Security standard

Innovation is important, but in a lot of cases, standards and requirements drive organizations compliancy

Prof. Sergio Saponara,
Dip. Ingegneria della Informazione, Università di Pisa
sergio.saponara@unipi.it, +39 3468790937

Outline

Introduction on security specifications

- Analysis of HW secure specifications and de-facto standards:

SHE (Secure HW extension),

EVITA (E-safety vehicle intrusion protected applications)

TPM (Trusted Platform Module)

- System-level Directives and Standards:

Brief on Automotive standards UN155/UN156

NIS2 directive

IEC 62443

Introduction on security specifications

For secure specifications we have:

Custom solution used by a set of industries, acquired by the market

1) Low-level details specifications or the facto standards, used by ICs providers to define specs for their products, focused on low-level components aspects but missing system-level aspects and organization-level aspects

Example:

This is not enough to ensure security of an entire plant or organization, just for a specific component (ex: safe helmet doesn't specify safety procedures)
If you just rely on this you will never get a secure element.

SHE (Secure Hardware Extension)

Evita: E-safety Vehicle Intrusion Protected Applications

TPM (Trusted Platform Module)

Introduction on security specifications

For secure specifications we have:

They give a high level suggestion but not a solution

2) High-level directives and standards specifications, typically addressing system-level aspects and giving general hints on organization aspects.

However, typically they miss specification of low-level details for hardware and software

Example:

NIS2 directive

UN- 155/156 (more focused on vehicles)

EACH FIELD MIGHT HAVE ITS OWN STANDARDS

IEC 62443 (more focused on industrial automation, process industry,..)

Introduction on security specifications

Practical guide

- Mix secure high-level directive and standards to define secure by design product development procedures and organization-level security aspects with low-level specification for Hardware and Software design guides and to reuse the solutions already embedded in COTS Hardware devices and in public SW libraries

Outline

Introduction on security specifications

- Analysis of HW secure specifications and de-facto standards:

SHE (Secure HW extension),

EVITA (E-safety vehicle intrusion protected applications)

TPM (Trusted Platform Module)

- System-level Directives and Standards:

Brief on Automotive standards UN155/UN156

NIS2 directive

IEC 62443

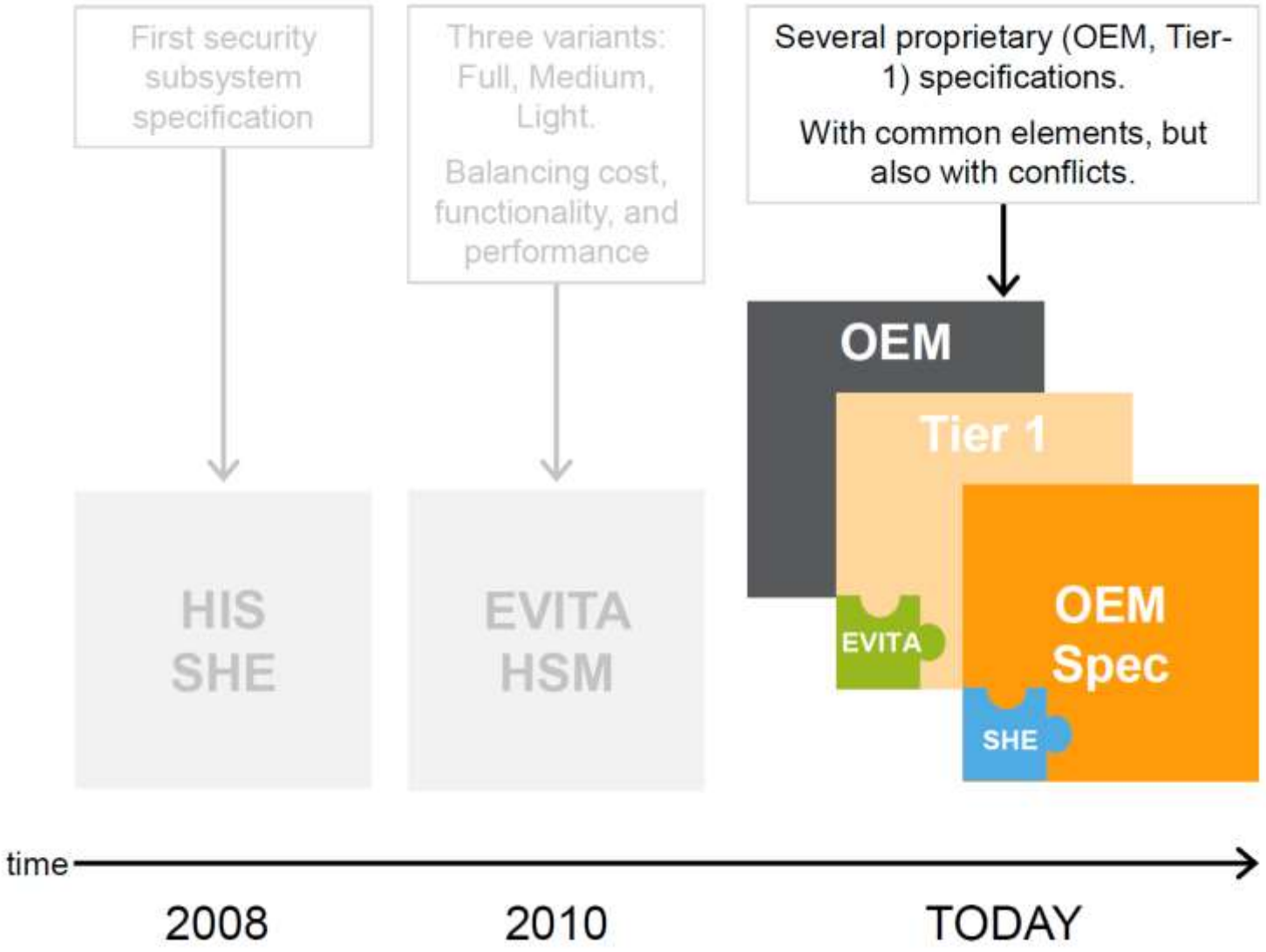
SHE and Evita security specifications

- The SHE (Secure Hardware Extensions) specification set the foundation, introducing the concept of a configurable (automotive) security subsystem

https://www.autosar.org/fileadmin/user_upload/standards/foundation/19-11/AUTOSAR_TR_SecureHardwareExtensions.pdf

- EVITA's HSM specification extended this concept into a programmable subsystem, in three flavors (Full, Medium, and Light), addressing a broader range of use cases
- Nowadays, OEMs are creating their own technical specifications, including selected aspects of SHE, EVITA, and FIPS (Federal Information Processing Standards, US) 140-2 to assess new security regulations

SHE and Evita security specifications



SHE and Evita security specifications coverage in Commercial Off The Shelf products (example NXP)

	SHE	EVITA (Light / Medium / Full)	More recent needs
ARCHITECTURE	• Configurable, fixed function	• Programmable (except EVITA Light)	• Acceleration close to the interfaces (CAN and ETH MAC/PHYs) • Support for Flash-less technologies
FUNCTIONALITY	• Secure boot • Memory update protocol • AES-128 (ECB, CBC) • CMAC, AES-MP • TRNG, PRNG • Key derivation (fixed algorithm) • 10+4 keys, key-usage flags	Same as SHE, plus: • AES-PRNG • monotonic counters (16x, 64bit) Plus, for EVITA Medium and Full: • WHIRLPOOL, HMAC-SHA1, ECDH and ECDSA (P256)	• Further crypto algorithms (e.g. RSA, SHA1-3, Curve25519, …) • Rollback protection • Key negotiation protocols • Communication protocol offloading (e.g. TLS, IPsec, MACsec, …) • Context separation / multi-application scenarios
OTHER			• Increased attack resistance (e.g. SCA, Fault Injection, …)
Covered by:	NXP CSE family (since 2010)		
	NXP HSM family (since 2015)		
	NXP HSE family (since 2019)		

SHE and Evita security specifications coverage in Commercial 0ff The Shelf products (Notes)

CSE (Crypto Security Engine), HSM (HW Security Module), HSE (Hardware Security Extension) are NXP commercial names for different types of HSM

Protocol offloading in new secure automotive MCUs thanks to HSM technology

Transport Layer Security (TLS), the successor of the now-deprecated Secure Sockets Layer (SSL), is a cryptographic protocol designed to provide communications security over a computer network. The protocol is widely used in applications such as email, instant messaging, and voice over IP, securing HTTPS remains the most publicly visible.

IEEE 802.1AE (MACsec) is a network security standard that operates at the medium access control layer and defines connectionless data confidentiality and integrity for media access independent protocols. MACsec frame format is similar to the Ethernet frame, but includes additional security fields (e.g. Security Tag, Message authentication code,…)

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

SHE and Evita security specifications coverage in Commercial 0ff The Shelf products (Notes)

Increase complexity and co-existence of many standards and both new and legacy applications (if a car model is in production for 10 years and the owner will use it up to 10 years the technology cycle is 20 years) may be a source of threats

Rollback attack, is a cryptographic attack (downgrade attack) on a computing system or communication protocol that makes it abandon a high-quality mode of operation (e.g. an encrypted connection) in favor of an older, lower-quality mode of operation (e.g. cleartext) that is provided for backward compatibility with older systems.

An example of such a flaw was found in OpenSSL (Open SW version of the Secure Sockets Layer) that allowed the attacker to negotiate the use of a lower version of **TLS (Transport Layer Security)** between the client and server.

Opportunistic encryption protocols such as STARTTLS are vulnerable to downgrade attacks, as they, by design, fall back to unencrypted communication. Websites which rely on redirects from unencrypted HTTP to encrypted HTTPS can also be vulnerable to downgrade attacks (e.g., sslstrip), as the initial redirect is not protected by encryption.

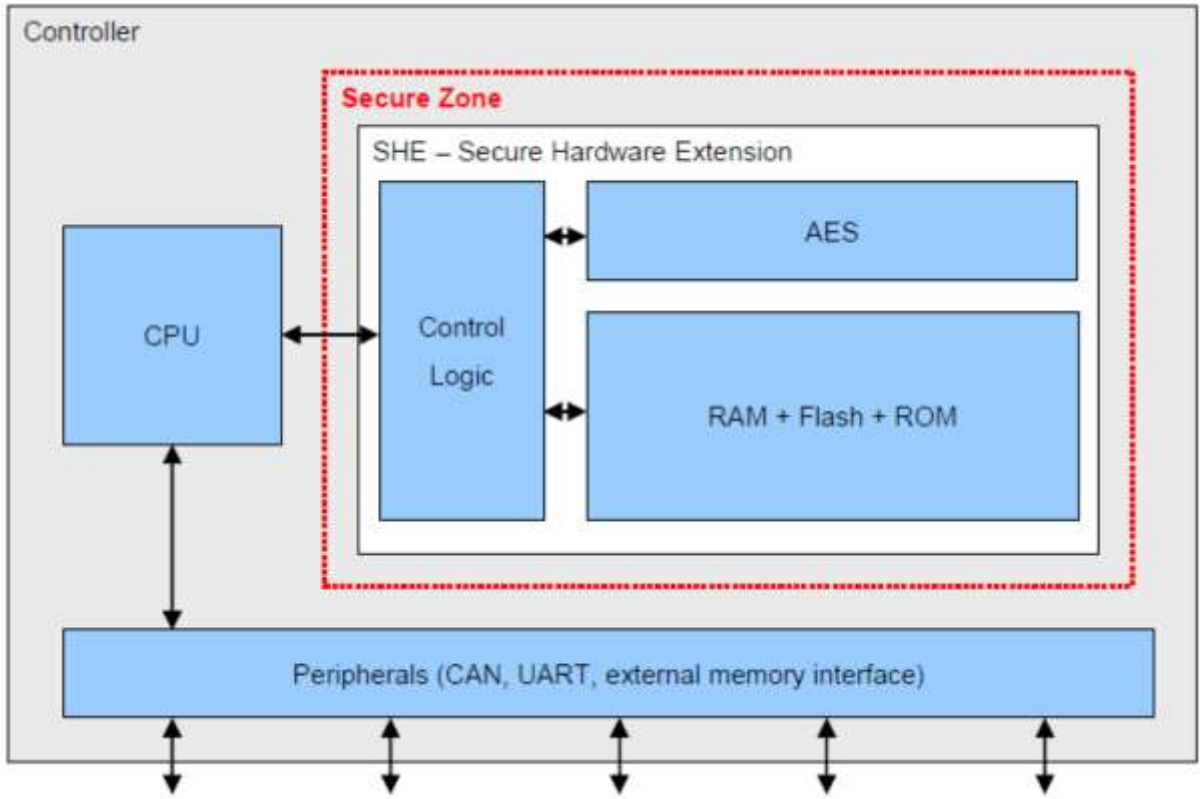
Secure Hardware Extension (SHE)

- The Secure Hardware Extension (SHE) is an on-chip extension to any given microcontroller.
- SHE is intended to move the control over cryptographic keys from the software domain into the hardware domain and therefore protect those keys from software attacks.
- SHE it is not meant to replace highly secure solutions like TPM chips (see later slide) or smart cards, i.e. no tamper resistance is required by the specification.

