Automotive SPICE and Cybersecurity

Are ISO 21434 and Security Engineering processes perfectly aligned ?

Rigels Gordani - INTECS Solutions S.p.A.

23/05/2024

Hackers spent 2+ years looting secrets of chipmaker NXP before being detected

Chipmaker claims breach had no "material adverse effect“

> The intrusion, by a group tracked under names including "Chimera" and "G0114," lasted from late 2017 to the beginning of 2020, according to Netherlands national news outlet NRC Handelsblad, which cited “several sources” familiar with the incident. During that time, the threat actors periodically accessed employee mailboxes and network drives in search of chip designs and other NXP intellectual property. The breach wasn’t uncovered until Chimera intruders were detected in a separate company network that connected to compromised NXP systems on several occasions. Details of the breach remained a closely guarded secret until now.

source: https://arstechnica.com/security/2023/11/hackers-spent-2-years-looting-secrets-of-chipmaker-nxp-before-being-detected/

Relay attack keyless repeater on sale on TikTok

In May 2023, a relay attack keyless repeater promising the ability to unlock and start vehicles manufactured between 2008-2023 from multiple OEMs was offered for sale on TikTok by a threat actor promoting a Polish automotive cybersecurity and hacking ecommerce website offering a wide selection of vehicle-hacking tools.[32] Relay attack keyless repeaters make it possible for malicious actors to gain unauthorized access to a vehicle and steal it without the physical key fob.

source: Upstream 2024 global automotive cybersecurity report, page 30.

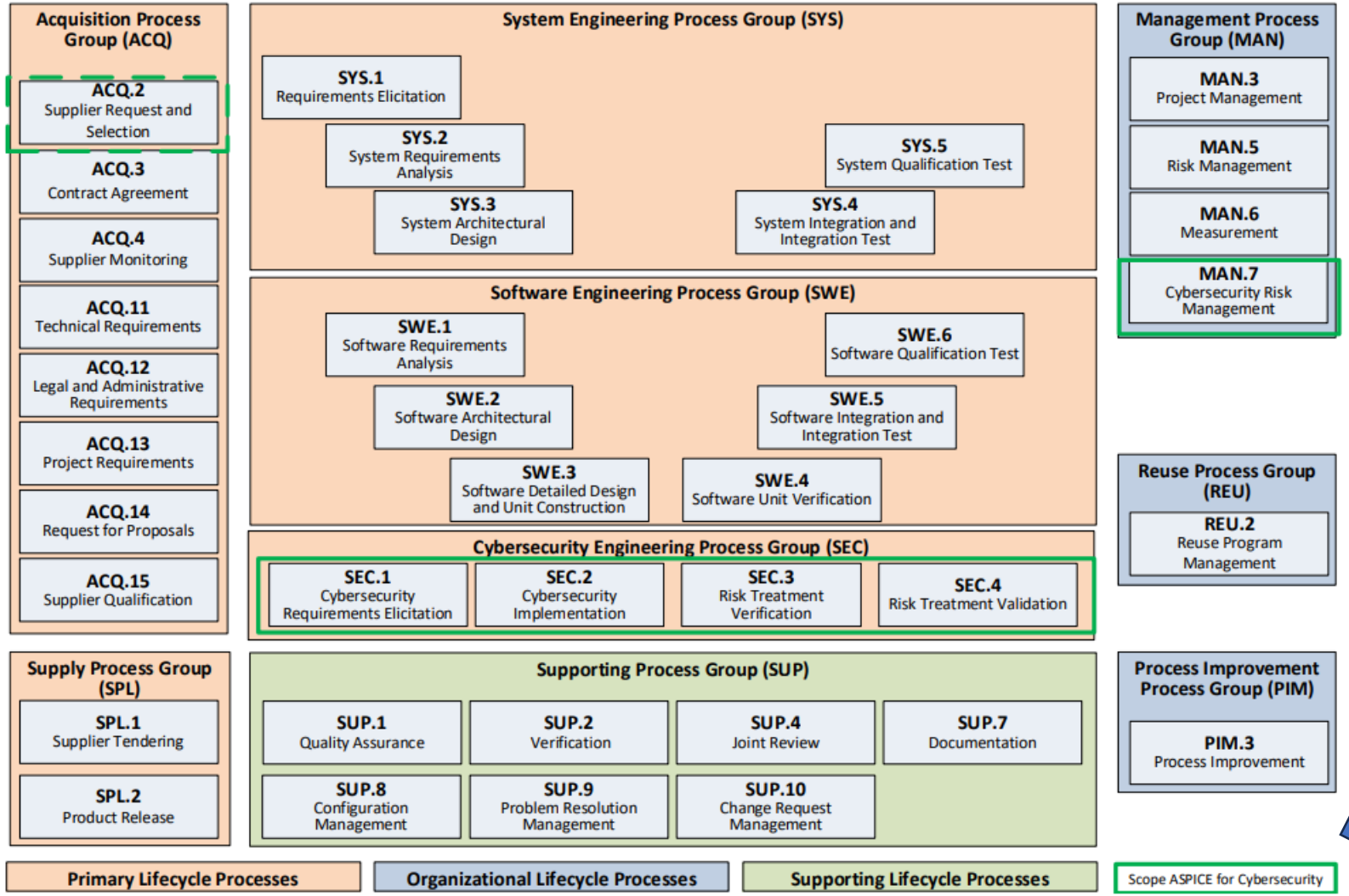
ASPICE and Security Engineering (SEC)

La cybersecurity è un aspetto importante nello sviluppo software automotive, e l'integrazione dei processi di security nel modello ASPICE è fondamentale.

