MASTER OF SCIENCE
IN ENGINEERING

TSM_SecIndOpT

Threat models in OT systems (II)

Version: 1.0, by K. Marty

Luca Haab | 25.04.2025 | Cours MSE

Whoami

Kilian Marty

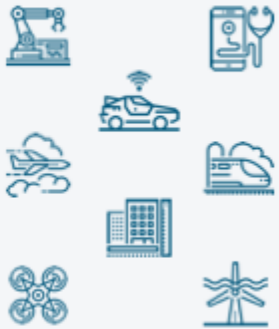
CEO | Cyber security consultant at CertX Solutions SA

Kilian.marty@certx.com

Our ecosystem

CertX AG is the First Swiss Certification Body for Functional Safety, Cyber Security and AI accredited by Swiss Accreditation Service (SAS)

CertX Solutions is a consultancy company supporting customers to design, implement and maintain best security, safety and AI practices for reaching compliance with regulatory framework and State-of-the-Art references



Threat models in OT systems – Agenda

MODULE A

Introduction to Threat Analysis & Risk Assessment [TARA]

Threat Analysis & Risk Assessment introduction & walkthrough

- Risk assessment scope: System vs Product perspective
- Key concepts: Security-by-design, holistic approach, defense-in-depth…
- TARA primitives & relationships
- TARA walkthrough part I
  - System definition & security attributes
  - Damage scenario & impact rating
  - Threat scenario identification

Medical environment use case – Domestic medical device – Part 1

- System under Considerations [SuC] definitions & damages scenario
- Threat scenario identification

MODULE B

Applied Threat Analysis & Risk Assessment [TARA]

Threat Analysis & Risk Assessment walkthrough follow-up

- TARA walkthrough part II
  - Attack path analysis & feasibility rating
  - Risk value computation & treatment decisions

Medical environment use case – Domestic medical device – Part 2

- Attack trees & feasibility rating
- Risk values & alternative treatment

Wrap-up and challenges

- Upcoming regulations & challenges

Medical environment use case – Professional medical device

[optional housework]

Use case #1: Domestic Medical Device

System definition

The Ankle Monitor Predictor of Stroke (AMPS)

AMPS is a fictional home use medical device worn at night (or when resting) by patients considered at risk for a stroke. The AMPS system gathers medical readings that can be later analyzed by a medical professional. While the system can help predict a patient's risk of experiencing a stroke, it does not alert – and is not intended to alert – if a stroke is imminent or occurring [1] [3]

- *Period of expected use: One to three months*
- *Medical capability: Diagnostic only*
- *Device invasiveness: Low (easily removable, like a wristwatch)*

Scenario

Alice has been informed by her doctor, based on her family history and several other risk factors, that she is at increased risk of experiencing a stroke. To gain further insight and determine a treatment plan, her doctor has instructed her to take the AMPS system home and wear it when she sleeps to take readings. She is also directed to install a **companion app on her phone** that will connect to the **AMPS system** (via Bluetooth Low Energy) and upload the readings every day to the **AMPS cloud service**, where they will be analyzed by an automated algorithm. Alice's doctor will check the results after the first week to identify any immediate causes of concern, and they will schedule a follow-up consult in two months

Use case #1: Domestic Medical Device

System definition

AMPS Device

AMPS is a health monitoring system worn on a patient's ankle when they are resting. It has the following specifications and capabilities:

- On/off switch
- Physical Bluetooth pairing button
- Proprietary stroke-predicting sensor.
- Heart rate monitor
- Body temperature sensor
- Bluetooth Low Energy (BLE) connectivity
- Onboard computer and flash storage that can store up to two weeks of patient data for later transmission

AMPS Cloud Service

The AMPSCS is a collection of virtual machines hosted in a cloud infrastructure. It consists of the following functionality:

- An application gateway server to inspect and limit traffic going into the AMPSCS systems
- A set of backend services that perform analysis of the patient data
- A collection of patient-facing services that communicate with the patient app, provide a web portal for patients to register their AMPS device, and authorize clinicians to view their data
- A collection of health delivery organization (HDO)-facing services that provide a web portal for clinicians to create an account and access a patient's data
    - Clinicians' access to the portal using a web browser.
    - Authentication is provided via username and password.
    - Clinician service identifiers that clinicians can provide to patients so the patients can authorize them through the app.
    - The clinicians can view a summary of the patient's raw data and the analysis performed by the AMPSCS backend algorithms.
    - The ability for clinicians to download a patient's data via an encrypted zip file.