The main goals for the SHE design are:

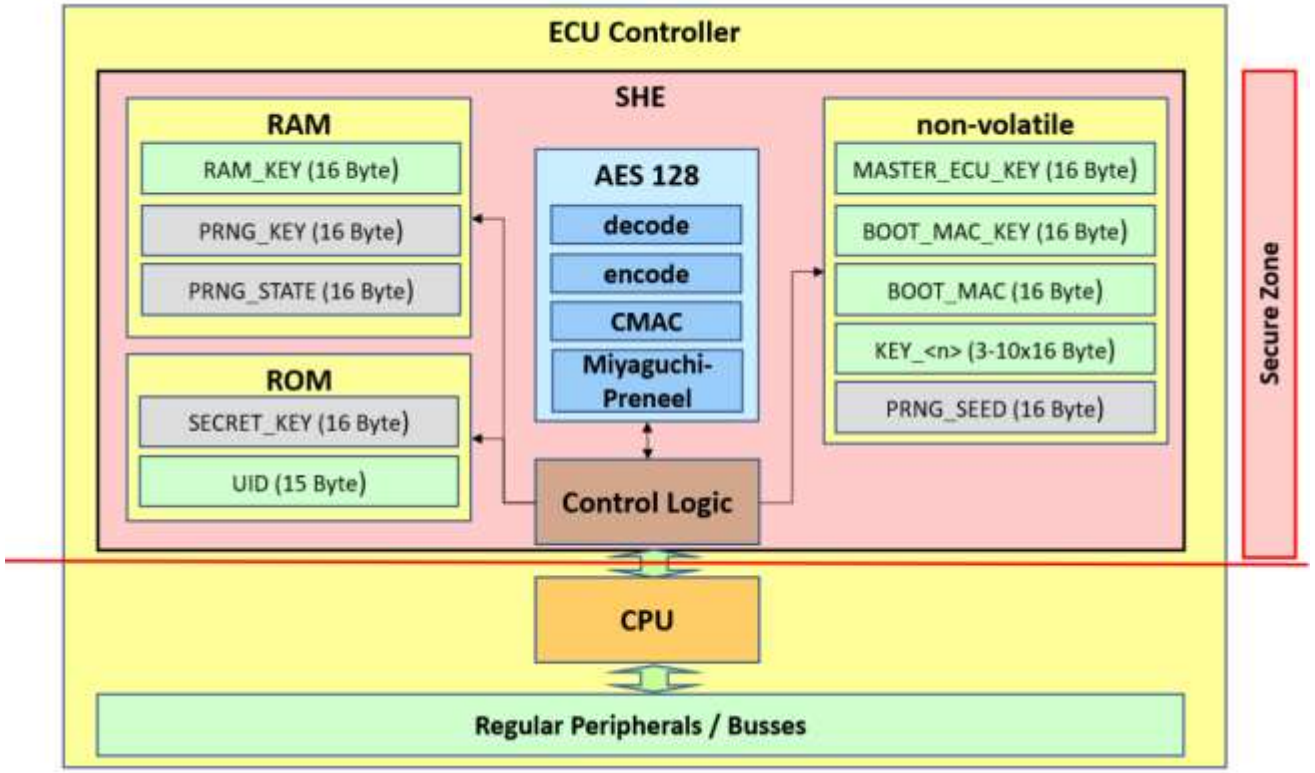
- Protect cryptographic keys from software attacks
- Provide an authentic software environment
- Let the security depend on the strength of the underlying algorithm and the confidentiality of the keys
- Keep the flexibility high and the costs low
- Basically SHE consists of three building blocks, a storage area to keep the cryptographic keys and additional corresponding information, a implementation of a block cipher (AES) and a control logic connecting the parts to the CPU of the microcontroller.
- SHE can be implemented in several ways, e.g. a finite state machine or a small dedicated CPU core.

Secure Hardware Extension (SHE)



SHE can be connected to the CPU in several ways, e.g. through a dedicated interface or an internal peripheral bus. The interconnection must be implemented in a way that no other peripheral or an external entity can modify the data transferred between the CPU and SHE.

Secure Hardware Extension (SHE)



Logic view of a SHE-compliant HSM in Autosar

Secure Hardware Extension (SHE)

All cryptographic operations of SHE are processed by an AES-128.
The latency of the AES must remain <2 us per encryption/decryption of a single block, including the key schedule

Minimum ECB and CBC modes of AES supported
CMAC supported for Message Authentication Code (verification/generation)

The performance of the AES must be high enough to allow for a secure boot of 5% of the flash memory, but 32kByte at minimum and 128kByte at maximum, of the microcontroller in <10ms.

SHE needs memory to store secure keys and MACs.
A non-volatile memory is required to store information that needs to be available after power cycles and resets of the microcontroller.
A volatile memory is required to store temporary information. The volatile memory may loose its contents on reset or power cycles. The memory of SHE should only be accessible by the SHE control logic.

At least 100 successful write-cycles to the non-volatile memory must be guaranteed per memory slot by the implementation, more write cycles must be possible

Key policy in the Secure Hardware Extension (SHE)

The **MASTER_ECU_KEY** is for the “owner" of the component using SHE and it can be used to reset SHE or change any of the other keys. The MASTER_ECU_KEY is only used for updating other memory slots inside of SHE

The **BOOT_MAC_KEY** is used by the secure booting mechanism to verify the authenticity of the software

The **BOOT_MAC** is used to store the MAC of the Bootloader of the secure booting mechanism and may only be accessible to the booting mechanism of SHE.

KEY_ n can be used for arbitrary functions. n is a number 3..10, i.e. SHE must at least implement three and at maximum ten keys for arbitrary use.

PRNG_SEED is used to store the seed for pseudo random number generator as described. in worst-case scenarios it is written on every power cycle/reset.

The **RAM_KEY** can be used for arbitrary operations. The PRNG_KEY and PRNG_state are used by the pseudo random number generator

R0M slots may be writable during production but not after leaving the fabrication.

Key policy in Secure Hardware Extension (SHE)

R0M slots may be writable during production but not after leaving the fabrication.

SHE must contain a unique secret key SECRET_KEY that shall not only be derived from the serial number or any other publicly available information.

The SECRET_KEY has to be inserted during chip fabrication by the semiconductor manufacturer and should not be stored outside of SHE. It can be generated by a certified physical random number generator, e.g. a Hardware Security Module (HSM).
The SECRET_KEY may only be used to import/export keys.

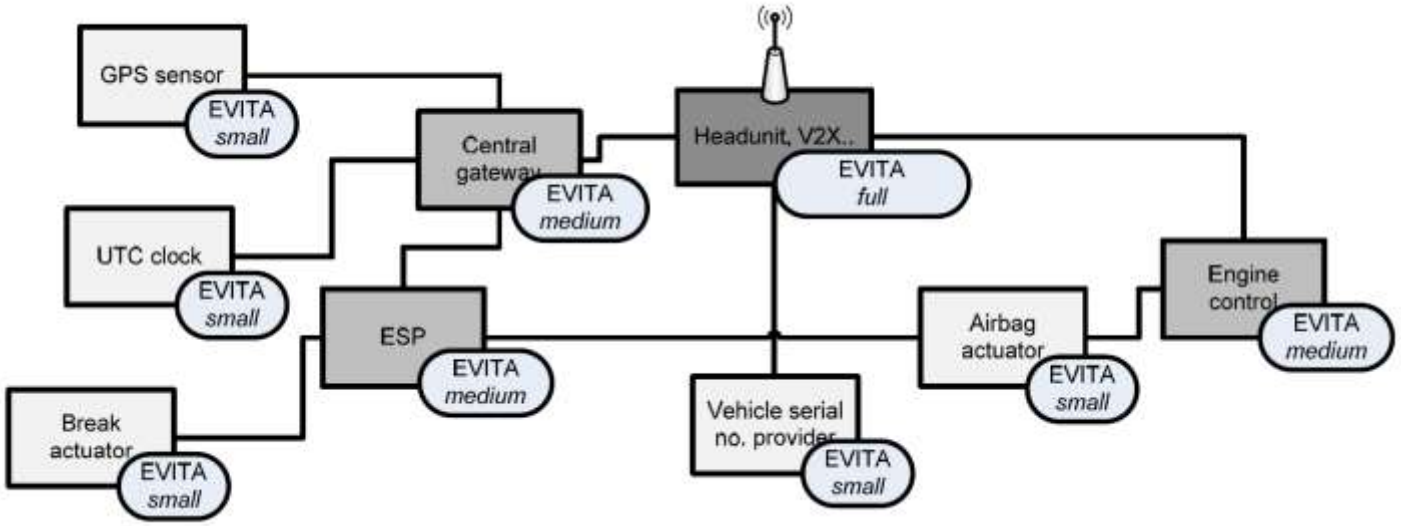
The UID is specified to 120 bit because it is always used in conjunction with two key ids or the status register to form a 128 bit block.
If the identification item is smaller than 120 bits it has to be padded with zero bits on the MSB side before feeding it into SHE.
The UID has to be inserted during chip fabrication by the semiconductor manufacturer

EVITA

Depending on the application minimal or full features can be deployed

(or disabled in the full version to save power)

→example to automotive from EVITA (E-safety Vehicle Intrusion proTected Applications) involving industrial partners like Infineon, Bosch, Continental, BMW, Escrypt, Fujitsu,… https://www.evita-project.org/

