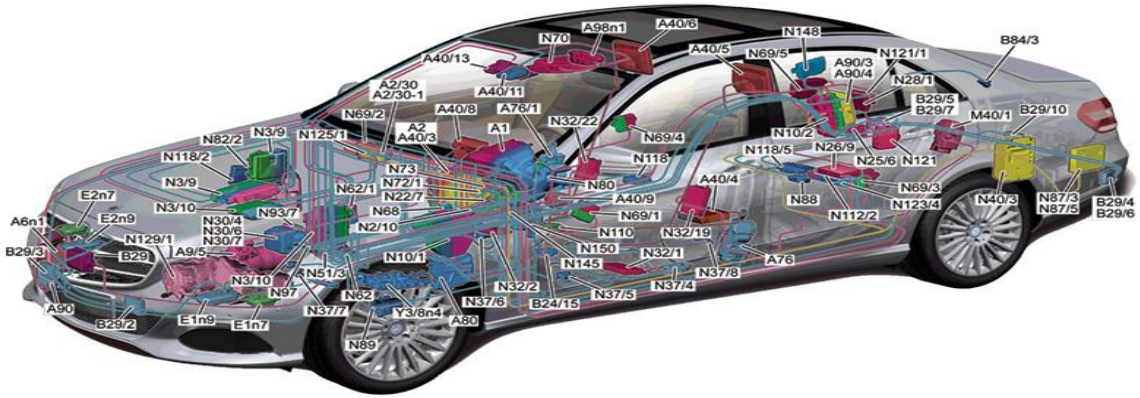
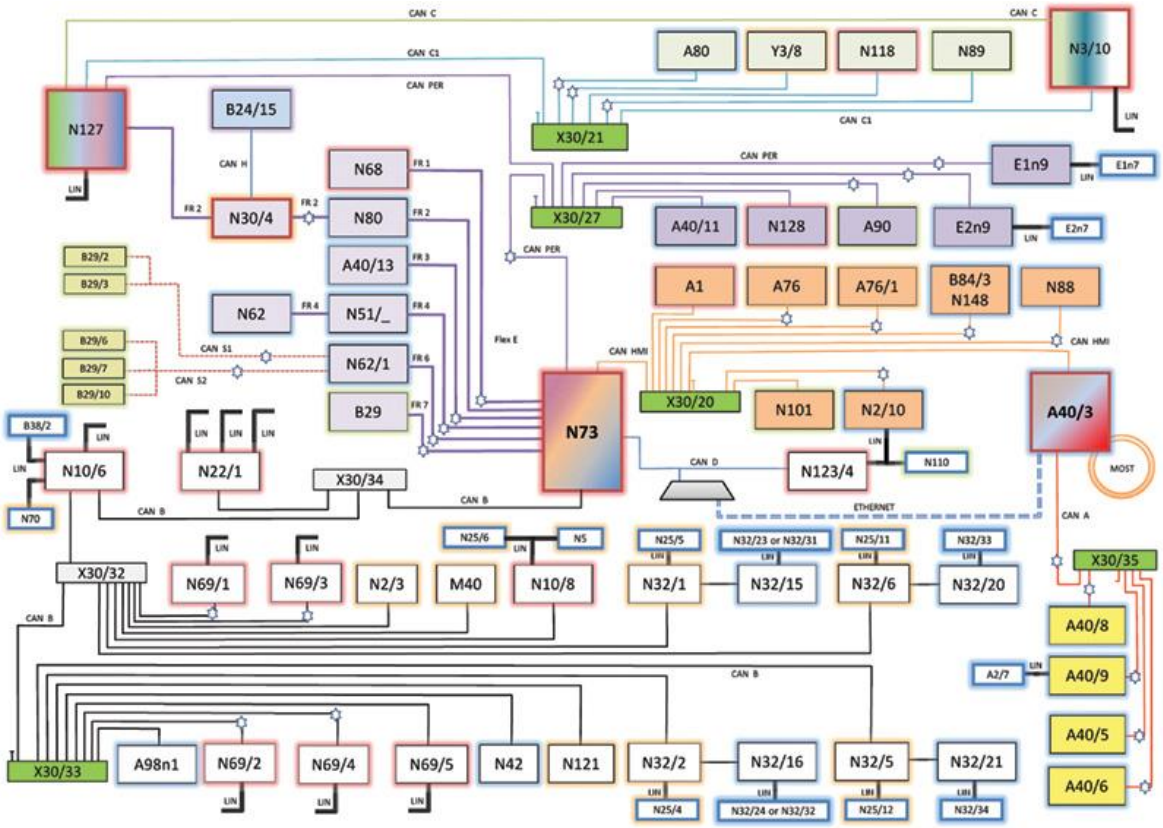
Automotive Security