ASPICE (Automotive SPICE) è uno standard utilizzato nell'industria automotive per valutare e migliorare i processi di sviluppo del software. In particolare, i processi **SEC (Security Engineering)** sono stati introdotti per affrontare le specifiche della cybersecurity sempre nel contesto automotive.

I processi SEC includono *l'identificazione dei requisiti di sicurezza* **(SEC.1),** *l'implementazione della sicurezza* **(SEC.2),** *la verifica del trattamento dei rischi* **(SEC.3)** e *la validazione del trattamento dei rischi* **(SEC.4).**

Cybersecurity Engineering Process Group (SEC)



Automotive SPICE and Automotive SPICE for Cybersecurity Process Reference Model – Overview

The processes in scope for ASPICE cybersecurity are SEC.1, SEC.2, SEC.3, SEC.4, ACQ.2 (Supplier Request and Selection), MAN.7 (Cybersecurity Risk Management)

Relation to ISO/SAE 21434:2021 - Road vehicles Cybersecurity engineering

The purpose of an Automotive SPICE assessment is to identify systematic weaknesses in the primary life cycle processes, management processes, and support processes. Automotive SPICE and Automotive SPICE for Cybersecurity are covering system engineering and software engineering.

Certain aspects of the ISO/SAE 21434 are not in the scope of this document, *as they are not performed in a development project context.* They are addressed by the Automotive Cybersecurity Management System (ACSMS). These aspects, such as:

- cybersecurity management
- continuous cybersecurity activities
- post-development phases

are subject to an audit of the cybersecurity management system.

SEC.1 – Cybersecurity Requirements Elicitation

The purpose of the **Cybersecurity Requirements Elicitation Process**

is to **derive** cybersecurity goals and requirements from the outcomes of risk management, and ensure consistency between the risk assessment, cybersecurity goals and cybersecurity requirements.

The following Best Practices are related to SEC.1:

SEC.1 – Best practices	
SEC.1.BP1	Derive cybersecurity goals and cybersecurity requirements.
SEC.1.BP2	Establish bidirectional traceability.
SEC.1.BP3	Ensure consistency.
SEC.1.BP4	Communicate agreed cybersecurity requirements.

SEC.2 – Cybersecurity Implementation

The purpose of the **Cybersecurity Requirements Elicitation Process**

is to **allocate** the cybersecurity requirements to the elements of the system and software and ensure they are implemented.

SEC.2 – Cybersecurity Implementation

The following Best Practices are related to SEC.2:

SEC.2 – Best practices	
SEC.2.BP1	Refine the details of the architectural design
SEC.2.BP2	Allocate cybersecurity requirements
SEC.2.BP3	Select cybersecurity controls
SEC.2.BP4	Refine interfaces
SEC.2.BP5	Analyze architectural design
SEC.2.BP6	Refine the details of the detailed design
SEC.2.BP7	Develop software units
SEC.2.BP8	Establish bidirectional traceability
SEC.2.BP9	Ensure consistency
SEC.2.BP10	Communicate agreed results of cybersecurity implementation

Security requirements

Architecture

Security controls

Interfaces

Detailed design

Develop SW units

Traceability

SEC.3 – Risk Treatment Verification

The purpose of the **Risk Treatment Verification Process**

is to **confirm** that the implementation of the design and integration of the components comply with the cybersecurity requirements, the refined architectural design and detailed design.

The following Best Practices are related to SEC.3:

SEC.3 – Best practices	
SEC.3.BP1	Develop a risk treatment verification and integration strategy
SEC.3.BP2	Develop specification for risk treatment verification
SEC.3.BP3	Perform verification activities
SEC.3.BP4	Establish bidirectional traceability
SEC.3.BP5	Ensure consistency
SEC.3.BP6	Summarize and communicate results

SEC.4 – Risk Treatment Validation Process

The purpose of the **Risk Treatment Validation Process**

is to **confirm** that the integrated system achieves the associated cybersecurity goals.

The following Best Practices are related to SEC.4:

SEC.4 – Best practices	
SEC.3.BP1	Develop a risk treatment validation strategy.
SEC.4.BP2	Develop specification for risk treatment validation
SEC.4.BP3	Perform and document risk treatment validation activities
SEC.4.BP4	Establish bidirectional traceability
SEC.4.BP5	Ensure consistency.
SEC.4.BP6	Summarize and communicate results.

ACQ.2 – Supplier Request and Selection
MAN.7 - Cybersecurity Risk Management

The remaining two processes in the ASPICE cybersecurity scope are ACQ.2 e MAN.7, they are not less important than security engineering group and may impact costs and deadlines.

ACQ.2 - The purpose of supplier request and selection process is to award a supplier for a contract/agreement based on relevant criteria.

MAN.7 - The purpose of the Cybersecurity Risk Management Process is to identify, prioritize, and analyze risks of damage to relevant stakeholders as well as monitor and control respective risk treatment options continuously.

Intecs Solutions S.p.A

Via Umberto Forti, 5
Loc. Montacchiello
56121 Ospedaletto - Pisa
Phone: +39 050 96 57 411
automotive.sales@intecs.it
www.intecs.it

Questions ?