POLITECNICO DI TORINO

Laurea MAGISTRALE in
INGEGNERIA INFORMATICA
(COMPUTER ENGINEERING)

Tesi di Laurea MAGISTRALE

Integrazione tra analisi HARA e TARA in ambito automobilistico

Supervisori

Prof. RICCARDO SISTO

Dr. CARLO LA TORRE

Candidato

ANDREA PERNO

DICEMBRE 2024

Sommario

L'installazione di dispositivi elettronici ed informatici all'interno degli autoveicoli è una pratica ormai consolidata; questo però comporta inevitabilmente l'introduzione di vulnerabilità e bugs del codice, i quali devono essere analizzati e gestiti in maniera corretta. Parallelamente è presente anche la Sicurezza Funzionale, la quale gestisce i malfunzionamenti dei vari componenti, in modo tale da non arrecare danni fisici agli utenti della strada. I due tipi di sicurezza sono complementari, e dunque, in assenza di una delle due, non è possibile garantire la completa sicurezza di un componente. Gli standard relativi alle due tipologie di sicurezza impongono ambedue l'analisi degli scenari di pericolo durante le fasi di progettazione dell'autoveicolo: TARA per la cybersecurity e HARA per la sicurezza funzionale; entrambi i tipi di analisi contengono l'identificazione degli scenari di pericolo che possono causare danno fisico; l'obiettivo è di sovrapporre parzialmente le due analisi, in modo tale da raggiungere un risultato più completo e coerente rispetto alla due analisi separate. Il risultato è una tabella che implementa un meccanismo di mappatura dei valori di ASIL, degli scenari ottenuti dall'analisi HARA, sul corrispettivo valore di severità del danno fisico dei medesimi scenari dell'analisi TARA, in modo da avere una miglior valutazione dei rischi all'interno dell'analisi di cybersecurity, in quanto i valori di ASIL sono più precisi e completi. L'applicazione dell'analisi è stata eseguita su un'astrazione teorica di un controllore di una batteria ad alto voltaggio: dai risultati ottenuti emerge come alcune delle valutazioni dei medesimi scenari, derivati dalle due analisi separate, mostrino delle differenze nella valutazione della gravità del danno fisico, identificando così un valore di severità a volte "sottostimato" da parte dell'analisi TARA, rispetto a quelli ottenuti mediante l'analisi integrata, mentre per altri scenari è stato dimostrato come l'analisi porti alla medesima valutazione di gravità del danno. Purtroppo in assenza di un componente fisico su cui applicare l'analisi integrata e la sua verifica, non è possibile dimostrarne l'effettiva efficacia, ma rimane comunque logico pensare che con la sua applicazione si potrebbe ottenere una miglior sicurezza del componente, una minor quantità di scenari di pericolo scoperti o modificati in fasi avanzate del progetto con una conseguente riduzione dei costi e dei tempi di sviluppo e produzione.

Elenco dei Contenuti

Elenco delle tabelle VI

Elenco delle figure VIII

Acronimi X

1 Introduzione 1
- 1.1 Tendenze nell'Industria Automobilistica . . . 1
- 1.2 Relazione tra Cybersecurity e Sicurezza Funzionale . . . 3

2 Cybersecurity in ambito Automobilistico 6
- 2.1 Minacce Informatiche in ambito Automobilistico . . . 6
  - 2.1.1 Attacchi Remoti . . . 7
  - 2.1.2 Attacchi Locali . . . 7

3 Norme e Regolamentazioni 9
- 3.1 ISO/SAE 21434 - Cybersecurity in ambiente Automobilistico . . . 9
- 3.2 UNECE R155 . . . 27
- 3.3 UNECE R156 . . . 35
- 3.4 ISO 26262 - Veicoli Stradali - Sicurezza Funzionale . . . 37

4 Penetration Testing in ambito Automotive 52
- 4.1 Strumenti per il Threat Modeling . . . 52
- 4.2 Tipologie di Penetration Testing . . . 55
  - 4.2.1 White Box . . . 55
  - 4.2.2 Black Box . . . 56
  - 4.2.3 Classificazione dei Test di Penetrazione . . . 56
- 4.3 Conduzione e Validazione . . . 58
- 4.4 La piattaforma Weseth . . . 59
  - 4.4.1 Struttura della piattaforma . . . 59

5 Approccio integrato ISO/SAE 21434 e ISO 26262 61
5.1 Descrizione della proposta d'integrazione di analisi HARA e TARA 63
5.2 Applicazione dell'integrazione di HARA e TARA 69
5.2.1 Analisi HARA del componente 69
5.2.2 Analisi TARA del componente 72
5.2.3 Validazione 76
5.2.4 Vantaggi 77

6 Conclusioni 78
6.1 Risultati Ottenuti 78
6.2 Difficoltà del percorso 78
6.3 Sviluppi Futuri 79

Bibliografia 81

Elenco delle tabelle

3.1 Classificazione della fattibilità di un attacco. 23
3.2 Classificazione ASIL della Gravità. 45
3.3 Classificazione ASIL di Esposizione. 45
3.4 Classificazione ASIL della Controllabilità. 46
3.5 Determinazione del valore di ASIL 46
3.6 Classificazione ASPICE dei processi 51

4.1 Metodi di threat modeling a confronto 55

5.1 Mappatura aziendale della severità del danno sui valori di ASIL . . 64
5.2 Mappatura aziendale della severità del danno sui valori di ASIL mediante colorazione 64
5.3 Rapporto dei valori con riduzione di severità secondo la mappatura aziendale 65
5.4 Mappatura proposta dei valori di ASIL sui valori di severità del danno 66
5.5 Mappatura proposta della severità del danno sui valori di ASIL mediante colorazione 66
5.6 Rapporto dei valori con riduzione di severità secondo la mappatura proposta 67
5.7 Confronto tra i rapporti di sottostima dei valori di ASIL secondo le due mappature 67
5.8 Analisi HARA del controllore dell'energia ad alto voltaggio 70
5.9 Determinazione del valore di ASIL per un possibile evento termico . 71
5.10 Determinazione del valore di ASIL per un possibile evento di troncamento della potenza 71
5.11 Analisi TARA del controllore dell'energia ad alto voltaggio 72
5.12 Valutazione di Impatto TARA per la manomissione del Firmware . 73
5.13 Valutazione di Impatto TARA per la manomissione del canale . . . 73
5.14 Valutazione TARA della fattibilità dell'attacco per la manomissione del Firmware 74

5.15 Valutazione TARA della fattibilità dell'attacco al canale di comunicazione 74
5.16 Valutazione del rischio dalla normativa ISO/SAE 21434 75
5.17 Valutazione e gestione del livello di rischio di manomissione del Firmware 75
5.18 Valutazione e gestione del livello di rischio dei manipolazione del canale 75

Elenco delle figure

3.1 Struttura della Normativa ISO/SAE 21434 11
3.2 Gestione dei Rischi di Cybersecurity nelle fasi del progetto 12
3.3 Esempio di metodo per determinare la rilevanza in cybersecurity . . 26
3.4 Modello per il simbolo di Conformità del Veicolo alla Normativa R155 34
3.5 Struttura normativa ISO 26262 39
3.6 Modello di riferimento per sviluppo del Software secondo normativa ISO 26262 48

5.1 Integrazione concettuale di analisi HARA e TARA 62
5.2 Integrazione tra analisi HARA e TARA 68

Acronimi

AI Artificial Intelligence

ASIL Automotive Safety Integrity Level

BCM Brake Control Module

CAL Cybersecurity Assurance Level

CAN Controller Area Network

CPS Cyber-Physical System

CSMS Cyber Security Management System

CVSS Common Vulnerability Scoring System

E/E Electric and Electronic

EBCM Electronic Brake Control Module

ECU Electronic Control Unit

EVITA E-Safety Vehicle Intrusion Protected Applications

FMEA Failure Mode and Effects Analysis

FTA Fault Tree Analysis

FMVEA Failure Mode Vulnerabilities and Effect Analysis

GPS Global Positioning System

HARA Hazard Analysis and Risk Assessment

HAZOP Hazard and Operability Study

HEAVENS HEAling Vulnerabilities to ENhance Software Security and Safety

hTMM hybryd Threat Modeling Method

IoT Internet of Things

ISO International Organization for Standardization

JTAG Joint Test Action Group

LTE Long Term Evolution

MITM Man in the Middle

OBD On Board Diagnostic

OCTAVE Operationally Critical Threat, Asset and Vulnerability Evaluation

OEM Original Equipment Manifacturer

OTA Over The Air

PASTA Process for Attack Simulation and Threat Analysis

PCM Powertrain Control Module

PRM Process Reference Model

QM Quality Management

RXSWIN RX Software Identification Number

SAE Society of Automobile Engineers

SAHARA Security-aware Hazard and Risk Analysis Method

SPICE Software Process Improvement and Capability dEtermination

STRIDE Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege

SUMS Software Update Management System

TARA Threat Analysis and Risk Assessment

TCM Transmission Control Module

TVRA Threat, Vulnerability and Risk Assessment

UN United Nations

USB Universal Serial Bus

UNECE United Nations Economic Commission for Europe

Weseth We secure things

WiFi Wireless Fidelity

Capitolo 1

Introduzione

1.1 Tendenze nell'Industria Automobilistica

Al giorno d'oggi l'integrazione di componenti elettroniche ed informatiche nel settore automobilistico risulta molto accentuata, al fine di garantire un maggior controllo dell'autoveicolo ed un'analisi più dettagliata dello stato dei componenti. Tali dispositivi sono denominati ECU (la quale è la sigla di Electronic Control Unit, tradotto "Unità di Controllo Elettronica") e sono delle centraline dedicate allo svolgimento di una particolare azione o funzione, che comprende il monitoraggio di uno stato associato ad una determinata grandezza fisica (quali ad esempio velocità, temperatura, luminosità, etc.) ed il derivato controllo di un attuatore (es. tergicristalli, luci anabbaglianti, etc.). [1] Per fare alcuni esempi possono essere citati: il modulo di controllo del propulsore (PCM) per la gestione del motore e dell'alimentazione, il modulo di controllo della trasmissione (TCM) per la gestione della trasmissione, il modulo di controllo dei freni (BCM or EBCM) per la gestione del sistema frenante, etc. Ad oggi si possono trovare nei veicoli anche fino a 150 ECUs [2] che dialogano tra loro e contribuiscono al corretto funzionamento di tutti i sistemi.
Possiamo identificare in questo andamento alcune macro aree verso cui si sta orientando il mondo dell'industria automobilistica, tra cui troviamo:

1. Veicoli Connessi
   Connessioni all'interno del veicolo tra le varie ECUs, o all'esterno verso il Cloud Computing o l'interazione con gli altri veicoli.

2. Internet of Things
   Fondamentale per l'interazione tra dispositivi connessi, quale ormai è considerato un autoveicolo, identificandosi tra gli "oggetti" più grossi.

3. Aggiornamenti OTA
   La gestione di questa enorme quantità di ECUs non è esente da aggiornamenti software, in quanto l'aggiornamento fa parte del Ciclo di Vita di un dispositivo, in modo da migliorare e correggerne i difetti. Al contempo però è impensabile dover richiamare, presso le case produttrici, tutti i veicoli circolanti per poter fisicamente installare un aggiornamento software ogni volta che ne venga rilasciato uno nuovo, perciò ci si è orientati verso la proceduta chiamata "Update OTA" che è la sigla per Over The Air, cioè un aggiornamento installato tramite connessione wireless.

4. Guida Autonoma
   Frontiera del "futuro", dove gli autoveicoli potranno essere condotti, senza l'ausilio di un conducente; futuro ormai prossimo, ma pieno di ostacoli e difficoltà a cui però si sta facendo fronte grazie al miglioramento del software e all'introduzione delle intelligenze artificiali.

5. Veicoli Elettrici
   Il numero dei veicoli a propulsione elettrica è in costante aumento, qualche anno fa si stimava che su 1 miliardo di vetture circolanti a livello globale, fossero presenti circa 2 milioni di auto elettriche [3], le quali, grazie alla grande disponibilità di corrente elettrica a bordo dell'autoveicolo, possono disporre di un'elevata quantità di ECUs e dispositivi elettronici che puntano a migliorare l'esperienza di guida.

6. Trasformazione del Cloud
   Il cloud offre flessibilità e consente una scalabilità efficiente, a favore di tecniche e strategie più evolute, quali l'analisi dati e le tecniche di apprendimento delle AI.

7. Questioni Ambientali
   Gli ultimi scandali relativi alla manomissione dei valori di emissioni inquinanti degli autoveicoli, indicano come il rispetto dei vincoli di inquinamento sia un argomento critico per le case costruttrici di autoveicoli.

8. Privacy dei dati e Normative
   Come già citato in precedenza, la collezione di dati su piattaforme Cloud, per quanto legittima in caso di anonimizzazione della sorgente, rimane comunque un argomento molto sensibile, perciò richiede una legislazione molto dettagliata e precisa, su cui le maggiori organizzazioni legislative internazionali hanno lavorato e stanno lavorando per tutelare gli utilizzatori finali.

L'introduzione dell'informatica all'interno degli autoveicoli, con lo scopo di raggiungere un miglior controllo e sicurezza alla guida, porta però inevitabilmente

all'introduzione delle debolezze intrinseche della materia quali ad esempio vulnerabilità e bugs del codice. A tal proposito è stata necessaria la creazione di una regolamentazione atta ad indicare: la corretta applicazione della Sicurezza Informatica, la sua corretta implementazione a livello aziendale e di progetto, e la verifica di quest'ultime. Parallelamente, a fianco della sicurezza informatica, è presente anche il contributo da parte della Sicurezza Funzionale, la quale ha come obiettivo la gestione dei malfunzionamenti e dei funzionamenti limite dei vari componenti, in modo tale da non arrecare danni fisici ai passeggeri dell'autoveicolo o ad altri utenti della strada.

1.2 Relazione tra Cybersecurity e Sicurezza Funzionale

Alla luce di quanto esposto negli esempi precedenti, possiamo distinguere tra due tipi di sicurezza:

- Sicurezza informatica (Cybersecurity): nota anche come sicurezza digitale, è la pratica volta a proteggere le informazioni digitali, i dispositivi e le risorse personali, compresi: le informazioni personali, gli account, i file, le fotografie, e il denaro. Viene generalmente descritta come la protezione delle proprietà di Confidenzialità, Integrità e Accessibilità di un componente. [4]

- Sicurezza fisica o funzionale (Functional Safety): è la caratteristica di un componente di non arrecare danno fisico al suo utilizzatore, o a chi ne sta vicino, durante il suo funzionamento e malfunzionamento.

Osservando più dettagliatamente il campo di appartenenza di questi due tipi di sicurezza, possiamo notare come la sicurezza funzionale si applichi a guasti sistematici o casuali, i quali risultano in un malfunzionamento di un sistema E/E, mentre la cybersecurity agisce contro problemi generati da attacchi mirati, con intento malevolo, esterni al componente. Tra questi due tipi di sicurezza non possiamo non notare una certa correlazione in quanto: un sistema, sicuro dal punto di vista della sicurezza funzionale, non arrecherà danno all'utente in caso di malfunzionamento, ma può essere comunque violato da un attaccante esterno ed essere manipolato con intenti malevoli; mentre un sistema sicuro dal punto di vista informatico, sarà protetto da attacchi esterni mirati a deviarne il comportamento, ma rimane tuttavia soggetto a errori casuali e sistematici interni, i quali, se non correttamente gestiti dalla sicurezza funzionale, possono causare danno all'utente finale. Si può quindi affermare che i due tipi di sicurezza siano complementari, e dunque, in assenza di una delle due, non si può garantire la completa sicurezza di un componente.

Per queste motivazioni, al giorno d'oggi, lo sviluppo di un qualunque autoveicolo stradale richiede l'attestazione di procedure e processi atti a garantire che entrambi i tipi di sicurezza siano considerati all'interno delle fasi di progettazione, costruzione e manutenzione del veicolo, in modo tale da poter garantire la sicurezza, entro un ragionevole livello di rischio, di un veicolo. Tra i vari standard e normative in materia sono stati presi in esame: lo standard "ISO/SAE 21434 - Cybersecurity in ambiente Automobilistico" per quanto riguarda la gestione e l'applicazione della sicurezza informatica durante le varie fasi del ciclo di vita dell'autoveicolo, le normative UNECE R155 e R156 che esprimono l'obbligatorietà di attenersi a quanto indicato all'interno dello standard ISO/SAE 21434 e lo estendono, indicando le metodologie per la sua certificazione e attestazione; mentre per quanto riguarda la Sicurezza funzionale, verrà preso in esame lo standard "ISO 26262 - Veicoli Stradali - Sicurezza Funzionale" per l'applicazione dei processi atti a garantire la sicurezza funzionale dei componenti e quindi degli autoveicoli nella loro interezza.
L'obiettivo di questa tesi è quello di integrare le due tipologie di analisi HARA (ISO 26262) e TARA (ISO/SAE 21434) in modo tale da rendere più coerenti e complete le valutazioni relative alla gravità dei danni fisici causati all'interno dei possibili scenari. Le motivazioni sono molteplici, ma tra queste possiamo sicuramente individuare una miglior gestione a livello aziendale con un conseguente minor dispendio di risorse in termini di costi e tempistiche in quanto, qualunque valutazione negativa in fase di validazione dei requisiti, porta inevitabilmente ad una revisione del progetto la quale può avere costi ingenti visto la fase avanzata; perciò l'obiettivo è quello di avere un lavoro migliore a partire sin dalle fasi iniziali. Per raggiungere questo scopo la tesi ha richiesto una fase iniziale di analisi delle normative e degli standard sopra citati per comprendere cosa è attualmente richiesto ai costruttori di autoveicoli; contemporaneamente è stata svolta un'analisi di svariati articoli relativi all'applicazione dei due tipi di analisi e possibili variazioni interne delle tecniche utilizzate in termini di tipologie di definizione delle minacce o delle metodologie di penetration testing applicate. Successivamente il lavoro è proseguito con la ricerca di un caso pratico su cui poter applicare la proposta di integrazione, da cui però è emerso solo un documento di un'azienda che internamente stava iniziando ad ipotizzare un processo del genere proposto, perciò lo sviluppo della tesi si è concentrato sull'analisi, discussione e modifica della strategia ipotizzata. In conclusione l'integrazione delle due analisi è stata applicata a livello teorico ad un sistema di gestione di una batteria ad alto voltaggio, in quanto non è stato possibile trovare un componente concreto su cui applicare l'analisi a causa dell'indisponibilità delle aziende contattate.

La struttura della tesi dunque è la seguente:

- Cybersecurity in ambito Automobilistico: contiene una breve panoramica delle vulnerabilità e delle tipologie di attacco principalmente utilizzati negli ultimi

anni;

- Norme e Regolamentazioni: descrizione e spiegazione nel dettaglio degli standard e delle normative analizzate con contestuale approfondimento delle tipologie di analisi prese in esame;
- Penetration Testing in ambito Automotive: descrizione e confronto delle principali tecniche utilizzate per l'elencazione e la valutazione delle minacce, con conseguente analisi delle varie tipologie di penetration testing atte alla validazione dei processi di sicurezza implementati;
- Approccio integrato ISO/SAE 21434 e ISO 26262: descrizione del processo d'integrazione proposto e confronto con il processo aziendale analizzato, con successiva applicazione pratica ad un modello teorico di un componente di esempio;
- Conclusioni: spiegazione ed analisi dei risultati ottenuti e possibili sviluppi futuri del progetto.

Capitolo 2

Cybersecurity in ambito Automobilistico

2.1 Minacce Informatiche in ambito Automobilistico

Negli ultimi anni, il settore automobilistico è diventato un obiettivo primario per i criminali informatici, tra le cause possiamo identificare la crescente interconnessione dei veicoli e la loro enorme complessità in termini di Hardware e Software. Si stima un incremento di circa il 99% del numero di incidenti relativi alla Cybersecurity, tra il 2019 e il 2020, e che nel 2022 siano incrementati fino al 380% gli attacchi informatici che sfruttavano API fornite dall'industria automobilistica. [5]

Considerando un autoveicolo moderno come un dispositivo informatico, è necessario quindi identificare un perimetro di sicurezza, cioè una zona, al cui interno, tutti i dispositivi siano sicuri e fidati. Un'ipotesi sarebbe quella di considerare come perimetro la carrozzeria dell'autoveicolo che separa l'interno dell'abitacolo, dall'esterno del veicolo, ma questo non basta, in quanto le connessioni wireless attive su un autoveicolo sono accessibili anche nelle immediate vicinanze all'esterno dello stesso, rendendo potenzialmente accessibile l'architettura interna, perciò l'unica opzione rimanente è quella di considerare ogni ECU come singolo componente con un proprio perimetro di sicurezza.
Possiamo tuttavia effettuare una distinzione tra attacchi remoti, i quali si svolgono senza accesso fisico all'autoveicolo, sfruttando una connessione wireless, e attacchi locali che implicano l'accesso all'abitacolo dell'autoveicolo, in modo tale da poter implementare un attacco mediante un'interfaccia hardware del dispositivo.

2.1.1 Attacchi Remoti

Gli attacchi remoti possono essere ulteriormente suddivisi in tre macro categorie, sfruttando diverse tecnologie wireless.

Corto raggio

In questo caso si parla di connessioni wireless di breve distanza, quale può essere considerata ad esempio una connessione di tipo Bluetooth, generalmente interna all'abitacolo, ma comunque senza connessione fisica con alcun dispositivo digitale.

Medio Raggio

Tra i possibili vettori a medio raggio possiamo citare la rete WiFi interna al veicolo (ove presente), la quale consente di creare una piccola rete locale, ma in quanto connessione di tipo wireless, è inevitabilmente disponibile anche all'esterno del veicolo, e per questo motivo va protetta.