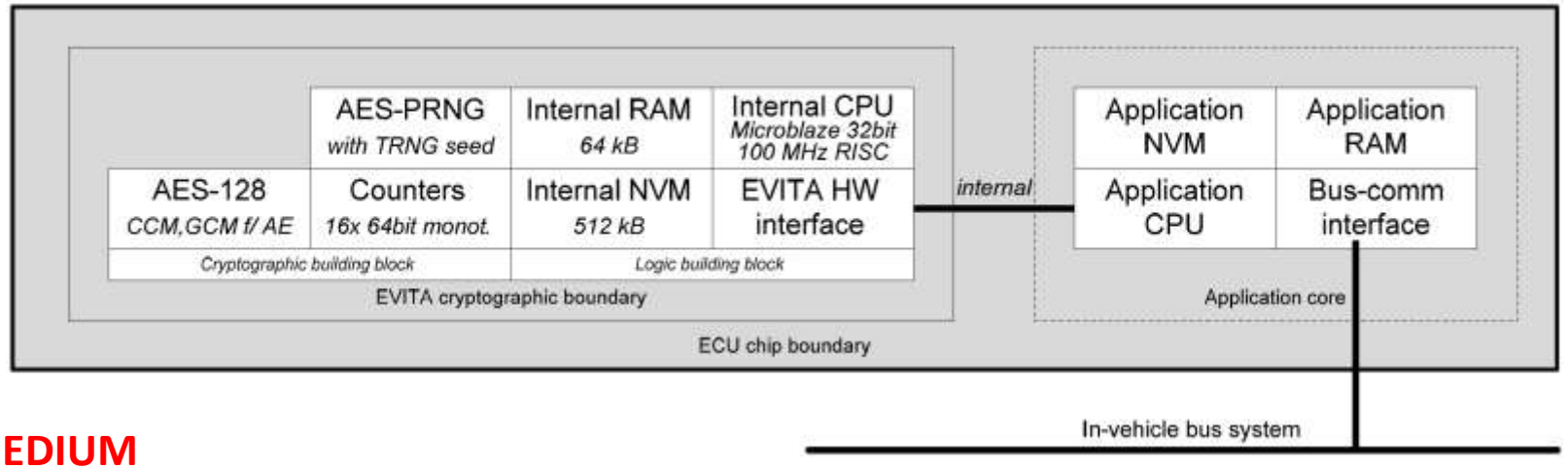


the "EVITA HSM Full Version" as hardware extension to the ECU specifically responsible for V2X applications,

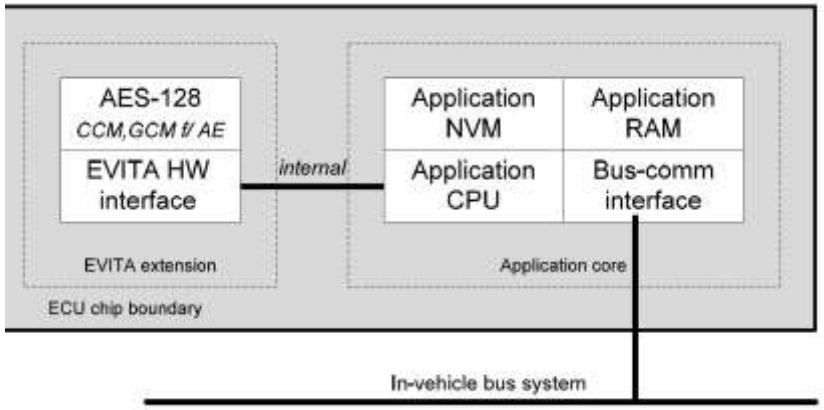
the "EVITA HSM Medium Version" as hardware extension to the ECU connected to the in-vehicle domain controls (e.g., power train control) and,

the "EVITA HSM Light Version" for security-critical sensors and actuators.

EVITA Medium & Small



EVITA MEDIUM

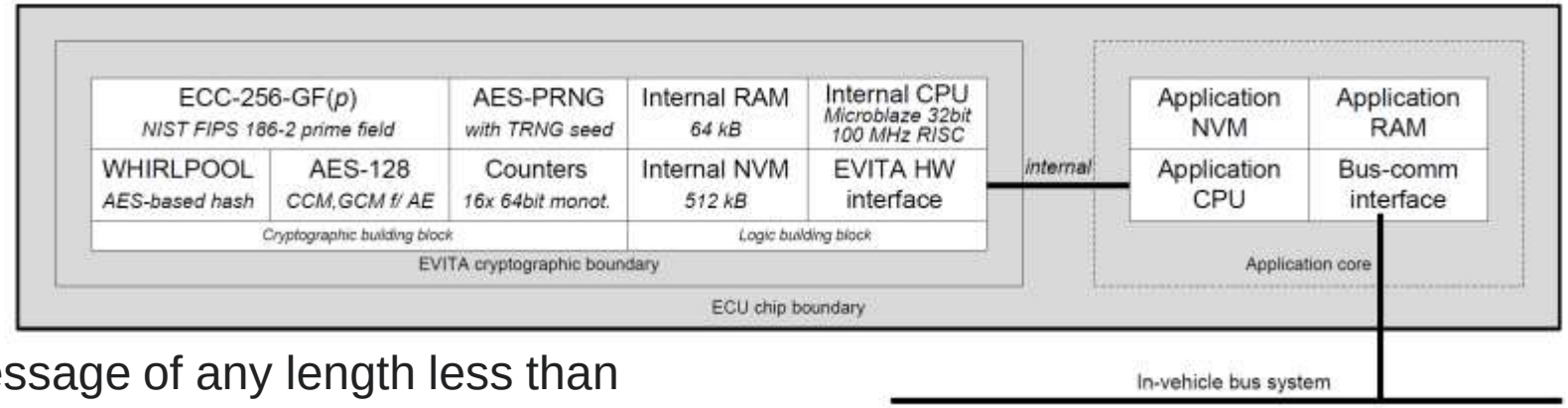


EVITA SMALL

(AES like in SHE but with modes ensuring confidentiality, authentication and integrity check)

EVITA Full

EVITA FULL



Whirlpool takes a message of any length less than 2^{256} bits and returns a 512-bit message digest

Building block	FPGA size (slices) estimation	Performance estimation
ECC-256-GF(p)	2,000	200 sig/s
WHIRLPOOL	3,000	1 Gbit/s
AES-128	1,000	1 Gbit/s
PRNG	200*)	1 Gbit/s
COUNTER	100	16x 64bit
CPU	2,000	32bit-RISC, 100MHz, 100 DMIPS
RAM	N/A (use block RAM)	64 kB
NVM	N/A (external)	512 kB
CONTROL / IF	1,000 – 2,000	N/A
Total	~ 10,000	

EVITA FULL COMPLEXITY

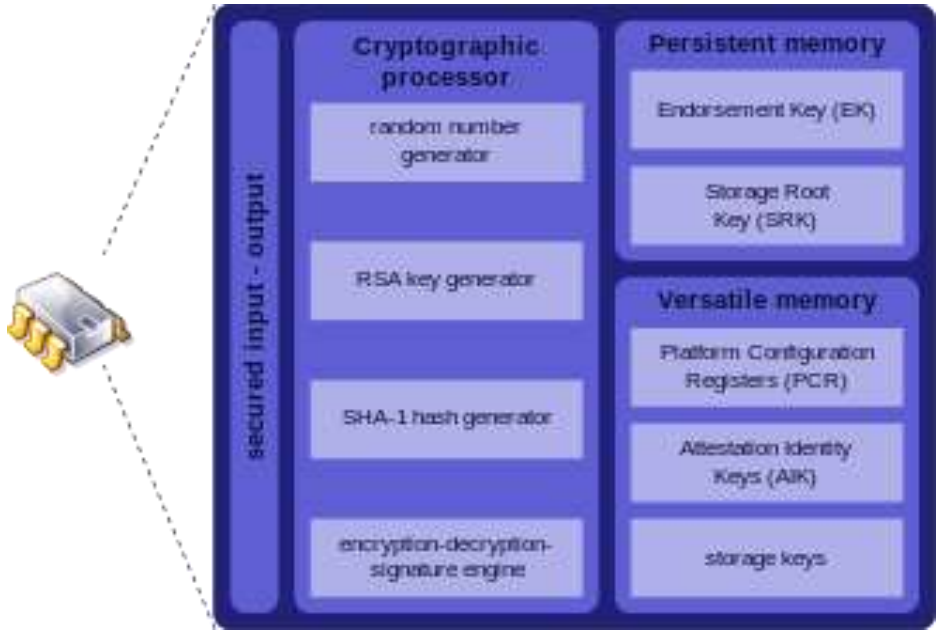
Trusted Platform Module (TPM)

Set of basic HSM foreseen in **Trusted Platform Module** (TPM)

Published as ISO/IEC 11889 Parts 1-4

TPM supports secure keys for **authentication** and **encryption functions**

TPM implemented as an external peripheral with a communication bus to another microcontroller in the system (**Co-processor**)



Trusted Platform Module (TPM)

TPM1.2

Specifies non-volatile memory, secret key storage, a random number generator (RNG)

RSA (RSA-2048 key): RSA is the Rivest, Shamir, Adleman algorithm for public key cryptography

SHA-1 (Secure Hash Algorithm) version1 is the basic for hashing (160 bit output tag) now considered breakbale in cryptoanalysis

HMAC (keyed-hash message authentication code)

Vernam (based on polyalphabetic Vigenère substitution cipher) one-time pad algorithm is a basic for encryption

In TPM1.2 use of AES (Advanced Encryption Standard) for symmetric cryptography is optional

Trusted Platform Module (TPM)

TPM1.2 used in personal computers, e.g. INTEL TEE (Trusted Execution Technology) chips and in Windows (server2016, server2019, Windows 10), and in industry 4.0/vehicles

https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/trusted-execution-technology-security-paper.pdf

https://www.infineon.com/dgdl/Infineon-data-sheet-SLB9670_1.2_Rev1.3-DS-v01_03-EN.pdf?fileId=5546d462689a790c016929e445ea4ff7

Versione TPM	Windows11	Windows10	Windows Server 2016	Windows Server2019
TPM 1.2		>= ver 1607	>= ver 1607	Sì
TPM 2.0	Sì	Sì	Sì	Sì

TPM2.0

Advanced secure features: it specifies also SHA-256 for hash, 128-b AES symmetric, ECC (Elliptic Curve Cryptography) using the Barreto-Naehrig 256-bit curve and NIST P-256 curve for public-key cryptography and asymmetric digital signature generation and verification

https://www.st.com/en/secure-mcus/st33gtpmai2c.html

TPM2.0 example ST33GTPMAI2C

AEC-Q100 "Failure Mechanism Based Stress Test Qualification For Integrated Circuits“ qualified (http://www.aecouncil.com/)

Compliant with Trusted Computing Group (TCG) Trusted Platform Module (TPM) Library speci. 2.0, Level 0, Revision 138

Fault-tolerant firmware loader that keeps the TPM fully functional when the loading process is interrupted (self-recovery)

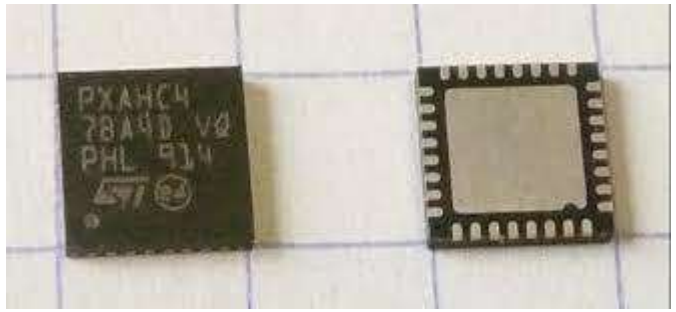
Arm® SecurCore® SC300™ 32-bit RISC (Reduced Instruction Set Computer) core

Automotive grade 2: −40 °C to 105 °C, ESD (Electro Static Discharge protection) up to 4 kV (Human Body Model), 1.8 V, 3.3 V or 5 V supply voltage range

Hardware and software protection against fault injection

FIPS compliant RNG built on SP800-90A compliant SHA256 DRBG (Deterministic Random Bit Generator) and an AIS-31 Class PTG2 compliant true random number generator (TRNG)

RSA key generation (1024, 2048 bits), RSA signature, RSA encryption



SHA-1, SHA-2 (256 and 384 bits), SHA-3 (256 and 384 bits)

