MASTER OF SCIENCE
IN ENGINEERING

TSM_SecIndOpT

Threat models in OT systems (I)

Version: 1.0, by K. Marty

Luca Haab | 25.04.2025 | Cours MSE

swissuniversities

Whoami

Kilian Marty

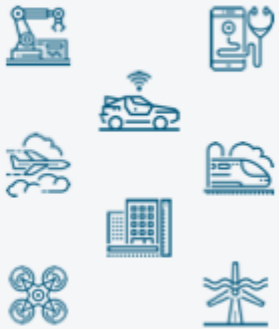
CEO | Cyber security consultant at CertX Solutions SA

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]

IT / OT Security vs Product Security…

[IT/OT] System cyber security

- Stakeholders: Internal actors & suppliers
- Objectives: Business continuity & resilience
- Regulatory context: Not (yet) fully legally binding, but obligations are coming for critical / important entities
- Main challenges:
  - Standard IT security practices vs OT considerations – What to reuse, extend, adjust, redefine ?
  - Assets heterogeneity & legacy parts
  - Patch management
  - “Do not be only seen as a cost center”

Product cyber security

- Stakeholders: Product integrators & end users
- Objectives: Product liability
- Regulatory context: Legally binding for any products embedding digital elements
- Main challenges:
  - Integration of cyber security considerations into existing product development & operation processes
  - Transversal to organizational units (e.g. product on the field vs connected services)
  - Compliance complexity
  - Decommissioning of products – who is responsible (?)

Disclaimer

This course part will mostly be oriented on product security cases

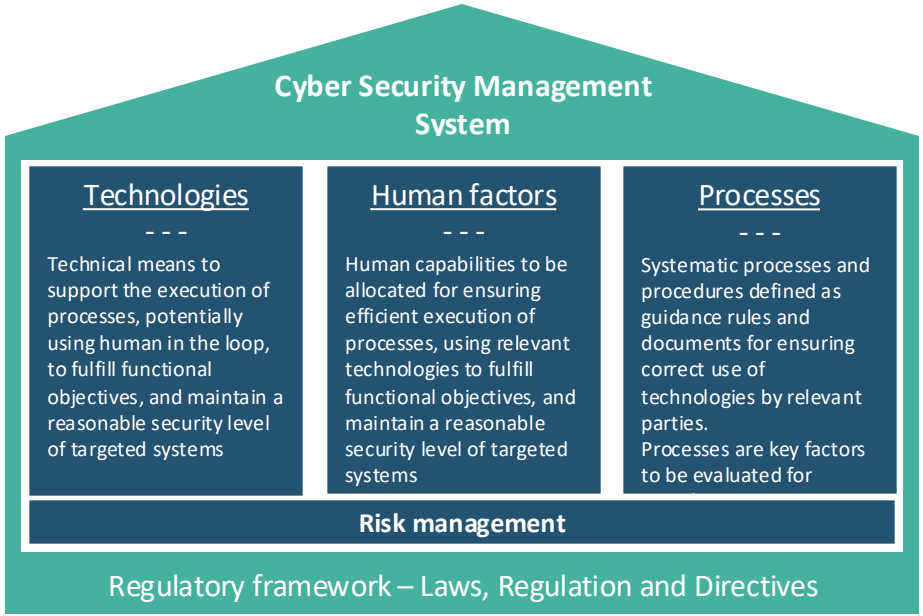
Threat Analysis & Risk Assessment - WHY

- What are my key assets & what potential consequences / damages ?
- What are the attack vectors against my assets ?
- How & on what invest effort to reach a reasonable security posture ?
- What security measures for which improvement ?
- What to monitor for securing a continuous acceptable residual risks

… and what security principles are we willing to follow ?

Threat Analysis & Risk Assessment - WHY

Targeted cyber security principle: Holistic approach



Threat Analysis & Risk Assessment - WHY

Targeted cyber security principle: Security by design

Integrate cyber security measures & controls

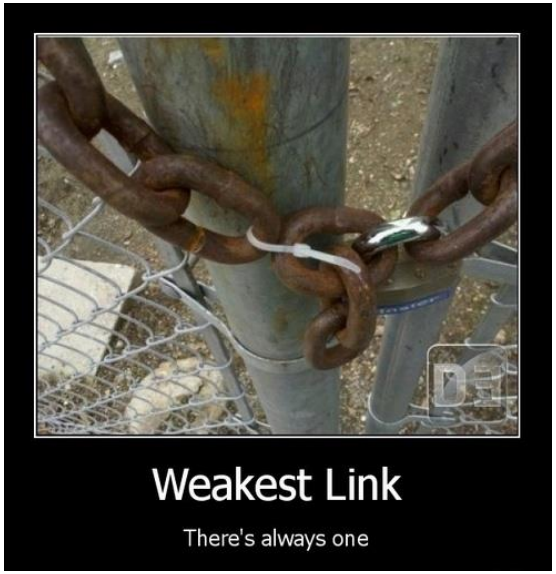
- ✓ right from the beginning of development to provide / use security capabilities
- ✓ where, when and how it matters, being pragmatic
- ✓ In the most efficient way to reduce risk levels down to an acceptable level
- ✓ keeping an up-to-date visibility over current threat landscape

Threat Analysis & Risk Assessment – WHY

Targeted cyber security principle: Secure the weakest link

[1]