Lungo Raggio

A concludere troviamo le connessioni a lungo raggio, che non implicano la vicinanza al veicolo, tra queste possiamo citare la connessione internet dell'autoveicolo, necessaria per il funzionamento della rete interna al veicolo, e per le comunicazioni verso il Cloud per la raccolta e analisi di dati diagnostici; un secondo esempio può essere la connettività GPS, che dev'essere inevitabilmente un tipo di connessione a lungo raggio, ma che, se non adeguatamente protetta, può essere bersaglio di attacchi informatici.

2.1.2 Attacchi Locali

Tra gli attacchi locali possiamo trovare ad esempio le connessioni tramite porta OBD, che normalmente viene utilizzata da meccanici specializzati per poter accedere alla centralina e controllarne i codici di errore, ma che, se mal intenzionalmente utilizzata, offre inevitabilmente un punto di ingresso verso la rete di dispositivi interna.

Tra le più comuni vulnerabilità conosciute, legate all'industria automobilistica, possiamo citare[5]:

- Chiave remota
  Sfruttando alcune vulnerabilità presenti sulle autovetture che implementano la tecnologia KeyLess (consente all'autista di aprire e chiudere l'autoveicolo, senza dover premere alcun tasto sulla chiave), è possibile ingannare i protocolli

di autenticazione, guadagnando così l'accesso al veicolo senza far scattare alcun allarme.

- Attacchi al sistema multimediale
  Utilizzando vulnerabilità nel sistema multimediale dell'autoveicolo, è possibile guadagnare l'accesso non autorizzato all'ECU del veicolo, compromettendone l'integrità e la sicurezza.

- Attacco di tipo Bruteforce alla rete
  Questo tipo di attacco mira a testare tutte le possibili combinazioni possibili fino a trovare le credenziali per l'accesso alla rete, causando così possibili fughe o perdite di dati, fino ad arrivare al possibile furto del veicolo.

- Attacchi di tipo Phishing
  Questo tipo di attacco non punta direttamente all'autoveicolo, ma mira ai dipendenti delle aziende automobilistiche: applicando tecniche di ingegneria sociale, si inducono i dipendenti delle aziende a rivelare informazioni sensibili, che possono fornire, ai malintenzionati, l'accesso a funzionalità di sistema o a dati sensibili.

- Dispositivi post produzione compromessi
  Fanno parte di questa categoria, tutti i dispositivi installati e collegati all'autoveicolo, una volta acquistato dall'utente finale, quali ad esempio, dispositivi forniti dalla Società di assicurazione, oppure smartphones connessi al sistema multimediale: tutti questi dispositivi forniscono ad hacker malintenzionati, ulteriori punti d'accesso, da poter potenzialmente sfruttare.

- Attacchi tramite Ransomware
  Tipologia di attacchi in cui il sistema bersaglio viene criptato, richiedendo al proprietario una somma in denaro per poterlo sbloccare nuovamente. Vittime di questo tipo di attacco è tutta la filiera automobilistica, comprendendo i costruttori, i venditori e gli utenti finali, portando a perdite economiche o possibili interruzioni dei servizi.

- Vulnerabilità dell'infrastruttura delle stazioni di ricarica per veicoli elettrici
  Tramite lo sfruttamento di vulnerabilità nei software delle colonnine di ricarica, generalmente mediante malware, è possibile fermare il corretto funzionamento della stazione di ricarica, generando così un malfunzionamento del processo di ricarica, impattando così sulle funzionalità del veicolo.

Lo scenario presentato mostra come tutta la filiera automobilistica abbia bisogno di un'infrastruttura sicura e protetta in quanto, ogni singolo componente può essere obiettivo di attacchi malevoli a diversi livelli: per questo motivo è stato necessario avere una regolamentazione completa e coerente per aiutare i costruttori di autoveicoli a rendere sufficientemente sicuri i propri progetti.

Capitolo 3

Norme e Regolamentazioni

3.1 ISO/SAE 21434 - Cybersecurity in ambiente Automobilistico

ISO è l'Organizzazione Internazionale per la Normazione[6], è il più importante organismo, a livello internazionale, che si occupa della definizione di norme tecniche, riconosciute a livello mondiale, con lo scopo di allineare tutte le nazioni verso uno standard comune. SAE International è una associazione globale formata da più di 128,000 ingegneri e relativi esperti tecnici nelle industrie Aerospaziali, Automobilistiche e Veicolo-Commerciali. Grazie al fatto di essere costituita da personale volontario che opera come individuo singolo, non come rappresentante della propria organizzazione, è riconosciuta apertamente come parte terza indipendente da qualunque processo industriale, ne consegue che i suoi standard rappresentano un ottimo contenuto tecnico, sviluppato tramite un processo collaborativo aperto e trasparente.
La normativa ISO/SAE 21434 riguarda l'applicazione della Cybersecurity a sistemi elettrici e elettronici (E/E) contenuti all'interno di veicoli stradali. Il documento include: un vocabolario, una lista di obiettivi, requisiti e linee guida relativi alla cybersecurity in modo tale da formare un piano base, per la comprensione della materia, attraverso tutta la catena di costruzione del prodotto finale.
Questo documento aiuta le organizzazioni nei processi di:

- definizione di politiche e processi riguardo la cybersecurity
- gestione dei rischi relativi alla cybersecurity
- creazione di una cultura riguardo alla cybersecurity

La normativa è strutturata secondo quanto mostrato in Figura 3.1 e comprende:

1. Scopo del Documento
2. Riferimenti ad altre Normative
3. Termini, Definizioni e Termini Abbreviati
4. Considerazioni Generali
5. Gestione della Cybersecurity all'interno dell'Organizzazione
6. Gestione della Cybersecurity relativa al Progetto
7. Distribuzione delle Attività relative alla Cybersecurity
8. Attività di Cybersecurity continuative
9. Fase concettuale
10. Fase di sviluppo del prodotto
11. Fase di Validazione della Cybersecurity
12. Fase di Produzione
13. Fase di Operatività e Manutenzione
14. Fine del supporto di Cybersecurity e Ritiro del prodotto
15. Metodi per l'analisi delle vulnerabilità e dei rischi.

Ciascuna sezione, a partire dalla numero 5 fino alla numero 15, prevede degli obiettivi, richiede alcuni documenti come dati di ingresso e restituisce altri documenti (denominati "work products") come prodotto di uscita, i quali saranno poi necessari per le fasi successive.

1. Scopo del Documento

Come già citato in precedenza, questo documento specifica i requisiti ingegneristici per la la gestione dei rischi relativi alla Cybersecurity applicati alle fasi di progettazione, sviluppo del prodotto, produzione, operatività, mantenimento e ritiro di sistemi Elettrici/Elettronici (E/E) all'interno di veicoli stradali. Viene definita una struttura che include i requisiti per i processi di cybersecurity ed un linguaggio comune per comunicare e gestire i rischi relativi a questo ambito.
Di questo documento è importante far notare che non prescrive alcuna tecnologia specifica o soluzione particolare relativa alla cybersecurity, impone solamente che i rischi vengano identificati e gestiti, senza prescrivere il come, lasciando libertà all'azienda di implementare le misure ritenute più sicure, salvo poi sottoporle ad un processo di verifica e validazione della corretta implementazione del processo.

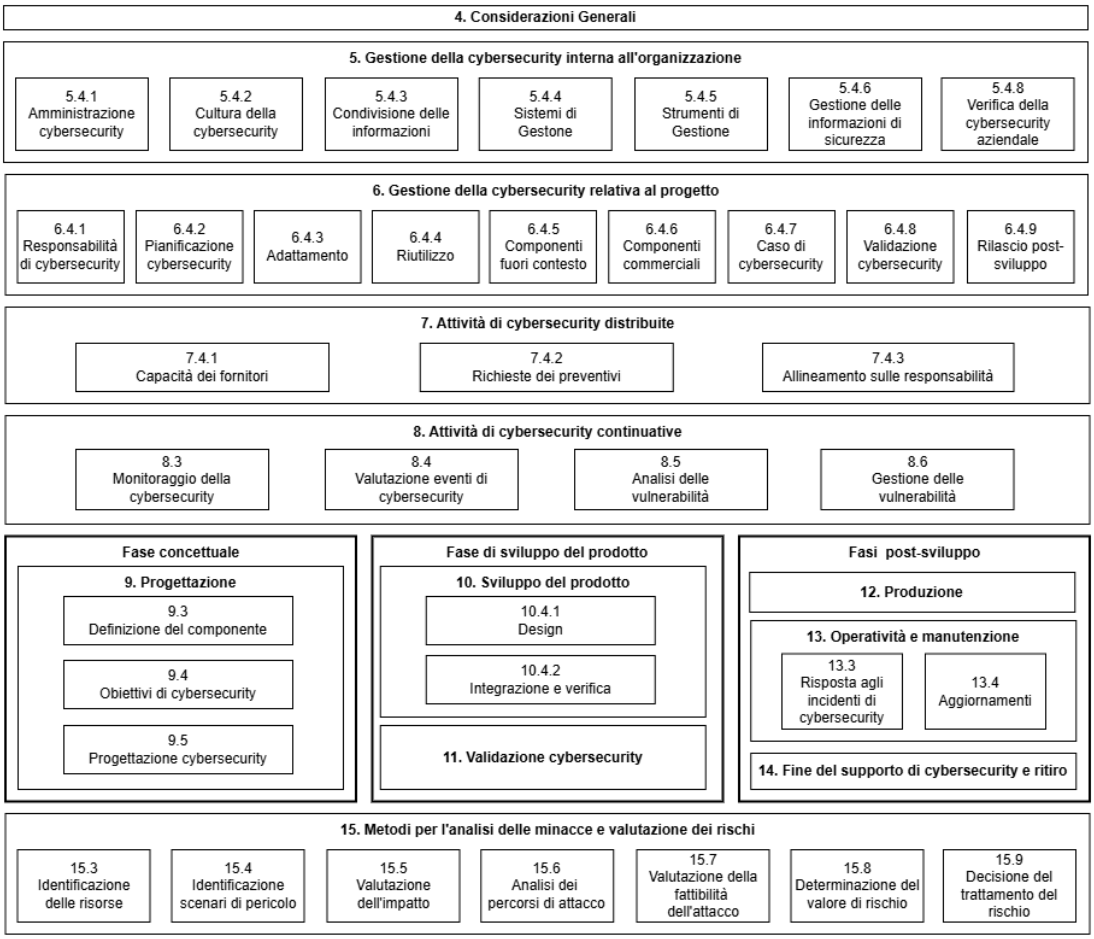

Figura 3.1: Struttura della Normativa ISO/SAE 21434

2. Riferimenti ad altre Normative

L'unica normativa esterna citata da questo documento è la ISO 26262-3:2018 relativa alla Sicurezza Funzionale dei Veicoli Stradali, indicando nello specifico la sezione numero 3, riguardante la fase concettuale di progettazione.

3. Termini, Definizioni e Termini Abbreviati

Nella prima parte è contenuta una lista di definizioni dei termini utilizzati all'interno del documento, in modo tale che non ci siano incomprensioni nella lettura dello stesso, comprensivi di riferimenti in caso di collegamento tra più termini.
Nella seconda parte è presente un elenco di tutte le abbreviazioni importanti e il

relativo significato esteso, in modo tale da poterlo recuperare facilmente nel caso in cui non lo si ricordasse durante la lettura del documento.

4. Considerazioni Generali

In questa sezione viene specificata la definizione di "oggetto", secondo cui questo è l'insieme di tutte le componenti elettroniche, hardware e software, che in un veicolo concorrono alla realizzazione di una funzione specifica a livello dell'autoveicolo (es. la frenata).
Una volta creata questa definizione, viene specificato che questo documento è limitato agli oggetti che sono rilevanti per le questioni di cybersecurity, di conseguenza descrive l'applicazione della cybersecurity dalla prospettiva del singolo oggetto, e non del sistema nella sua interezza.
Lo schema consigliato per l'organizzazione generale della Gestione dei Rischi relativi alla Cybersecurity all'interno di un'azienda, viene applicato attraverso tutte le fasi di progettazione, sviluppo, produzione, operatività, mantenimento e ritiro di un prodotto, come indicato nella Figura 3.2.

Figura 3.2: Gestione dei Rischi di Cybersecurity nelle fasi del progetto

L'obiettivo è quello di identificare a priori ed esplorare potenziali azioni eseguite da avversari astratti con intenti malevoli, e comprendere il possibile danno che può conseguire dalla compromissione di un sistema E/E del veicolo. Il monitoraggio, la creazione di rimedi e i servizi per la denuncia di incidenti informatici, completano le fasi di progettazione e sviluppo del prodotto come un approccio reattivo che prende in considerazione anche l'evoluzione della tecnologia, e l'identificazione delle

vulnerabilità nei sistemi, prima che possano venire sfruttate in modo malevolo.
La strategia a cui si sta puntando è quella della cybersecurity "in profondità", cioè compresa in tutte le fasi che compongono il ciclo di vita del prodotto, in modo tale da avere alla fine un prodotto coerente, sicuro e ben definito.

5. Gestione della Cybersecurity all'interno dell'Organizzazione

Per fare in modo che la cybersecurity venga applicata in maniera efficiente, è necessario che i dipendenti che lavorano al progetto, siano correttamente formati riguardo ai temi della cybersecurity, e l'obiettivo di questa sezione è quello di istruire le organizzazioni su come mantenere la Governance aziendale ed una cultura aziendale sulla sicurezza informatica, includendo attività di informazione sui pericoli della cybersecurity ed un costante aggiornamento sulle principali novità del settore. Ne consegue che diventa necessario definire una serie di regole e processi a livello aziendale, che verranno giudicati da un ente esterno indipendente, per garantirne la conformità alla normativa stessa.
Gli obiettivi quindi sono:

a) Definizione di una politica per la cybersecurity e di processi e regole aziendali per il suo mantenimento;

b) Assegnazione delle responsabilità a personale competente e con il compito di far rispettare le politiche aziendali;

c) Implementazione della cybersecurity e gestione dell'interazione tra il processo di cybersecurity e i relativi processi preesistenti;

d) Gestione dei rischi relativi alla cybersecurity;

e) Istituzione e mantenimento di una cultura sulla cybersecurity all'interno dell'azienda;

f) Gestione dello scambio di informazioni relative alla cybersecurity;

g) Istituzione e mantenimento dei sistemi di gestione che supportano l'applicazione della cybersecurity ai processi;

h) Fornire prove del fatto che l'utilizzo di strumenti nei processi, non sia contrario all'applicazione delle tecniche di cybersecurity;

i) Eseguire una verifica della cybersecurity a livello di organizzazione;

I documenti prodotti da questa sezione sono dunque:

- Politica sulla Cybersecurity, insieme all'elenco di regole e processi applicati;

- Prove relative ai processi di gestione delle competenze e della gestione della consapevolezza aziendale riguardo alla cybersecurity;
- Prove di un sistema di gestione dell'organizzazione;
- Prove dell'analisi e della gestione degli strumenti utilizzati;
- Rapporto sulla verifica delle competenze aziendali in materia di cybersecurity.

6. Gestione della Cybersecurity relativa al Progetto

Una volta verificato che a livello aziendale ci siano i presupposti per una corretta gestione della cybersecurity all'interno di un progetto, bisogna anche dimostrare di averli applicati, perciò in questa sezione vengono riportati i requisiti relativi alla gestione della cybersecurity, e delle sue attività, per uno specifico progetto. Sono inclusi in questa sezione anche l'assegnazione delle responsabilità e la pianificazione delle attività di cybersecurity. Questo documento è volutamente generico, in modo tale da poter essere applicato ad una grande varietà di oggetti e componenti.
Viene anche tenuto conto del fatto che alcuni oggetti, vengono progettati e sviluppati in maniera "out-of-context", cioè senza una destinazione specifica, in modo tale da essere adattabili a più contesti per cui un altro costruttore deciderà di utilizzarli: in questi casi non è possibile specificare il contesto di utilizzo del componente, perciò il costruttore è autorizzato a fare delle assunzioni sul possibile utilizzo futuro dell'oggetto, e basandosi su questo, certificare l'applicazione dei meccanismi di cybersecurity.
La verifica della cybersecurity giudica in maniera imparziale il livello di sicurezza di un oggetto o componente, ed il suo risultato è il valore necessario per la decisione sul proseguimento del progetto alla fase di post-sviluppo.
Gli obiettivi di questa sezione quindi sono:

a) assegnazione delle responsabilità riguardanti le attività di cybersecurity all'interno del progetto;
b) pianificazione delle attività di cybersecurity, includendo quelle relative all'adattamento di componenti esterni alle specifiche del progetto;
c) esecuzione di una verifica delle proprietà di cybersecurity;
d) decisione sul proseguimento dell'oggetto per la fase di post-sviluppo.

Sono inoltre specificate tutte le caratteristiche necessarie per quanto riguarda la persona che ha il compito di valutare le proprietà di cybersecurity, sotto forma di livello di indipendenza dal progetto (esterno al progetto, esterno al dipartimento o esterno all'azienda), di livello di conoscenza e di cosa e come deve valutare nella

fase di test e verifica.
I documenti prodotti in questa sezione sono dunque:

- Piano delle attività di cybersecurity;
- Il caso relativo all'oggetto sotto osservazione;
- Rapporto sulla verifica della cybersecurity;
- Rapporto sul proseguimento alla fase di post-sviluppo.

7. Distribuzione delle Attività relative alla Cybersecurity

In questa sezione vengono discusse le interazioni tra fornitori di componenti e produttori finali, nei casi in cui le attività di produzione dei componenti siano distribuite, in modo tale da avere ben definite le responsabilità di ognuno in termini di cybersecurity. Per garantire questo allineamento, è prevista una procedura secondo la quale, il fornitore del componente, è tenuto a dimostrare, al cliente, la sua capacità di poter ottemperare a tutte le attività relative alla cybersecurity, previste dalla normativa, quali ad esempio le prove di una processo aziendale interno per la gestione della cybersecurity.
L'obiettivo di questa sezione è quindi quello di allineare fornitore e cliente su una stessa decisione riguardo a chi deve occuparsi di una determinata attività di cybersecurity (e quindi chi ne è responsabile), e di fornire alla controparte le prove di essere in grado di ottemperare ai requisiti indicati nella normativa. L'unico documento prodotto in questa sezione è l'accordo sulle interfacce della cybersecurity, firmato e accettato da entrambe le parti.

8. Attività di Cybersecurity continuative

Questa sezione contiene la descrizione di tutte quelle attività che vengono svolte durante tutte le fasi del ciclo di vita di un progetto, e che servono a garantirne la sicurezza fino alla fine del periodo di supporto.
Gli obiettivi di questa sezione sono:

a) monitoraggio e collezione di informazioni di sicurezza informatica per l'identificazione di eventi di cybersecurity;

b) analisi e valutazione degli eventi segnalati e determinazione dell'effettiva presenza di una debolezza in un oggetto o componente;

c) identificazione delle vulnerabilità derivanti dalle debolezze rilevate;

d) analisi delle vulnerabilità con lo scopo di valutare se una particolare debolezza può essere sfruttata da un attaccante o meno;

e) gestione delle vulnerabilità identificate;

9. Fase concettuale

In questa fase vengono presi in considerazione le funzionalità a livello del veicolo nella sua interezza e, per ciascun oggetto che le implementa, viene definito il suo ambiente operativo, creando il modello per le analisi successive. Vengono anche specificati gli obiettivi di cybersecurity per ciascun oggetto, i quali sono i requisiti di più alto livello, e per farlo, vengono prima analizzati i rischi di cybersecurity (utilizzando anche metodi descritti al punto 15) e poi catalogati in base alla loro pericolosità.
Perciò gli obiettivi di questa sezione sono:

a) definizione di un oggetto, del suo ambiente operativo e delle sue interazioni nel contesto della cybersecurity;

b) definizione degli obiettivi di cybersecurity;

c) definizione del Piano Concettuale di Cybersecurity per raggiungere gli obiettivi.

Per ciascun oggetto vanno quindi identificati i suoi confini, le sue funzionalità e la sua architettura preliminare in modo tale da poter estrapolare tutti i vincoli di cybersecurity che il prodotto finale dovrà rispettare. Tutto questo contribuisce al primo documento di output di questa sezione, identificato come "Definizione dell'Oggetto".
Nella seconda parte, viene utilizzato il documento di Definizione dell'Oggetto con l'obiettivo di identificare:

a) risorse;

b) scenari con minacce;

c) valutazione dell'impatto;

d) analisi dei percorsi di attacco;

e) classificazione della fattibilità dell'attacco;

f) determinazione dell'effettivo valore di rischio.

Gli obiettivi di Cybersecurity sono dei requisiti per proteggere le risorse in uno scenario di minaccia identificato.
Il tipo di analisi sopra citata è chiamata TARA il quale è l'acronimo di Threat Analysis and Risk Assessment, che tradotta è "Analisi delle Minacce e Valutazione dei Rischi".
Al termine di questa analisi, viene condotta una fase di verifica con lo scopo di confermare:

a) completezza e correttezza dei risultati dell'analisi;

b) completezza, correttezza e consistenza delle decisioni prese per contrastare i rischi;

c) completezza, correttezza e consistenza degli Obiettivi di Cybersecurity.

I documenti prodotti da questa seconda parte infine sono:

1. Rapporto sulla TARA;
2. Lista degli Obiettivi di Cybersecurity;
3. Lista delle affermazioni e dei requisiti della cybersecurity;
4. Rapporto sulla verifica degli Obiettivi di Cybersecurity.

In conclusione, per ciascun obiettivo di cybersecurity, va definito il meccanismo operativo che concorre alla garanzia dell'obiettivo, e per ciascun meccanismo va analizzata la sua interazione con gli altri meccanismi implementati e con la funzionalità dell'oggetto.
La descrizione dei meccanismi di cybersecurity, va a completare la specifica e l'allocazione dei requisiti di cybersecurity e dei requisiti dell'ambiente operativo, i quali tutti insieme costituiscono il Piano Concettuale di Cybersecurity, che è il vero documento di output di questa sezione. Infine è presente una fase di verifica per garantire la correttezza, completezza e consistenza con gli obiettivi di cybersecurity precedentemente descritti.