HMAC SHA-1, SHA-2 and SHA-3

AES-128, 192 and 256 bits

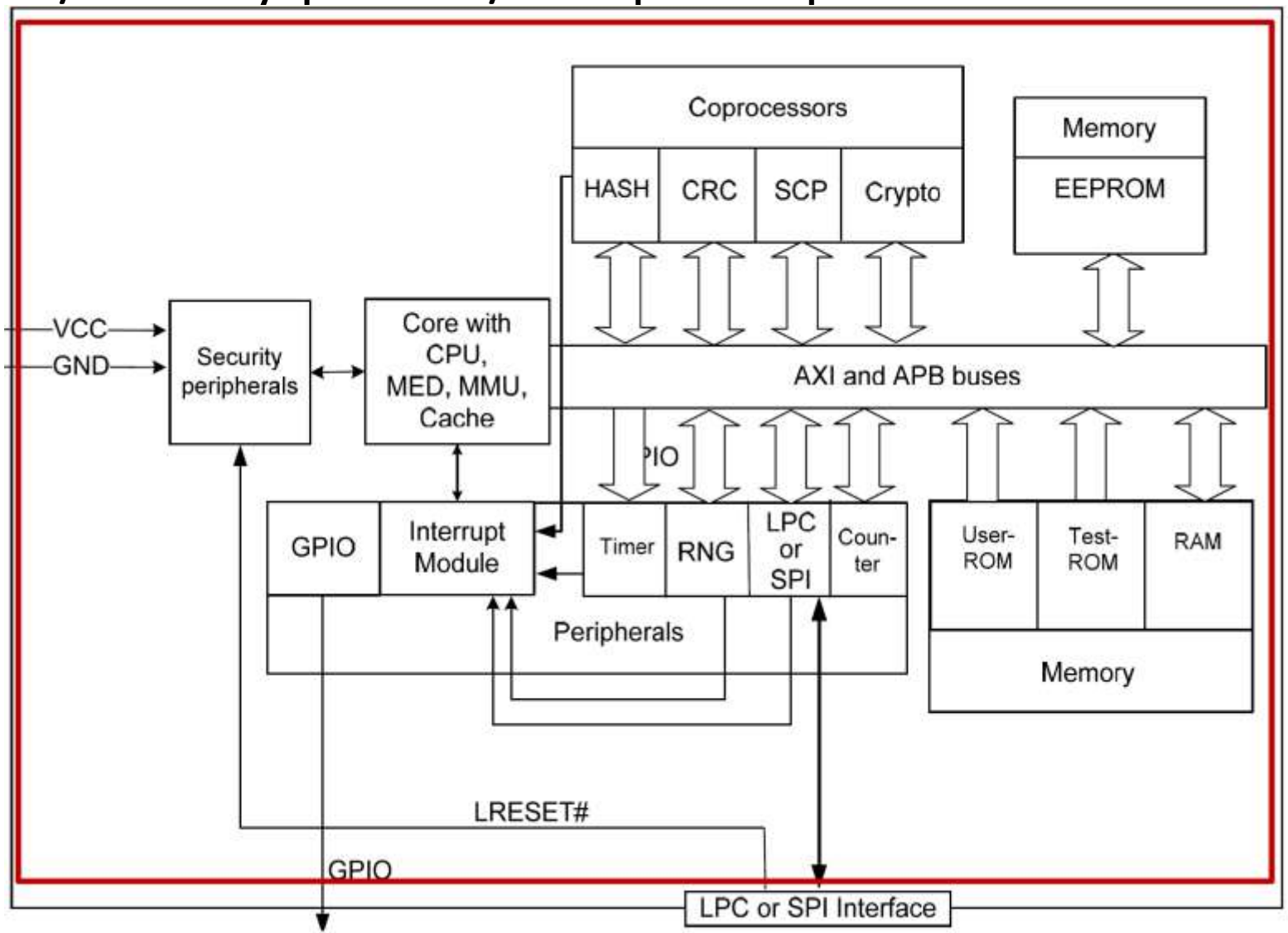
Triple DES (Data Encryption Algorithm) 192 bits

ECC (NIST P-256/384): Key generation, ECDH (Elliptic-curve Diffie–Hellman), ECDSA (Elliptic-curve Digital Signature Algorithm)

Device provided with 3 EK (Endorsement Key. This is an asymmetric key contained inside the TPM and injected at manufacturing time). The EK identifies the TPM. The EK cannot be changed or removed) and 3 EK certificates (RSA2048, ECC NIST P_256 and ECC NIST P 384): A TPM manufacturer-issued certificate for EKPub.

TPM2.0 example SLB 9660/9665/9670

- https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2959.pdf



TPM2.0 example SLB 9660/9665/9670

MMU (memory management with privilege levels)
MED (Memory Encrypt/Decrypt)
SCP (symmetric co-processor) for AES hardware acceleration
Asymmetric Crypto Co-processor (labeled Crypto) for modular math (e.g. RSA 2048-bit, ECC) acceleration
The checksum module (labeled CRC) allows simple calculation of 16-bit CRC checksums for Error Detection And Correction

Role ID	Role Description
CO	Cryptographic Officer, also known as the TPM Administrator or Admin Role. Controls certification of objects and changes Authentication Data of objects.
User	User, also known as the object owner. Uses the TPM to create cryptographic objects and to obtain cryptographic services for cryptographic objects.
DUP	Duplication Officer. Uses the TPM to duplicate TPM objects.

TPM Identification and Authentication Methods

Password Verification: Operators in the CO or User roles are authenticated by a demonstration of knowledge of a Password as authentication data.

When using the password verification mechanism, a password consisting of at least 12 alphanumeric characters shall be used. Assuming as a worst case that the operator uses 12 decimal digits only, but still randomly chosen, the probability that a single random authentication attempt (by guessing the password value) will succeed is 10^{-12}.

A very conservative estimate of the maximum authentication rate is 10^6/minute (60 μs per attempt). Under this assumption the probability that random authentication attempts will succeed within a oneminute interval is $10^6 * 10^{-12} = 10^{-6}$

HMAC Challenge-Response Authentication

This Challenge-Response Authentication is described as HMAC Authorization Session within TCG Specifications. Operators in the CO or User roles are authenticated by a challenge and response demonstration of knowledge of a shared secret. The shared secrets are HMAC-SHA1 and HMAC-SHA256 cryptographic keys. The TPM HMAC authorization session mechanism includes nonce values (pseudo random values used once) to prevent replay attacks.

As a worst case it is assumed that for challenge-response authentication HMAC-SHA1 is used, which has smaller key length and smaller tag length (160 bit each) than HMAC-SHA256. Under this assumption the probability that a random authentication attempt (by guessing key value or tag value) will succeed is: $2^{-160} = 6.8 * 10^{-49}$
With the same assumed maximum authentication rate of 106/minute as above, the probability that random authentication attempts will succeed within a one-minute interval is $6.8 * 10^6 * 10^{-49} = 6.8 * 10^{-43}$

TPM Identification and Authentication Methods

Enhanced Authorization for Authentication

Operators in the CO or User roles can be authenticated via a policy digest, which requires as action the use of an authentication mechanism. Password Verification or HMAC Challenge-Response Authentication as described above, or Challenge-Response Authentication based on a Public Key Digital Signature Algorithm (RSA 2048-bit or ECDSA 256-bit) can be used as authentication mechanism. The TPM policy authorization session mechanism includes nonce values to prevent replay attacks.

For challenge-response authentication using a Public Key Digital Signature Algorithm as required authentication mechanism it is assumed as worst case that RSA 2048-bit is used, which provides 112-bit security strength (ECDSA 256-bit provides 128-bit security strength). Therefore the probability that a random authentication attempt will succeed using this authentication mechanism is:

$2^{-112} = 1.9\times10^{-34}$

With the same assumed maximum authentication rate of 10^6/minute as above, the probability that random authentication attempts will succeed within a one-minute interval is:

$10^6 \times 1.9\times10^{-34} = 1.9\times10^{-28}$

Outline

Introduction on security specifications

- Analysis of HW secure specifications and de-facto standards:

SHE (Secure HW extension),

EVITA (E-safety vehicle intrusion protected applications)

TPM (Trusted Platform Module)

- System-level Directives and Standards:

Brief on Automotive standards UN155/UN156

NIS2 directive

IEC 62443

What's Next: UN R155 and IS0/IEC 21434

- From July 2022 onward, vehicle manufacturers must comply with the **R155 automotive cybersecurity** regulation (respect of security best practices to have a "secure by design" vehicle) for new vehicle type launches in Europe, Japan and Korea.
- UN R155 covers aspects from the design to the production to the operation to the maintenance and assistance to the decomissioning of vehicles.
- UNR155 secure by design is linked to process-related aspects (Cyber Security Management System or CSMS) and product-related aspects
- The standard **ISO/SAE 21434** (cybersecurity engineering for road vehicles) released in 2021 is deemed very supportive in implementing the requirements on the Cyber Security Management System (CSMS), as specified in UN R155, in organizations along the supply chain.
- ISO/SAE 21434 complete on the secure side what IS0 26262 does on the functional safety side.
- ISO/SAE 21434 covers security aspects from the design to the decomissioning of components.
- The relation between customers and technology (Tier-1 vs Tier2, 0EM vs Tier-1) providers is covered in ISO/SAE 21434

What's Next: UN R155 and ISO/IEC 21434

- ISO/SAE 21434 like the ISO/IEC 18045:2008 includes the definition of rating of fesibility of an attack and the potentiality of attack
- ISO/SAE 21434 like SAE J3061l includes the continuum process for cyber security management and the support of a cybersecuity culture
- ISO/SAE 21434 like ISO 26262 define rules for sharing information collected from vehicles and the need for an assessment of the quality of the protection processes used.
- ISO/SAE 21434 and UN R155 do not provide technologies, methods or solutions to be implemented to obtain safe components and compliance with the standard.
- This situation wants to keep the standards at a generic level and leave the manufacturer free to adopt the best solutions for each system. On the other hand, this lack of defined technologies and methods can create situations in which each company uses its own proprietary solution, creating possible conflicts in a highly connected environment.
- For example, the lack of defined limits for risk analyzes can allow having similar components from different manufacturers with different levels of cyber security, without however the customer having perception, because both are ISO / SAE 21434 and UNR155 compliant.

What's Next: NIS (Network& Information Security) 2

Important to define the categories of org. to be compliant with NIS 2.
If an activity is critical, it should not only be safe, also cybersecure. ④

Strategia comune di cybersecurity per tutti gli Stati EU

Si integra con altre normative (GDPR, DORA, Cyber Resilience Act)

Nuove categorie di operatori, basate sulla criticità del servizio

Numero maggiore di settori e servizi critici (*piattaforme di cloud computing, data center e servizi sanitari e logistica e industria 4.0 e energia e trasporti e banche e acque..*)

Requisiti per identificare, prevenire e rispondere alle minacce

Segnalazione tempestiva di incidenti significativi alle autorità competenti

④ Good to reach that CS relates to the entire org. across all sectors, not just IT.