[13]

Use case #1: Domestic Medical Device

System definition

AMPS Patient App

There are two different versions of the patient app, one for Apple iOS, and another for Android devices. Both apps contain the following functionality:

- It can pair with the AMPS device via Bluetooth.
- It contains an interface for a patient to create an account with the AMPS cloud services, register an AMPS device, and authorize clinicians to view their data.
- If the patient gives permission to the app, it will automatically connect to the AMPS device once a day and upload readings to the AMPSCS. If the patient does not give it permission, the app will store the data retrieved from the AMPS device until a manual upload is initiated. The amount of data transferred per upload is typically less than 1 megabyte a day.
- The app will display status information to the patient, including the last time the app synced with the AMPSCS, a log of the days the app was able to pull data from the AMPS device, and a log listing if the AMPS device was successfully collecting data.
- There is a device management screen that primarily focuses on diagnosing Bluetooth connection problems, and common issues that may prevent the AMPS device from collecting data. In addition:
  - The app can wipe patient data from the AMPS device.
  - The app can check for and update the firmware of the AMPS device with new versions.
  - The app can revert the AMPS device to factory default settings.
- If the device does not successfully sync to the cloud services once every 24 hours, an in-app notice will appear directing the patient to sync their data. After 72 hours have elapsed since a successful sync, the patient will be emailed an automatic reminder. [13]

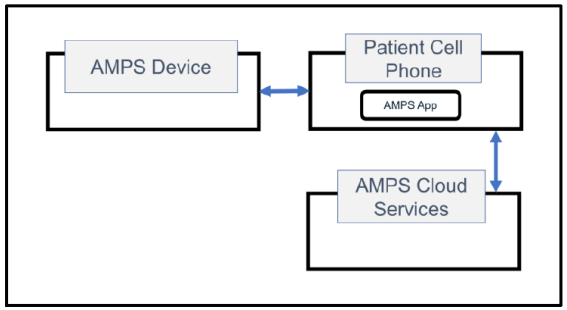
Use case #1: Domestic Medical Device

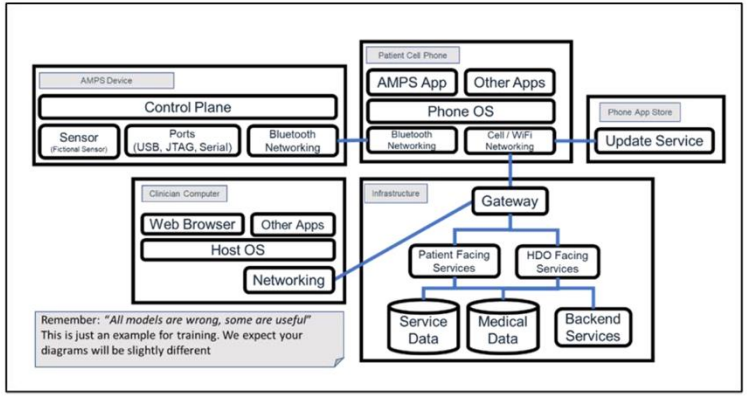
Exercice 1 – Data Flow Diagram

Draw the data flow diagram from Domestic Medical Device defined on previous slides, incl. system parts, communication flows and trust boundaries

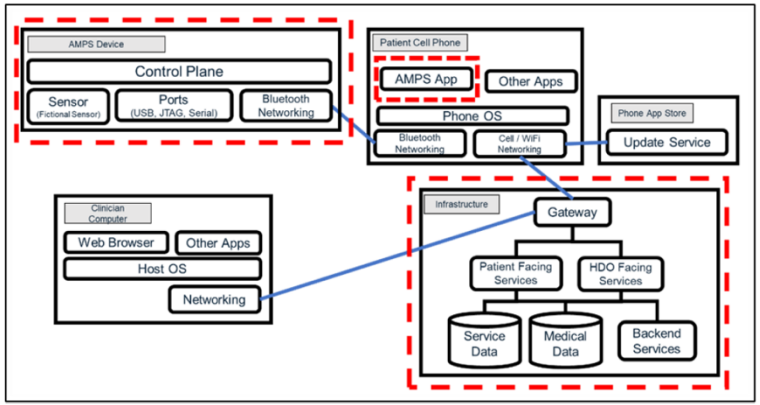
Use case #1: Domestic Medical Device

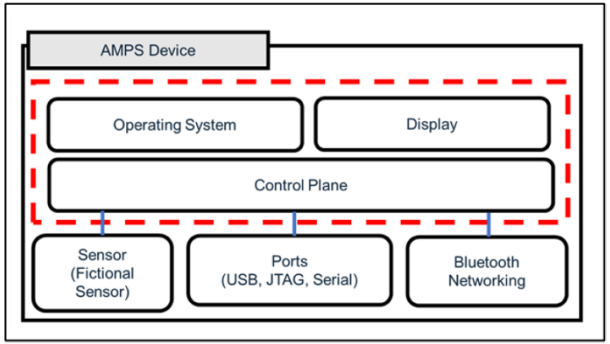
Ex1 Data Flow Diagram





[13]





swissuniversities

TARA Process – Walk through

How to identify the relevant threats, assess them using reasonable metrics and initiate the integration of such key security principles ?

By approaching the risk using a **systematic & holistic methodology**

I **Understand your system / product**

II Identify the potential consequences

II Identify how feasible compromissions are

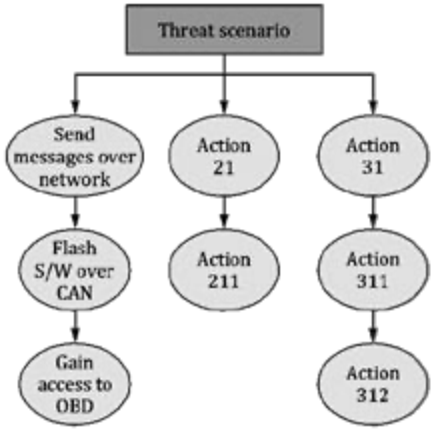
III Compute risk values & take risk-based treatment decisions, either

