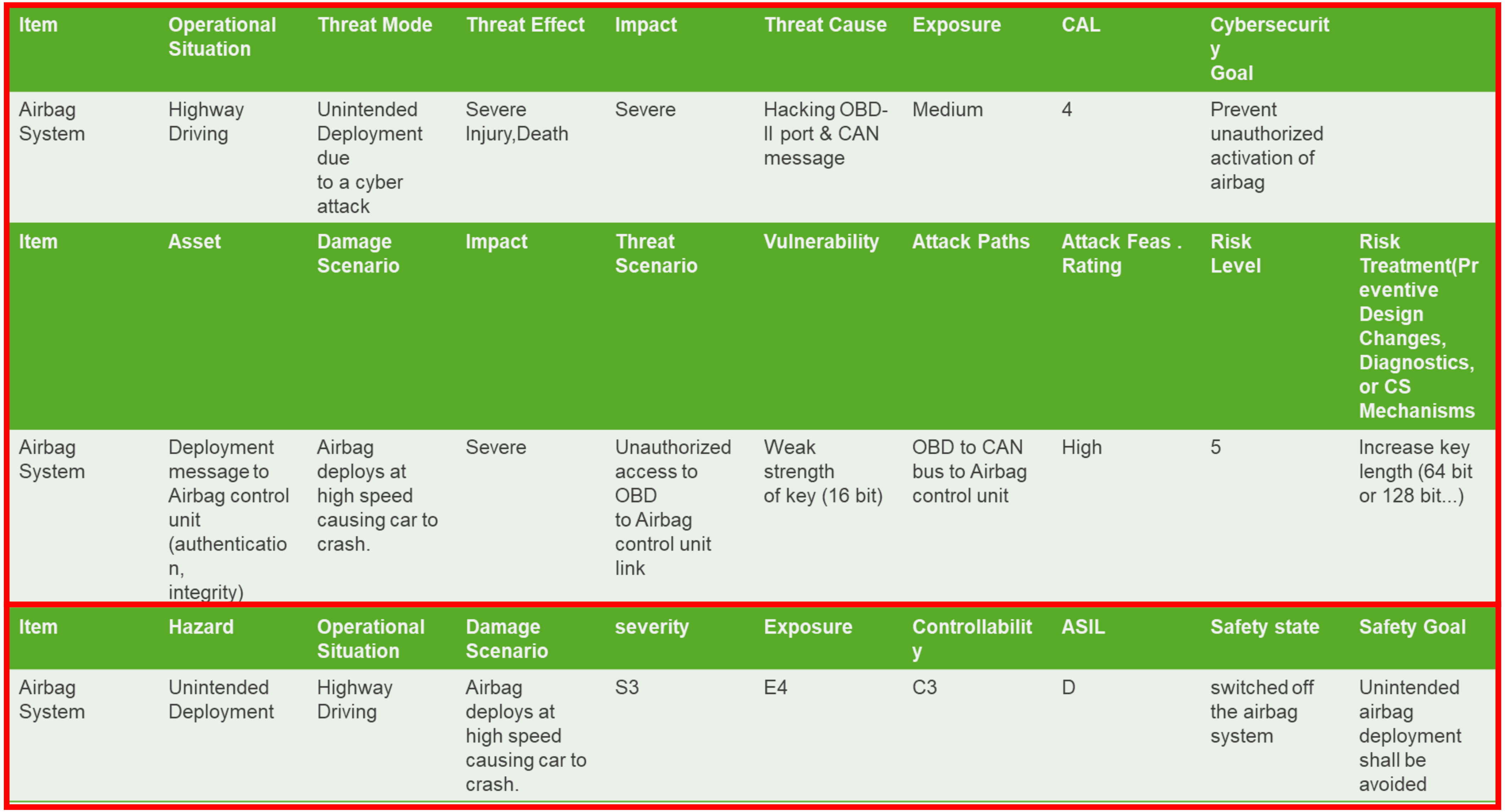
08

ISO/SAE 21434 vs. ISO 26262

Relationship between FuSa and Cyber-Security

Item	Functional Safety	Cyber-Security
Focus	系統安全的目的是通過分析潛在安全風險使得在系統設計時建立安全機制解決安全風險或降低由安全風險引起的危害。	由攻擊者引起的潛在威脅其目的是造成危害、獲取經濟或其他利益、或僅是得到名聲。
response to identified threats	分析人員相對易於識別潛在危害，並採取合適的行為消除潛在的後果。	潛在威脅是故意的、有計劃的，比潛在危害難處理。需要分析人員像駭客一樣思考，預測攻擊者行為，幫助分析人員知道網絡安全保護免於受到駭客可能攻擊的行為。
statistics	用於可接受的風險等級	大量的未知資訊難以統計
Additional factors	不需考慮額外因素	需要考慮的額外因素包括：攻擊者獲取的知識（私人途徑或者公眾途徑），攻擊者的經驗水準，從攻擊者獲取進入系統的途徑，攻擊者必備的特殊裝備等
Analysis method	FTA, FMEA, FMEDA	攻擊樹分析 (ATA)
In the implementation and verification/validation stages, static code analysis	靜態代碼分析被用於幫助識別直接影響基礎功能的程式錯誤	靜態代碼分析被用來識別代碼中潛在網絡安全性漏洞。從安全角度看，合法或者正確的代碼可能仍然會有網絡安全性漏洞。
verification/validation methods	故障注入測試	攻擊（漏洞）測試或者滲透測試

Relationship between FuSa and Cyber-Security



Item	Operational Situation	Threat Mode	Threat Effect	Impact	Threat Cause	Exposure	CAL	Cybersecurity Goal
Airbag System	Highway Driving	Unintended Deployment due to a cyber attack	Severe Injury,Death	Severe	Hacking OBD-II port & CAN message	Medium	4	Prevent unauthorized activation of airbag

Item	Asset	Damage Scenario	Impact	Threat Scenario	Vulnerability	Attack Paths	Attack Feas . Rating	Risk Level	Risk Treatment(Preventive Design Changes, Diagnostics, or CS Mechanisms