What's Next: NIS (Network& Information Security) 2

European Directive NIS 2, defined in October 2023, imposes to the EU membering states to adopt within October 2024 laws about cybersecurity with at least should ensure:

- (a) policies on risk analysis and information system security;
- (b) incident handling;
- (c) business continuity, such as backup management and disaster recovery, and crisis management;
- (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

What's Next: NIS (Network& Information Security) 2

- (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures; penetration tests for instance (in case of critical systems, in which pen-test on critical tests can cause damage (DOS) you work on a digital twin)
- (g) basic cyber practices and cybersecurity training;
- (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- (i) human resources security, access control policies and asset management;
- (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

What’s Next: NIS (Network& Information Security) 2

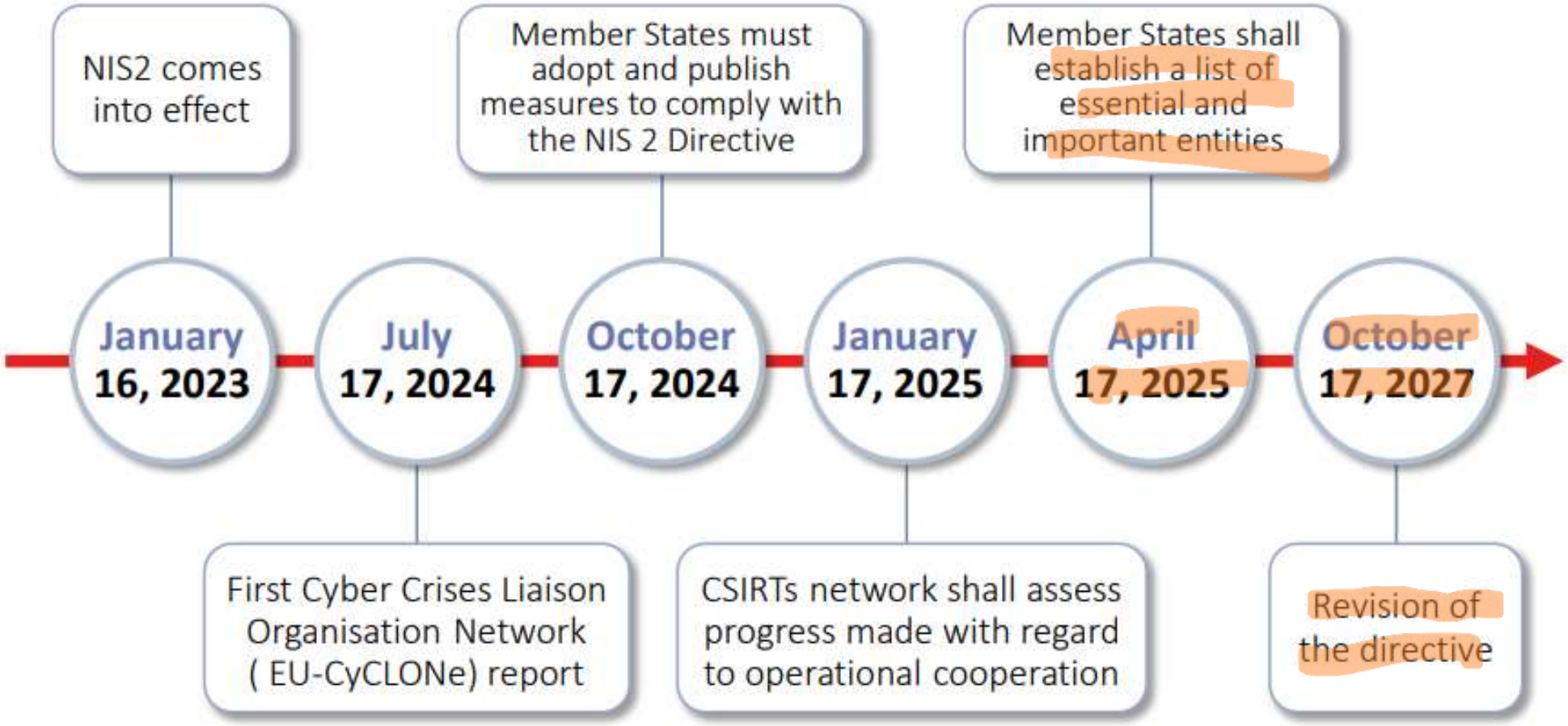
NIS2 applies to:

- OES <operatore di servizi essenziali> such as water, energy, digital infrastructures; banking; Health; transports

- FSD <fornitore di servizi digitali> such as web browsing engines, Cloud computing, e-commerce…..

What’s Next: NIS (Network& Information Security) 2

Computer Security Incident Response Team https://www.csirt.gov.it/



What's Next: NIS (Network& Information Security) 2

included in Italian law by 17/10/2024

17 Ottobre 2024

- Termine entro il quale la NIS2 dovrà essere recepita dalla normativa nazionale

Marzo 2025

- ACN (Agenzia Cybersecurity Nazionale) definirà l'elenco dei soggetti che rientrano nella direttiva NIS2

Dicembre 2026

- Termine per implementare le misure di sicurezza previste da parte dei soggetti interessati

IEC 62443 →

NIS gives you general requirements, but not how to implement them. Defined in multiple parts, detailed procedures to ensure requirements are met. This standard is middle level kind of. IEC 62443 is not directly related to NIS 2, but more or less if you follow it you are compliant.

General	Terminology, concepts, and models 62443-1-1	Terminology, concepts, and models 62443-1-2	Terminology, concepts, and models 62443-1-3	Terminology, concepts, and models 62443-1-4	
Policies & Procedures	Security program requirements for IACS asset owners 62443-2-1	IACS security program ratings 62443-2-2	IACS Patch management 62443-2-3 (how to handle patches)	Security program requirements for IACS service providers 62443-2-4 (related to supply chain)	Implementation guidance for IACS asset owners 62443-2-5
System	Technologies for IACS 62443-3-1	Risk assessments for system design 62443-3-2	System security requirements and security levels 62443-3-3		
Component	Product security development lifecycle requirements 62443-4-1	Technical security requirements for IACS components 62443-4-2	Application to Industrial Internet of Things (IIoT) 62443-4-3 (DRAFT)		

WHAT'S IMPORTANT:

1. It is divided into multiple chapters, so you can be compliant only partially too (MODULARITY)
   1.1. General defines concepts, terminology etc.
   1.2. There are paragraphs defining policies and procedures: how to write risk analyses for info, automation control systems (IACS), how to write requirements for asset owners of IACS (who is the asset owner? Already concept of one company (Autoschade) relying on external company for provision of systems (the one giving IACS)).
   Of course you can find standards that are industry specific (ex for vehicles).
   You also have one paragraph for IACS security program ratings, all the aspects related to patch management (you have procedures to create update securely), how to define security program requirements for IACS service providers this time (more related to supply chain) and info for implementation guidance.
   1.3. Systems: how to define system security requirements and security levels, risk assessments for the design
   1.4. Components: all component level product security development lifecycle requirements and technical security requirements for IACS components; in a new draft there is interest in Industrial IoT.

> IEC 62443 is an international series of standards focused on cybersecurity for industrial automation and control systems (IACS). It's basically the go-to framework for making sure critical industrial systems—like those in factories, power plants, water treatment facilities, and even smart buildings—are protected against cyber threats.
>
> The standard was developed by the **International Electrotechnical Commission (IEC)**, and it's designed to be used by everyone involved in the lifecycle of these systems: asset owners, system integrators, and product suppliers.

ISO 21434 was developed having in mind vehicles, IEC 62443 was developed having in mind industrial plants. Anyway those are the go-to for implementation of NIS / high level standards. Then of course you have low level standards.

- **Asset Owners** are the organizations or individuals who **own and operate** the industrial automation and control systems. They're the ones whose operations depend on these systems—like a power plant operator, a factory manager, or a water utility. They're responsible for the **security of the environment** where the system runs and often make the final decisions on risk acceptance and system configuration.
- **Service Providers**, on the other hand, are third parties (or internal teams, sometimes) who **design, install, maintain, or manage** parts of the IACS. Think of them as system integrators, vendors, or managed service companies. Their job is to deliver services **in line with the security policies** set by the asset owner, and to ensure their own operations don't introduce vulnerabilities.

In short: **asset owners define the rules** and own the risks, while **service providers follow those rules** and are expected to bring their own best practices to support secure operations.

- Asset owner = industrial plant
- Service provider = supply chain

Ah, **IEC 62443-3-1**—now you're stepping into the territory of **security technologies for IACS**. This part is kind of like a bridge between high-level policies and the practical, technical stuff. It gives **guidance on applying existing IT security technologies** to industrial settings, which, as you probably guessed, isn't always straightforward.

Here's what makes 3-1 interesting:

It doesn't introduce new security tech, but rather **analyzes how traditional IT security controls**—like firewalls, VPNs, intrusion detection, anti-malware, etc.—**fit into industrial automation systems**, which often have unique constraints like:

- real-time performance requirements,
- long life cycles (systems may run for 20+ years),
- limited processing power in field devices,

So while 3-1 talks about applying existing tech, **4-1 is all about the development lifecycle**. It says: if you're a **product supplier**, here's how to build your stuff so it's not a cybersecurity disaster waiting to happen.

It covers the **Secure Development Lifecycle (SDL)**—which is basically the cybersecurity equivalent of brushing your teeth regularly instead of going to the dentist once every few years. It includes:

- Defining security requirements from the beginning
- Designing with security in mind (think threat modeling, secure architecture)
- Secure coding practices
- Rigorous testing (static, dynamic, fuzzing, etc.)
- Managing vulnerabilities (disclosure policies, patching)
- Ongoing maintenance and updates

(ONLY FOR PRODUCT SUPPLIERS)

↳ With respect to product development

IEC 62443 – Maturity Level

like little care but no strong development

Maturity Level	Description
Maturity Level 1	Initial: Product suppliers usually carry out product development ad hoc and often undocumented (or not fully documented). (customised)
Maturity Level 2	Managed: The product supplier is able to manage the development of a product according to written guidelines. To be demonstrated that the personnel who carry out the process have the appropriate expertise, are trained and/or follow written procedures. [Training is something new!] The processes are repeatable.* Guidelines can be used by multiple people [Can apply multiple times]
Maturity Level 3	Defined (practiced): The process is repeatable throughout the supplier's organization. Maybe the procedures are the same, but there is repeatability for entire org. and practice The processes have been practiced and there is evidence that this has been done.
Maturity Level 4	Improving: Procedure has been digested and there's continuous improvement. Product suppliers use appropriate process metrics to monitor the effectiveness and performance of the process and demonstrate continuous improvement in these areas.

- Defines Maturity Levels. Why? You are a company asked to be CS compliant. In the market this requires time. So idea is going up the maturity levels and you can be compliant with different maturity levels.

For most companies, problem is moving from L0, L1 to L2. Big jump also from L2 to L3.

- 1 to 2 is a change of mindset, that is difficult to do alone.

Good one, Giovanni. When IEC 62443 talks about **Maturity Level 2 (ML2)** and says "**the processes are repeatable,**" it means the organization isn't just doing security stuff once in a while or when someone remembers—they've reached a point where **security-related tasks are done consistently** across projects and people.