Analogie e differenze con il mondo IT

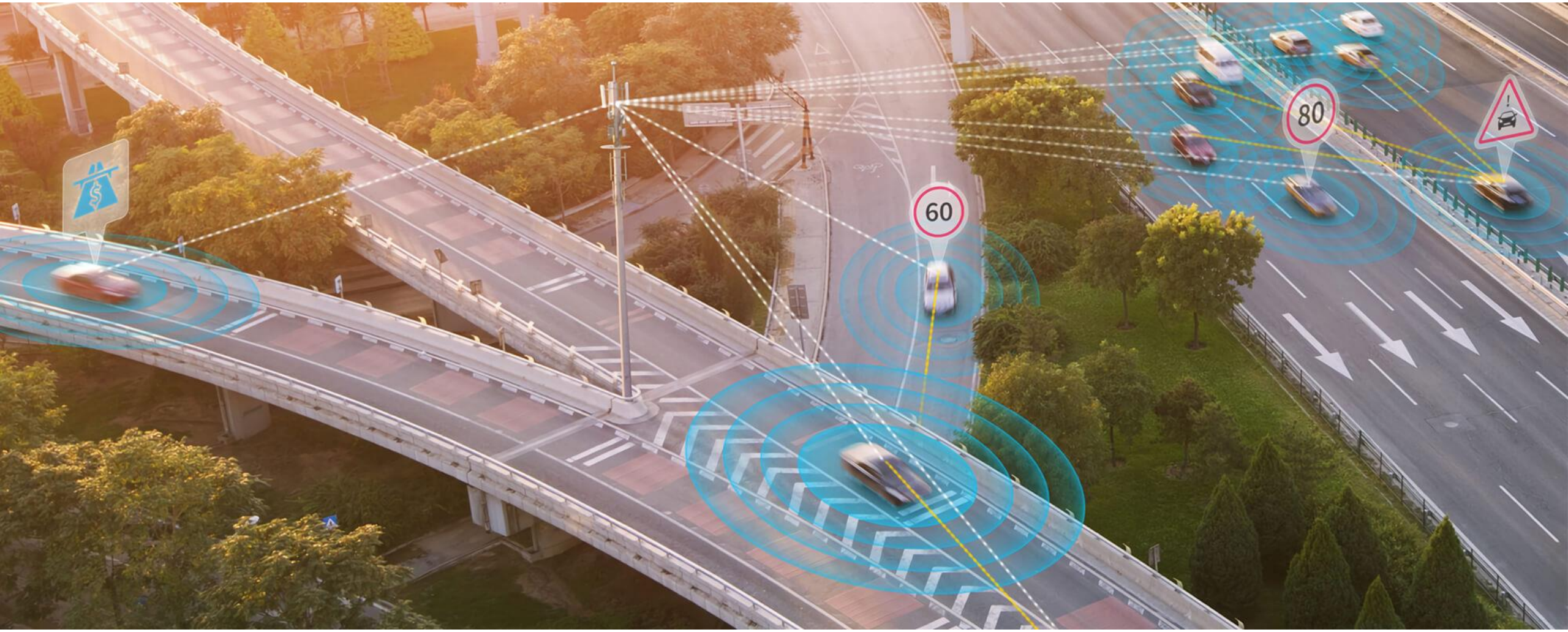
Sistema veicolo





Source: https://automotivetechinfo.com/2017/06/can-bus-review/

V2X – Comunicare con il mondo



Source: https://https://iot-automotive.news

Monetizzazione dei servizi: "Vehicle or Function-as-a-Service"

Il mercato dell'automotive sta vivendo una trasformazione radicale grazie all'adozione delle **function-as-a-service (FaaS),** ovvero dei servizi basati su **funzioni cloud** che permettono di sviluppare e gestire applicazioni in modo scalabile, flessibile ed economico.