10. Fase di sviluppo del prodotto

In questa fase vengono descritte le specifiche dei requisiti di cybersecurity e della struttura architetturale, concludendo con la descrizione dell'integrazione tra le due e le attività di verifica. Queste attività sono eseguite in maniera iterativa, procedendo per raffinamenti successivi, fino ad ottenere una descrizione completa e coerente con tutti i requisiti precedentemente specificati.
Le specifiche relative alla cybersecurity, dovrebbero essere basate su:

- specifiche di cybersecurity provenienti da livelli superiori o da astrazioni architetturali;
- meccanismi di cybersecurity selezionati per l'implementazione;
- progetti architetturali preesistenti.

Le specifiche di cybersecurity devono poi essere verificate per garantirne la completezza, correttezza e consistenza con le specifiche di cybersecurity dei livelli più alti dell'astrazione architetturale. I metodi di verifica possono includere: revisioni, analisi, simulazioni e prototipi.
Infine è presente una fase di Integrazione e Verifica delle specifiche, per garantirne una capacità sufficiente a supportare le funzionalità definite nelle specifiche di cybersecurity, e la conformità con il modello progettato, la struttura del progetto e le linee guida relative alla scrittura del codice. Tra i principali metodi di analisi possiamo trovare:

- test basati su requisiti;
- test sulle interfacce;
- valutazione dell'utilizzo delle risorse;
- verifica del flusso di controllo e del flusso di dati;
- analisi dinamica;
- analisi statica.

Nel caso in cui venga adottata una tecnica di verifica basata sui test, possono essere selezionati specifici ambienti da analizzare separatamente dagli altri, prevedendo una successiva integrazione del sistema. Tra i metodi per creare i casi di test possiamo trovare:

- analisi dei requisiti;
- generazione e analisi di classi di equivalenza;
- analisi di valori di confine;
- indovinare i possibili errori basandosi sulla conoscenza e/o sull'esperienza.

Una volta eseguiti i test, bisogna però verificarne la copertura, cioè quante parti dell'oggetto sono state effettivamente testate, utilizzando metriche ben definite. La fase di test dovrebbe essere eseguita in maniera da assicurare che tutte le debolezze e vulnerabilità non identificate, che rimangono nel componente, siano il minimo numero possibile. Tra i principali metodi di test possiamo trovare:

- test funzionale;
- scansione delle vulnerabilità;
- test con input casuale (fuzz testing);

- test di penetrazione (penetration testing).

Lo scopo è quello di analizzare le debolezze identificate in cerca di vulnerabilità, e gestire quelle che vengono effettivamente riconosciute come tali.
I documenti finali prodotti da questa sezione sono:

- specifiche di cybersecurity;
- requisiti di cybersecurity per la fase di post-sviluppo;
- Documentazione sulla modellazione del prodotto, linguaggi di programmazione e linee guida sulla programmazione;
- rapporto sulla verifica delle specifiche di cybersecurity;
- elenco delle debolezze identificate durante lo sviluppo del prodotto;
- specifiche sull'integrazione e la verifica;
- rapporto sull'integrazione e la verifica.

11. Fase di Validazione della Cybersecurity

In questa sezione sono descritte le attività per la validazione della cybersecurity degli oggetti a livello di integrazione nel veicolo: l'oggetto in questione è considerato all'interno del suo ambiente operativo, insieme alla configurazione identificata per la produzione in serie, in modo tale da essere analizzato il più vicino possibile alle sue future condizioni di utilizzo.
Gli obiettivi di questa fase sono quindi:

a) validazione degli obiettivi di cybersecurity;

b) conferma che i componenti soddisfino i requisiti di cybersecurity;

c) conferma che nessun irragionevole rischio rimanga all'interno del sistema.

Le attività di validazione possono includere: la revisione dei documenti di output delle fasi precedenti, test di penetrazione per dimostrare l'adeguatezza e il raggiungimento degli obiettivi di cybersecurity e infine la revisione di tutti i rischi identificati e gestiti.
Come unico documento di output di questa sezione si ha il Rapporto sulle Validazioni effettuate.

12. Fase di Produzione

La fase di produzione riguarda le attività di costruzione e assemblaggio del componente all'interno del veicolo; durante questa fase viene creato un Piano di Controllo della Produzione il quale ha lo scopo di garantire che i requisiti di cybersecurity, per la fase di post-sviluppo, vengano applicati al componente e che, durante le fasi della produzione, non vengano introdotte altre vulnerabilità.
Il Piano di Controllo della Produzione deve includere:

a) sequenza dei passaggi per applicare i requisiti di cybersecurity per la fase di post-sviluppo;

b) strumenti per la produzione e gli equipaggiamenti utilizzati;

c) controlli di cybersecurity per prevenire eventuali alterazioni durante il processo di produzione;

d) metodi che confermino che i requisiti di cybersecurity per la fase di post-sviluppo siano rispettati.

Il Piano di Controllo della Produzione è l'unico documento prodotto in questa fase.

13. Fase di Operatività e Manutenzione

In questa sezione vengono descritti i processi di risposta agli incidenti segnalati e quello di aggiornamento di un oggetto o componente. Gli aggiornamenti sono modifiche fatte su un oggetto durante la fase di post-sviluppo il quale può includere maggiori informazioni, oppure fornire miglioramenti funzionali o eliminare delle nuove vulnerabilità appena scoperte.
Gli obiettivi di questa fase possono quindi essere identificati come:

a) determinare e implementare delle azioni per rimediare e gestire i nuovi incidenti di cybersecurity riportati;

b) mantenere il livello di cybersecurity durante e dopo gli aggiornamenti successivi alla produzione, fino alla fine del periodo di supporto della cybersecurity.

Per ciascuna segnalazione di incidente di cybersecurity è utile ricavare ulteriori informazioni relative alla vulnerabilità che ha causato il problema, successivamente per ciascuna vulnerabilità, effettuarne l'analisi.
A questo proposito viene suggerita una procedura per la creazione di un Piano di Gestione degli Incidenti di Cybersecurity, il quale deve includere:

1. le azioni per correggere le vulnerabilità;

2. un piano di comunicazione della problematica;

3. assegnazione delle responsabilità relative alle azioni correttive da implementare;
4. una procedura per la collezione di nuove informazioni relative all'incidente in questione;
5. un metodo per determinare il progresso nella risoluzione dell'incidente;
6. azioni per la chiusura della segnalazione.

Per quanto riguarda invece gli aggiornamenti e le funzionalità che risentono delle modifiche, l'unico vincolo è che devono essere sviluppati in conformità con quanto detto ai punti precedenti.

14. Fine del supporto di Cybersecurity e Ritiro del prodotto

Ritiro del prodotto è differente dalla fine del supporto di Cybersecurity in quanto, un organizzazione può decidere di terminare il supporto alla cybersecurity di un prodotto, ma questo prodotto può ancora continuare a funzionare nell'ambiente per cui è stato progettato. Entrambe le situazioni presentano implicazioni a livello di cybersecurity, ma queste vengono comunque considerate separatamente. La fine del supporto alla cybersecurity e il ritiro sono considerati nelle fasi di Concetto e Sviluppo.
Gli obiettivi di questa fase sono quindi:

a) comunicazione della fine del supporto della cybersecurity;
b) abilitare il ritiro per vecchiaia dei componenti rispetto alla cybersecurity.

A tal proposito è necessario creare una procedura per la comunicazione ai clienti della fine del supporto, quando l'organizzazione ne decide la fine, quali ad esempio una comunicazione tramite un messaggio all'autoveicolo, il quale mostrerà poi una notifica all'utilizzatore.

15. Metodi per l'analisi delle vulnerabilità e dei rischi

Generalmente chiamati "Metodi TARA" in quanto il loro scopo è quello di valutare quanto un utente della strada può essere coinvolto da una situazione di pericolo; l'analisi è condotta dal punto di vista dell'utente della strada che sperimenta la situazione. I metodi definiti in questa sezione sono moduli generali che possono essere sistematicamente invocati in qualunque punto del ciclo di vita del componente, e comprendono:

- identificazione delle risorse;
- identificazione degli scenari di pericolo;

- valutazione del valore di impatto;
- analisi dei percorsi di attacco;
- valutazione della fattibilità dell'attacco;
- determinazione del valore di rischio;
- decisione su come trattare il rischio in questione.

Ciascuna risorsa, la cui compromissione di una proprietà di cybersecurity può condurre ad uno scenario di danno, deve essere identificata sulla base di:

- analisi della definizione dell'oggetto;
- calcolo della valutazione dell'impatto;
- derivazione delle risorse sensibili fornite dagli scenari di pericolo;
- utilizzo di categorie predefinite.

Per scenario di pericolo si intende una qualunque relazione tra una funzionalità di un componente ed una conseguenza avversa, oppure una descrizione di un danno ad un utente della strada oppure semplicemente delle risorse rilevanti. Perciò gli scenari di pericolo devono essere identificati, in modo tale da poterne comprendere:

- risorsa che ne risente;
- quale proprietà di cybersecurity della risorsa viene compromessa;
- causa della compromissione della proprietà.

Una volta definiti gli scenari di pericolo e quelli che portano a danni effettivi, si effettua una classificazione degli stessi, identificando in primo luogo a quale categoria di impatto appartengono tra: Sicurezza, Finanziario, Operatività o di Privacy (S, F, O, P). Successivamente viene valutata la severità dell'impatto dello scenario di danno secondo uno dei seguenti valori:

- severo;
- elevato;
- moderato;
- ignorabile.

Per la valutazione degli impatti relativi alla categoria Sicurezza, si possono utilizzare le categorizzazioni derivanti dalla normativa ISO 26262-3:2018 (valore di ASIL). Una volta determinata la severità dello scenario di pericolo, questo va ulteriormente analizzato per determinare i possibili percorsi di attacco. Generalmente un'analisi dei percorsi di attacco può essere basata su due tipi di approccio:

- approccio top-down, nel quale vengono dedotti i percorsi di attacco, analizzando i diversi modi in cui uno scenario di pericolo può essere realizzato;
- approccio bottom-up, in cui si costruisce il percorso di attacco, partendo dalla lista di vulnerabilità identificate.

Una volta determinati i percorsi di attacco, si procede con l'analisi della fattibilità, determinandone il valore secondo la tabella 3.1.

Fattibilità dell'attacco	**Descrizione**
Alta	Eseguibile con poche difficoltà
Media	Eseguibile con media difficoltà
Bassa	Eseguibile con alta difficoltà
Molto bassa	Eseguibile con molto alta difficoltà

Tabella 3.1: Classificazione della fattibilità di un attacco.

Il metodo utilizzato per classificare la fattibilità degli attacchi dovrebbe essere basato su uno dei seguenti approcci:

a) basandosi sul potenziale dell'attacco: in questo caso la valutazione della fattibilità dell'attacco dovrebbe essere determinata sulla base di:
   - tempo impiegato;
   - esperienza dell'attaccante;
   - conoscenza del componente;
   - finestra di opportunità;
   - equipaggiamento.

b) basato sul CVSS: in questo caso la valutazione della fattibilità dell'attacco dovrebbe essere calcolata basandosi sulla sfruttabilità delle metriche base:
   - vettore di attacco;
   - complessità dell'attacco;
   - privilegi richiesti;
   - interazioni dell'utente.

c) basandosi sul vettore di attacco: in questo caso la valutazione della fattibilità dell'attacco dovrebbe essere determinata basandosi sulla valutazione del principale vettore di attacco.

Una volta determinati gli scenari di pericolo, la possibile entità del danno, i relativi percorsi di attacco e l'effettiva fattibilità dell'attacco, per ciascuno scenario di pericolo, si può procedere con la determinazione del valore di rischio effettivo, il quale sarà rappresentato da un valore compreso tra 1 e 5 (estremi inclusi), dove il valore 1 rappresenta il minimo rischio.
Infine si può concludere con la determinazione delle azioni da intraprendere per gestire ciascun rischio dove, per ogni scenario di pericolo, una delle seguenti azioni viene selezionata:

- evitare il rischio, semplicemente rimuovendo la sorgente del pericolo;
- riduzione del rischio, tramite implementazione di ulteriori meccanismi;
- condivisione del rischio, informando tramite contratto l'utente finale o interagendo con un ente assicurativo;
- trattenere il rischio, che consiste nell'accettare il rischio, nel caso in cui sia sufficientemente basso;

Ulteriori allegati

Alla fine del documento sono presenti alcuni allegati ulteriori alla normativa, con lo scopo di chiarire, semplificare ed esplicare meglio concetti indicati nel documento. Tra questi troviamo:

a) **Allegato A:** Sommario delle attività di cybersecurity e dei documenti prodotti.
Consiste in una enorme tabella in cui sono elencate tutte le attività di Cybersecurity sopra elencate (a partire dal punto 5) e specificando per ciascuna di esse i documenti prodotti, in modo tale da aver un elenco preciso e compatto di tutti i documenti previsti.

b) **Allegato B:** Esempi di cultura di cybersecurity.
Al suo interno è presente una tabella che elenca alcune situazioni comuni mettendo a confronto i casi che indicano una scarsa cultura sulla cybersecurity contro quelli che invece ne dimostrano una corretta applicazione. Si tratta generalmente di cultura aziendale e di processi all'interno di essa, ma fornisce un'idea dettagliata della situazione attuale dell'organizzazione riguardo alla cultura sulla cybersecurity, fornendo un esempio di paragone.

c) **Allegato C:** Esempio di un Documento per l'accordo sulle interfacce di Cybersecurity.
Questo documento viene utilizzato nel caso in cui diverse organizzazioni siano coinvolte nella progettazione di un componente, in modo tale da raggiungere un accordo sulle responsabilità e i ruoli a cui spettano, sul livello di accesso alle informazioni e altre condizioni burocratiche.

d) **Allegato D:** Rilevanza in cybersecurity, criteri ed esempi.
Questo allegato propone alcuni metodi ed esempi per determinare se un componente è rilevante dal punto di vista della cybersecurity, su cui quindi va applicata questa normativa. Il metodo proposto è quello esposto nella figura 3.3, la quale esprime un semplice processo per valutare la rilevanza di un componente per la cybersecurity.

e) **Allegato E:** Livelli di sicurezza della Cybersecurity (CAL).
Questo allegato descrive uno schema di classificazione che può essere utilizzato per dimostrare il rigore impiegato nell'applicazione della cybersecurity, in modo tale da garantire che la protezione delle risorse di un componente sia adeguatamente sviluppata. Questo livello di CAL è indirettamente collegato al valore rischio, ma non può essere direttamente determinato da questo, in quanto il valore del rischio è dinamico ed evolve nel tempo, mentre il valore di CAL esprime un livello di rigore che rimane fisso nel tempo, durante tutta la durata del progetto. Il rigore viene espresso sotto forma di tempo e risorse impiegate per garantire i requisiti di cybersecurity, comprendendo le fasi di analisi, implementazione e test, definendo ad esempio le tipologie di test da applicare (più il valore di CAL è elevato, più i test devono essere esaustivi), o il grado di indipendenza al momento della verifica di un documento (diverso da chi l'ha creato, esterno al progetto, esterno al dipartimento, etc.).

f) **Allegato F:** Linee guida per la valutazione dell'impatto.
Questo allegato fornisce dei criteri di esempio per la valutazione dell'impatto per le seguenti categorie:

   (a) Danni alla sicurezza personale (ferite lievi, gravi, pericolo di vita, etc.);

   (b) Danni finanziari (inconvenienze, conseguenze legali, etc.);

   (c) Danni operativi (degradazione di una funzione, perdita di una funzionalità importante o necessaria, etc.);

   (d) Danni alla Privacy (dal punto di vista dell'utente della strada).

g) **Allegato G:** Linee guida per la valutazione della fattibilità di un attacco.
Questo allegato fornisce indicazioni su come valutare il potenziale di un attacco basandosi sugli approcci consigliati:

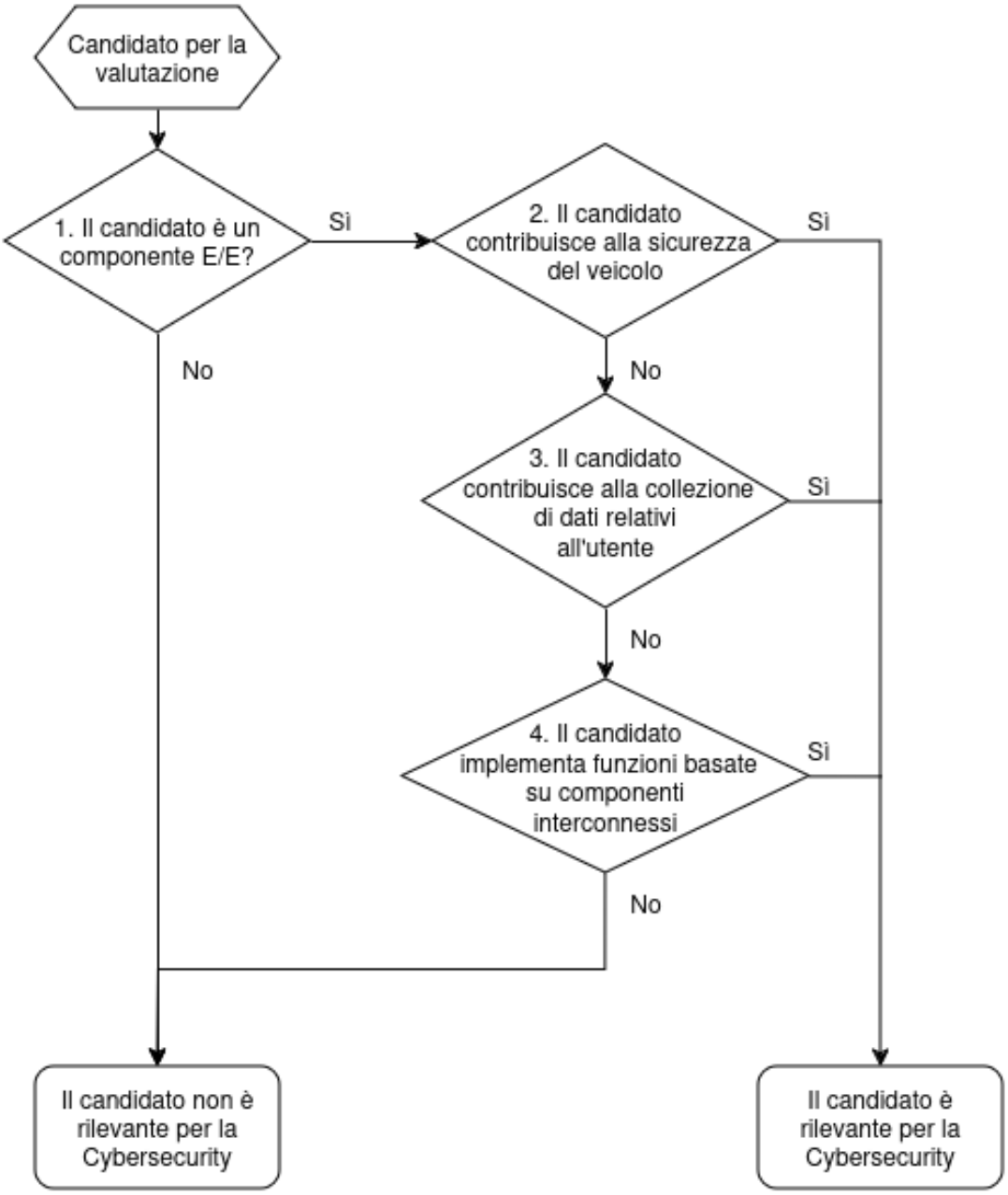

Figura 3.3: Esempio di metodo per determinare la rilevanza in cybersecurity

a) basandosi sul potenziale dell'attacco;

b) basato sul CVSS;

c) basandosi sul vettore di attacco.

Per ciascuno di esse esamina le caratteristiche importanti da valutare, al fine di ottenere un valore ragionevole.

h) **Allegato H:** Esempi di applicazione dei metodi di TARA.
Questo allegato consiste in un esempio di applicazione di un'analisi di tipo TARA, applicata ad un componente quale è in questo caso il sistema dei fari in un autoveicolo, eseguendo tutti i punti dell'analisi:

   a) identificazione delle risorse;
   b) valutazione dell'impatto;
   c) identificazione degli scenari di pericolo;
   d) analisi dei percorsi di attacco;
   e) valutazione della fattibilità degli attacchi;
   f) determinazione del valore di rischio;
   g) decisione delle azioni da intraprendere per gestire il rischio;

3.2 UNECE R155

L'UNECE è l'acronimo di United Nations Economic Commission for Europe, cioè l'ente preposto dalle Nazioni Unite per tutto quello che riguarda l'emanazione di Regolamenti relativi all'ambito Economico per gli stati membri. La normativa UNECE R155 è la regolamentazione delle Nazioni Unite, il cui titolo è "Disposizione uniformata riguardo all'approvazione di veicoli rispetto alla cybersecurity e al sistema di gestione della cybersecurity"[7], la quale ha lo scopo di essere un unico punto di riferimento per tutti i paesi delle Nazioni Unite, in modo da rendere possibile anche la mutua e reciproca accettazione dei processi svolti. Questo regolamento viene applicato su tutti i veicoli, per quanto concerne la cybersecurity, di categoria M (veicoli per il trasporto di persone), N (veicoli per il trasporto di merci), O (rimorchi) se equipaggiati con almeno una ECU e L6/L7 (quadricicli leggeri e non) se equipaggiati con una funzionalità di guida autonoma superiore al livello 3.[8]
La struttura della normativa è la seguente:

1. Obiettivi;
2. Definizioni;
3. Richiesta di approvazione;
4. Simboli di conformità;

5. Approvazione;
6. Certificato di conformità del Sistema di Gestione della Cybersecurity;
7. Specifiche;
8. Modifiche ed estensioni del tipo di veicolo;
9. Conformità della produzione;
10. Sanzioni in caso di non conformità della produzione;
11. Termine definitivo della produzione;
12. Nomi e indirizzi dei Servizi Tecnici responsabili della conduzione dei Test di Approvazione, e delle Autorità per l'Approvazione;
13. Ulteriori allegati.