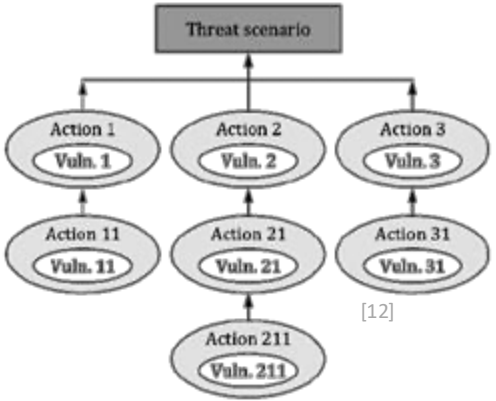
swissuniversities

TARA Process – 2nd step (a) – Attack trees

Threat scenarios shall be analyzed to describe possible attack paths. An attack path analysis approach can be based on:

- Top-down approaches such as attack trees, attack graphs, taxonomy mnemonic-based approaches (e.g., STRIDE): is useful in the concept and development phases when implementation of the current item or component is not available, or when effort is directed toward building attack hypotheses or attack path models.
- Bottom-up approaches (e.g., the output of vulnerability analysis): is most commonly used when an implementation of the item or component is available, or when hypotheses or attack model are to be confirmed.
- Combination of top-down and bottom-up



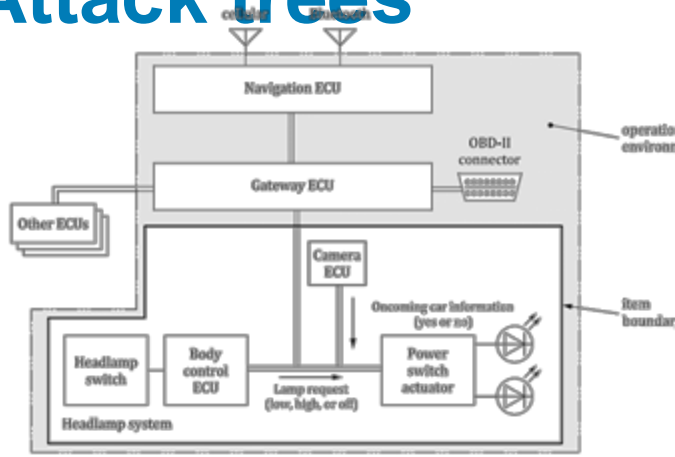


[12]

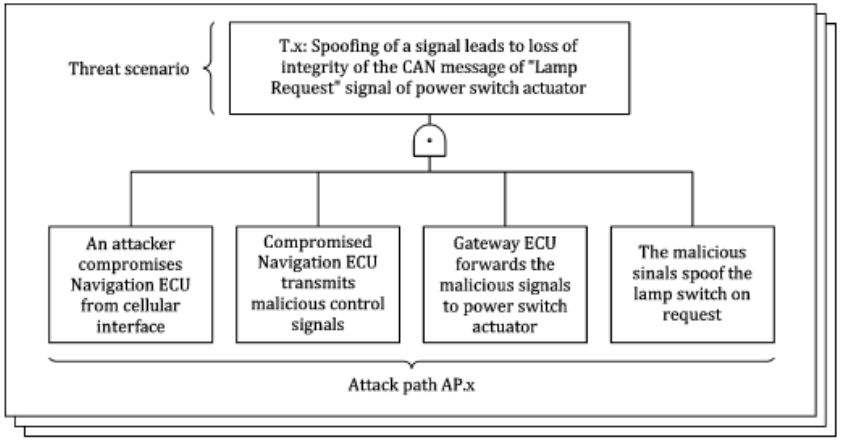
TARA Process – 2nd step (a) – Attack trees

Example from automotive industry [ISO/SAE 21434, annex H]

Threat Scenario No.	Threat Scenario	Attack Path No.	Attack Path
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	An attacker compromise Navigation ECU from Cellular interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		AP.y	An attacker compromise Navigation ECU from Bluetooth interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		AP.z	An attacker sends malicious control signals from OBD2 connector
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		:	:



[12]



TARA Process – 2nd step (a) – Attack feasibility

For each attack path the attack feasibility rating shall be determined as one of the following: high, medium, low, or very low. Several methods are existing, depending on company strategy, available information and maturity of system / product development and implementation

- Attack vector-based approach: based on the evaluation of the predominant attack vector of the attack path -> basic approach but could be useful for early-stage assessment

[12]

- CVSSx based approach: should be determined based on the exploit metrics group of the base metrics, including attack vector, attack complexity, privileges required, and user interaction

- Attack potential-based approach (see ISO/IEC 18045 for factors): should be determined based on core factors including elapsed time, specialist expertise, knowledge of the item or component, window of opportunity, and equipment

[12]

TARA Process – 2nd step (a) – Attack feasibility

Attack vector-based approach (see ISO/SAE 21434 annex G for additional information about criteria)

Attack feasibility rating	Criteria
High	**Network:** Potential attack path is bound to network stack without any limitation. EXAMPLE 1 Cellular network connection making the ECU directly connected and accessible on the internet.
Medium	**Adjacent:** Potential attack path is bound to network stack; however, the connection is limited physically or logically. EXAMPLE 2 Bluetooth interface, virtual private network connection.
Low	**Local:** Potential attack path is not bound to network stack and threat agents require direct access to the item for realizing the attack path. EXAMPLE 3 Universal serial bus mass storage device, memory card.
Very low	**Physical:** Threat agents require physical access to realize the attack path.