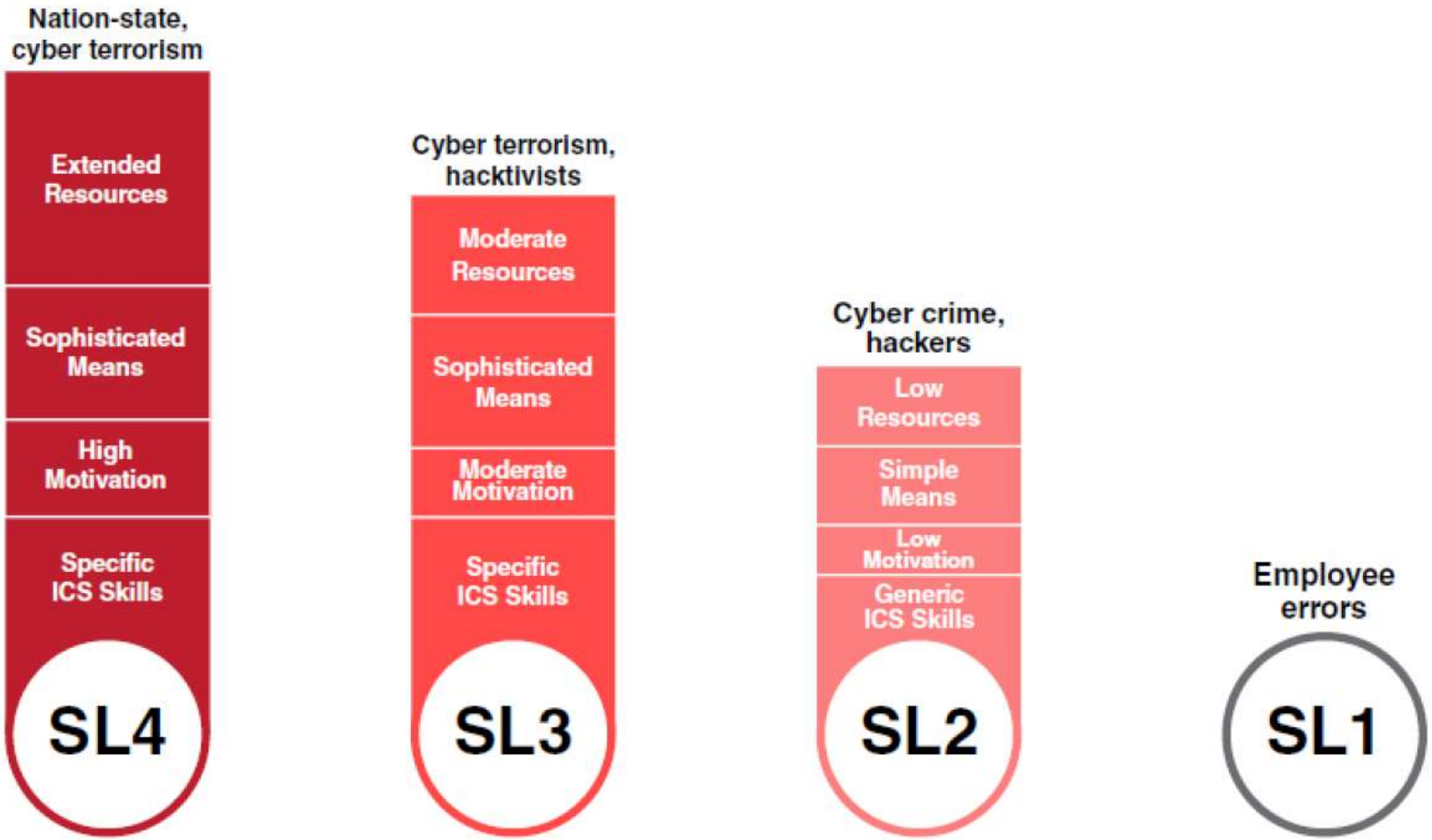
So, "repeatable" here means:

- There are **defined processes** (like how you test for vulnerabilities or review code)
- People actually **follow those processes**, not just wing it
- The processes can be **repeated with similar results** across different projects or products

So, **Maturity Level 2** says:
"**The process is repeatable.**"
That means *individual teams or projects* have developed consistent ways of doing things. You might have one development team that always runs a security test before release, but another team might not—or maybe they do it differently.

Now, **Maturity Level 3** kicks it up a notch:
"**The process is repeatable throughout the supplier's organization.**"
Here, **the whole organization** has adopted those practices—not just pockets of good behavior. The processes are no longer informal habits of a few teams; they're **standardized, documented, and expected everywhere** across the company. Everyone is on the same page, following the same secure development and operational practices.

IEC 62443 – Security Levels



Security level vs: you can be compliant with different levels of security depending on the profile of attacker. SL vs not how practical you are, but an interpretation of the security level. It takes into account skills, motivations, resources and target of the attacker. (Also means!)
This has effects on the level of authentication, anti tampering etc: it helps you understand the trade-off you pay for security.

IEC 62443 – Security Levels

Secure Level	Definition	Means	Resource	Skills	Motivation
SL-0	No special requirement or protection required	—	—	—	—
SL-1	Protection against unintentional or accidental misuse	Simple	Low	Generic	Low
SL-2	Protection against intentional misuse by simple means with few resources, general skills and low motivation				
SL-3	Protection against intentional misuse by sophisticated means with moderate resources, IACS-specific knowledge, and moderate motivation	Sophisticated	Medium	ICS specific	Moderate
SL-4	Protection against intentional misuse using sophisticated means with extensive resources, IACS-specific knowledge, and high motivation	Sophisticated	Extended	ICS specific	High

Biometric systems would make sense from level 2 or more. Level 2 is not that expensive, but L3, L4 becomes more expensive. Plus, for supply chain at L2 you do not consider extraordinary attacks at supply chain too.

- SL3 is skill not absent nation-s or complex resourcer groups, but they are motivated groups.
- SL4 can be nation states, political motivation, lots of money, maximum expertise etc.

So ML and SL creates a combination so that a desired level can be achieved.

You have a matrix of flexibility so you can adapt to what you really need.

The security level can also be associated to products used, and also linked with what happens with combining policies with use of products (device offers L1, but if you guarantee A, B, C... you can reach lvl 2-3 etc.)

IEC 62443 – Security Levels

1.SL0: Non sono necessari requisiti specifici o protezione di sicurezza;
2.SL1: Protezione contro violazioni casuali; (employee errors,..)
3.SL2: Protezione contro la violazione intenzionale utilizzando mezzi semplici con basso livello di esperienza delle risorse coinvolte, competenze generiche e scarsa motivazione; (hackers, bad employee,…)
4.SL3: Protezione contro la violazione intenzionale utilizzando mezzi sofisticati con risorse moderate, competenze specifiche su Industrial Control Systems e motivazione moderata; (hacktivist, cyber terrorism,..)
5.SL4: Protezione contro la violazione intenzionale utilizzando mezzi sofisticati con risorse estese, competenze specifiche su Industrial Control Systems ed elevata motivazione (nations, states, cyber terrorism,..)

One example of how we adapt a solution to the SL as given for authentication:

IEC 62443 – Authetication specs vs. Security Levels

How do we change authn in terms of security levels?

1. **SL1:** ho solo il requisito che impone l'obbligo di identificare e autenticare tutti gli utenti; Only identify and authenticate: maybe pin is enough, nothing that difficult [not in unique way]
2. **SL2:** al requisito precedentesi deve aggiungere l'obbligo di identificare e autenticare tutti gli utenti "in modo univoco"; [Procedure should avoid possibility of cloning]
3. **SL3:** al requisito precedente si deve aggiungere l'obbligo di identificare e autenticare tutti gli utenti utilizzando una Multi Factor Authentication (MFA) sulle reti considerate non-fidate (untrusted);
4. **SL4:** al requisito precedente aggiungo l'obbligo di identificare e autenticare tutti gli utenti utilizzando una Multi Factor Authentication (MFA) su tutte le reti.

But in practice—and especially in industrial settings covered by IEC 62443—**authentication doesn't always guarantee uniqueness**. Here's why:

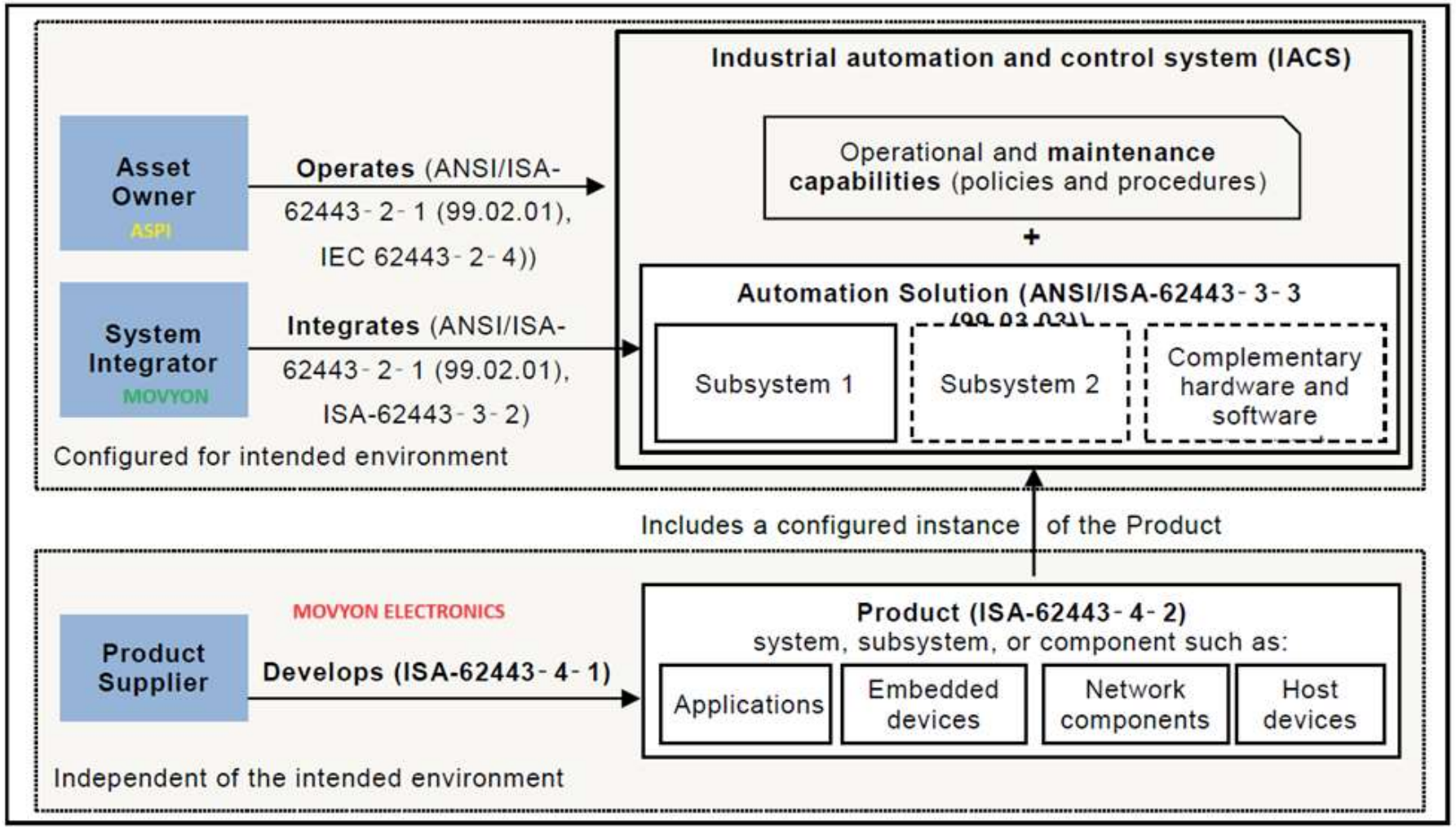
At **Security Level 1**, authentication might be implemented using **shared credentials**. For example:

- Everyone uses the same **"operator"** account,
- Or all maintenance staff log in as **"maintenance"** with the same password.

That's technically authentication, because the system checks credentials—but it's **not unique**. You can't tell which *person* logged in, just which *role* or generic account.

SL2, by requiring **"in modo univoco"**, explicitly rules that out. It says: "You must be able to distinguish between users. No more anonymous or shared access."

IEC 62443 – Industry roles



Description also of Industry roles: you have an asset owner (Autostrade), a system integrator selling the whole system (Telepass). The system integrator has its own network of product suppliers for each of the subsystems (ex: camera for Telepass).
For each of the roles, we have chapters applying to them.
Product suppliers often don't see the entire picture: they are not responsible for system requirements. They look at embedded devices, Apps, Network components, host devices.
A system integrator should consider which SC we are targeting (and ML). They should also take care of maintenance of the system.