2. Definizioni

Contiene le definizioni per la terminologia tecnica utilizzata all'interno del documento (sono presenti per esempio quelle di rischio, minaccia, vulnerabilità, etc.), in modo tale da non avere dubbi sull'effettivo significato inteso dalla normativa.

3. Richiesta di approvazione

Questa sezione descrive la procedura per richiedere la Certificazione di Approvazione, la quale può essere richiesta dal costruttore del veicolo o da un loro debito rappresentante. Tra i documenti da consegnare troviamo:

- Una descrizione del tipo di veicolo (coerente con l'Allegato 1, descritto in seguito);
- il Certificato di Conformità del Sistema di Gestione della Cybersecurity (CSMS).

La documentazione dev'essere disponibile in due parti:

a) La documentazione formale per l'approvazione (coerente con i contenuti dell'Allegato 1) consegnata all'Autorità per l'Approvazione, o al suo Servizio Tecnico, utilizzata come riferimento di base per il processo di approvazione: questa documentazione deve rimanere disponibile alla consultazione per almeno 10 anni, a decorrere dal momento in cui la produzione del veicolo è definitivamente terminata.

b) eventuali altri documenti importanti per questa regolamentazione, possono essere conservati dal produttore, ma disponibili alla consultazione al momento dell'approvazione se necessario. Anche questi documenti devono essere mantenuti consultabili per almeno 10 anni successivi alla data di fine di produzione del veicolo.

4. Simboli di certificazione

Questo certificato va esposto visivamente e in un posto facilmente accessibile, specificato nel documento di approvazione, di qualunque veicolo che sia conforme al Tipo di Veicolo approvato sotto questa regolamentazione. Questo simbolo consiste in una lettera "E" inscritta all'interno di un cerchio, seguita da un numero distintivo della nazione che ha garantito l'approvazione. Inoltre è presente anche il numero di approvazione, che contraddistingue il Tipo di Veicolo (vedi Allegato 3 per un esempio).

5. Approvazione

Le Autorità di Approvazione devono garantire l'approvazione del Tipo di Veicolo, rispetto alla cybersecurity, solo ai veicoli che rispettano tutti i requisiti di questa regolamentazione. L'autorità in questione o il Servizio Tecnico devono verificare, tramite il controllo dei documenti, che il costruttore del veicolo abbia preso le misure necessarie a:

a) collezionare e verificare le informazioni richieste da questa regolamentazione, durante la fornitura del prodotto, in modo tale da dimostrare che tutti i rischi, riguardanti il fornitore, siano stati identificati e gestiti;

b) Documentare l'analisi dei rischi (condotta durante la fase di sviluppo), i risultati dei test e le mitigazioni applicate, includendo anche le informazioni del progetto a supporto dell'analisi dei rischi;

c) Implementare le misure di cybersecurity appropriate al Tipo di Veicolo

d) Rilevare e gestire possibili attacchi alla cybersecurity

e) Collezionare dati per supportare la rilevazione di attacchi informatici e di fornirgli una caratteristica forense, in modo tale da poter consentire l'analisi di successo o fallimento di un attacco.

L'Autorità di Approvazione deve verificare, mediante una fase di test su un veicolo, del tipo di cui è stata richiesta l'approvazione, che il produttore dello stesso ha implementato tutte le misure di cybersecurity elencate nei documenti consegnati. In caso di riscontro di uno o più requisiti di cybersecurity non soddisfatti, l'Autorità per l'Approvazione deve rifiutare l'emissione del certificato di conformità, ad esempio:

- analisi dei rischi non esaustiva da parte del costruttore;
- presenza di rischi identificati e non gestiti, o gestiti in maniera non proporzionale all'entità del rischio;
- assenza di un ambiente sicuro e dedicato, per l'esecuzione e la memorizzazione di software esterno, servizi, applicazioni e dati;
- fase di test, precedente alla richiesta di approvazione, non sufficiente a verificare l'efficacia delle contromisure informatiche applicate.

L'Autorità di Approvazione può anche negare la certificazione nel caso in cui non le siano state fornite sufficienti informazioni, da parte del costruttore, per verificare le proprietà di cybersecurity del veicolo.
L'ente di approvazione deve garantire di:

- possedere personale qualificato con capacità di cybersecurity e conoscenze specifiche relative all'analisi dei rischi in ambiente automobilistico;
- aver implementato procedure per la valutazione uniforme di tutti i richiedenti, in maniera conforme a questa regolamentazione.

Ciascun ente è tenuto anche alla pubblicazione dei metodi e criteri utilizzati per la valutazione delle richieste, presso un database comune creato dall'UNECE, in modo tale da poter essere condivise e riutilizzate per migliorare i servizi.

6. Certificato di conformità del Sistema di Gestione della Cybersecurity

La certificazione di conformità del Sistema di Gestione della Cybersecurity (CSMS) deve essere richiesta dal produttore del veicolo o da un suo legale rappresentante, ad un'Autorità di Approvazione preposta, consegnando il documento che ne descrive il processo, secondo l'esempio contenuto nell'Allegato 1. Con questo documento il produttore dichiara di essere in grado di eseguire i processi necessari per essere conformi a tutti i requisiti secondo questa Regolamentazione. Una volta verificati tutti i passaggi, l'autorità preposta è autorizzata ad emettere un Certificato di Conformità per il CSMS, il quale rimarrà valido per un periodo massimo di 3 anni, ad eccezione del caso in cui sia revocato. L'autorità di Approvazione, che ha emesso il certificato, può in ogni momento verificare che i requisiti siano ancora rispettati e, nel caso in cui riscontri delle violazioni, revocare il certificato con effetto immediato. L'azienda costruttrice ha l'obbligo di informare l'Autorità di Approvazione in caso di modifiche che influenzino la validità del Certificato di Conformità, in questo caso l'ente avrà il compito di valutare le modifiche effettuate e decidere se siano necessari ulteriori controlli per il rinnovo dello stesso.
Nel caso in cui un certificato per il CSMS scada o venga revocato per un qualunque

motivo, anche il Certificato per l'approvazione del Tipo di Veicolo viene revocato, in quanto questo si basava su un CSMS ormai più non valido.

7. Specifiche

In questa sezione vengono fornite ulteriori specifiche riguardo alla verifica del Sistema di Gestione della Cybersecurity e alle aree che questo deve coprire all'interno dell'azienda costruttrice. Viene specificato come il CSMS debba essere applicato durante le fasi di sviluppo, produzione e post-produzione di un veicolo all'interno di tutti i processi che concorrono:

a) processo per la gestione della cybersecurity all'interno dell'organizzazione;

b) processo per l'identificazione dei rischi dei Tipi di Veicoli;

c) processo per la valutazione, la categorizzazione e la gestione dei rischi identificati;

d) processo per verificare che i rischi identificati siano correttamente gestiti;

e) processi per eseguire test di controllo sulla cybersecurity di un Tipo di Veicolo;

f) processi utilizzati per garantire che l'analisi e la valutazione dei rischi siano costantemente aggiornate;

g) processi utilizzati per monitorare, rilevare e rispondere ad attacchi informatici, minacce informatiche e vulnerabilità sui veicoli, e quelli utilizzati per valutare se le misure di sicurezza precedentemente implementate siano ancora efficaci;

h) processi per la raccolta di dati su attacchi informatici tentati o che hanno avuto successo.

Viene anche specificato come il costruttore del veicolo debba dimostrare di essere in grado di poter rispondere e gestire vulnerabilità e pericoli informatici, che richiedono il suo intervento, entro un tempo ragionevole dalla segnalazione. Anche per questo motivo il monitoraggio di queste situazioni dev'essere continuo, includendo l'analisi dei dati dei veicoli già circolanti, in modo tale da determinare il prima possibile la presenza di vulnerabilità e minacce.
Il costruttore deve anche dimostrare di aver gestito, tramite il CSMS, le dipendenze che possono formarsi con fornitori esterni di componenti e/o servizi.

Dopo le specifiche sul CSMS e sui processi aziendali, sono presenti alcune specifiche sui requisiti del Tipo di Veicolo, quali ad esempio il fatto che, per l'approvazione di Tipi di Veicoli precedenti al 1 Luglio 2024, se il produttore può dimostrare che il veicolo non può essere costruito in conformità al suo CSMS, può comunque

ricevere l'approvazione di conformità, dimostrando di aver comunque considerato adeguatamente la cybersecurity durante le fasi di sviluppo e progettazione del Tipo di Veicolo in considerazione. Il costruttore è comunque tenuto a considerare anche i rischi derivanti dai suoi fornitori di componenti e servizi.
L'azienda è comunque tenuta ad effettuare un resoconto annuale, all'Autorità di Approvazione, contenente i risultati dei processi di monitoraggio, includendo tutte le informazioni relative a nuove vulnerabilità e attacchi informatici, a come sono stati implementati i meccanismi di contrasto e mitigazione, e informazioni relative a quelli che erano già presenti e alla loro effettiva efficacia. In caso venissero determinate delle lacune, l'ente di approvazione potrà richiedere al costruttore di rimediare a ciascuna inefficacia identificata. Nel caso peggiore, in cui l'Autorità di Approvazione ritenesse che il rapporto fornito non sia sufficiente, può procedere con la revoca del Certificato di Conformità del CSMS.

8. Modifiche ed Estensioni del Tipo di Veicolo

Ciascuna modifica del Tipo di Veicolo che riguarda le sue prestazioni tecniche rispetto alla cybersecurity e/o documentazioni richieste da questa regolamentazione, va dichiarata all'Autorità di Approvazione che ha approvato il Tipo di Veicolo. L'ente di approvazione dovrà di conseguenza:

1. Valutare le modifiche e determinare quali requisiti sono inficiati;
2. valutare se siano necessari ulteriori test rispetto a quelli precedentemente compiuti, e nel caso eseguirli;
3. comunicare la conferma, l'estensione o il rifiuto dell'approvazione mediante un modulo predefinito (vedi Allegato 2), specificando le modifiche in questione.

9. Conformità della Produzione

Il detentore del Certificato di Approvazione deve garantire che i risultati della conformità dei test di produzione siano disponibili, all'Autorità preposta, per un periodo di tempo predeterminato con l'autorità stessa, ma comunque inferiore ai 10 anni dopo la fine definitiva della produzione del veicolo. L'Autorità di Approvazione che ha garantito l'approvazione per il Tipo di Veicolo, può verificare in qualunque momento i metodi di controllo della conformità applicati in qualunque impianto di produzione. La frequenza normale per un'operazione di questo tipo è di circa 3 anni.

10. Sanzioni in caso di non conformità della produzione

In caso di valutazioni negative da parte dell'Autorità di Approvazione, riguardo al rispetto dei vincoli posti da questa normativa, o in caso di valutazione negativa dei

test condotti su un veicolo di esempio, l'ente può procedere alla revoca dell'approvazione, e comunicare la revoca a tutti coloro che sono parte integrante del sistema e che applicano quindi questa regolamentazione.

11. Termine definitivo della produzione

Al momento della dismissione completa della produzione di un veicolo che aveva ricevuto l'approvazione a questa regolamentazione, il produttore ha il compito di comunicarlo all'Autorità di Approvazione che aveva approvato il Tipo di Veicolo precedentemente, la quale procederà a segnare la produzione come "Terminata".

12. Nomi e indirizzi dei Servizi Tecnici responsabili della conduzione dei Test di Approvazione, e delle Autorità per l'Approvazione

Ciascuna nazione, che applica questa regolamentazione, deve comunicare alla Segreteria delle Nazioni Unite, i nomi e gli indirizzi dei Servizi Tecnici, responsabili per l'esecuzione dei test di approvazione, e delle Autorità di Approvazione dei Tipi di Veicolo che garantiscono le approvazioni e a cui bisogna inoltrare le certificazioni emanate in altre nazioni che applicano questa regolamentazione, per avere l'effettività anche nel territorio locale.

13. Ulteriori allegati

- **Allegato 1:** Documento delle Informazioni
  La prima parte di questo allegato contiene l'elenco delle informazioni necessarie per la richiesta di Approvazione del Tipo di Veicolo che il documento deve contenere, ad esempio: nome del costruttore, numero di Certificato di Conformità del CSMS, analisi dei rischi, schematici del veicolo, etc.
  Successivamente è presente un'appendice che mostra un fac-simile del documento che il costruttore utilizza per dichiarare la propria conformità del CSMS a questa normativa, la quale dovrà poi essere verificata dall'Ente di Approvazione.

- **Allegato 2:** Comunicazione
  Questo allegato contiene un esempio del documento con cui l'Autorità di Approvazione comunica, al costruttore richiedente, l'esito della sua richiesta di approvazione o estensione.

- **Allegato 3:** Disposizione del simbolo di approvazione
  Questo allegato descrive il posizionamento e la struttura del simbolo di certificazione, il quale indica la conformità, del veicolo in questione, a questa

normativa, il codice della nazione che lo ha approvato e il numero del Certificato di Conformità del Tipo di Veicolo. Un esempio di marcatura è mostrata in figura 3.4.

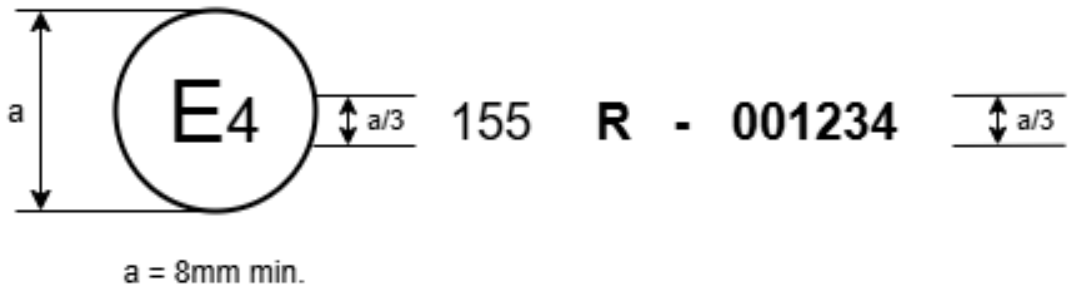

Figura 3.4: Modello per il simbolo di Conformità del Veicolo alla Normativa R155

- **Allegato 4:** Modello del Certificato di Conformità del Sistema di Gestione della Cyber Security (CSMS)
  Modello che indica la conformità del CSMS a questa normativa, contenente i dati dell'Autorità di Approvazione, i dati del Costruttore, il numero di certificato e le date di inizio e fine del periodo di validità. Viene anche previsto che in allegato sia presente un documento che descrive il CSMS del costruttore.
- **Allegato 5:** Lista di potenziali pericoli informatici e relative contromisure
  Questo allegato consiste di tre parti:
  - Parte A: descrive il minimo indispensabile riguardo ai pericoli, alle vulnerabilità e alle metodologie di attacco informatico più comuni.
  - Parte B: descrive le possibili mitigazioni ai pericoli, elencati nella parte precedente, relativi ad aree interne al veicolo.
  - Parte C: descrive le possibili mitigazioni ai pericoli, elencati nella parte A, relativi ad aree esterne al veicolo.

  Per ciascuna vulnerabilità di alto livello, ne viene descritto il tipo e viene descritto un possibile esempio: la numerazione viene mantenuta coerente tra le parti, in modo tale da poter collegare ciascuna vulnerabilità con una lista di possibili mitigazioni, nelle sezioni successive. L'analisi dei rischi proposta, tiene conto anche del possibile impatto dell'attacco, assegnando così un valore relativo alla severità del rischio, in modo tale da poter gestire meglio i casi più pericolosi. Tra le categorie di possibile impatto dell'attacco sono presenti:

  1. Operatività in sicurezza compromessa

2. Funzioni del veicolo che smettono di funzionare
3. Modifiche al Software, prestazioni alterate
4. Modifiche al software senza effetti sull'operatività
5. Integrità dei dati
6. Confidenzialità dei dati
7. Indisponibilità dei dati
8. Altro, includendo la criminalità

3.3 UNECE R156

La normativa UNECE R156 è la regolamentazione delle Nazioni Unite, il cui titolo è "Disposizione uniformata riguardo all'approvazione di veicoli rispetto all'aggiornamento del software e al sistema di gestione degli aggiornamenti del software (SUMS)". Spesso è associato come estensione della normativa UN R155, in quanto è un'estensione, a livello pratico, dei concetti espressi nella normativa R155. La struttura del documento inoltre è molto simile a quello della R155:

1. Obiettivi
2. Definizioni
3. Richiesta di Approvazione
4. Simbolo di Conformità
5. Approvazione
6. Certificato di conformità del Sistema di Gestione degli Aggiornamenti del Software
7. Specifiche
8. Modifiche ed estensioni del Tipo di Veicolo
9. Conformità della produzione
10. Sanzioni in caso di non conformità della produzione
11. Termine definitivo della produzione
12. Nomi e indirizzi dei Servizi Tecnici, responsabili della conduzione dei Test di Approvazione, e delle Autorità per l'Approvazione

Fondamentalmente tutti i processi di certificazione descritti nella sezione precedente, sono ripetuti anche per questo tipo di certificazione, cambiando il sistema di gestione certificato, verranno perciò descritte in seguito solamente le sezioni che presentano rilevanti differenze tra le due normative.

7. Specifiche

In questa sezione sono specificati i requisiti che il Sistema di Gestione degli Aggiornamenti Software (SUMS) deve avere; tale documentazione dev'essere conservata dal costruttore, in caso di verifiche da parte dell'ente di certificazione.
Ciascun Software è identificato da un numero identificativo (RXSWIN) il quale distingue tra di loro le varie versioni, identificando quindi eventuali aggiornamenti eseguiti, in modo tale da poter elencare le modifiche applicate tra due versioni, oltre ad eventuali informazioni e dati per la verifica dell'integrità. L'acronimo RXSWIN è la sigla di "Regulation x Software Identification Number" dove il carattere 'x' indica il numero della Regolamentazione UNECE relativa al sistema che riceve l'aggiornamento, mentre il numero successivo è quello identificativo del software installato. Tale identificativo permette il riconoscimento dei software installati nei vari componenti, in modo tale da determinare quali dispositivi contengano un software che necessita un aggiornamento disponibile.
Il processo in questione dev'essere in grado di identificare, verificare e registrare se un aggiornamento software avrà un effetto su un sistema precedentemente approvato, modificando valori su cui si basava la valutazione di conformità precedente, causando quindi una modifica del Tipo di Veicolo. Il costruttore è tenuto a garantire che la procedura di aggiornamento software sia ragionevolmente protetta, prevenendo eventuali manipolazioni precedenti o successive all'installazione dello stesso, compresi il meccanismo di consegna dell'aggiornamento, e il processo di verifica dell'integrità del software installato. Merita una menzione particolare il caso di aggiornamento di tipo OTA, ovvero consegnato tramite rete mobile, eseguito durante la guida dell'autoveicolo, il quale non deve in alcun modo inficiare sui meccanismi di sicurezza in funzione durante la guida. Il costruttore deve garantire che, in caso di errore durante l'esecuzione di un aggiornamento o non completamento dello stesso, il veicolo possa tornare ad una versione stabile precedente, riportando il veicolo in una condizione di sicurezza. A questo proposito il costruttore è anche tenuto a garantire che un aggiornamento venga eseguito solamente quando il veicolo abbia sufficiente energia per poterlo portare a termine.
Il costruttore è anche tenuto ad informare l'utente del veicolo di un aggiornamento imminente, fornendo le informazioni riguardanti alle motivazioni dello stesso, alle tempistiche relative all'installazione e all'importanza dell'aggiornamento, dal punto di vista della sicurezza.

3.4 ISO 26262 - Veicoli Stradali - Sicurezza Funzionale

La normativa ISO 26262 è lo standard internazionale per la sicurezza funzionale dei sistemi elettrici e/o elettronici, che sono installati all'interno di veicoli prodotti in serie, definita dal Organizzazione Internazionale per la Normazione nel 2011, e poi revisionata nel 2018.[9]
Questa normativa si applica a tutte le attività durante il ciclo di vita della sicurezza di sistemi di controllo, comprensivi di componenti elettrici, elettronici e software. Con il termine "sicurezza", all'interno di questo documento, viene intesa la proprietà di non arrecare danno, principalmente fisico, ad un utente della strada, perciò con il termine "Sicurezza Funzionale" si intende la caratteristica di un componente di non causare danni durante il suo funzionamento e, soprattutto, malfunzionamento. La sicurezza è uno dei problemi chiave nella progettazione di un veicolo stradale, lo sviluppo e l'integrazione di nuove funzionalità, incrementa sempre più la necessità di applicare la sicurezza funzionale e fornire prove che tutti gli obiettivi di sicurezza siano stati raggiunti. Con l'incremento della complessità tecnologica, dei contenuti software e delle implementazioni meccatroniche all'interno dei veicoli, i rischi di errori di sistema ed errori hardware imprevedibili è sempre maggiore, perciò questa normativa ha l'obiettivo di fornire una serie di standard e linee guida per l'applicazione di requisiti e processi, in modo tale da mitigare il più possibile questi rischi.
Per raggiungere la sicurezza funzionale, la serie di standard della ISO 26262:

a) fornisce un riferimento per il ciclo di vita della sicurezza per l'ambito automobilistico, e supporta l'integrazione delle attività da svolgere durante le fasi del ciclo di vita del prodotto (sviluppo, produzione, operatività, manutenzione, fine produzione);

b) fornisce un approccio, specifico per l'ambiente automobilistico, basato sull'analisi dei rischi, per determinare il livello di integrità della sicurezza (ASIL);

c) utilizza la categorizzazione ASIL per specificare quali requisiti di questa normativa devono essere applicati in modo tale da evitare qualunque irragionevole rischio residuo;

d) fornisce requisiti per la gestione, progettazione, implementazione, verifica, validazione e misure di conferma della sicurezza funzionale;

e) fornisce requisiti per le relazioni tra clienti e fornitori.