[12]

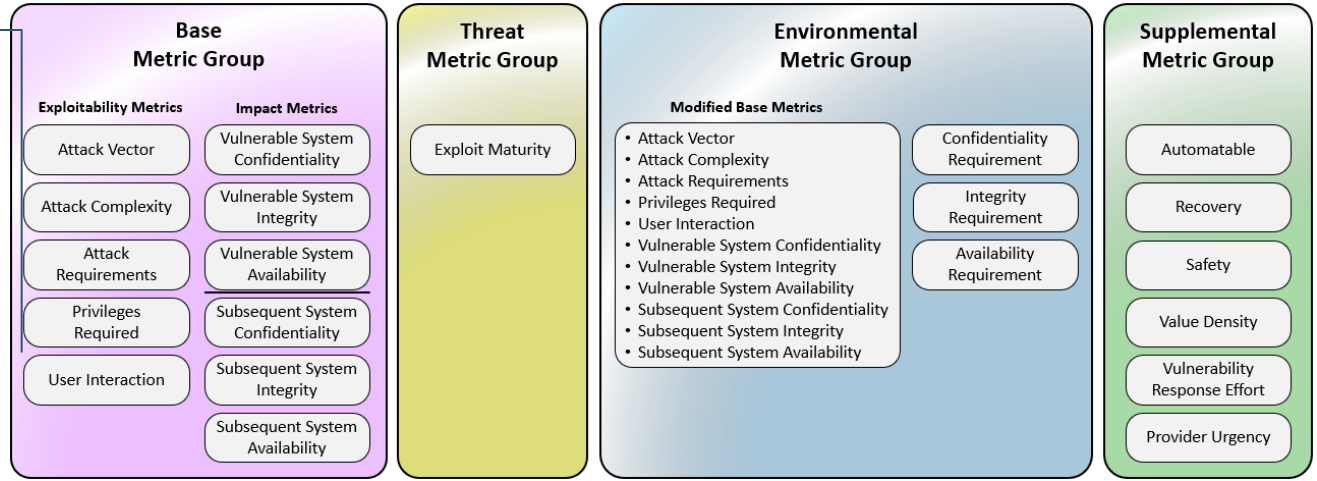
TARA Process – 2nd step (a) – Attack feasibility

CVSS4 based approach (may provide both impact & feasibility information since CVSS4)

- Require a higher level of cyber security maturity
- Allow a smooth integration of later stages vulnerability considerations

E = 8,22 x V x C x P x U

Attack feasibility rating	CVSS exploitability value
High	2,96 - 3,89
Medium	2,00 - 2,95
Low	1,06 - 1,99
Very low	0,12 - 1,05



TARA Process – 2nd step (a) – Attack feasibility

Attack potential-based approach (see ISO/IEC 18045 for factors):

Elapsed time		Specialist expertise		Knowledge of the item or component		Window of opportunity		Equipment	
Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value
≤1 day	0	Layman	0	Public	0	Unlimited	0	Standard	0
≤1 week	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
≤1 month	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
≤6 months	17	Multiple experts	8	Strictly confidential	11	Difficult/ none	10	Multiple bespoke	9
>6 months	19								

Attack feasibility rating	Values
High	0 - 9
	10 - 13
Medium	14 - 19
Low	20 - 24
Very low	≥ 25

[12]

TARA Process – 2nd step (a) – Attack feasibility

Attack vector-based approach applied to automotive use case

Threat Scenario No.	Threat Scenario	Attack Path No.	Attack Path
Tx	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	APx	An attacker compromise Navigation ECU from Cellular interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		APy	An attacker compromise Navigation ECU from Bluetooth interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		APz	An attacker sends malicious control signals from OBD2 connector
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		:	:

	Attack path	Attack feasibility rating
i.	Attacker compromises navigation ECU **from cellular interface.**	High
ii.	Compromised navigation ECU transmits malicious control signals.	
iii.	Gateway ECU forwards malicious signals to power switch actuator.	
iv.	Malicious signals spoof the lamp request (ON).	
i.	Attacker compromises navigation ECU **from Bluetooth interface.**	Medium
ii.	Compromised navigation ECU transmits malicious control signals.	
iii.	Gateway ECU forwards malicious signals to power switch actuator.	
iv.	Malicious signals spoof the lamp request (ON).	
i.	Attacker sends malicious control signals **from OBD2 connector.**	Low
ii.	Gateway ECU forwards the malicious signals to power switch actuator.	
iii.	Malicious signals spoof the lamp request (ON).	