Le FaaS offrono **ai produttori e ai fornitori la possibilità di creare soluzioni innovative** per la mobilità, la sicurezza, la connettività e l'efficienza energetica dei veicoli.

Alcuni esempi di FaaS applicate all'automotive sono i sistemi di **assistenza alla guida**, i servizi di **infotainment**, le piattaforme di **car-sharing** e le **reti intelligenti per la ricarica** delle auto elettriche.

Alcune particolari implementazioni del paradigma FaaS hanno ricevuto un’accoglienza molto divisiva, vedi il caso BMW: https://www.thedrive.com/news/bmw-responds-to-fury-over-heated-seats-subscription-fee

Monetizzazione dei servizi: "Vehicle or Function-as-a-Service"

Executive Summary

SBD

Vehicle X.0 – The evolution from functions to services

Vehicle X.0 describes the capability of an OEM & its vehicle platform based on technologies, processes, and business models, progressing from 1.0 up to 4.0.

Common evolution path for OEMs

	Definition	Characteristics	Technologies/Enablers
Vehicle 1.0 *Functional*	**Features developed & implemented in conjunction with underlying hardware**	No over-the-air updates	Microcontroller ECUs
		Tightly coupled ECUs	Real-time operating systems
		Basic infotainment services	CAN-based architecture
Vehicle 2.0 *Digital*	**Enhanced infotainment domain with apps, connectivity, and limited updateability**	Embedded or brought-in infotainment applications	Embedded 4G connectivity
		Limited software updates for infotainment	Cloud platform for content, services
		Limited driver personalization	Driver identity provider
Vehicle 3.0 *Updateable*	**Core domains (ADAS, digital cockpit, connectivity) implement abstracted software runtime & middleware**	Regular software updates for core functional domains	Ethernet E/E backbone
		Dynamic HMI for vehicle functions (voice, multiple screens, etc.)	Domain-based middleware
		OEM and/or 3rd party software applications	OEM-managed software development
Vehicle 4.0 *Software-Defined*	**Computing workloads can be dynamically shifted between vehicle computers & offboard infrastructure**	Redundant application processing across domains/zones	5G connectivity
		Continuous software delivery	Edge application runtime (i.e. edge containers)
		Dynamic data processing between vehicle, edge, & cloud	Homogenous computing platform between vehicle & cloud

Funzioni di connectivity molto accentuate e non più solamente verso gli OEM

+

Funzionalità presenti in hardware ma disabilitate via SW (FaaS/SDV)

=

Potenziale massiccio incremento degli attacchi alle vetture

Source: https://www.automotiveworld.com/articles/what-will-it-take-to-realise-the-software-defined-car/ (Original Source: SBD)

Governance della Security nei prodotti Automotive

IT:

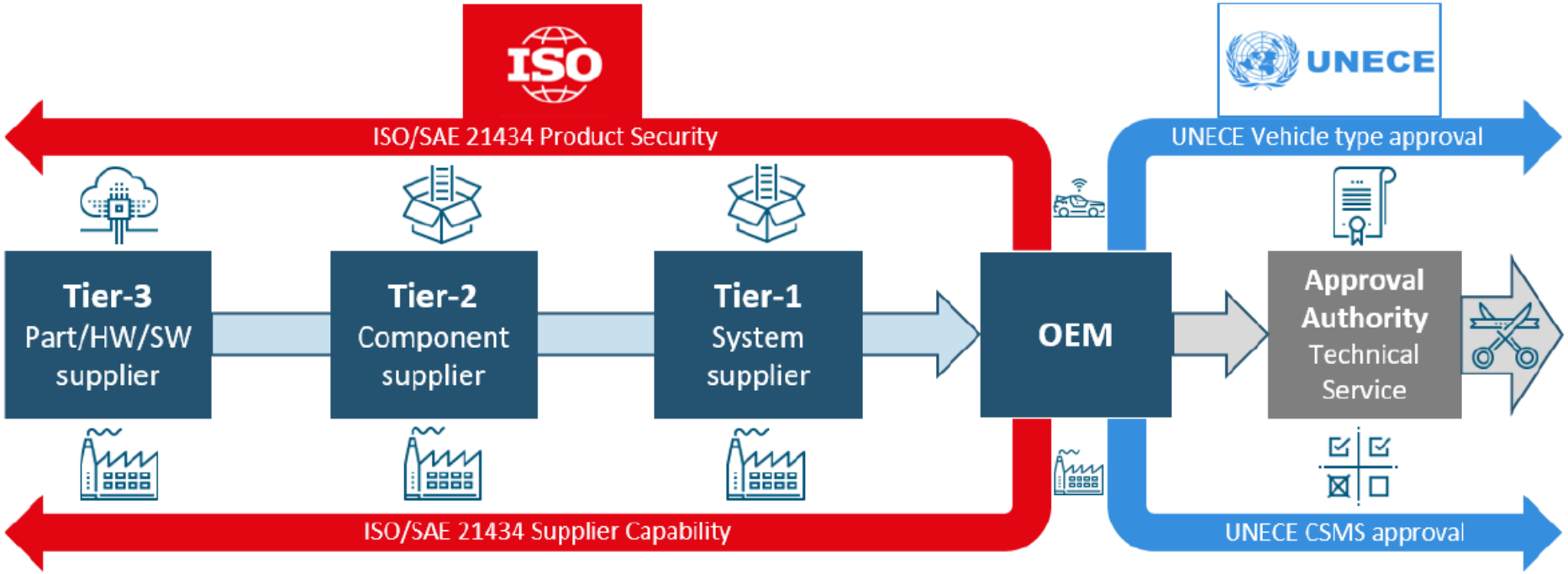
ISO 27000 family

OT:

IEC 62443

Automotive:

IATF 16949
ISO 21434
TISAX



Source: https://certx.com/automotive/cyber-security-for-road-vehicles-ep-1/

Governance: Distribuzione delle responsabilità

Governance aziendale e normative:

- **UNECE R155** → OEM (vincolante per il Type Approval/Omologazione)
- **ISO 21434** → Tier Xs
- **Assicurazioni** → RC Prodotti, assicurazioni infrastruttura IT, danni cyberwarfare

Governance di Prodotto:

- **Cybersecurity Interface Agreement** → Accordo mutuo da definire tra le parti (RASIC Matrix)
- **Contratti e Requisiti cliente** → General Terms and Conditions e **Cyber Security Basic Requirements**
- **Cyber Security** → “fascicolo” che contiene le evidenze documentali che comprovano la gestione del rischio Cyber sui prodotti fino al livello di appetito per il rischio definito dai **Cyber Security Goals**

Governance: Cybersecurity Goals

I **cybersecurity goals** in automotive sono obiettivi che mirano a proteggere i veicoli, i dati e le persone da minacce informatiche.

Per questo motivo è molto importante che vengano trattati come business requirements, ovvero come **requisiti che definiscono il valore e il successo di un prodotto e dell'azienda.**

Ciò significa integrare la sicurezza in tutte le fasi del ciclo di vita del veicolo, dalla progettazione alla produzione, dalla manutenzione al fine vita. In questo modo, si ottengono benefici sia per l'azienda che per i clienti:

- **Ridurre i rischi di attacchi informatici** che possono compromettere la funzionalità e la sicurezza del veicolo
- Rispettare le **normative** e gli **standard omologativi**
- Aumentare la **competitività** e la **reputazione** dell'azienda nel mercato
- Soddisfare le **aspettative e le esigenze dei clienti** in termini di **protezione dei dati** e della **privacy**

Governance: Cost of Poor Security

- Perdita di dati sensibili
- Furto di informazioni riservate
- Interruzione delle attività aziendali
- Danneggiamento della reputazione
- Costi legali e regolatori
- Richiesta di risarcimento danni
- Costi di ripristino
- Perdita di produttività
- Costi per la formazione e la sensibilizzazione
- Costi di consulenza
- Costi per l'implementazione di misure di sicurezza aggiuntive
- Perdita di opportunità di business
- Costi di riparazione dell'immagine aziendale
- Manipolazione dei dati
- Perdite finanziarie dirette
- Etc…

Source: https://www.vecteezy.com

“Security (like Quality) is free!”
(adapted from Philip Crosby)