La struttura generale di questa normativa è la seguente (rappresentata in Figura 3.5):

1. Vocabolario
2. Gestione della sicurezza funzionale
3. Fase di progettazione
4. Sviluppo del prodotto a livello di sistema
5. Sviluppo del prodotto a livello di hardware
6. Sviluppo del prodotto a livello di software
7. Produzione, operatività, manutenzione e fine produzione
8. Supporto ai processi
9. Analisi basate su classificazione ASIL e orientate alla sicurezza
10. Linee guida sulla ISO 26262
11. Linee guida per l'applicazione della ISO 26262 ai semiconduttori
12. Adattamento della ISO 26262 ai motocicli

Come si può notare in Figura 3.5, la normativa 26262 è basata su un modello chiamato "Modello a V", nel quale è previsto che, per ogni attività inerente al progetto rappresentate sul ramo discendente sinistro, sia presente un'attività di verifica dei requisiti sul ramo destro ascendente, in modo tale da correggere e/o incrementare eventuali mancanze o incompletezze il prima possibile all'interno del processo.

1. Vocabolario

In questa sezione è presente un elenco di tutti i termini tecnici utilizzati all'interno della normativa, per un totale di circa 190 termini, comprensivi di descrizione ed eventuale esempio; in seguito è presente anche un elenco di termini abbreviati e sigle, con le relative definizioni, utilizzati all'interno del vocabolario.

2. Gestione della Sicurezza Funzionale

In questa sezione viene descritta una struttura, riguardo la sicurezza funzionale, per lo sviluppo di sistemi E/E sicuri, la quale è stata pensata per integrare le attività di sicurezza funzionale all'interno di una struttura di processi, propria di un'azienda, in modo tale da essere adattabile a più contesti diversi fra loro. Questo documento specifica i requisiti per la gestione della sicurezza funzionale, in ambito automobilistico, includendo insieme:

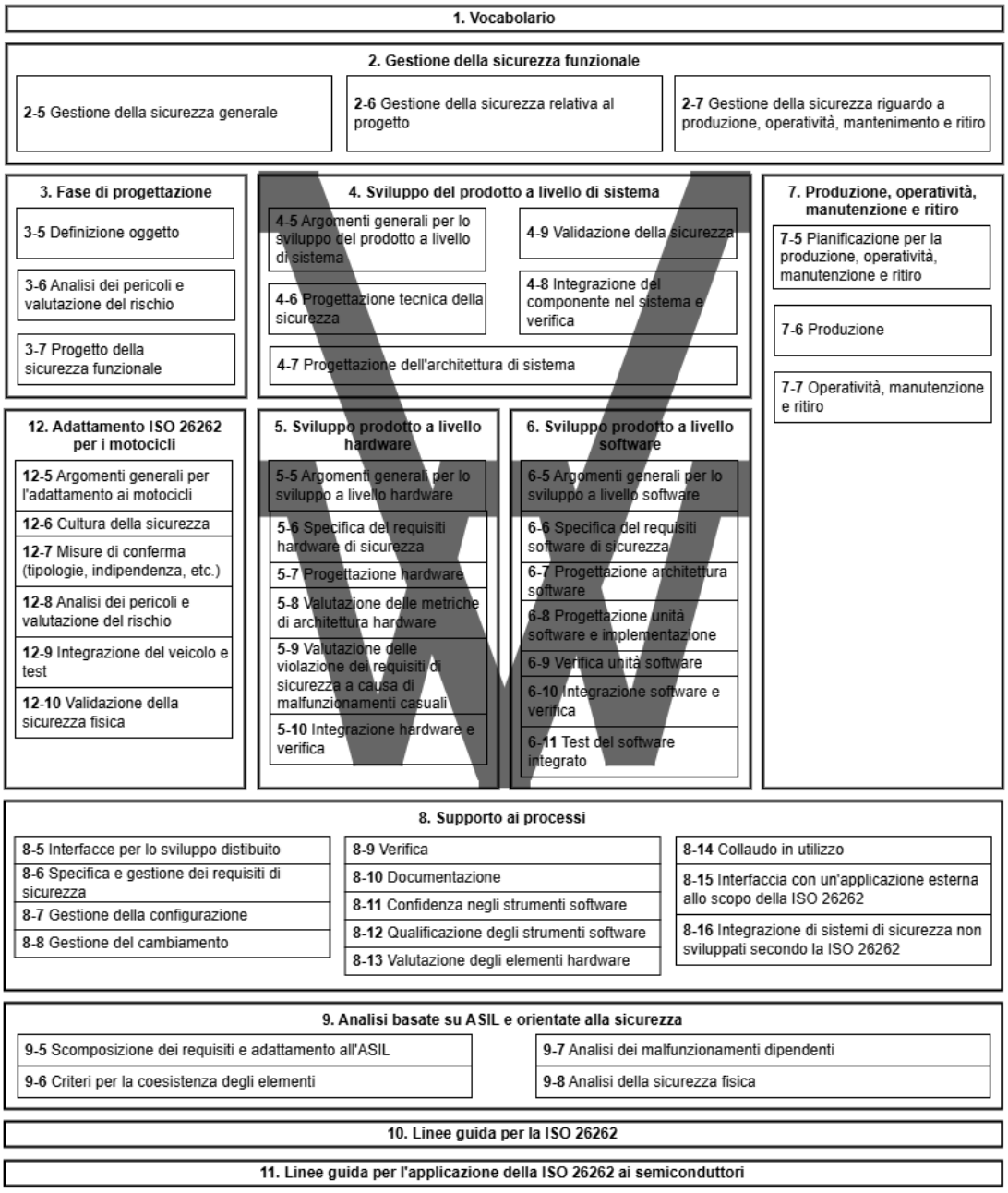

Figura 3.5: Struttura normativa ISO 26262

- requisiti indipendenti dal progetto, cioè la gestione a livello aziendale della sicurezza funzionale in maniera complessiva;
- requisiti specifici del progetto, riguardanti le attività per la gestione del ciclo

di vita della sicurezza.

Gestione della Sicurezza Complessiva
L'intento di questa sezione è quello di garantire che le organizzazioni coinvolte nell'esecuzione di attività del ciclo di vita della sicurezza, raggiungano i seguenti obiettivi:

a) istituire e mantenere una cultura, riguardo alla sicurezza, che supporti e incoraggi il raggiungimento effettivo di un alto livello di sicurezza, e che promuova l'effettiva comunicazione con altre discipline legate alla sicurezza funzionale;

b) istituire e mantenere regole e processi adeguati, specifici dell'organizzazione, per la sicurezza funzionale;

c) istituire e mantenere processi per garantire un'adeguata risoluzione delle anomalie di sicurezza identificate;

d) istituire e mantenere un sistema di gestione delle competenze, in modo tale da garantire che la competenza delle persone coinvolte sia commisurata con le loro responsabilità;

e) istituire e mantenere un sistema di gestione della qualità a supporto della sicurezza funzionale.

Il ciclo di vita della sicurezza, descritto all'interno della normativa ISO 26262, comprende tutte le principali attività di sicurezza svolte durante le fasi di progettazione, sviluppo del prodotto, produzione, operatività servizio e fine produzione. L'obiettivo è quello di pianificare, coordinare e monitorare i progressi delle attività di sicurezza, così come le responsabilità di garantire che le misure per confermare l'applicazione della sicurezza, siano applicate.

Fasi e sotto-fasi del Ciclo di Vita della Sicurezza

a) definizione del componente (sotto-fase della fase di Progettazione)
Sviluppare una descrizione dell'oggetto, descrivendo le sue funzionalità, interfacce, condizioni ambientali, requisiti legali, rischi conosciuti, etc. Inoltre vanno anche definiti i confini del componente e i suoi punti di contatto con l'esterno, facendo assunzioni riguardo ai componenti esterni.

b) Analisi dei Pericoli e Valutazione del Rischio (HARA)
Questo tipo di analisi, chiamata HARA (acronimo di Hazard Analysis and Risk Assessment), ha l'obiettivo di identificare tutti i rischi, relativi alla sicurezza funzionale, che potenzialmente possono arrecare danno all'utente

finale. Il primo passo è quello di stimare la probabilità di esposizione, la controllabilità da parte degli utenti della strada e la gravità di un evento pericoloso: questi valori, tutti insieme, contribuiscono alla determinazione del valore del ASIL, cioè del livello di integrità della sicurezza da applicare al componente, il quale ne identifica quindi l'importanza e la criticità dal punto di vista della sicurezza funzionale. Successivamente alla determinazione dei rischi, la HARA determina quindi gli obiettivi di sicurezza del componente, che vengono posti come obiettivi principali del componente, e l'ASIL, valutato per l'evento pericoloso, viene assegnato al corrispondente obiettivo di sicurezza.[10]

c) progettazione della sicurezza funzionale (sotto-fase della fase di progettazione)
Basandosi sugli obiettivi di sicurezza, una progettazione concettuale della sicurezza viene sviluppata, considerando le assunzioni architetturali preliminari; mentre dagli obiettivi di sicurezza vengono ricavati i requisiti di sicurezza dettagliati, da applicare agli elementi del componente.

d) sviluppo del prodotto a livello di sistema
Dopo aver sviluppato il progetto della sicurezza, il componente viene sviluppato a livello di sistema. Il processo di sviluppo di un sistema è basato sul concetto di "Modello a V", con le specifiche dei requisiti di sicurezza tecnici, l'architettura del sistema, la progettazione e implementazione del sistema sul lato sinistro, e l'integrazione, la verifica e la validazione della sicurezza sul lato destro. In questa fase sono presenti anche le attività per determinare:

- le assunzioni tecniche rilevanti per la classificazione ASIL;
- la validazione delle assunzioni riguardanti il comportamento umano, includendo la controllabilità e la capacità di reazione;
- la validazione degli aspetti di sicurezza funzionale implementati da altre tecnologie esterne al componente;
- la validazione delle assunzioni riguardanti l'efficacia delle prestazioni di eventuali misure esterne.

e) sviluppo del prodotto a livello di hardware
Basandosi sulle specifiche del progetto di sistema, viene sviluppato l'hardware del prodotto: anche questo processo è basato su un "Modello a V", con la specifica dei requisiti hardware, la progettazione dell'hardware e l'implementazione sul lato sinistro, e l'integrazione hardware e la verifica sul lato destro.

f) sviluppo del prodotto a livello di software
Basandosi sulle specifiche del progetto di sistema, viene sviluppato il software del prodotto: anche questo processo è basato su un "Modello a V" con la specifica dei requisiti software, del progetto architetturale del software e la

sua implementazione sul lato sinistro, e l'integrazione e la verifica del software sul lato destro.

g) produzione, operatività, supporto e fine della produzione
La progettazione di questa fase e la derivazione dei requisiti associati, inizia durante la fase di sviluppo del prodotto a livello di sistema, e ha uno svolgimento parallelo alle fasi di progettazione a livello di sistema, hardware e software, in modo tale da poter scambiare informazioni, o requisiti caratteristici, che possono migliorare la capacità di produrre il prodotto finale. Questa fase riguarda i processi, le conoscenze e le istruzioni per garantire la sicurezza funzionale relativa alla produzione, l'operatività, il supporto e il fine vita del prodotto.

Gestione della Sicurezza relativa al Progetto

Lo scopo di questa sezione è quello di garantire che tutte le aziende e le organizzazioni, coinvolte nella progettazione e/o nello sviluppo, a livello di sistema, hardware o software del prodotto, soddisfino i seguenti obiettivi:

a) definire e assegnare i ruoli e le responsabilità riguardanti le attività di sicurezza;

b) eseguire un'analisi di impatto, a livello di prodotto, per capire se l'oggetto sia un progetto nuovo, una modifica di un oggetto precedente o un oggetto preesistente utilizzato in un ambiente diverso, ed in caso di modifiche, capirne le implicazioni sulla sicurezza funzionale;

c) eseguire un'analisi di impatto, a livello di elemento, in caso sia presente un elemento riutilizzato, per valutare se l'elemento in questione possa soddisfare i requisiti di sicurezza, considerando il nuovo ambiente operativo;

d) definire le attività di sicurezza e come integrarle all'interno del processo di progettazione e produzione;

e) pianificare le attività di sicurezza;

f) coordinare e tenere traccia del progresso delle attività di sicurezza, rispetto al piano della sicurezza;

g) pianificare lo sviluppo distribuito

h) garantire il corretto svolgimento delle attività di sicurezza, attraverso tutto il ciclo di vita della sicurezza

i) creare un caso di funzionamento sicuro comprensibile, in modo tale da poterlo paragonare alla situazione attuale per determinare il raggiungimento degli obiettivi di sicurezza funzionale;

j) giudicare se un componente soddisfa i requisiti di sicurezza o il suo contributo al raggiungimento della sicurezza funzionale di un altro elemento;

k) decidere se, alla fine dello sviluppo, un componente può essere inviato alla fase di produzione, sulla base di risultati che assicurano la sicurezza funzionale del componente.

Misure di Conferma

La sicurezza funzionale di un componente e dei suoi elementi dev'essere verificata e confermata sulla base di:

1. una revisione di conferma del fatto che i documenti, prodotti dal processo, forniscano prove sufficienti e convincenti del loro contributo alla sicurezza funzionale;

2. una verifica dell'implementazione dei processi di sicurezza funzionale rispetto ai requisiti definiti in questa normativa;

3. una verifica per giudicare l'effettivo raggiungimento della sicurezza funzionale del componente, o del contributo al raggiungimento della stessa in un altro componente.

Viene definito, per ciascuna misura di conferma, un livello di indipendenza, in base al valore di ASIL assegnato al componente, che indica quanto la persona che effettua la verifica, debba essere indipendente da chi ha creato il documento relativo al prodotto. Sono definiti quattro livelli di indipendenza:

- - : Nessun requisito di indipendenza specificato
- I0 : la misura di conferma dovrebbe essere eseguita, e nel caso in cui venga eseguita, senza obbligatorietà dell'indipendenza dal progetto;
- I1 : la misura di conferma dev'essere eseguita da una persona diversa rispetto alla persona responsabile della creazione del documento di progetto;
- I2 : la misura di conferma dev'essere eseguita da una persona indipendente dal gruppo di lavoro responsabile della produzione del documento di progetto;
- I3 : la misura di conferma dev'essere eseguita da una persona indipendente da gestione, risorse, autorità e dipartimento responsabile della creazione del documento di progetto.

Nel pratico, più il valore di ASIL è alto, più è necessaria rigorosità nell'applicazione dei meccanismi di sicurezza funzionale, e per questo motivo, è necessario uno sguardo "esterno" al progetto, che possa valutarne in maniera indipendente la sicurezza

applicata.

Allegati esterni

- Allegato A: Panoramica sulla Gestione della Sicurezza Funzionale
  Contiene una tabella che riassume gli obiettivi da raggiungere, tramite la gestione della sicurezza funzionale, nelle varie fasi di un progetto.
- Allegato B: Cultura sulla Sicurezza
  Propone una tabella, contenente esempi pratici a confronto, di situazioni in cui la sicurezza funzionale viene considerata e non considerata, fornendo così un valido esempio con cui paragonare la propria situazione aziendale.
- Allegato C: Guida alle Misure di Conferma
  Fornisce alcune linee guida per l'esecuzione dei processi, relativi alle misure di conferma, le quali possono essere utilizzate per giudicare il contributo, alla sicurezza funzionale, atteso dal corrispondente prodotto o documento di lavoro.
- Allegato D: Esempio di agenda per la verifica della Sicurezza Funzionale
  Contiene un esempio di struttura delle attività da applicare, in caso di lavoro su un componente con ASIL D (cioè il caso più dettagliato), attraverso tutto il ciclo di vita di gestione della sicurezza funzionale.
- Allegato E: Guida su potenziali interazioni della Sicurezza Funzionale con la Cybersecurity
  Mentre la sicurezza funzionale punta a gestire difetti sistematici e casuali che risultano in un comportamento di malfunzionamento di un sistema E/E, la Cybersecurity mira a risolvere problemi derivanti da intenti malevoli esterni al sistema E/E. Per questo motivo le interazioni tra le due devono essere gestite in modo tale che una misura di sicurezza, funzionale o informatica, non vada a inficiare e/o comprometterne un'altra.

3. Fase di Progettazione

All'interno di questa sezione, viene spiegato come implementare la sicurezza funzionale durante la progettazione di un componente, partendo dall'analisi degli obiettivi del ciclo di vita della sicurezza. Per fare un riassunto degli obiettivi del ciclo di vita della sicurezza possiamo elencarne i punti chiave:

1. Raccogliere informazioni riguardanti il sistema;
2. Analizzare il funzionamento atteso del componente
3. Elencare e classificare i rischi derivanti da malfunzionamenti (mediante ASIL);

4. Definire i requisiti principali (Obiettivi di Sicurezza e Stati di Sicurezza);

5. Sviluppare i concetti di sicurezza funzionale (cosa deve fare il sistema in caso di malfunzionamento);

6. Sviluppare i concetti tecnici a livello Hardware e Software (come vengono implementati i concetti di sicurezza durante il periodo di vita del componente);

7. fornire prove che la sicurezza funzionale sia stata raggiunta, attraverso misure sul prodotto e sul processo (Misure di Sicurezza).

Livello di Integrità della Sicurezza in ambito Automobilistico (ASIL) [10] Questo valore viene determinato, mediante l'analisi dei rischi (HARA), classificando ciascuno scenario di pericolo ricostruito, secondo i seguenti parametri:

- Gravità: è la stima dell'entità del danno causato a una o più persone che può verificarsi durante un evento potenzialmente pericoloso, ossia considerando danni al conducente, ai passeggeri o ad altri utenti all'esterno del veicolo. La classificazione secondo la Tabella 3.2.

	Classe			
	S0	**S1**	**S2**	**S3**
Descrizione	Nessun danno	Danni lievi o moderati	Danni gravi o potenzialmente mortali (sopravvivenza probabile)	Danni potenzialmente mortali (sopravvivenza incerta) o fatali

Tabella 3.2: Classificazione ASIL della Gravità.

- Esposizione: indica la probabilità, o la durata dell'esposizione, che lo scenario di pericolo possa realizzarsi. La classificazione secondo la Tabella 3.3.

	Classe				
	E0	**E1**	**E2**	**E3**	**E4**
Descrizione	Incredibile	Probabilità molto bassa	Bassa Probabilità	Media Probabilità	Alta Probabilità

Tabella 3.3: Classificazione ASIL di Esposizione.

- Controllabilità: è la capacità di evitare un determinato danno attraverso le reazioni tempestive delle persone coinvolte, eventualmente con il supporto di misure esterne. La classificazione secondo la Tabella 3.4.

	Classe			
	C0	**C1**	**C2**	**C3**
Descrizione	In genere controllabile	Facilmente controllabile	Normalmente Controllabile	Difficile da controllare o incontrollabile

Tabella 3.4: Classificazione ASIL della Controllabilità.

Componendo insieme tutti questi parametri, è possibile determinare l'effettivo valore di ASIL secondo la Tabella 3.5.

Gravità	**Esposizione**	**Controllabilità**		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Tabella 3.5: Determinazione del valore di ASIL

Il valore "QM" sta per "Quality Management", indicando quindi che i processi di qualità sono sufficienti per gestire il rischio individuato, senza bisogno di ulteriori misure.
Come si può notare dalla Tabella 3.5, più sono alte: la gravità dello scenario, la probabilità che questo si verifichi e la difficoltà di controllabilità da parte dell'utente; più aumenta il valore di ASIL, indicando la necessità di un maggior rigore nell'applicazione della sicurezza funzionale.

6. Sviluppo del prodotto a livello di Software

Questo documento specifica i requisiti relativi allo sviluppo di un prodotto a livello software per l'applicazione in ambito automobilistico, tra cui troviamo:

- argomenti generali per lo sviluppo di un prodotto a livello software;
- specifiche dei requisiti di sicurezza del software;
- progettazione e implementazione delle unità software;
- integrazione e verifica del software;
- test del software.

Anche questo documento propone un processo basato su un "Modello a V", il quale contiene: sul ramo sinistro, la specifica dei requisiti software di sicurezza, successivamente, basandosi sui requisiti trovati, la progettazione dell'architettura del software, ed infine la progettazione e l'implementazione delle singole unità software; mentre sul lato destro sono presenti la verifica delle unità software separatamente, dopodiché la verifica dell'integrazione del software, successivamente la fase di test del software nella sua interezza ed infine l'integrazione e il test del software nel suo ambiente operativo, all'interno del componente. Tutto il processo è mostrato all'interno della Figura 3.6.

Requisiti e raccomandazioni
Quando si sviluppa il software per un componente, dovrebbero essere usati processi e ambienti di sviluppo del software, con le seguenti caratteristiche:

- siano adatti per sviluppare software integrati sicuri, includendo metodi, linee guida, linguaggi e strumenti;
- supportino la consistenza, attraverso le varie sotto-fasi del ciclo di vita dello sviluppo software, dei relativi documenti di lavoro;
- siano compatibili con le fasi di sviluppo del sistema e dell'hardware riguardo le interazioni necessarie e lo scambio di informazioni consistenti.