[12]

TARA Process – 2nd step (a) – Attack feasibility

Attack potential based approach applied to automotive use case

- Most comprehensive approach
- Applied by major actors across industries, incl. automotive, railway, automation, medical, pharmaceutical etc

Threat scenario	Attack path	Attack feasibility assessment						
		ET	SE	KoIC	WoO	Eq	Value	Attack feasibility rating
Denial of service of oncoming car information	i. Attacker compromises navigation ECU from cellular interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Attacker floods the communication bus with a large number of messages.	1	8	7	0	4	20	Low
	i. Attacker attaches a Bluetooth-enabled OBD dongle to OBD connector when vehicle is parking unlocked. ii. Attacker compromises driver's smartphone with Bluetooth interface. iii. Attacker sends message via smartphone and Bluetooth dongle to Gateway ECU. iv. Gateway ECU forwards malicious signals to power switch actuator. v. Attacker floods the communication bus with a large number of messages.	1	8	7	4	4	24	Low

Key
ET elapsed time
SE specialist expertise
KoIC knowledge of the item or component
WoO window of opportunity
Eq equipment

[12]

Threat Analysis & Risk Assessment – HOW

How to identify the relevant threats, assess them using reasonable metrics and initiate the integration of such key security principles ?

By approaching the risk using a **systematic & holistic methodology**

I **Understand your system / product**

II Identify the potential consequences

Identify how feasible compromissions are

III Compute risk values & take risk-based treatment decisions, either

swissuniversities

TARA Process – 3rd step – Risk matrices

A risk matrix is a representation of a mapping of levels of impact and attack feasibility respectively on given scales to risk values. The purpose of the determination of a risk value can be one of the following:

- to support criteria for decisions on risk treatment, incl. selection of controls;
- prioritization of risks for treatment;
- report to stakeholders; and
- monitoring of risk.

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	2	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

[12]

TARA Process – 3rd step – Risk matrices

Threat scenario	Aggregated attack feasibility rating	Impact rating	Risk value
Spoofing of a signal leads to loss of integrity of the data communication of "Lamp Request" signal for power switch actuator ECU	High	Severe	S: 5
Denial of service of oncoming car information	Low	Moderate	O: 2

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	2	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

Or mathematically

$$R = 1 + I \times F$$

where

Impact rating	Numerical value *I* for impact
Negligible	0
Moderate	1
Major	1,5
Severe	2

Attack feasibility rating	Numerical value *F* for attack feasibility
Very low	0
Low	1
Medium	1,5
High	2

[12]

TARA Process – 3rd step – Risk matrices

Finally, a risk treatment option shall be determined, considering impact categories, attack paths and the results from risk determination. Typically, risk treatment options are:

- avoiding the risk by removing the risk sources, or deciding not to start or continue with the activity that gives rise to the risk;
- reducing the risk -> cyber security measures to be identified
- sharing or transferring the risk (e.g., through contracts, buying insurance); and/or
- accepting or retaining the risk.

For risk acceptance and risk transfer, the corresponding rationales are recorded as cyber security claims and subject to validation, monitoring and vulnerability management

TARA Process – Wrap up

How to identify the relevant threats, assess them using reasonable metrics and initiate the integration of such key security principles ?

By approaching the risk using a **systematic & holistic methodology**

I

Understand your system / product, including
- What function does it provide ?
- What architecture part do we have ? What security properties matters (CIA) ?
- What lifecycle phases do exist ?
- What are my internal / external stakeholders ? Which (trust) boundary do we have ?
- What are my assumptions around its operational environment ?

II

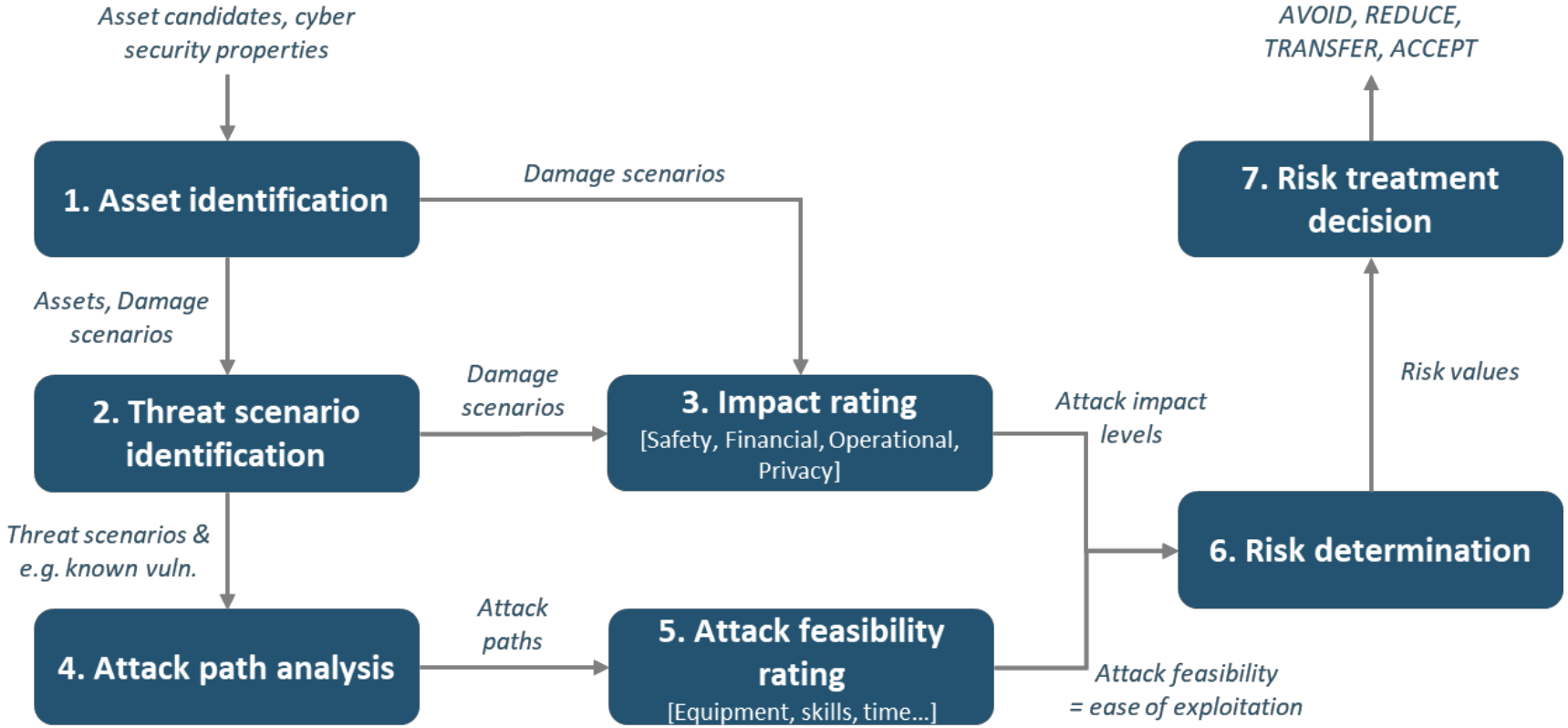
Identify the potential consequences
- Safety | Financial | Operation. | Legal
- What regulatory binding rules ?