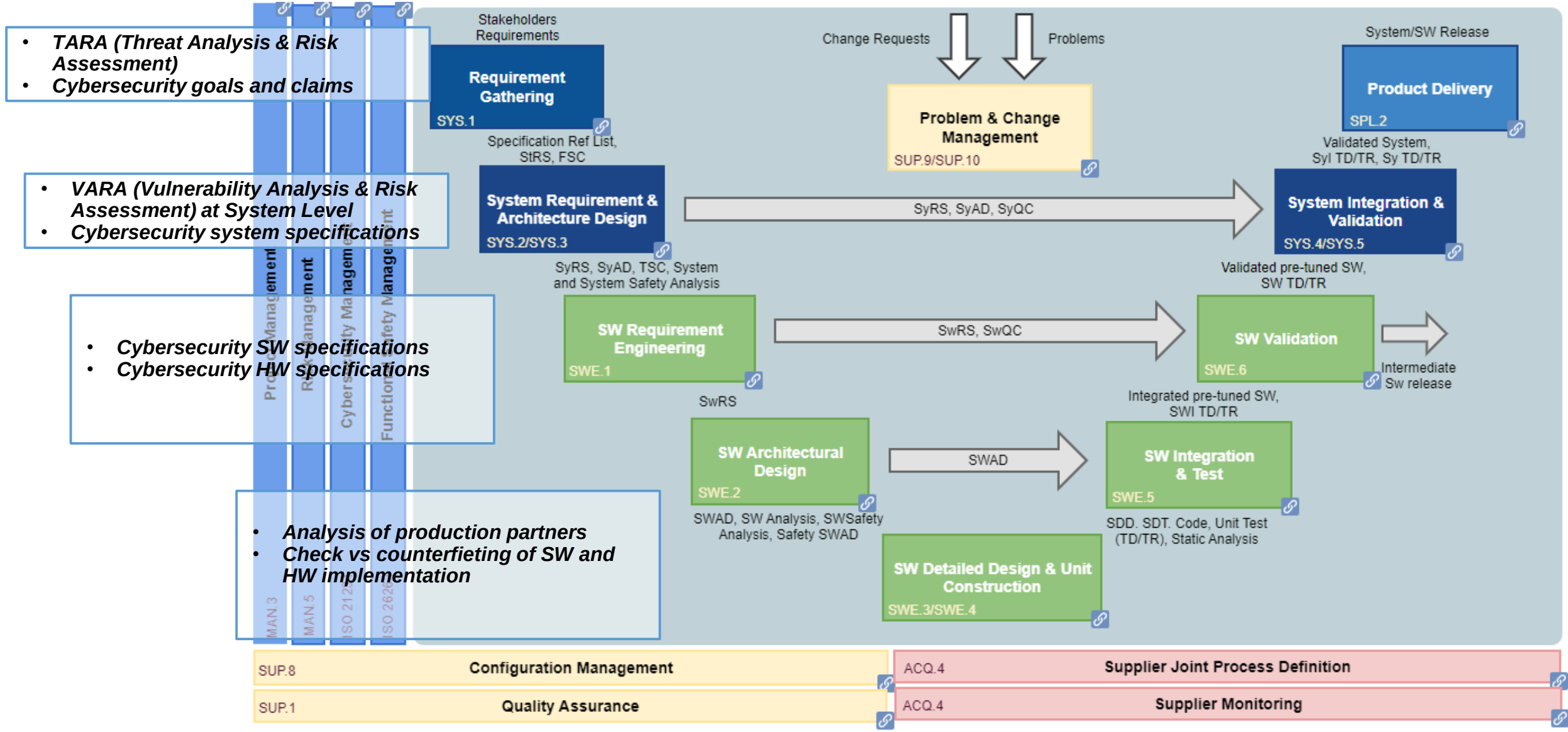
Cybersecurity activities in HW & SW development process

- *TARA (Threat Analysis & Risk Assessment)*
- *Cybersecurity goals and claims*

- *VARA (Vulnerability Analysis & Risk Assessment) at System Level*
- *Cybersecurity system specifications*

- *Cybersecurity SW specifications*
- *Cybersecurity HW specifications*

- *Analysis of production partners*
- *Check vs counterfieting of SW and HW implementation*



HW & SW development process related to product supplier. Selling a combination of HW or SW. In this process which is the flow? We follow a V model: we go from specification to implementation to testing and assessing level. Y axis: from top level to low level. X axis: before designing and implementing / the testing and verification.

1st point: requirement gathering (you have customer that wants your solution, so you talk with (sell other to understand their needs). First part encompasses TARA: Threat analysis and Risk assessment for the specific product tailored to specification (for ours Kemper, where are we putting camera?). So you define your CS goals and claims.

From this, you can make a 2nd document in which you specify how to achieve what you claimed (at high level). This is the phase of System Req. and Architecture Design.

From this point you can separate the flow: CS of the HW and CS of the SW. Only after Sys level you have clear what you want to specify.

For SW (and sometimes even HW), an analysis of production partners is important: prove reliability of partners that do parts you outsource. On top of this you should certify that you have a procedure to test the entire system.

So this includes also counterfeiting checks for SW and HW (backdoors, bugs etc.)

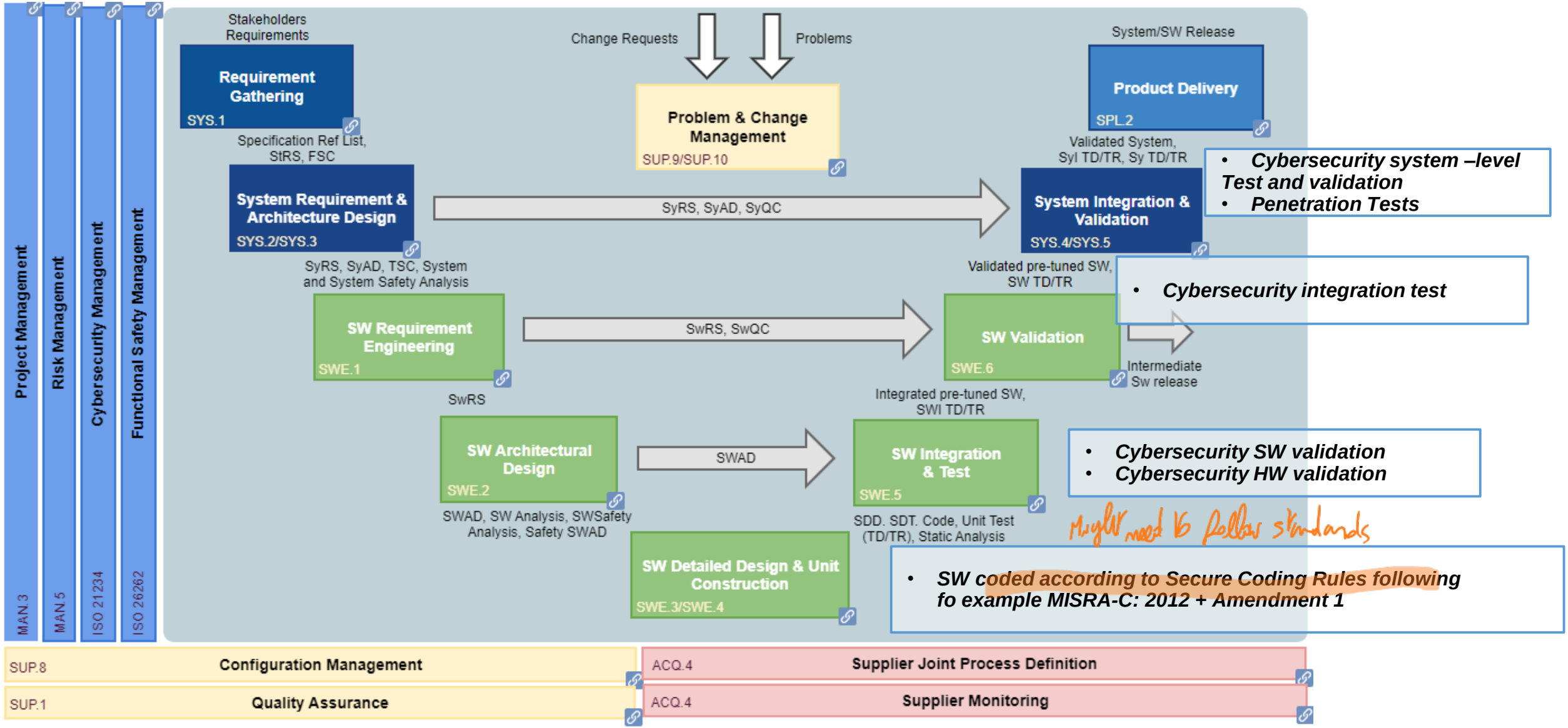
[NIS 2 and regulations are important for this. Companies wouldn't invest in this normally, but if Autoschade asks for NIS 2 compliance, you are forced!]

- At the end (bottom) you have implemented the HW/SW system! But you need assessment. Testing can be done at low level (ex: static analysis of code) or higher level (whole SW test) or higher (test the entire multi-engraving system). Also for this we start to see automatization for this activity.

We move from SW validation to System integration and validation. We then reach program delivery.

NOTE: for classical non dangerous conditions you do actual testing. For corner cases or dangerous to replicate tests you do simulations.

Cybersecurity activities in HW & SW testing process



Cybersecurity document list for HW/SW product

1. TARA (Threat Analysis & Risk Assessment)
2. VARA (Vulnerability Analysis & Risk Assessment) at System Level
3. Cybersecurity goals and claims including target security levels and target maturity level

   (Analisi di contesto operativo, analisi delle minacce, requisiti di cybersicurezza con identificazione di responsabilità ed applicabilità)Cybersecurity system specifications
4. Cybersecurity SW specifications
5. Cybersecurity HW specifications
6. SW Supply chain analysis (analisi di fornitori e componenti SW esterni)
7. HW Supply chain analysis (analisi di fornitori e componenti HW esterni)
8. SW coding style There can be an analysis of coding style or not
9. Test plan SW implementation } done by different teams
10. Test plan HW implementation
11. Test plan SW-HW integration

Cybersecurity certification

I Security Levels dello standard ISO 15408 meglio noto come Common Criteria, che guida la Cybersecurity alla certificazione di prodotti IT, sono meglio noti come EAL (Evaluation Assurance Levels).
Per un generico prodotto hardware o software o che comprende entrambe le parti, sono stabiliti 7 diversi livelli: da EAL1 a EAL7, con la seguente importanza in ordine crescente:

1. **EAL1:** testato funzionalmente;
2. **EAL2:** testato strutturalmente;
3. **EAL3:** testato e controllato;
4. **EAL4:** progettato, testato ed esaminato secondo metodologie;
5. **EAL5:** progetto semiformale e testato;
6. **EAL6:** progetto semiformale, verificato e testato;
7. **EAL7:** progetto formale, verificato e testato.

Cybersecurity certification

Once obtained the ISA/IEC 62443 certificate will be considered valid for three (3) years Because secure now ≠ secure forever

Cyber security Certification is done by entities like TUV SUD Bureau Veritas

Cybersecurity requirements – life cycle (IN IEC 62443)

For life cycle, CS req. include:

1) secure design (HW): Prevede sicurezza gestione chiavi, analisi di fornitori e componenti HW e/o SW esterni.

2) secure implementation: Punto 3 specifica come si implementano i punti 1 e 2, incluse linee guida per programmazione SW e FW del sistema.

3) secure verification and validation: Come si verifica e valida (inclusi penetration test) dovendo garantire indipedenza del team di test da quello di design? Contratti con partner terzi per Penetration Test su dispositivi e/o a livello infrastrutturale oltre a strumenti per verifica del SW.

4) management of secure issues: Aspetti anche organizzativi su come e chi riceve, rivede, risponde a, comunica problemi di sicurezza, incluso una revisione periodica di queste procedure.