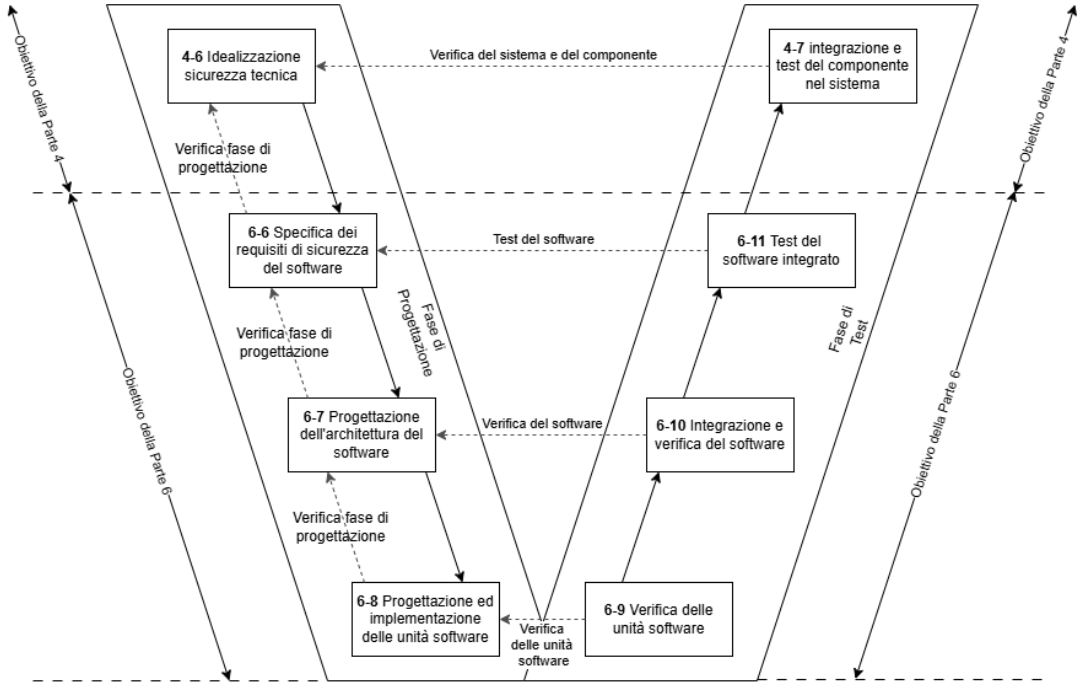

Figura 3.6: Modello di riferimento per sviluppo del Software secondo normativa ISO 26262

Automotive SPICE

[11] Generalmente abbreviato in A-SPICE, è uno standard riconosciuto a livello mondiale, utilizzato dai principali OEM e fornitori per valutare i processi di sviluppo di sistemi software, interni ed esterni ad un veicolo. La sigla SPICE è l'acronimo di "Software Process Improvement and Capability dEtermination" cioè uno standard per la determinazione delle effettive capacità di un processo, legato allo sviluppo software, e delle sue possibili migliorie.
L'Automotive SPICE è costituito da due dimensioni:

- Modello di Riferimento dei Processi (PRM): contiene tutti i processi che sono stati esplicitamente definiti per l'applicazione all'interno dell'industria automobilistica;
- Struttura per la misurazione: contiene la descrizione dei sei livelli di capacità che identificano la maturità di un processo, indicando come questi possono essere raggiunti;

Livello di Maturità (Capacità)
Quando viene eseguita una valutazione dei processi aziendali, viene calcolato il

livello di maturità di ciascun singolo processo, in modo tale da ottenere un'immagine dettagliata della robustezza e del potenziale di miglioramento del progetto in esame. Ciascun processo viene valutato in base ad attributi predefiniti e classificato in uno dei seguenti sei livelli:

- Livello 0 - Incompleto: significa che i risultati attesi da un processo non esistono, sono incompleti o che le attività del processo non vengono condotte;
- Livello 1 - Eseguito: i risultati del processo esistono, ma non sono controllati, e neanche le attività del processo lo sono;
- Livello 2 - Gestito: l'implementazione delle attività del processo sono pianificate e monitorate, le responsabilità sono assegnate e i risultati del processo sono sistematicamente memorizzati e qualitativamente controllati;
- Livello 3 - Stabilito: i processi standard sono definiti all'interno dell'organizzazione aziendale, e di conseguenza applicati nel progetto;
- Livello 4 - Prevedibile: il processo stabilito opera prevedibilmente all'interno di determinati limiti;
- Livello 5 - Innovativo: è presente un'innovazione continua dei processi prevedibili.

Modello di Riferimento dei Processi
Il modello di riferimento dei processi di ASPICE definisce i processi e le loro interazioni, ciascuno definito da nome, descrizione ed esiti associati. Per ciascun processo sono definiti anche i documenti di lavoro che questo deve produrre, la cui presenza identifica la conclusione positiva di una determinata attività. Lo standard categorizza questi processi (32 in totale) all'interno di tre categorie:

- Processi del Ciclo di Vita base: ne fanno parte i processi di acquisizione (lato cliente), di fornitura (lato fornitore) e di ingegneria necessari per le fasi di specifica, progettazione, sviluppo, integrazione e test dei prodotti a livello di sistema e software;
- Processi del Ciclo di Vita di supporto: includono processi quali la documentazione, la verifica, la revisione e la gestione delle modifiche, assieme ai processi di manutenzione e supporto del progetto;
- Processi del Ciclo di Vita di organizzazione: includono i processi di gestione aziendale, riutilizzo e miglioramento dei processi, consentendo di sviluppare processi e prodotti riutilizzabili in altri progetti.

Struttura per la Misurazione
Consente di valutare la dimensione di capacità di ogni singolo processo sulla base di attributi o caratteristiche di processo misurabili (prodotti di lavoro disponibili, testimonianze di chi esegue e gestisce i progetti, etc.). Le valutazioni degli attributi dei processi sono assegnate su una scala a quattro livelli:

- N - Non raggiunto;
- P - Parzialmente raggiunto;
- L - In gran parte raggiunto;
- F - Completamente raggiunto.

Per raggiungere un determinato livello di capacità specifico per un processo, tutti gli attributi di quel livello dovranno essere valutati come in gran parte raggiunti (L) o completamente raggiunti (F), mentre quelli dei livelli inferiori dovranno essere valutati tutti come completamente raggiunti (F).
Nella tabella 3.6 è possibile vedere un riassunto della classificazione dei vari livelli di ASPICE.

Livello	Descrizione	Attributi e Valutazioni
Livello 0 - Incompleto	Il processo non ha raggiunto il suo scopo e deve essere rivisto.	-
Livello 1 - Eseguito	Il processo soddisfa l'obiettivo prefissato.	Prestazioni di processo (L)
Livello 2 - Gestito	Il processo è gestito e monitorato, i risultati sono controllati e mantenuti.	Prestazioni di processo (F) Gestione delle prestazioni (L) Gestione dei prodotti di lavoro (L)
Livello 3 - Stabilito	Il processo è strutturato ed implementato a livello di organizzazione.	Prestazioni di processo (F) Gestione delle prestazioni (F) Gestione dei prodotti di lavoro (F) Definizione del processo (L) Distribuzione dei processi (L)
Livello 4 - Prevedibile	L'approccio è collaudato e funziona perfettamente, entro determinati limiti, per garantire il raggiungimento dei suoi obiettivi; i dati e la gestione sono correttamente implementati; è in grado di rilevare variazioni e determinarne le cause.	Prestazioni di processo (F) Gestione delle prestazioni (F) Gestione dei prodotti di lavoro (F) Definizione del processo (F) Distribuzione dei processi (F) Analisi quantitativa (L) Controllo quantitativo (L)
Livello 5 - Innovativo	Il processo precedentemente delineato è in continua evoluzione per stare al passo con i cambiamenti organizzativi	Prestazioni di processo (F) Gestione delle prestazioni (F) Gestione dei prodotti di lavoro (F) Definizione del processo (F) Distribuzione dei processi (F) Analisi quantitativa (F) Controllo quantitativo (F) Innovazione di processo (L) Implementazione dell'innovazione (L)

Tabella 3.6: Classificazione ASPICE dei processi

Capitolo 4

Penetration Testing in ambito Automotive

L'approccio tradizionale per valutare la sicurezza di un sistema è l'esecuzione di un test di penetrazione, analizzando quindi la situazione dal punto di vista di un attaccante esterno che voglia accedere al componente senza le dovute autorizzazioni, o di stress di un componente per valutarne la robustezza in situazioni complesse. Lo scopo principale del test di penetrazione è quello di trovare vulnerabilità che non siano state individuate durante i test di sicurezza interni.
Questo tipo di procedura è normalmente condotto in stadi molto avanzati del progetto, perciò qualunque difetto di sicurezza, rilevato a questo punto, richiede costi e risorse maggiori per essere corretto, perciò una combinazione di test White Box, durante lo sviluppo del progetto (per rilevare il prima possibile eventuali difetti), e di test Black Box alla fine del progetto, è un buon compromesso per tentare di ridurre i costi di modifiche del progetto.[12]

4.1 Strumenti per il Threat Modeling

Il Threat Modeling è il processo di sicurezza con il quale vengono identificate, classificate e analizzate potenziali minacce, valutandone il rischio e fornendo le necessarie contromisure. Il suo scopo è quello di modellare i pericoli, rendendoli pratici ed adattabili al caso in questione, fornendo così una lista delle risorse da proteggere, e dei relativi meccanismi di sicurezza da implementare e successivamente testare.
Nel pratico i metodi di threat modeling sono utilizzati per creare:

- un'astrazione del sistema;
- profili dei potenziali attaccanti, includendo i loro obiettivi e metodologie;

- una lista di potenziali minacce che possono sorgere.

Esistono molteplici metodologie, ciascuna con le sue peculiarità, più o meno adattabili all'ambito automobilistico, perciò una combinazione di più metodi può essere considerata una buona scelta. Di seguito ne sono elencati alcuni:

- OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation): sviluppato per la valutazione dei rischi al livello di impresa, perciò non mira a specifici attributi dell'ambiente automobilistico, il quale lo rende una metodologia poco significativa in questo dominio; [12]
- HEAVENS (HEAling Vulnerabilities to ENhance Software Security and Safety): metodologia basata sul modello di classificazione STRIDE sviluppato da Microsoft, il quale aiuta a definire ed elencare le possibili minacce, procedendo un ambito per volta; l'obiettivo di STRIDE è focalizzato principalmente sulla sicurezza informatica, perciò spetta al responsabile della sicurezza decidere se una minaccia è anche un pericolo per la sicurezza fisica del veicolo oppure no;[12]
- EVITA (E-Safety Vehicle Intrusion Protected Applications): sfrutta scenari che comprendono utilizzi non previsti dei componenti, in modo tale da identificare possibili minacce alla sicurezza; si focalizza sulle connessioni veicolo-veicolo più che su quelle interne al veicolo; l'identificazione delle minacce dipende molto dagli scenari utilizzati, con il risultato di tralasciare molti pericoli con impatto sulla sicurezza fisica;[12]
- TVRA (Threat, Vulnerability and Risk Assessment): è il metodo più generico che consiste nell'identificazione delle risorse, successivamente nell'analisi delle vulnerabilità, determinando infine i valori di rischio e ordinandoli in base alla gravità effettiva; può definire il livello di rischio di un sistema basandosi sulla probabilità che sia attaccato e sull'impatto che quest'ultimo avrebbe;[13]
- SAHARA (Security-aware Hazard and Risk Analysis Method): ha l'obiettivo di includere l'analisi HARA con l'applicazione del modello STRIDE per la ricerca di vulnerabilità;[12]
- FMEA (Failure Mode and Effects Analysis): tecnica strutturata che investiga sulle probabilità e modalità di guasto di un componente, e sull'effetto che questo malfunzionamento può avere;[14]
- hTMM (hybryd Threat Modeling Method): questo approccio combina i metodi delle "Carte di Sicurezza" e di "Persona non Grata" per l'identificazione di rischi e pericoli; il primo utilizzato nella fase di brainstorming, con l'effetto collaterale di non potersi focalizzare sull'identificazione dei pericoli alla sicurezza, e di non poter riutilizzare risultati derivanti da precedenti analisi della sicurezza;[12]

- HAZOP (Hazard and Operability Study): tecnica per l'identificazione di pericoli e questioni operative di un sistema, è stato sviluppato inizialmente per l'industria Chimica, ma successivamente adattato a numerosi ambiti;[15]

- FMVEA (Failure Mode Vulnerabilities and Effect Analysis): estende il meccanismo della metodologia FMEA, includendo anche le vulnerabilità all'interno dell'analisi;[14]

- FTA (Fault Tree Analysis): tecnica utilizzata per comprendere la catena di guasti dei componenti, per capire meglio come un componente può guastarsi e poter creare meccanismi migliori per evitarlo;[12]

- STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege): valuta la struttura del sistema nel dettaglio, basandosi sulla sua classificazione, identificando le entità del sistema e i suoi confini;[16]

- PASTA (Process for Attack Simulation and Threat Analysis): metodologia di threat modeling incentrata sul rischio, sulla prospettiva dell'attaccante e sull'elenco delle risorse;[16]

- CVSS (Common Vulnerability Scoring System): metodologia basata sull'analisi delle principali vulnerabilità di un sistema, assegnandogli un valore di severità;[16]

- Alberi degli attacchi: metodologia basata su diagrammi che evidenziano i percorsi degli attacchi, a forma di albero, dove in cima è presente l'obiettivo dell'attacco, e sulle foglie tutti i metodi per raggiungerlo;[16]

- Persona non Grata: si basa sull'analisi della personalità, delle capacità e sulle motivazioni dell'attaccante;[16]

- Carte di Sicurezza: tecnica di brainstorming utilizzata per identificare attacchi inconsueti, rispetto al sistema in questione. [16]

Criterio	SAHARA	FMVEA	EVITA	HEAVENS
Ambito di applicazione	Sistemi Automobilistici	Sistemi Cyber-Fisici (CPS)	Sistemi Automobilistici	Sistemi Automobilistici
Approccio di Threat Modeling	STRIDE	STRIDE	Scenari malevoli e alberi di attacco	STRIDE
Confronto tra sicurezza fisica e informatica	Pericoli e minacce sono identificati, minacce informatiche che hanno conseguenze sulla sicurezza fisica sono inviate a specifiche analisi	Modalità di fallimento e minacce sono identificate, ma trattate separatamente	Solo valutazione dei rischi di sicurezza fisica	Solo valutazione dei rischi di sicurezza fisica

Tabella 4.1: Metodi di threat modeling a confronto

Confrontando le caratteristiche e le metodologie di analisi, è possibile notare come alcune di queste metodologie siano più adatte ad analisi di rischi informatici (OCTAVE, STRIDE, hTMM), altre ad analisi di sicurezza fisica (EVITA, HEAVENS), mentre alcune siano ibride e permettano l'analisi di entrambi i domini, seppur con limitazioni (SAHARA, FMVEA).[12]
All'interno della tabella 4.1 è possibile osservare un rapido confronto tra le principali tecniche di threat modeling, per la sicurezza fisica, menzionate nel contesto dell'industria automobilistica.

4.2 Tipologie di Penetration Testing

Esistono principalmente due tipi di Penetration Testing: quello denominato "Black Box" e quello denominato "White Box": la loro differenza risiede nella conoscenza che l'esecutore ha del sistema.

4.2.1 White Box

Questa tipologia di test di penetrazione, prevede che l'esecutore abbia pieno accesso a materiale e documentazione relativi all'oggetto in esame, in modo tale da conoscerne perfettamente le caratteristiche e la struttura. Generalmente questo

tipo di test è eseguito internamente all'azienda, con lo scopo di valutare l'effettiva efficacia delle misure di sicurezza implementate, andando a "stressare" il meccanismo di sicurezza in maniera mirata.

4.2.2 Black Box

Questa tipologia di test di penetrazione, prevede che l'esecutore non abbia informazioni sul componente, quindi di conseguenza che debba esplorarlo nella sua interezza per scoprirne le possibili vulnerabilità. Questa procedura è generalmente eseguita da personale esterno al gruppo che ha progettato il componente, in modo tale da avere una visione diversa ed esterna dello stesso, con lo scopo di determinare il livello di resistenza contro attaccanti esterni.

4.2.3 Classificazione dei Test di Penetrazione

I test effettuabili su un sistema informatico sono di vario tipo, generalmente classificati nelle seguenti categorie[17]:

- Raccolta di informazioni:
  La raccolta di informazioni è il primo passo per i test di penetrazione, consiste nel recuperare informazioni da tutte le sorgenti disponibili (siti web, documentazione tecnica, documenti pubblici, etc.) e analizzarli in modo tale da identificarne le vulnerabilità da poter sfruttare;

- Test della Configurazione e della Gestione:
  Il test sulla configurazione degli strumenti permette di comprenderne il funzionamento e la logica di funzionamento, identificando le configurazioni di base vulnerabili e le mal configurazioni sfruttabili per portare a termine un attacco;

- Test di Autenticazione:
  Testare i meccanismi di autenticazione, aiuta a comprenderne il funzionamento e le possibili limitazioni, in modo da poter aggirare il meccanismo ed entrare nel sistema. L'autenticazione è il primo meccanismo di difesa perchè consente di verificare una connessione e di identificare una persona, ed è la base che permette di effettuare il controllo degli accessi tramite strumenti e protocolli;

- Test della gestione delle Identità:
  Le informazioni in un sistema sono protette, l'accesso è regolamentato dalla definizione di ruoli e privilegi associati a ciascuna identità digitale. Questo tipo di test mira ad aggirare queste limitazioni, trovando delle debolezze all'interno dei meccanismi di controllo degli accessi alle risorse;

- Test delle Autorizzazioni:
  L'autorizzazione è il processo successivo all'identificazione: una volta identificato l'utente, si verifica cosa questi può fare e cosa non, alla ricerca di autorizzazioni e/o privilegi non coperti dai meccanismi di sicurezza;

- Test sulla Gestione delle Sessioni:
  Il meccanismo delle sessioni permette di mantenere nel tempo lo stato di un utente attraverso diverse pagine di un applicazione web, ad esempio la sua identità; con questo tipo di test si controllano le interazioni, tra l'utente e il sistema, alla ricerca di possibili meccanismi e informazioni, da poter ripetere al sistema, per guadagnarne l'accesso in un secondo momento, con un'altra identità;

- Test sulla Validazione degli Input:
  Una delle debolezze più comuni in un sistema è la mancata validazione dei dati di input, considerandoli attendibili a prescindere; questa tipologia di test consiste nell'inserimento di dati, costruiti per l'occasione, in modo tale da deviare il corretto funzionamento del software, con lo scopo di trovare una vulnerabilità sfruttabile nel meccanismo di controllo degli input;

- Test lato Client:
  Nelle applicazioni web con struttura Client-Server, consiste nella ricerca di vulnerabilità all'interno dell'applicativo eseguito dal Client (generalmente un Browser) con lo scopo di guadagnare informazioni, generalmente non accessibili, dai dati provenienti dal server;

- Gestione degli Errori:
  Una cattiva gestione dei messaggi di errore, può portare a fornire informazioni importanti ad un utente malevolo, come il servizio che lo ha generato o il motivo dell'errore troppo specifico: la gestione degli errori dev'essere implementata dall'inizio del progetto, in modo tale da non rivelare alcuna informazione relativa al funzionamento interno dell'oggetto;

- Crittografia Debole:
  Questo tipo di test mira a ricercare eventuali meccanismi di crittografia ormai obsoleti o erroneamente implementati, in modo tale da poter guadagnare informazioni tramite la decifrazione di messaggi crittografati;

- Test sulla Logica dei Processi:
  Questa tipologia di test mira ad analizzare il sistema nella sua interezza, ricercando difetti nell'ordine delle azioni o creati involontariamente dall'integrazione di più componenti all'interno del sistema, che permettano ad un utente malevolo un margine di operatività per aggirare i meccanismi di sicurezza.

4.3 Conduzione e Validazione

Generalmente i test di penetrazione seguono il seguente schema[18]:

1. Ricognizione:
   Durante questa fase, chi è incaricato di eseguire i test di penetrazione, raccoglie informazioni riguardanti il componente da testare, in modo tale da capirne la struttura ed ipotizzarne i processi logici; in caso di attacco white-box, queste informazioni vengono fornite dall'azienda di sua spontanea volontà;

2. Rilevazione e Sviluppo del Bersaglio:
   In questa fase vengono sfruttate le informazioni, ricavate al punto precedente, per l'identificazione di possibili vulnerabilità sfruttabili nel sistema, andando a stressare il sistema, meglio se in modi imprevisti da chi lo ha creato;

3. Sfruttamento:
   In questa fase vengono creati gli strumenti per sfruttare le vulnerabilità precedentemente identificate, diversi in base alla tipologia di attacco e al componente a cui si applica;

4. Escalation:
   Una volta guadagnato l'accesso al sistema tramite una vulnerabilità correttamente sfruttata, lo scopo del test è quello di guadagnare i privilegi di accesso ed esecuzione, più alti possibili, all'interno del sistema, eludendo le misure di sicurezza presenti;

5. Pulizia e reportistica:
   Alla fine dell'attacco, si cerca di eliminare tutte le tracce lasciate dall'attacco, in modo tale da non fornire indicazioni ai proprietari del sistema riguardo alla vulnerabilità sfruttata, ad eventuali materiali installati, etc. Infine viene preparato un documento di riassunto sullo svolgimento del test, il quale indica la presenza delle vulnerabilità rilevate, come sono state sfruttate, come si sono evitate le misure di sicurezza e le descrizioni delle risorse a cui si è avuto accesso. Il team incaricato della sicurezza utilizzerà poi questo rapporto per aggiornare il sistema e correggere tutte le vulnerabilità rilevate dalla conduzione dei test.

Come si può notare però, il risultato della conduzione dei test è fortemente influenzato dalla capacità ed esperienza di chi lo conduce, portando diverse persone a diverse soluzioni. Inoltre è evidente come due sistemi simili possano essere bersaglio degli stessi test, o comunque della stessa tipologia, rendendo le attività di test ripetitive ed automatizzabili, per lo meno nella prima fase di identificazione delle vulnerabilità. Per questo motivo sono stati creati dispositivi per l'automazione dei test, in modo tale da rendere più efficacie e completa la loro esecuzione, un esempio è la piattaforma Weseth descritta in seguito.