Governance: Privacy e Security

La protezione della privacy e della security in ambito automotive è una sfida cruciale per il settore e presenta anche alcuni problemi da affrontare, come ad esempio:

- La necessità di garantire la **conformità alle normative vigenti**, come il GDPR, che richiedono il **consenso degli utenti** e la **trasparenza sul trattamento dei dati personali**
- La difficoltà di **bilanciare la sicurezza dei dati** con la **facilità d'uso e l'accessibilità dei servizi**, come la connettività, la navigazione, l'infotainment e l'assistenza alla guida
- L'impatto delle misure di protezione sulla **performance** e sull'**efficienza dei veicoli**, che devono essere in grado di gestire grandi quantità di dati in tempo reale e di comunicare con altri dispositivi e infrastrutture
- La **responsabilità** legale e reputazionale in caso di **violazione dei dati** o di **incidenti** causati da malfunzionamenti o attacchi informatici

Ciclo di vita della security: pre-produzione

La nostra gestione dei requisiti è basata su tre livelli:

- **requisiti di sicurezza** → misure preventive per proteggere i sistemi e i dati (e.g., autenticazione, cifratura, firme digitali ecc...)

- **requisiti di resilienza** → capacità di rilevare, rispondere e ripristinare le funzionalità dei sistemi (e.g. IDPS, ecc..)

- **requisiti di conformità** → rispetto delle normative e degli standard applicabili alla cybersecurity in ambito automotive, come il GDPR e la UNECE R155

E' fondamentale - soprattutto per gli OEM - la costruzione di una **raccolta di requisiti che siano validi per tutti i componenti a prescindere dal loro livello di rischio: Cyber Security Basic Requirements**

In seguito all'analisi dei rischi e la creazione di un concept, vengono definiti i requisiti specifici per i singoli componenti

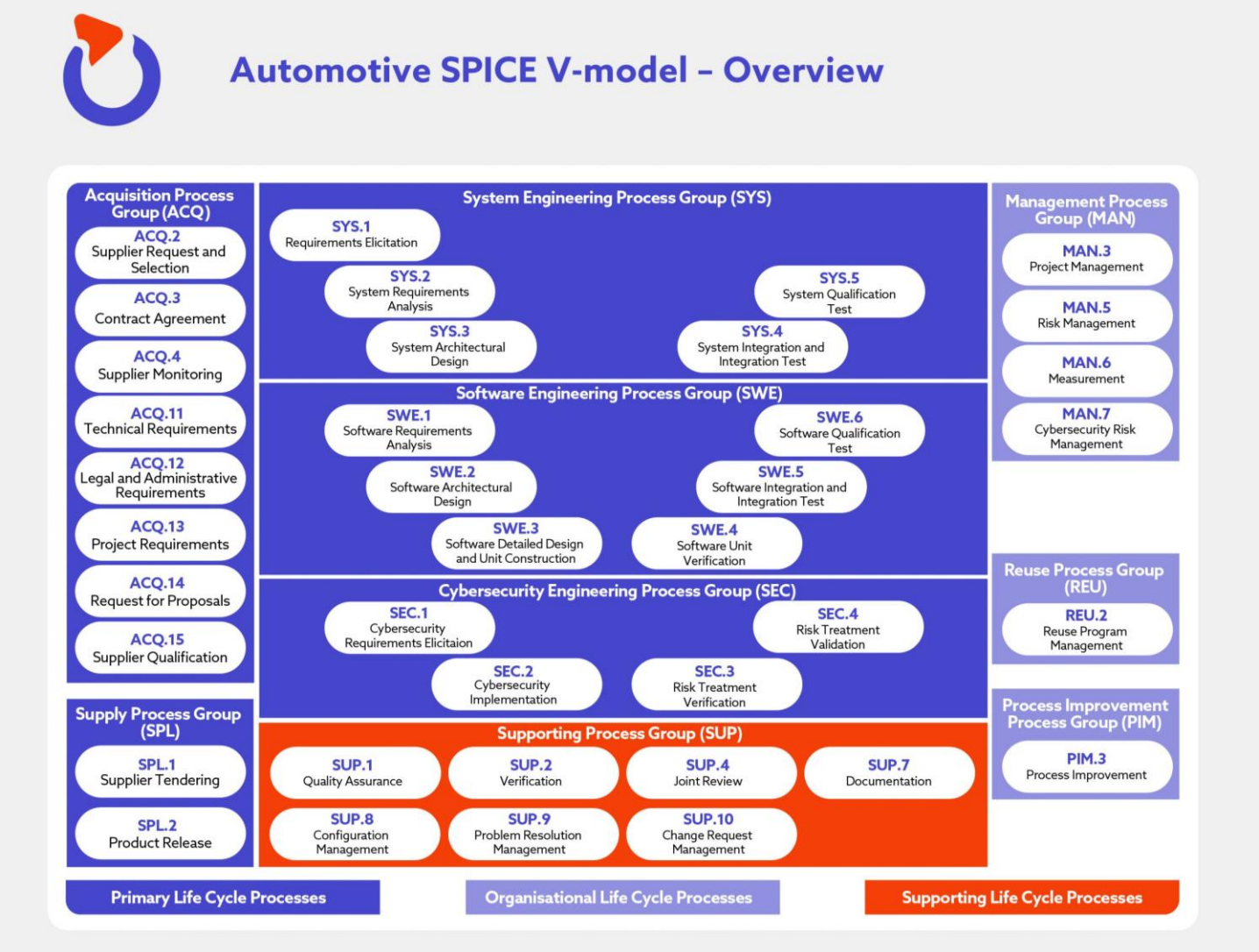
Ciclo di vita della security: post-produzione