Identify how feasible compromissions are
- What attack vectors & chain ?
- How «feasible» or complex ?

III

Compute risk values & take risk-based treatment decisions, either
- Accept the risk – Document rationale for acceptance
- Reduce the risk – identify security measures & controls to be implemented and controlled
- Avoid the risk – remove risk sources | *not that usual..*
- Transfer the risk – identify risk sharing with other parties (e.g. integrators, insurances…)

TARA Process details



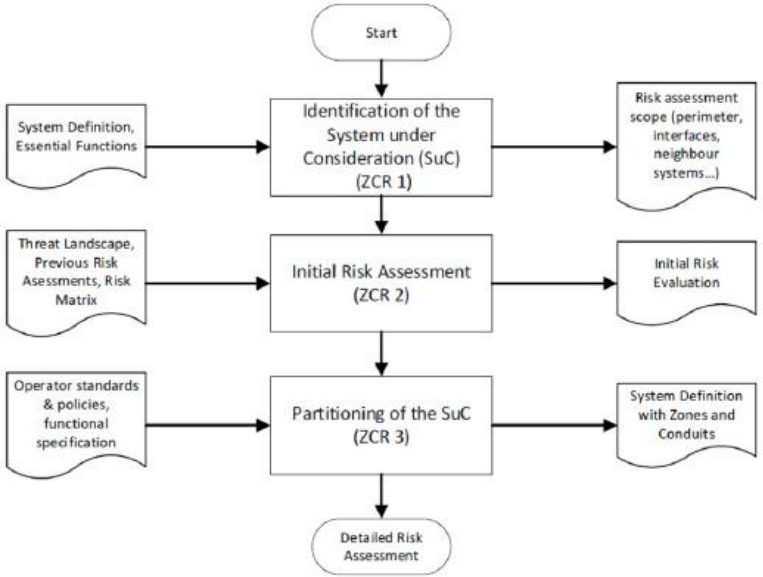
TARA Process reviews

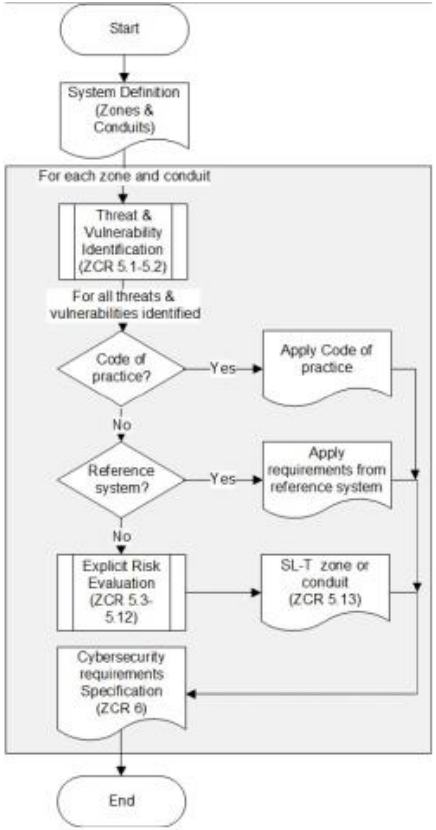
Checklist for Evaluating a "Good Job" in Documentation