4.4 La piattaforma Weseth

Questa piattaforma è stata ideata dall'azienda italiana Drivesec[19], fondata come compagnia di sicurezza informatica, con lo scopo di sviluppare soluzioni per la sicurezza nel mercato IoT. Il nome Weseth è l'abbreviazione di "We secure things" cioè "Noi rendiamo sicure le cose", il quale è l'obiettivo pratico del progetto. La piattaforma in analisi rende possibile l'esecuzione di test, con lo scopo di valutare la sicurezza del componente e l'efficacia delle contromisure di sicurezza, in modalità remota, ovvero senza la presenza fisica dell'esecutore, e senza che l'operatore debba avere concretamente sottomano il componente fisico.
Vantaggi dell'utilizzo della piattaforma:

- Risparmio di tempo ed efficacia: lo svolgimento di test, in modalità remota, non solo riduce la durata della fase di valutazione delle vulnerabilità e test di penetrazione, ma consente l'esecuzione dei test in un ambiente realistico, azzerando i tempi logistici e di configurazione delle variabili;

- Semplificazione della fase di test: la piattaforma consente di svolgere test di sicurezza informatica insieme a test di sicurezza funzionale, prevenendo problemi che sarebbero stati identificabili solamente durante le fasi finali dei test di penetrazione, risultando quindi in un abbassamento dei costi necessari per le modifiche di fine progetto, e nella limitazione dei ritardi di messa sul mercato;

- Semplificazione di Certificazione: la piattaforma aiuta il cliente ad ottenere le certificazioni di conformità in quanto consente la tracciabilità della valutazione delle vulnerabilità e delle attività dei test di penetrazione, particolarmente importanti per la valutazione da parte delle Autorità di Certificazione che dovranno valutare la conformità del componente alla normativa.

4.4.1 Struttura della piattaforma

- Weseth Applicazione Web:
  Questa pagina web permette al cliente di assumere, in tutta efficienza, dei ricercatori informatici per poter eseguire una valutazione delle vulnerabilità e un test di penetrazione sui propri dispositivi;

- Weseth Client:
  Uno strumento che consente l'accesso remoto alla Weseth Box, permettendo la selezione e l'esecuzione dei test ed altre attività relative, fornendo un ambiente di test realistico, riducendo tempi e costi;

- Weseth Server:
  Componente Software gestita da Drivesec, implementa le funzionalità interne del sistema: autenticazione, comunicazione, sicurezza e sessioni di test; permette alla Weseth Box la connessione al database contenente i test da eseguire e la memorizzazione dei risultati dei test di penetrazione;

- Weseth Box:
  Oggetto chiave del sistema, consiste in un componente plug-and-play, il che significa che basta collegarlo al dispositivo da testare e sarà subito pronto a funzionare; il cliente ha una grande varietà di alternative di test in quanto la Box è fornita di interfacce multiple e può essere connessa direttamente al dispositivo tramite:

  – CAN;
  – WiFi;
  – Bluetooth;
  – Ethernet;
  – USB;

  consentendo anche lo streaming di audio e video. Una particolarità degna di nota è la caratteristica di connettersi al Weseth Server tramite una connessione wireless, utilizzando il protocollo LTE (connessione 4G), consentendo il trasferimento di dati e informazioni, senza richiedere l'accesso alla rete interna del cliente, evitando così ogni problema di sicurezza informatica e di proprietà intellettuale, legato alla conoscenza aziendale.

Una volta connessa la Weseth Box al componente da testare, sarà possibile selezionare tutti i test da eseguire, scaricandoli dal database della piattaforma: in questo modo si risparmiano tempo e risorse in quanto si riutilizzano test precedentemente scritti per altri componenti, tutt'al più adattati al caso in questione, con l'aggiunta di nuovi test specifici dove necessario. Questo costituisce un sistema in espansione, che crescerà in continuazione, aggiornando i test presenti con le nuove vulnerabilità scoperte, e aggiungendo ogni volta nuovi test, rendendo molto più facile e completa la fase di test. Infine non è richiesta capacità o conoscenza di scrittura dei test al cliente, in quanto la fase di test è completamente delegata all'azienda proprietaria della piattaforma, la quale consegnerà successivamente un rapporto contenente l'elenco e i risultati dei test.

Capitolo 5

Approccio integrato ISO/SAE 21434 e ISO 26262

La tesi che si vuole dimostrare è che l'integrazione tra i due processi di analisi di sicurezza funzionale (HARA) e di sicurezza informatica (TARA), porti a notevoli benefici in termini di tempo, costi, completezza degli scenari esaminati e una migliore definizione dei requisiti minimi che il componente deve rispettare per ridurre, entro un limite accettabile, il rischio di danno fisico, rispetto all'esecuzione separata dei due processi.

Al giorno d'oggi il processo di progettazione e costruzione di un veicolo ha subito notevoli cambiamenti in fatto di integrazione di tecnologie informatiche ed elettroniche all'interno dei veicoli e delle normative atte a controllare e valutare la sicurezza dei nuovi componenti. Vista la rapida evoluzione degli impianti e la sfrenata corsa all'innovazione, sorge però il problema di avere una normativa comune a tutti i costruttori, che sia uguale per tutti e al contempo aggiornata alle vulnerabilità odierne. Questo porta ad una rapida evoluzione delle leggi e dei regolamenti che obbligano i costruttori a conformarsi a quanto espresso nelle normative, mettendo in atto processi che possano garantire gli standard di sicurezza richiesti, talvolta modificando procedure preesistenti e radicate all'interno dell'organizzazione. Per quanto le normative entrino in vigore alcuni mesi dopo la propria emanazione (un esempio ne è la UNECE R155 emanata ed approvata dall'Unione Europea a Marzo 2021[7], entrò in vigore a giugno 2022 per i veicoli di nuova omologazione ed estesa a luglio 2024 a tutti i veicoli prodotti, definendo per le aziende dell'automotive specifici obblighi di cybersicurezza)[20], rimane comunque la difficoltà dei produttori di modificare il proprio processo interno, rimanendo al passo con le regolamentazioni e gli standard di sicurezza. Per questo motivo le aziende costruttrici e gli OEM sembrano essere molto raffazzonati in

materia di processi per l'applicazione e la valutazione di quanto espresso in queste normative riguardanti la sicurezza informatica e la sicurezza funzionale, modificando eventualmente il singolo processo interno ogni qual volta vi sia una modifica alla normativa, a discapito dell'integrazione e dell'ottimizzazione del processo intero.
Un secondo problema che si può riscontrare è la difficoltà di integrazione a causa del fatto che generalmente i due tipi di analisi TARA e HARA sono eseguiti da gruppi di lavoro differenti, ciascuno dei quali è esperto nel proprio campo di appartenenza. La proposta di integrazione ha come obiettivo quello di risolvere questa situazione senza bisogno di una formazione congiunta riguardo alla sicurezza informatica e alla sicurezza funzionale, fungendo da interfaccia di comunicazione tra i due risultati.
L'approccio a cui si sta puntando è descritto in maniera generale dalla figura 5.1 dove possiamo riconoscere il modello a V, precedentemente descritto all'interno delle normative ISO/SAE 21434 e ISO 26262, esprimendo concettualmente l'unione tra i due tipi di analisi: sul ramo discendente sinistro sono presenti le varie fasi di analisi (in rosso quelle legate al concetto di sicurezza funzionale, in nero quelle legate alla sicurezza informatica), mentre sul ramo destro ascendente, cronologicamente successivo alla fase di sviluppo del prodotto, sono presenti le varie fasi di valutazione e validazione delle misure di sicurezza implementate, considerando dapprima i singoli elementi e poi via via le varie integrazioni, fino ad arrivare alla fase di test del sistema nella sua interezza.

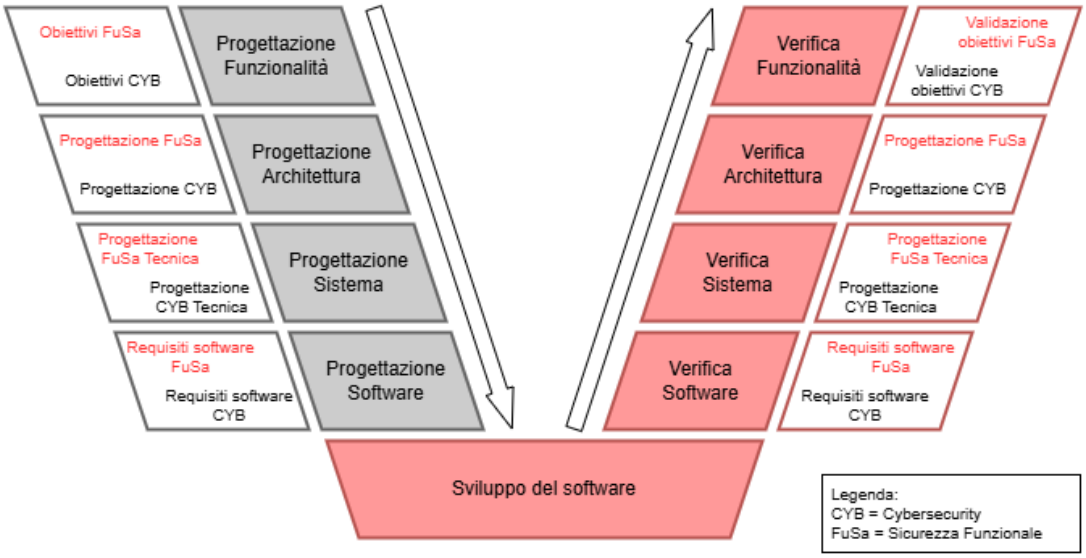

Figura 5.1: Integrazione concettuale di analisi HARA e TARA

Il punto focale di questa analisi integrata è la definizione delle interazioni tra le scale di misura di gravità del danno, adottando una soluzione che comprenda sia il

rischio di danno fisico, che quello di tipo informatico. La scelta è motivata dal fatto che il valore di severità di impatto del danno personale, ottenuto tramite l'analisi TARA, non tiene conto dei valori della durata e probabilità di Esposizione e della Controllabilità dell'evento da parte del conducente del veicolo o di un altro utente della strada, dando origine perciò a valori di rischio che potrebbero essere classificati diversamente tra i due tipi di analisi, risultando per questo motivo sottostimate o sovrastimate, in uno o nell'altro senso. Inoltre viene anche specificato come questo tipo di analisi non comprenda anche il tasso di rotture o di malfunzionamenti dei componenti, all'interno del periodo di utilizzo. Per raggiungere questo obiettivo si è optato per l'identificazione di una tabella che consenta la mappatura dei valori di ASIL, ottenuti con l'analisi HARA, sui valori di gravità dell'impatto definiti nell'analisi TARA, in modo tale da avere un contributo coerente dalla Sicurezza Funzionale, senza dover applicare ulteriori analisi, riducendo i tempi di progettazione e quindi i costi. Questo tipo di integrazione è già predisposto all'interno della normativa ISO/SAE 21434: lo si può trovare all'interno dell'allegato F in cui viene riportato come il valore di severità dell'impatto, relativo al danno fisico personale, sia tratto singolarmente dalla normativa ISO 26262, ma che se si volessero includere anche i valori di Esposizione e Controllabilità, sarebbe possibile farlo, fornendo un documento che ne spieghi l'integrazione logica.

5.1 Descrizione della proposta d'integrazione di analisi HARA e TARA

Analisi di un processo aziendale attuale

Durante la fase di ricerca del materiale e di conoscenza della materia, è stato possibile esaminare parzialmente un documento riguardante la proposta di un processo aziendale interno che mira ad applicare in parte l'integrazione tra analisi HARA e TARA. All'interno di questo documento è inclusa una tabella, identificata internamente all'azienda, con lo scopo di avere una comparazione tra i valori di ASIL e i valori di gravità del danno fisico, riportata in tabella 5.1.

Valore di ASIL (HARA)	**Gravità del danno (TARA)**
ASIL QM	Ignorabile (S0)
ASIL A, B	Moderato (S1)
ASIL C	Elevato (S2)
ASIL D	Severo (S3)

Tabella 5.1: Mappatura aziendale della severità del danno sui valori di ASIL

In tabella 5.2 si può osservare una rappresentazione dei valori di ASIL, ottenuti secondo quanto scritto all'interno della normativa ISO 26262, e colorati per gruppi di lettere ottenuti dalla classificazione indicata nella tabella 5.1, in modo tale da osservarne facilmente la distribuzione.

Gravità	**Esposizione**	**Controllabilità**		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Tabella 5.2: Mappatura aziendale della severità del danno sui valori di ASIL mediante colorazione

Come si può notare dalla tabella, la mappatura creata dall'azienda in questione, tende a sottostimare alcune delle casistiche identificate dalla singole celle, in particolare:

- Le casistiche con valore di ASIL C sono in totale tre ((S2, E4, C3), (S3, E3, C3) e (S3, E4, C2)) e possiamo notare come due di queste abbiano un valore di severità pari a S3, mentre seguendo la mappatura proposta dall'azienda, il valore di severità relativo ad un valore di ASIL C verrebbe approssimato su un valore di severità pari solamente ad Elevato (S2).

- Le casistiche con ASIL A e B invece sono sparse attraverso tutti i valori di severità del danno, e sono indicativamente quasi la metà dei valori (14 casi su 36 identificati) perciò raggrupparli tutti insieme come valore di severità del danno Moderato (S1) risulta essere riduttivo in quanto, in questo modo, alcuni valori, come ad esempio i casi relativi ad S3, vengono ridotti fino a due livelli di gravità.

Per visualizzare meglio il rapporto tra i valori di ASIL, mappati sui relativi valori di gravità, e il numero di casistiche che hanno subito una riduzione del valore di severità iniziale, si può osservare la tabella 5.3

Valore di ASIL	**Valore di Gravità**	**Numero di casi con riduzione**
ASIL QM	Ignorabile (S0)	18 su 30
ASIL A, B	Moderato (S1)	11 su 14
ASIL C	Elevato (S2)	2 su 3
ASIL D	Severo (S3)	0 su 1

Tabella 5.3: Rapporto dei valori con riduzione di severità secondo la mappatura aziendale

Proposta di integrazione

Per i motivi elencati alla fine della sottosezione precedente, la proposta di integrazione di questa tesi modifica la tabella 5.1 proponendo la mappatura dei valori secondo quanto indicato in tabella 5.4.

Valore di ASIL (HARA)	**Gravità del danno (TARA)**
ASIL QM	Ignorabile (S0)
ASIL A	Moderato (S1)
ASIL B	Elevato (S2)
ASIL C, D	Severo (S3)

Tabella 5.4: Mappatura proposta dei valori di ASIL sui valori di severità del danno

La nuova mappatura proposta è facilmente visualizzabile in tabella 5.5

Gravità	**Esposizione**	**Controllabilità**		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Tabella 5.5: Mappatura proposta della severità del danno sui valori di ASIL mediante colorazione

In maniera analoga alla tabella 5.3 possiamo nuovamente calcolare il rapporto

tra il numero di casistiche che hanno subito una riduzione del valore di severità e il numero dei casi con lo stesso valore di ASIL: il risultato è visibile in tabella 5.6.

Valore di ASIL	**Valore di Gravità**	**Numero di casi "sottostimati"**
ASIL QM	Ignorabile (S0)	18 su 30
ASIL A	Moderato (S1)	6 su 8
ASIL B	Elevato (S2)	3 su 6
ASIL C, D	Severo (S3)	0 su 4

Tabella 5.6: Rapporto dei valori con riduzione di severità secondo la mappatura proposta

Con la nuova mappatura proposta è interessante notare come i casi con valore di ASIL C e D, ovvero quelli che richiedono più rigorosità nel processo di mitigazione del rischio di danno, vengano mappati nel livello di gravità del danno Severo (S3) che è il massimo equivalente nella scala di gravità all'interno dell'analisi TARA, richiedendo ugualmente il massimo rigore.
Inoltre dal punto di vista strettamente numerico, il rapporto tra il numero di casi che hanno subito una diminuzione del valore di severità del danno, con la mappatura proposta, rispetto a quelli ottenuti mediante quella aziendale in esame, è visibile in tabella 5.7.

Valore di ASIL	**Confronto numero di casi "sottostimati"**
ASIL A, B	9 contro 11
ASIL C, D	0 contro 2

Tabella 5.7: Confronto tra i rapporti di sottostima dei valori di ASIL secondo le due mappature

Si può facilmente notare come la mappatura proposta abbia un minor numero di diminuzioni del valore di severità del danno, indice del fatto di non sottostimare alcune casistiche basandosi solo sui valori di Controllabilità ed Esposizione allo scenario, i quali restano comunque delle stime analitiche e probabilistiche, che non rispecchiano a pieno la realtà. Per chiarire il concetto è sufficiente osservare le tabelle 3.4 e 3.3 ove possiamo trovare nelle definizioni delle classificazioni i termini "probabilità", "in genere", "facilmente", etc. Per questo motivo la scelta di proporre la mappatura presentata in tabella 5.4 sovrastimando alcuni casi (ad esempio (S1,

E4, C3) o (S2, E4, C3)), dando più peso al valore di severità del danno rispetto ai valori di controllabilità ed esposizione, punta ad avere una gestione dello scenario di rischio secondo requisiti potenzialmente superiori a quelli necessari, ma in ogni caso cercando di sottostimarne il meno possibile.

Una volta creata la tabella di interfaccia tra i valori di ASIL e il valore di severità del danno fisico, gli scenari di pericolo identificati dall'analisi HARA, relativi alla sicurezza funzionale, possono essere aggiunti e/o eventualmente sostituiti a quelli identificati tramite l'analisi TARA, in modo tale da avere una copertura, il più possibile coerente e completa, dei possibili scenari di pericolo, secondo quanto brevemente rappresentato dal diagramma di flusso riportato in figura 5.2.

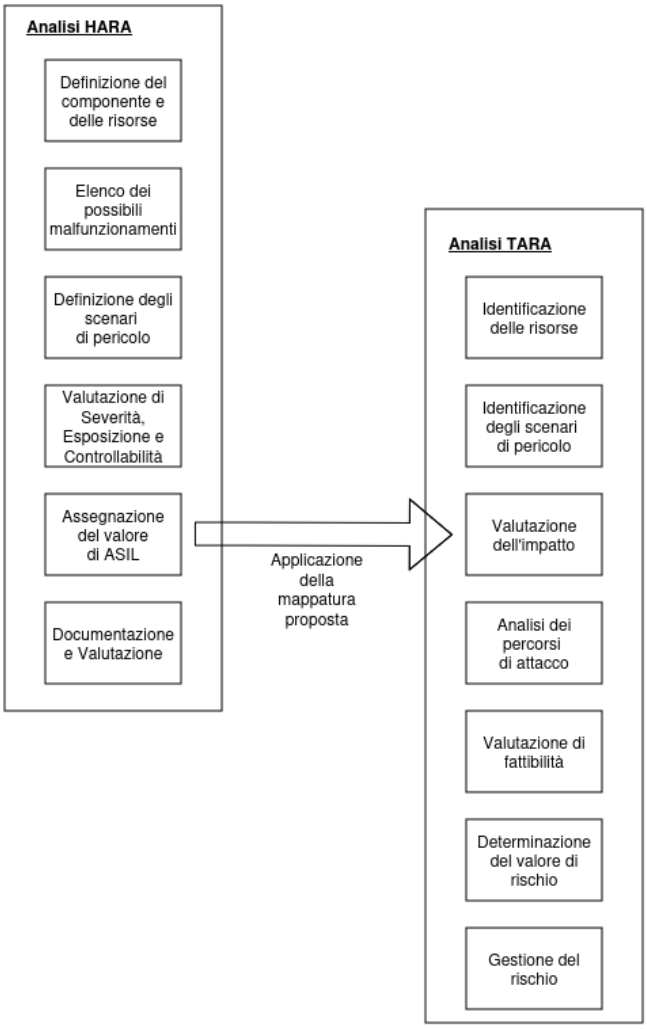

Figura 5.2: Integrazione tra analisi HARA e TARA

5.2 Applicazione dell'integrazione di HARA e TARA

Il progetto iniziale di questa tesi prevedeva l'applicazione dell'analisi proposta ad un caso reale, utilizzando un componente concreto, all'interno della progettazione di un autoveicolo: purtroppo non è stato possibile realizzare questo obiettivo in quanto le fasi di sviluppo, progettazione e validazione di un autoveicolo sono fasi delicate e difficilmente accessibili a personale esterno all'azienda che le sta eseguendo, oltre ad avere tempistiche decisamente superiori alla durata di un progetto di tesi. Per via di queste difficoltà le fasi di applicazione e validazione dei risultati di questa proposta d'integrazione, saranno svolte su un modello astratto di un dispositivo reale. Il componente sotto esame è un generico controllore con la funzione di "Gestione di Batteria ad Alto Voltaggio" (High Voltage Battery Management), presente sui veicoli a propulsione completamente elettrica o ibrida: il suo scopo è quello di gestire e fornire energia all'autoveicolo, evitando sovraccarichi ed eventuali danni alla batteria ed al mezzo, e trasportare l'energia ai componenti che la richiedono.

5.2.1 Analisi HARA del componente

In tabella 5.8 è rappresentata un estratto esemplificativo di un'applicazione dell'analisi HARA al caso in questione, con lo scopo di elencare le possibili casistiche che possano recare danno al conducente, ai passeggeri o ad eventuali altri utenti della strada.