Il ciclo di vita di un componente in ambito cybersecurity nel post produzione si articola in quattro fasi principali:

- **Monitoraggio**: si tratta di rilevare e analizzare le potenziali minacce e vulnerabilità che possono compromettere la sicurezza del componente e del veicolo.
- **Valutazione**: si tratta di valutare il livello di rischio e l'impatto delle minacce e delle vulnerabilità rilevate, nonché di definire le misure di mitigazione e le priorità di intervento.
- **Aggiornamento**: si tratta di implementare le misure di mitigazione, come ad esempio l'installazione di patch o la modifica delle configurazioni, per ridurre il rischio e aumentare la sicurezza del componente e del veicolo.
- **Verifica**: si tratta di verificare l'efficacia delle misure di mitigazione implementate, nonché di monitorare il comportamento del componente e del veicolo dopo l'aggiornamento.

Durata della maintenance in automotive: ~15 anni (alcuni OEM arrivano a 25!)

Ciclo di vita dell'automotive – Modello ASPICE

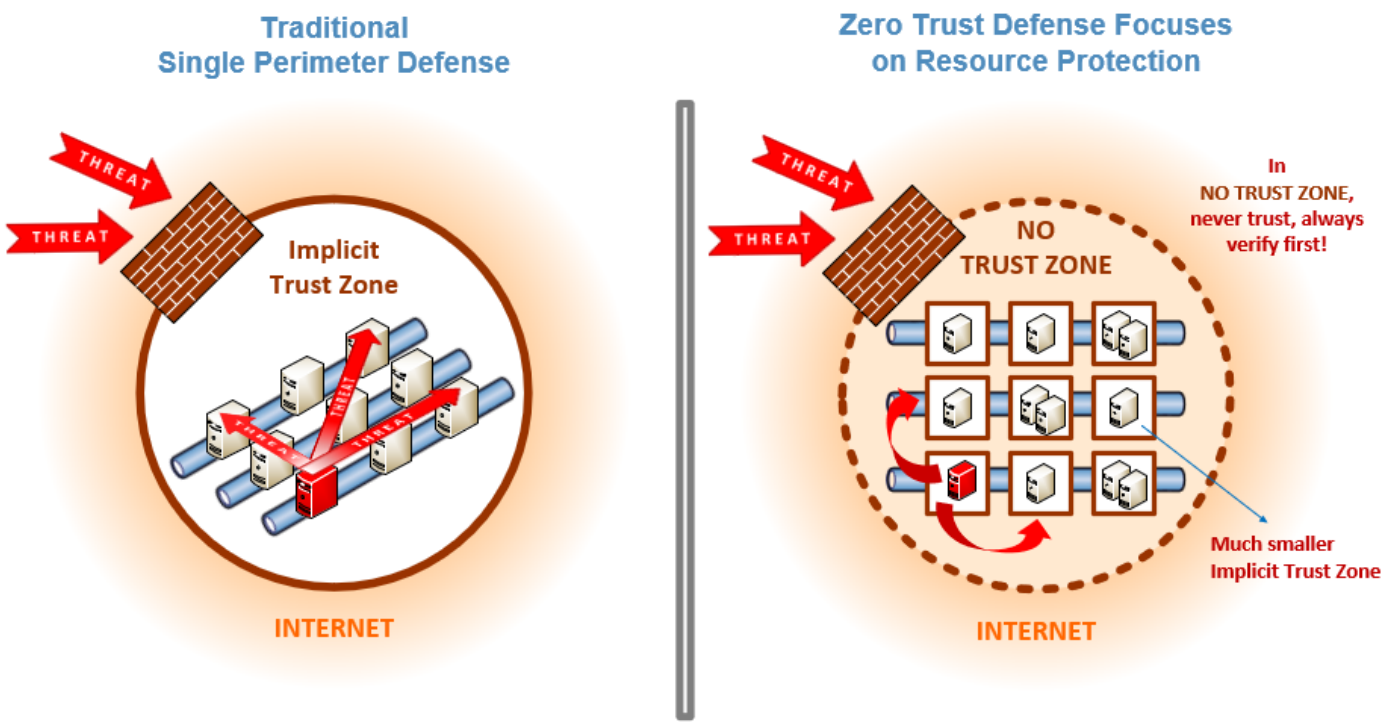


https://spyro-soft.com/blog/cybersecurity-aspice

Trust: il Business Attribute di base

Nessun contratto, legge o norma possono essere perfetti: tutte le **transazioni** si poggiano su una base comune di **fiducia. Senza fiducia reciproca non ci può essere business**: il costo di un contratto che copra tutte le possibili casistiche è solitamente sproporzionato rispetto al ritorno di investimento che esso genera.

Il concetto di fiducia è anche la base di molti meccanismi di security (es. PKI)



Source: https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

Trust: il Business Attribute di base

Da ciò ne consegue che la reputazione è probabilmente il bene più importante di un’azienda, particolarmente per quelle operanti nel settore della Cybersecurity.

E’ necessario monitorare e mantenere integri quei KPI che rappresentano la *trustworthiness* della propria azienda/del proprio prodotto verso il mondo esterno.