- **Completeness**: Is all information within the STRIDE analysis (or other analyses) complete? Within each aspect of the threat model, are all sub-elements complete? For example, Attack Trees can be more dependent on ability and expertise of the threat modeler to come up with sufficiently comprehensive set of attacks that inexperienced developers might not think of. Were the strongest possible mitigations identified, and for each component? If there are gaps, is it well understood why those gaps exist?
- **Clarity**: Is each threat, mitigation, etc., clearly explained? Does it make sense for the intended audience(s)? Ideally, clarity would emerge naturally with the iterative nature of threat modeling across a variety of participants within the organization, but there would still be external consumers—and some issues of clarity could be explained in meetings or email without being updated within the documentation itself.
- **Specificity**: Is each element appropriately specific and at the right level of detail for the intended audience(s)? For example, giving the name of a protocol might be sufficient in some cases, whereas the protocol, version number, and configuration mode might be necessary for others.
- **Traceability**: Are interrelationships between different components of the threat model easily traceable? If identifiers are used, are they consistent and correct? Are there any identifiers that are cited but not defined? Are there multiple entries or descriptions for the same concept within the same context (i.e., duplicates)?
- **Consistency**: Is there consistency between the intended design and the implementation of the manufactured device? Documentation can change frequently due to the iterative approach of threat modeling, so inconsistencies can arise.
- **Roles and responsibilities**: When applicable to the threat model or risk analysis, are the roles and responsibilities of the medical device operators, patients, and other parties clearly identified, particularly when discussing risk?
- **Assumptions**: Are all assumptions clearly identified? Are these assumptions "reasonable"?
- **Rationales**: Are rationales for decisions included in sufficient detail, especially for cases in which risks are accepted or transferred; is there some ability to revisit why one mitigation is selected over another; etc.?

System security risk assessment within OT

Risk assessment on system (=infrastructure) level is usually not following the same strategy, due to the wider landscape of sub systems and threats to be addressed. **ISA/IEC 62443-3-2** is defining another framework to approach cyber security risk assessment based on Zone & Conduits segmentations – to be developed in upcoming modules

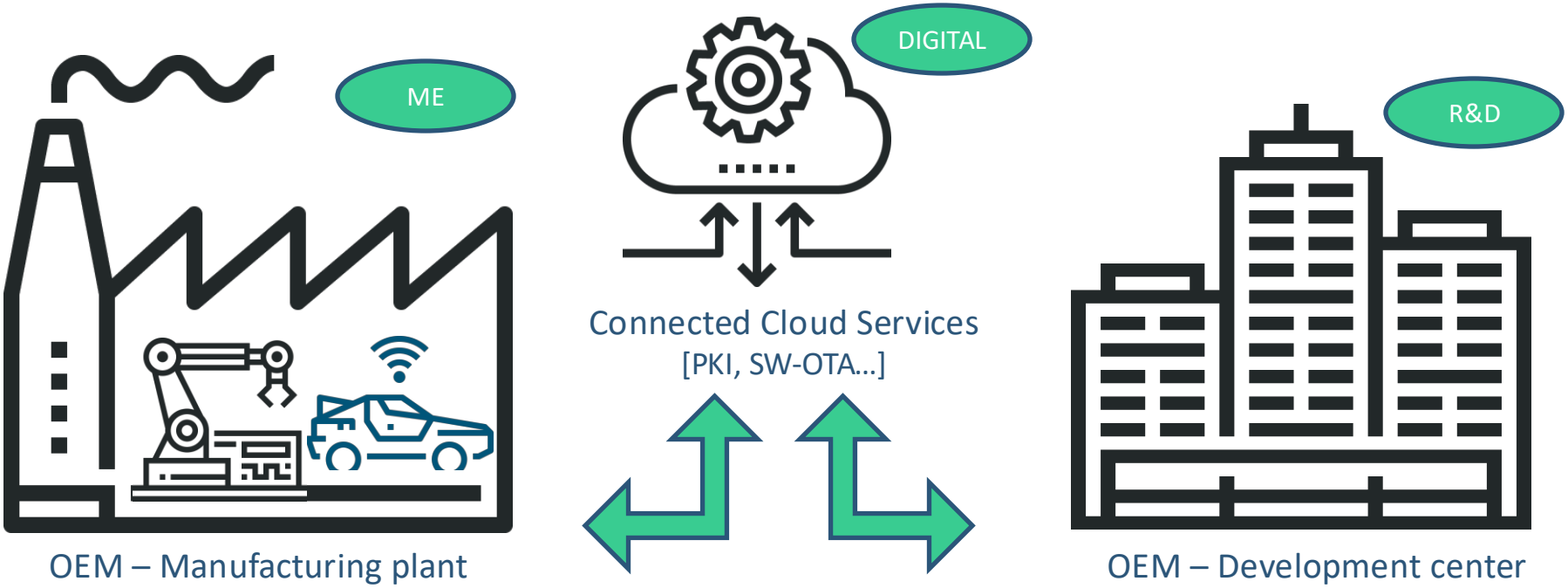




[15]

Example from Automotive industry

Complexity: risk ownership all along product lifecycle phases



Example from Automotive industry

Scenario: Vehicle produced within manufacturing plants

- Vehicle cyber security legally bound to cyber security requirements [UNECE R155]
- Whole vehicle lifecycle has to be addressed by cyber security considerations

7.2.2.1.	The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases: (a) Development phase; (b) Production phase; (c) Post-production phase.
7.3.3.	The vehicle manufacturer shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately. The risk assessment shall consider the individual elements of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external systems. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 5, Part A, as well as any other relevant risk.