↳ Force you to define structure for CS at org. level

Serve definire, strutturare, e documentare i processi e le responsabilità.

Inoltre serve, portare a standard 62443-4-1 il processo di ciclo di vita del prodotto.

5) security update: Aspetti di qualifica e documentazione

Cybersecurity foundational requirements (FRs)

asked by the skaulands
[All tailored to different SL and ML]

FR1) identification and authentication control (IAC): politiche di gestione

Identificazione e autenticazione di utenti umani (1.1) o di processi SW o di dispositivi (1.2);

politiche di gestione degli account utente (1.3);

politiche di gestione dei mezzi di identificazione autenticazione (1.4-1.5);

gestione autenticazione via chiavi asimmetriche pubbliche/private o tramite strumenti di tipo PAM (Privileged Access Management) per avere identificazione utente a livello di dominio

FR2) controllo dell'uso (UC): politiche di gestione delle sessioni (session lock; remote session termination; Concurrent session contro) e relative audit; uso di time-stamp e meccanismi di non ripudio; interfacce di test devono essere disabilitate. Come punto di partenza si potrebbe usare le linee guida ASPI disponibili da https://dwisrv.cto-utilities.prod.aws.autostrade.it/en/Public/wiki-security/abb-repository/audit-trail-abb

FR3) integrità di sistema ottenuta come Communication integrity (3.1); Protection from malicious code (3.2); Security functionality verification (3.3); Software and information integrity (3.4); Input validation (3.5); Deterministic output (3.6); Error handling (3.7); session integrity (3.8); protection audit (3.9). Questo è tutto sviluppo sicuro del codice, che, al momento, non è presente in MovyonElectronics. Non vuol dire che il prodotto finale non abbia queste caratteristiche, ma vuol dire che non ce ne è evidenza. E' fondamentale che MovyonElectronics segua al più presto, le pratiche di sviluppo sicuro individuate da Movyon nel documento Ref#3: MOVYON_PR_ICT_01_rev02.

Cybersecurity foundational requirements (FRs)

FR4) confidenzialità dei dati (non critica in MARTA Data Logger non trattando dati utente)

FR5) creazione di zone sicure e flussi dati restricted tramite Network segmentation (5.1), zone boundary protection (5.2), people communication restrictions (5.3), application partitioning (5.4). Al momento per permettere un uso più ampio possibile e flessibile di Marta Data Logger, su richiesta di ASPI, non sono da prevedere tecniche di segmentazione della rete.

FR6) timely response to events via accesso a log di audit (6.1) e monitoraggio continuo (6.2)

FR7) disponibilità delle risorse via protezione da DOS (denial of service), gestione risorse, backup dati sistema di controllo, e loro eventuale ripristino

Software application requirements riguardano: Embedded device requirements/host device requirements/network device (mobile code, update protection, Use of physical diagnostic and test interfaces, access form untrusted wireless networks; protection form malicious SW, Physical tamper resistance and detection; boot process; root of trust)

Nice, Giovanni—you're now stepping into the **core framework** of IEC 62443. Those things listed on your slide—**identification and authentication control, usage control, system integrity**, and so on—are what the standard calls **Foundational Requirements (FRs)**.

There are **seven** of them (but I'll weave them into the conversation naturally, not as a list, don't worry).

So, think of the **Foundational Requirements** as the **security pillars** that define *what needs to be achieved* in an Industrial Automation and Control System (IACS). They don't specify *how* to do it—but they say *this* is what your system must provide if you want to meet a particular **Security Level (SL)**.

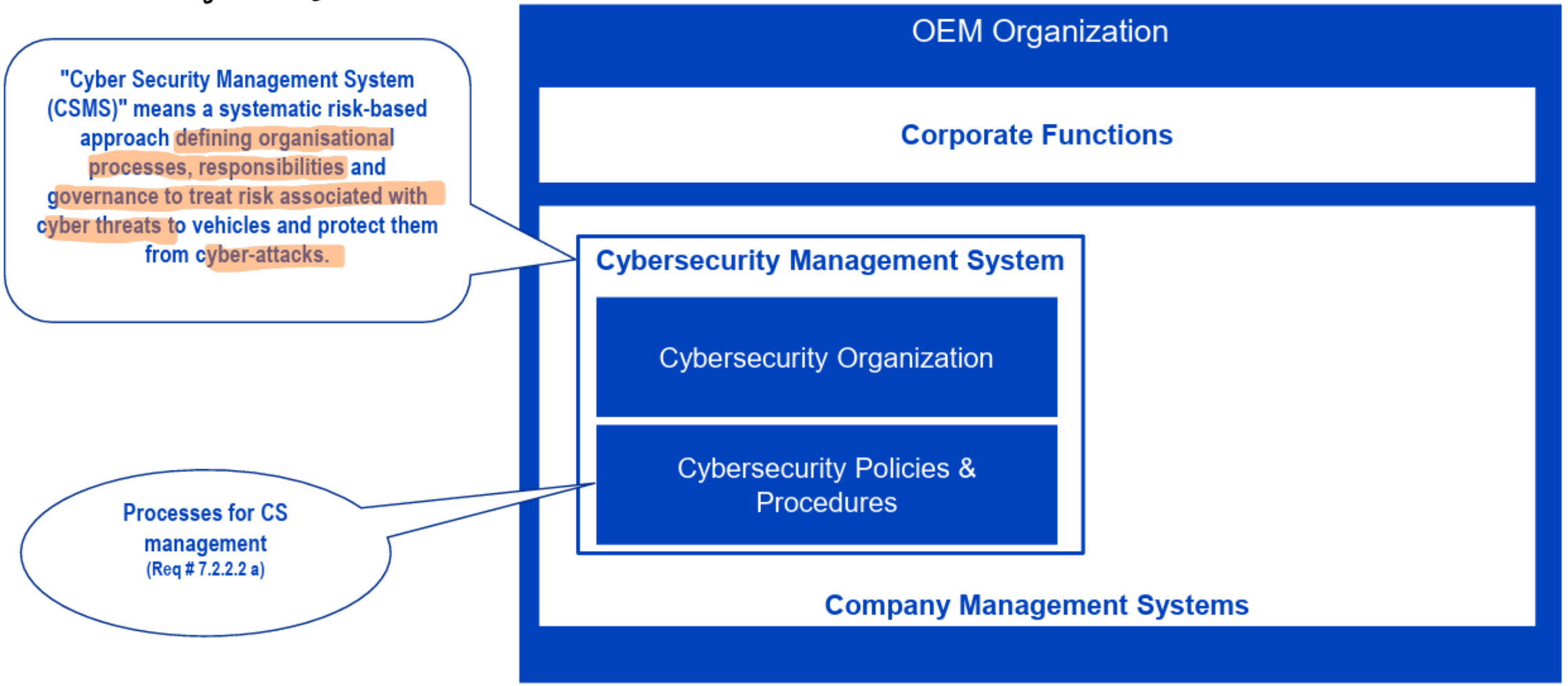
Exactly, Giovanni—**you nailed it.** They really *are* like the Ten Commandments of industrial cybersecurity.

No matter which part of IEC 62443 you're in—whether you're talking about system design, component features, or supplier development practices—**everything ties back** to those foundational requirements. They represent the **core goals** every secure IACS should aim for.

So whenever you're looking at a specific requirement in the standard—say, "users must be uniquely identified," or "software updates must be verified"—you're basically looking at a *detailed interpretation* of one of those commandments, applied at a specific **security level** and **scope**.

Cybersecurity impact on the organization

You should guarantee a CS management system, department and everything related to security.
Standard guides you to definition of this team, so it works even at higher level.



Cybersecurity impact on the organization

So the structure spans from vulnerability management, to a detective one, to a response and post incident management team. Size is tailored for org.

Cyber Threat Intelligence

Vulnerability Management

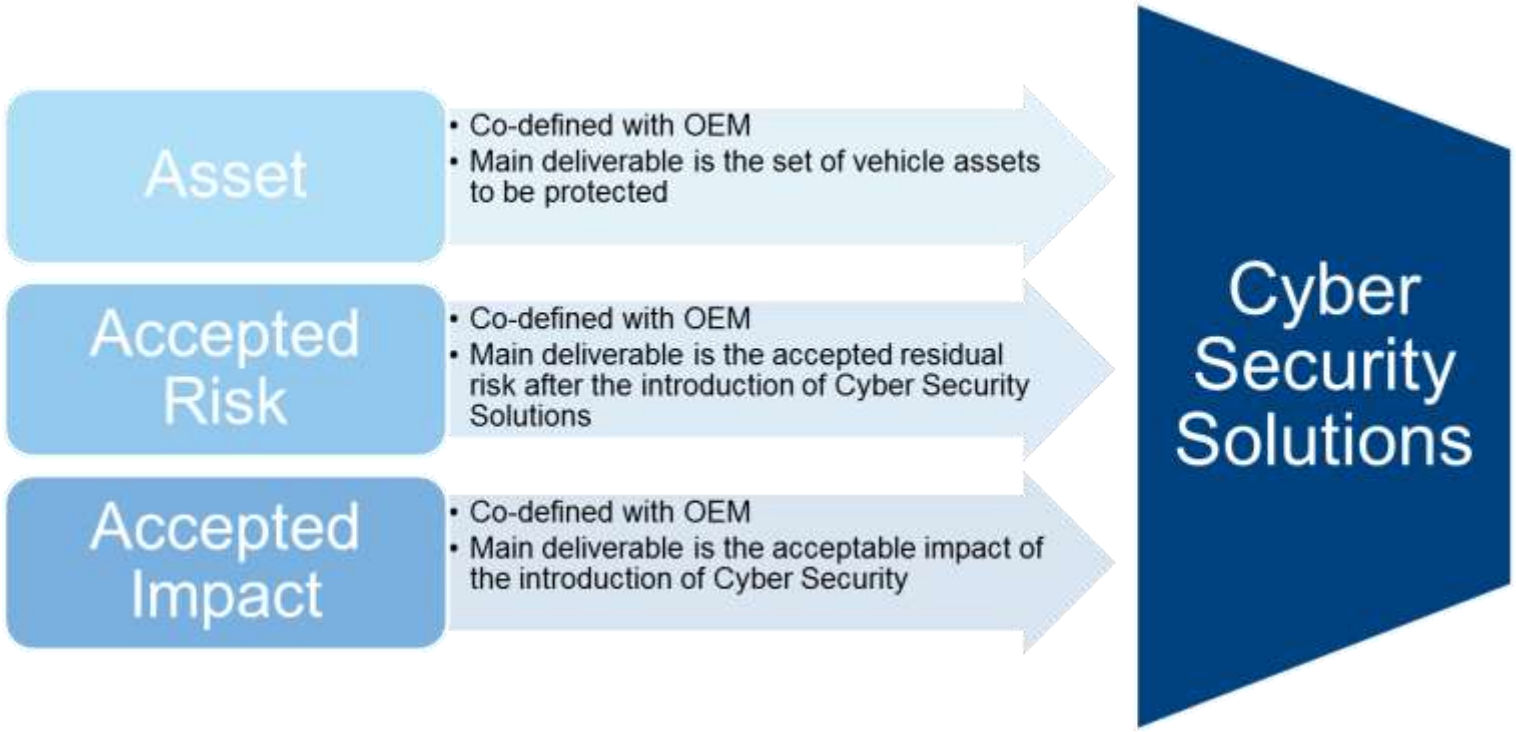
Preparation & Protection

Detection and analysis

Response

Post Incident Management Team

Cybersecurity impact on the organization



A solution for CS should come from asset analysis, acceptable risks and acceptable impacts. So a group of people doing this is important. And those people should work closely with all the other departments.