Funzionalità	**Malfunzionamento**	**Pericolo**
Immagazzinare energia ad alto voltaggio	Voltaggio troppo alto alla batteria	Evento termico (surriscaldamento/incendio)
	Voltaggio troppo basso alla batteria	Scaricamento della batteria
	Sbilanciamento della carica nelle celle	Evento termico (surriscaldamento/incendio)
Fornire energia ad alto voltaggio	Voltaggio troppo alto dalla batteria	Evento termico (surriscaldamento/incendio)
		Danni ad altre ECU
	Voltaggio troppo basso dalla batteria	Perdita di potenza e funzionalità
Disconnettere la batteria in caso di malfunzionamento	Interruttore non si apre	Evento termico (surriscaldamento/incendio)
		Danni ad altre ECU
		Corto circuito e folgorazione
	Interruttore si apre senza un malfunzionamento	Troncamento della potenza e perdita di funzionalità

Tabella 5.8: Analisi HARA del controllore dell'energia ad alto voltaggio

Una volta identificati i possibili pericoli si procede con l'identificazione dei potenziali scenari di pericolo che possono causarli e alla loro classificazione secondo il valore di ASIL. Per semplificare l'analisi, sono stati riportati solo gli scenari relativi ai due casi peggiori: un evento termico dovuto ad un sovraccarico durante la fase di ricarica e l'improvvisa interruzione di energia a causa dell'apertura dell'interruttore di sicurezza durante la guida per via di un malfunzionamento. I risultati dell'analisi degli scenari sono riportati rispettivamente nelle tabelle 5.9 e 5.10.

Scenario	**Severità**	**Controllabilità**	**Esposizione**
Il veicolo è parcheggiato ed in carica, ambiente chiuso (es. garage)	Danno severo da evento termico	Più del 90% delle persone nelle vicinanze possono allontanarsi dal veicolo appena percepito il fumo/fuoco, ma lo spazio può essere limitato.	Si assume la ricarica quotidiana del veicolo
	3	2	4
Obiettivo di sicurezza: evitare un evento termico	ASIL C		

Tabella 5.9: Determinazione del valore di ASIL per un possibile evento termico

Scenario	**Severità**	**Controllabilità**	**Esposizione**
Il veicolo è in movimento su strada pubblica	Arresto del veicolo e possibile tamponamento	Perdita di propulsione e funzionalità di aiuto in sterzo e frenata	Si assume l'utilizzo quotidiano del veicolo
	3	3	4
Obiettivo di sicurezza: evitare la disconnessione improvvisa della batteria in caso di falso malfunzionamento	ASIL D		

Tabella 5.10: Determinazione del valore di ASIL per un possibile evento di troncamento della potenza

Dall'analisi dello scenario relativo all'evento termico, identificato in tabella 5.9, possiamo notare come la casistica di gravità, controllabilità ed esposizione (S3, C2, E4) equivalga, secondo la tabella 3.5, ad un valore di ASIL C; per quanto riguarda invece lo scenario relativo alla perdita di potenza, in tabella 5.10, abbiamo una casistica pari a (S3, C3, E4) che corrisponde ad un valore di ASIL D.
Una seconda informazione da notare è che entrambi gli scenari hanno un valore di

gravità pari a Severo(S3) in quanto entrambi possono causare danni permanenti, sino in estremo il decesso.

5.2.2 Analisi TARA del componente

Parallelamente all'analisi HARA possiamo svolgere un'analisi TARA esemplificativa del componente con la quale andiamo ad analizzare i possibili comportamenti di un attaccante esterno con lo scopo di deviarlo dal corretto funzionamento; un esempio è rappresentato in tabella 5.11.

Risorsa	**Proprietà**	**Danno**
Parametri operativi del gestore della batteria in memoria	Integrità	Parametri invalidi salvati in memoria
Canale di comunicazione tra i sensori e il controllore	Integrità, Autenticità	Eliminazione delle informazioni (deletion)
		Manomissione dei dati sul canale (alteration)
		Inserimento di valori falsi (creation)
Canale di comunicazione tra il controllore e l'interruttore	Integrità, Autenticità	Eliminazione delle informazioni (deletion)
		Inserimento di valori falsi (alteration)

Tabella 5.11: Analisi TARA del controllore dell'energia ad alto voltaggio

All'interno della tabella 5.11 stiamo ipotizzando lo scenario di un attaccante che vada a:

- modificare i parametri operativi di ricarica della batteria;
- ottenere il controllo del canale di comunicazione tra il controllore e i sensori e/o tra il controllore e l'attuatore, acquisendo la capacità di filtrare, modificare o inserire dati.

In entrambi i casi è possibile creare le condizioni per causare i malfunzionamenti osservati nell'analisi HARA del punto precedente (tabelle 5.9 e 5.10).
A questo punto si può procedere con le valutazioni dei livelli di rischio delle casistiche rilevate dalla tabella 5.11, prevista dall'analisi TARA, riportate rispettivamente nelle tabelle 5.12 e 5.13.

Gravità danno fisico	**Impatto Finanziario**	**Impatto Operativo**	**Impatto su Privacy**	**Livello di Impatto**
Manomissione del firmware attraverso la porta JTAG porta a rischi per l'utente	L'abuso della porta JTAG può diventare una vulnerabilità ad alto rischio delle ECU e portare a costi di manutenzione addizionali	L'abuso non autorizzato della porta JTAG porta a malfunzionamenti delle funzioni principali	Nessuno	
S2: Elevato	F2: Elevato	O2: Elevato	P0: Ignorabile	**IL3**

Tabella 5.12: Valutazione di Impatto TARA per la manomissione del Firmware

Gravità danno fisico	**Impatto Finanziario**	**Impatto Operativo**	**Impatto su Privacy**	**Livello di Impatto**
Manomissione del canale di comunicazione CAN-bus porta a rischio di incidente	Il controllo malevolo del canale è una vulnerabilità ad alto rischio delle ECU e può portare a costi di manutenzione e riparazione addizionali	L'abuso non autorizzato del canale di comunicazione porta a malfunzionamenti delle funzioni principali	Nessuno	
S3: Severo	F2: Elevato	O3: Severo	P0: Ignorabile	**IL4**

Tabella 5.13: Valutazione di Impatto TARA per la manomissione del canale

Una volta identificati i possibili modi in cui un attaccante possa modificare i parametri operativi o guadagnare l'accesso al canale, si procede con l'analisi di fattibilità dei percorsi di attacco riportate nelle tabelle 5.14 e 5.15.

Pericolo	**Scenario di pericolo**	**Percorso d'attacco**	**Potenzialità dell'attacco**	**Livello di fattibilità dell'attacco**
Modificare il software della ECU	Utilizzo illegale della porta JTAG	(1) Ottenere informazioni sull'interfaccia JTAG dalla scheda hardware (2) Uso illegale della porta JTAG	Tempo: <1 settimana Esperienza: Esperto Conoscenza: Ristretta Finestra di Opportunità: Difficile Equipaggiamento: Specializzato	**FL1**: Molto basso
Obiettivo di sicurezza	Creare un meccanismo di controllo dell'autorizzazione all'accesso per prevenire la manomissione dei dati			

Tabella 5.14: Valutazione TARA della fattibilità dell'attacco per la manomissione del Firmware

Pericolo	**Scenario di pericolo**	**Percorso d'attacco**	**Potenzialità dell'attacco**	**Livello di fattibilità dell'attacco**
Filtrare, modificare o creare falsi dati sul CAN-bus	Utilizzo illegale della porta OBD	(1) Sniffing dei pacchetti dati sul canale CAN-bus (2) Invio di informazioni malevole al controllore per deviarne il comportamento	Tempo: <1 settimana Esperienza: Esperto Conoscenza: Ristretta Finestra di Opportunità: Difficile Equipaggiamento: Specializzato	**FL1**: Molto basso
Obiettivo di sicurezza	Creare un meccanismo di controllo di autenticazione del mittente e dell'integrità dei dati per prevenirne la manomissione			

Tabella 5.15: Valutazione TARA della fattibilità dell'attacco al canale di comunicazione

Una volta effettuata la valutazione delle fattibilità degli attacchi, si procede con

la determinazione dell'effettivo valore di rischio secondo la tabella 5.16, estratta dalla normativa ISO 21434, e la conseguente scelta di gestione del rischio.

Valore di Rischio		**Livello Fattibilità dell'attacco (FL)**			
		FL1	**FL2**	**FL3**	**FL4**
Livello di Impatto (IL)	**IL1**	1	1	1	1
	IL2	1	2	2	3
	IL3	1	2	3	4
	IL4	2	3	4	5

Tabella 5.16: Valutazione del rischio dalla normativa ISO/SAE 21434

Per quanto riguarda lo scenario di manomissione del firmware abbiamo ottenuto un livello di impatto pari a IL3 (tabella 5.12) e di fattibilità dell'attacco pari a FL1 (tabella 5.14), perciò risulta un valore di rischio pari a 1, riportato in tabella 5.17.

Valore di Rischio	**Scelta di gestione**	**Obiettivo di Sicurezza**
1	Riduzione del rischio	Fornire un meccanismo di autorizzazione all'accesso per evitare manomissioni di dati non autorizzate

Tabella 5.17: Valutazione e gestione del livello di rischio di manomissione del Firmware

Invece per lo scenario di manipolazione dei canali di comunicazione abbiamo ottenuto un livello di impatto pari a IL4 (tabella 5.13) e di fattibilità dell'attacco pari a FL1 (tabella 5.15), perciò risulta un valore di rischio pari a 2, riportato in tabella 5.18.

Valore di Rischio	**Scelta di gestione**	**Obiettivo di Sicurezza**
2	Riduzione del rischio	Fornire un meccanismo di autenticazione del mittente e integrità dei dati in modo tale da evitare attacchi di tipo MITM

Tabella 5.18: Valutazione e gestione del livello di rischio dei manipolazione del canale

5.2.3 Validazione

Nella sezione precedente possiamo osservare come lo scenario di pericolo relativo all'evento termico, identificato con l'analisi HARA in tabella 5.9, venga classificato con un livello di ASIL C, il quale indica quindi la necessità di un impegno elevato per rendere il dispositivo sicuro.
Per quanto concerne invece l'analisi TARA, il valore di gravità del danno fisico, indicato nella prima colonna della tabella 5.12, è stato valutato come Elevato(S2), secondo le indicazioni fornite all'interno della normativa ISO 21434.
La proposta di integrazione dei due tipi di analisi, espressa in tabella 5.4, effettua la mappatura dei valori di ASIL dell'analisi HARA, sui valori di gravità del danno fisico utili per l'analisi del livello di impatto, la quale è necessaria per l'analisi TARA.
Come è possibile notare, si ha una discrepanza tra il valore di gravità del danno, ricavato dall'analisi TARA, pari ad Elevato(S2) (tabella 5.12), rispetto al valore di severità del danno Severo(S3) (tabella 5.9), ricavato dall'analisi HARA, per lo stesso scenario di pericolo: si può quindi affermare che l'analisi TARA "minimizza" l'entità del danno rispetto all'analisi HARA. Applicando invece l'integrazione proposta in questa tesi (in tabella 5.4), si ha una mappatura del valore di ASIL C su un valore di gravità del danno pari a Severo(S3), mantenendo così una corrispondenza tra le valutazioni delle due analisi ed evitando così eventuali sottostime della gravità del danno.
Per questo scenario la modifica non causa alcuna variazione al valore di rischio generale, ma comporta comunque una maggiore richiesta di risorse per rendere sicuro il singolo scenario.

Per quanto riguarda invece lo scenario di pericolo relativo alla perdita di potenza dovuta alla disconnessione ingiustificata della batteria per un falso allarme, identificato in tabella 5.10, possiamo notare che venga classificato come un ASIL D, in quanto il troncamento di potenza durante la marcia può essere causa di incidenti gravi.
Parallelamente, nella conduzione dell'analisi TARA, il valore di gravità del danno fisico, della manomissione del canale CAN-bus che può causare lo scenario di pericolo identificato, indicato nella prima colonna della tabella 5.13, è stato valutato come Severo(S3), secondo le indicazioni fornite all'interno della normativa ISO 21434, in quanto può causare gravi danni a causa dei malfunzionamenti riscontrabili.
In questo secondo caso è possibile notare come la mappatura proposta in questa tesi in tabella 5.4, effettui la correlazione del valore di ASIL D identificato, proprio sul valore di gravità del danno Severo(S3) identificato nell'analisi TARA: questo a dimostrazione del fatto che la mappatura può essere anche coerente tra le due

tipologie di analisi.

5.2.4 Vantaggi

Il vantaggio principale di questo tipo d'integrazione è la delega, da parte dell'analisi TARA, della determinazione del valore di gravità del danno fisico causato in uno scenario di pericolo, all'analisi HARA la quale ha lo specifico compito di valutare la severità del danno fisico in caso di malfunzionamento di un componente. In questo modo si ha una valutazione potenzialmente più precisa dello scenario ma soprattutto si ha una corrispondenza coerente tra le due analisi.
Una corretta valutazione dell'impatto porta ad una migliore gestione dello scenario di pericolo, la quale si traduce in un'adeguata quantità di lavoro e meccanismi di protezione implementati, in modo tale da poter ottenere una maggior sicurezza nell'utilizzo del componente.

Capitolo 6

Conclusioni

6.1 Risultati Ottenuti

L'integrazione tra i valori ottenuti mediante l'analisi HARA e l'analisi TARA porterebbe ad una miglior valutazione dell'entità del danno fisico in quanto: la valutazione è completamente delegata all'analisi HARA la quale, tenendo conto anche delle proprietà di controllabilità ed esposizione allo scenario di pericolo, offrirebbe una valutazione di severità del danno più accurata. Nel capitolo precedente viene spiegato come l'applicazione della proposta d'integrazione, di questa tesi, cerchi di non sottostimare il rischio di danno fisico rispetto a quanto si potrebbe ottenere considerando solo l'analisi TARA.
Purtroppo i vantaggi ottenuti mediante l'applicazione dell'integrazione non sono effettivamente misurabili se non a posteriori dell'applicazione ad un componente reale, su cui poter effettuare anche una successiva fase di test (ad esempio tramite la piattaforma Weseth descritta precedentemente) e di prove su strada, valutando il numero di scenari di pericolo che hanno effettivamente provocato danni e paragonando i risultati con quelli di un componente analogo su cui però siano state applicate le due analisi in maniera separata. L'integrazione proposta punta ad avere un valore coerente tra le due analisi ed eventualmente a sovrastimare alcune casistiche, in modo tale da sottostimarne il minor numero possibile: questo si traduce in una quantità di lavoro richiesta maggiore, perciò è logico immaginare come a maggior lavoro, atto a rendere sicuro un componente, corrisponda ad una maggiore sicurezza del componente stesso.

6.2 Difficoltà del percorso

Durante la produzione di questa tesi abbiamo dovuto superare molte difficoltà tecniche e pratiche: l'obiettivo iniziale era quello di applicare l'integrazione tra

l'analisi HARA e l'analisi TARA proposta ad un caso di studio concreto (un autoveicolo in fase di progettazione), comprendendo anche le fasi di testing per dimostrare l'effettiva efficacia dei concetti espressi. Purtroppo abbiamo dovuto ricrederci molto presto in quanto la mole di lavoro necessaria era decisamente superiore a quanto una sola persona possa fare durante il periodo necessario per lo svolgimento di una tesi di laurea, perciò è stato necessario deviare su altre strategie, tra cui l'applicazione dell'analisi integrata ad analisi HARA e TARA già svolte su veicoli di recente progettazione e produzione. Purtroppo si è stati nuovamente obbligati a cambiare piani poiché ci si è imbattuti in un'indisposizione generale, delle varie aziende contattate, al fornire i risultati delle analisi sopra citate in quanto non ufficialmente un dipendente. Tutto questo, sommato insieme, ha portato la mia tesi a concludersi con una semplice applicazione teorica su un componente astratto, dimostrando solo sulla carta la sua effettiva efficacia.

6.3 Sviluppi Futuri

Sicuramente un possibile sviluppo di questa tesi sarebbe la sua applicazione pratica all'interno delle fasi di progettazione di un autoveicolo, dimostrando in questo modo gli effettivi vantaggi prodotti in termini di sicurezza, verificabili completamente solo dopo la sua costruzione. Questo ulteriore lavoro comprenderebbe anche lo sviluppo di test, per valutare la corretta gestione degli scenari di rischio, e la loro applicazione tramite ad esempio la piattaforma Weseth dell'azienda Drivesec[19] descritta nel capitolo 3.
Purtroppo penso che l'implementazione di una strategia simile a quella proposta all'interno di questa tesi non sarà applicata in tempi brevi dalle aziende in quanto i meccanismi di applicazione e verifica dei due tipi di analisi sono ancora molto differenti, oltre ad essere eseguite da gruppi di lavoro separati, con diverse conoscenze e capacità.

Bibliografia

[1] Bruno Crispo Cesar Bernardini Muhammad Rizwan Asghar. «Security and privacy in vehicular communications: Challenges and opportunities». In: *Vehicular Communications* 10 (2017), pp. 13–28 (cit. a p. 1).

[2] Christoph Hammerschmidt. *Number of automotive ECUs continues to rise.* 2019. URL: https://www.eenewseurope.com/en/number-of-automotive-ecus-continues-to-rise/ (cit. a p. 1).

[3] Marianna Capozi Milena Gabanelli Diego Antonelli. *Dove va il mercato: 600 milioni di auto elettriche entro 20 anni.* 2017. URL: www.report.rai.it/dj/auto-elettriche-mercato-futuro/ (cit. a p. 2).

[4] Microsoft Security. *Che cos'è la sicurezza informatica?* URL: https://support.microsoft.com/it-it/topic/che-cos-%C3%A8-la-sicurezza-informatica-8b6efd59-41ff-4743-87c8-0850a352a390#articleFooterSupportBridge=discoverBridge (cit. a p. 3).

[5] Inc. Infoshare Systems. *How cyber security threats are impacting the automotive industry.* 2023. URL: https://www.linkedin.com/pulse/how-cyber-security-threats-impacting-automotive-industry-1f (cit. alle pp. 6, 7).

[6] *Road Vehicles - Cybersecurity Engineering.* Ginevra, SW: ISO/SAE 21434, 2021 (cit. a p. 9).

[7] *Cyber security and cyber security management system.* Ginevra, SW: UNECE R155, 2021 (cit. alle pp. 27, 61).

[8] *Classificazione dei veicoli.* Codice della Strada - Art.47, 2023 (cit. a p. 27).

[9] *Road vehicles — Functional safety.* Ginevra, SW: ISO/SAE 26262, 2018 (cit. a p. 37).

[10] Byhon. *ISO 26262 ASIL: cos'è l'Automotive Safety Integrity Level.* 2018. URL: https://www.byhon.it/it/iso-26262-asil-cose-lautomotive-safety-integrity-level/ (cit. alle pp. 41, 45).

[11] *Automotive Software Process Improvement and Capability Determination.* Berlino, DE: VDA Working Group 13, 2023 (cit. a p. 48).

[12] Marcel Rumez Jürgen Dürrwang Johannes Braun, Reiner Kriesten e Alexander Pretschner. «Enhancement of Automotive Penetration Testing with Threat Analyses Results». In: *SAE International Journal of Transportation Cybersecurity and Privacy* (nov. 2018) (cit. alle pp. 52–55).

[13] Zhaojing Zhang Feng Luo Yifang Jiang, Yi Ren e Shuo Hou. «Threat Analysis and Risk Assessment for Connected Vehicles: A Survey». In: *Hindawi - Security and Communication Networks* 2021 (2021), p. 19 (cit. a p. 53).

[14] Christoph Schmittner, Thomas Gruber, Peter Puschner e Erwin Schoitsch. «Security Application of Failure Mode and Effect Analysis (FMEA)». In: *Lecture Notes in Computer Science* 8666 (set 2014), pp. 310–325 (cit. alle pp. 53, 54).

[15] National Protective Security Authority. *Security-Informed Hazard and Operability study*. 2022. URL: `https://www.npsa.gov.uk/resources/cae-security-informed-hazard-operability-study-hazop` (cit. a p. 54).

[16] Nataliya Shevchenko. «Threat Modeling: 12 Available Methods». In: *Enterprise Risk and Resilience Management* (dic. 2018) (cit. a p. 54).

[17] Filiberto Santoro. *Penetration test, cos'è, come funziona e a che serve*. 2018. URL: `https://www.cybersecurity360.it/soluzioni-aziendali/penetration-test-cose-come-funziona-e-a-che-serve/` (cit. a p. 56).

[18] IBM. *Che cos'è un test di penetrazione?* 2018. URL: `https://www.ibm.com/it-it/topics/penetration-testing` (cit. a p. 58).

[19] DriveSec. *Weseth*. 2023. URL: `https://www.drivesec.com/weseth/` (cit. alle pp. 59, 79).

[20] Nicoletta Buora. *Cybersecurity nell'automotive: a giugno la normativa Unece R155*. Mar. 2022. URL: `https://www.automazionenews.it/cybersecurity-nellautomotive-a-giungo-la-normativa-unece-r155/` (cit. a p. 61).

Ringraziamenti

Alla fine di questo elaborato, mi sembra doveroso dedicare uno spazio per ringraziare tutte le persone che, con il loro supporto, mi hanno aiutato e supportarto lungo tutto questo percorso di approfondimento delle conoscenze acquisite durante gli anni universitari.

Per prima cosa, vorrei ringraziare il mio relatore professore Riccardo Sisto, per i suoi consigli e per la sua disponibilità.

In secondo luogo vorrei ringraziare il mio tutor aziendale dott. Carlo La Torre, presso l'azienda 4S Group dove ho svolto la mia tesi, per avermi supportato durante il percorso nella ricerca del materiale, nelle riunioni con altre aziende e nella ricerca di un caso pratico di studi.

Una menzione speciale risulta necessaria anche per l'ingegner Gaetano Fiaccola e l'ingegner Siavash Aslani per il loro aiuto nel chiarire i molti dubbi e nel trovare un esempio su cui poter applicare la tesi proposta.

Infine desidero ringraziare i miei familiari e Claudia, i quali mi hanno supportato e accompagnato durante tutti questi anni e mi hanno permesso di arrivare fino a questo traguardo.