Airbag System	Deployment message to Airbag control unit (authentication, integrity)	Airbag deploys at high speed causing car to crash.	Severe	Unauthorized access to OBD to Airbag control unit link	Weak strength of key (16 bit)	OBD to CAN bus to Airbag control unit	High	5	Increase key length (64 bit or 128 bit...)

Item	Hazard	Operational Situation	Damage Scenario	severity	Exposure	Controllability	ASIL	Safety state	Safety Goal
Airbag System	Unintended Deployment	Highway Driving	Airbag deploys at high speed causing car to crash.	S3	E4	C3	D	switched off the airbag system	Unintended airbag deployment shall be avoided

ISO 21434

Asset:一般會包硬體、軟體及機密資訊需要加以保護，避免非法存取、使用、揭露、更改、破壞或是被竊，也避免造成的損失

ISO 26262

DEKRA 優勢

全台唯一能提供車用客戶完整解決方案

AUTOMOTIVE SPICE® ASPICE for Cyber-Security

TISAX ISO 24089 ISO 26262

ISO/SAE 21434 Road vehicles — Cybersecurity Engineering ISO/PAS 21448

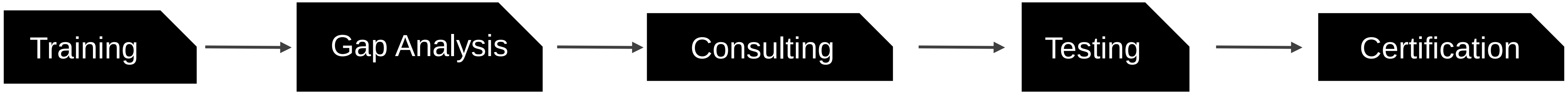
擁有全台最多車用系統廠合作認證公司

FOXCONN 鴻海科技集團 英業達 Inventec AUO INNOLUX TTE

E-LEAD 怡利電子 DELTA LITEON USI PEGATRON 和碩聯合科技

TYC LIGHTS. PRECISION. SAFETY Lextar GARMIN CUBTEK

- **一次性全面導入**整合方案讓客戶同時符合ISO 26262, ISO/PAS 21448, ASPICE, ASPICE for Cyber-Security and ISO/SAE 21434流程
- **全台唯一同時擁有ASPICE首席/主任評估師**團隊 Automotive SPICE汽車產業軟體開發流程評估
- **全本土化顧問/稽核團隊**協助貴公司用最快速度導入流程並取得**德國DAKKS 證書**



Training → Gap Analysis → Consulting → Testing → Certification

聯絡資訊

Contact Information

DEKRA

聯絡我們｜DEKRA德凱

DEKRA
www.dekra.com.tw

Line@
@dekra.taiwan

facebook
www.facebook.com

www.linkedin.com

THANK YOU

DevOps Tec.
戴博斯科技股份有限公司

Facebook

官網