- If manufacturing services are provided by third parties, this has to be properly managed as well, incl. cyber risks handling throughout supply chain

7.3.2.	The vehicle manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks.

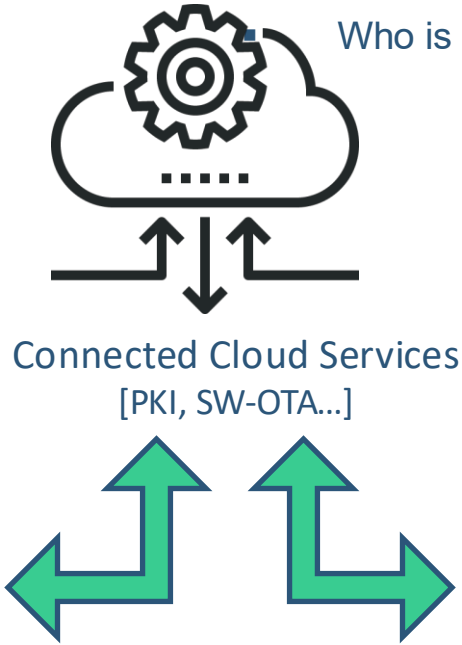
High level and sub-level descriptions of vulnerability/threat			*Example of vulnerability or attack method*	
4.3.6. Threats to vehicle data/code (Continued)	20	Manipulation of vehicle data/code	20.1.	Illegal/unauthorized changes to **vehicle's electronic ID**
			20.2.	**Identity fraud.** For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend
			20.3.	Action to **circumvent monitoring systems** (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)
			20.4.	Data manipulation to **falsify vehicle's driving data** (e.g. mileage, driving speed, driving directions, etc.)
			20.5.	Unauthorized changes to **system diagnostic data**
	21	Erasure of data/code	21.1.	Unauthorized deletion/manipulation of **system event logs**
	22	Introduction of malware	22.2.	Introduce **malicious software** or malicious software activity
	23	Introduction of new software or overwrite existing software	23.1.	**Fabrication of software** of the vehicle control system or information system
	24	Disruption of systems or operations	24.1.	**Denial of service**, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging
	25	Manipulation of vehicle parameters	25.1.	Unauthorized access of **falsify the configuration parameters** of vehicle's key functions, such as brake data, airbag deployed threshold, etc.
			25.2.	Unauthorized access of falsify the charging

[14]

Example from Automotive industry

- Who is taking decisions on which risks ?
- Who is monitoring the risk over time ?
- Who is owning which assest ?
- Who is responsible in the case of incident ?

OEM – Manufacturing plant



OEM – Development center

[14]

Threat Analysis & Risk Assessment – Challenges

- Lack of cyber security competences across organizations (esp. for realistic attack path evaluations)
- Lack of general cyber security strategy which lead to inconsistencies
  - Initial assumptions & rationales missing
  - Considerations about existing protection measures giving analysis bias
- Weak maturity of tooling & software support
- Need for stakeholder interactions
  - Interfaces with other risk assessments (e.g. quality, functional safety, reliability…)
  - Interfaces between IT-Sec, OT-Sec and Product-Sec
  - RASIC [Responsible, Accountable, Supportive, Informed, Consultative]
- Maintenance complexity
  - Risks are continuously evolving (e.g. attack technics, tools, known vulnerabilities…)
  - Integration of vulnerability considerations during operation phase

Threat Analysis & Risk Assessment – Resources

- **Microsoft Threat Modeling Tool**: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool
  - Open source tool to generate parts of TARAs based on data flow representations, STRIDE-based
  - Open source stencils & templates to be found online
  - Link: https://attack.mitre.org/matrices/enterprise/
- **MITRE ATT&CK frameworks**: globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community
  - IT: https://attack.mitre.org/matrices/enterprise/
  - OT: https://attack.mitre.org/matrices/ics/
  - Mobile: https://attack.mitre.org/matrices/mobile/
- **MITRE EMB3D threat model**: provides a cultivated knowledge base of cyber threats to embedded devices, providing a common understanding of these threats with security mechanisms to mitigate them
  - Embedded devices: https://emb3d.mitre.org/

TARA courses – external references

1) https://sarasch.com/events/the-biggest-threat-to-cybersecurity-is-often-humans/
2) https://jlou.eu/optimisez-votre-azure-2-4-la-securite/
3) https://www.stormshield.com/news/iec-62443-the-essential-standard-for-industrial-cybersecurity
4) https://softwareg.com.au/blogs/cybersecurity/fail-safe-defaults-fail-secure-cybersecurity
5) https://www.infosys.com/toons/cybersecurity.html
6) https://imgflip.com/i/1jgg5c
7) https://commitstrip.com
8) https://www.darkreading.com/cloud-security/cartoon-c-suite-cybersecurity-
9) https://www.jklossner.com/humannature
10) https://www.jklossner.com/humannature/vqmglje5sqm27mkm6x47bggyl7v4z1
11) https://www.researchgate.net/publication/351929062_Integration_of_Security_Standards_in_DevOps_Pipelines_An_Industry_Case_Study
12) ISO/SAE 21434 – Road vehicles — Cybersecurity engineering, https://www.iso.org/standard/70918.html
13) https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf
14) WP29 – UN ECE R155, https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
15) ISA/IEC 62443-3-2 – Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design, https://webstore.iec.ch/en/publication/30727