Warwick: one of the top UK universities

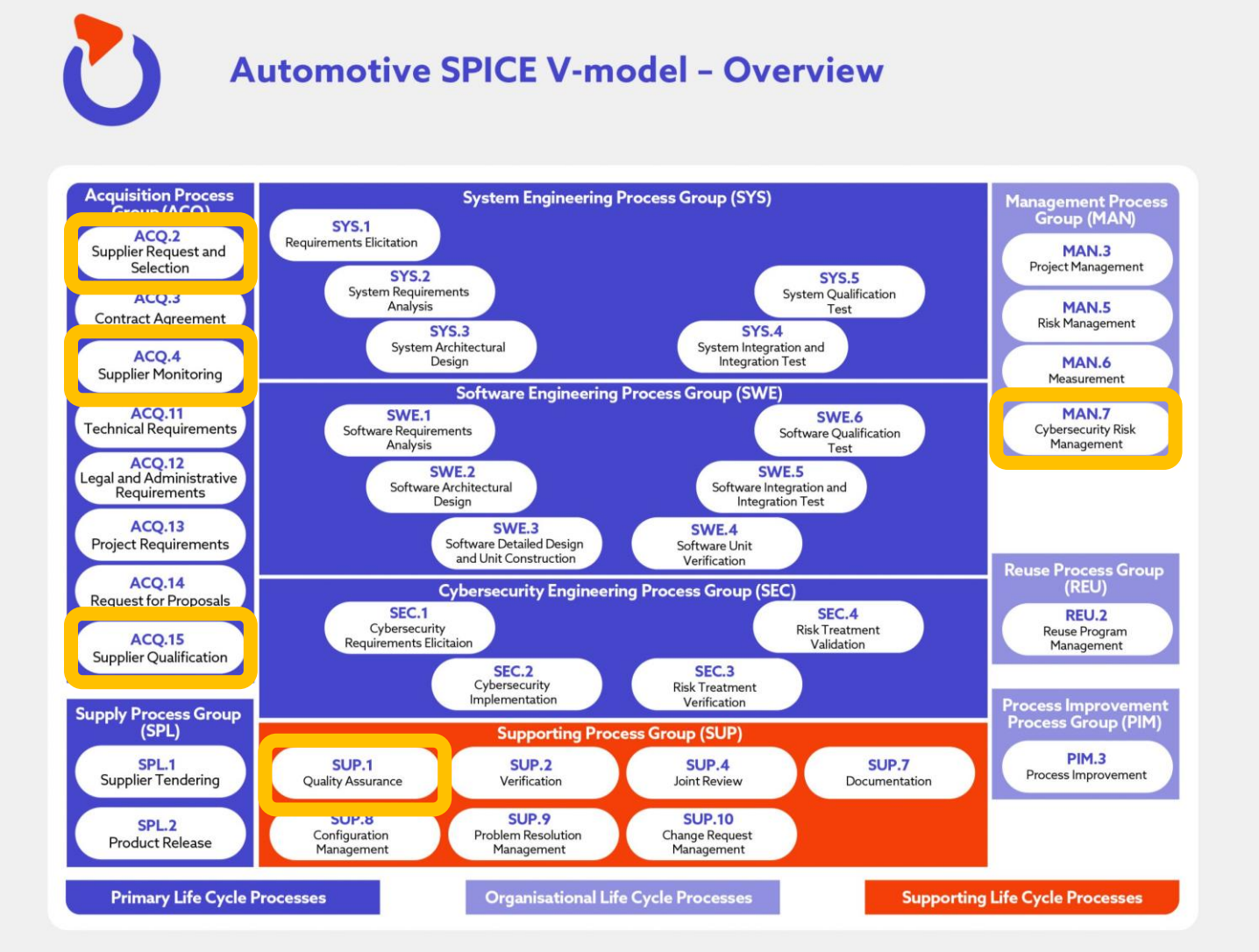
The University of Warwick has a reputation for excellence. This sees us highly placed in university rankings, achieving top 10 status in UK league tables and recognition as one of the top universities in the world.

Whether it is our teaching, research, student life or business collaboration, we aim to give people the best experience of Warwick at all times.

By doing this, we'll keep making an impact on the lives of those both close to home and further afield. And we'll continue to be globally recognised for our excellence.

Source: https://warwick.ac.uk/about/profile/ranking/

Posso fidarmi della mia supply chain?



https://spyro-soft.com/blog/cybersecurity-aspice

Monitoring della supply chain

COME?

- Processo di selezione fornitori (KPI, Assessment, Potential Analysis, Qualifica, Review periodiche)
- Certificazioni (es. IATF 16949, TISAX, ISO 21434)
- Audit di terze parti qualificate
- Cybersecurity Interface Agreement (RASIC Matrix)

Quali contributi può offrire il mondo IT a quello Automotive?

- **Steering normative**
  - Definizione Capability Maturity Model, Cybersecurity Assurance Levels…
- **Expertise tecnica, strategica e operativa**
  - Design architetture embedded/cloud, vulnerability assessment/penetration tests, selezione e certificazione dei fornitori...
- **Vision multidimensionale sul futuro della Cybersecurity in automotive**
  - Vista la maturità dell'ambito IT, il mondo automotive può beneficiare di una prospettiva integrata e scevra dei bias del settore
- **Soluzioni di gestione del SDLC Automotive/Embedded**
  - Pipelines, CI/CD, SAST/DAST, Unit/Integration Testing, Verifica e Validazione, Secure Development Guidelines…
- **Soluzioni di integrazione con ISO 27001 e ISMS**
  - La gestione centralizzata permette all'azienda di gestire tutti i rischi di sicurezza in un solo punto, favorendo le realtà più contenute come Tier 1/Tier 2 che sono più a rischio di non-compliance (ad es. per mancanza di risorse o skills)

ART ADVANCED SOLUTION

www.artgroup-spa.com

CYBER ACT FORUM 2023

ART GERMANY

MATE ADVANCED LABORATORY