Considering whole asset lifecycle

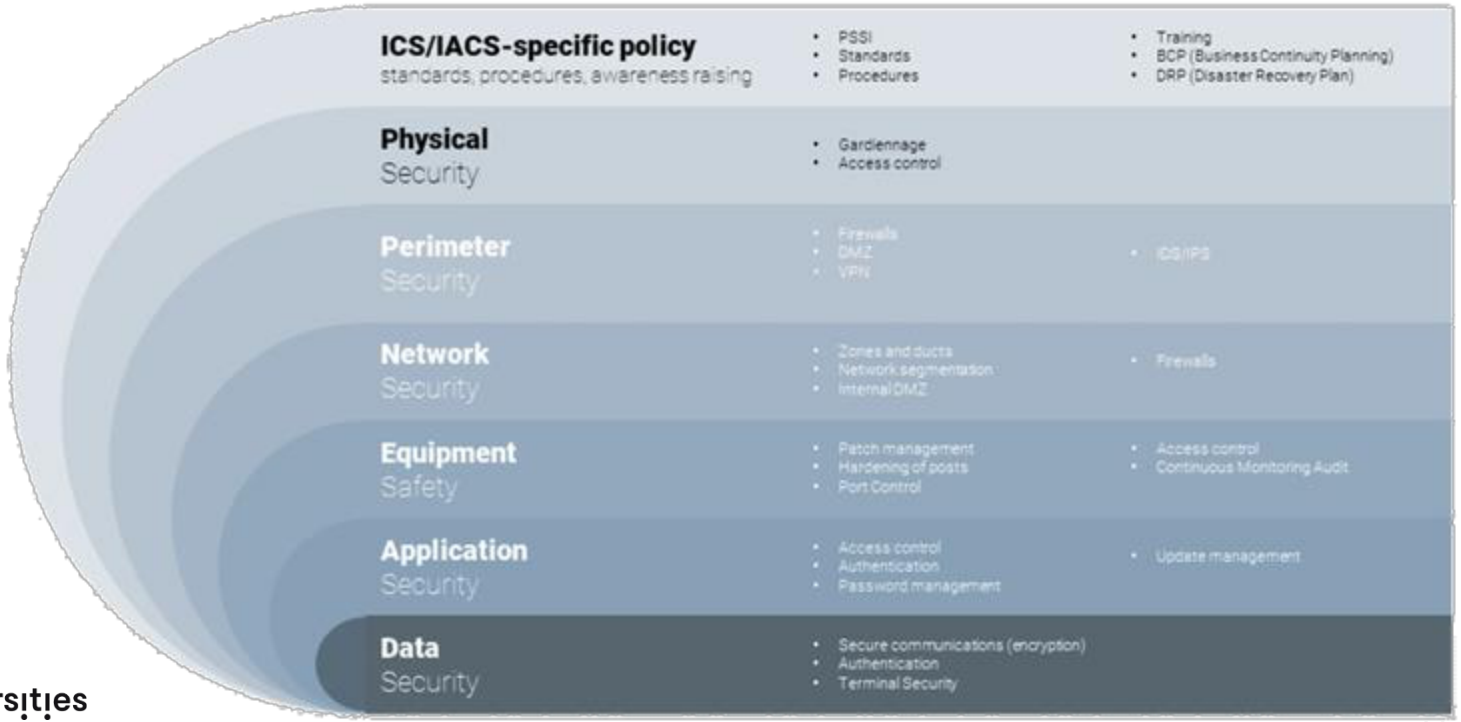


[2]

Considering whole attack chain / path

Threat Analysis & Risk Assessment – WHY

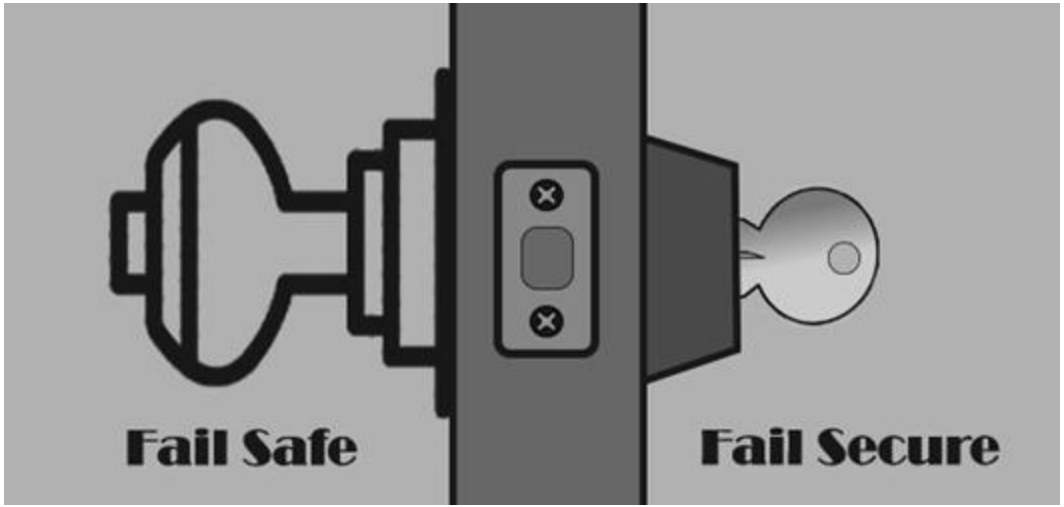
Targeted cyber security principle: Defense in depth



[3]

Threat Analysis & Risk Assessment – WHY

Targeted cyber security principle: Fail secure

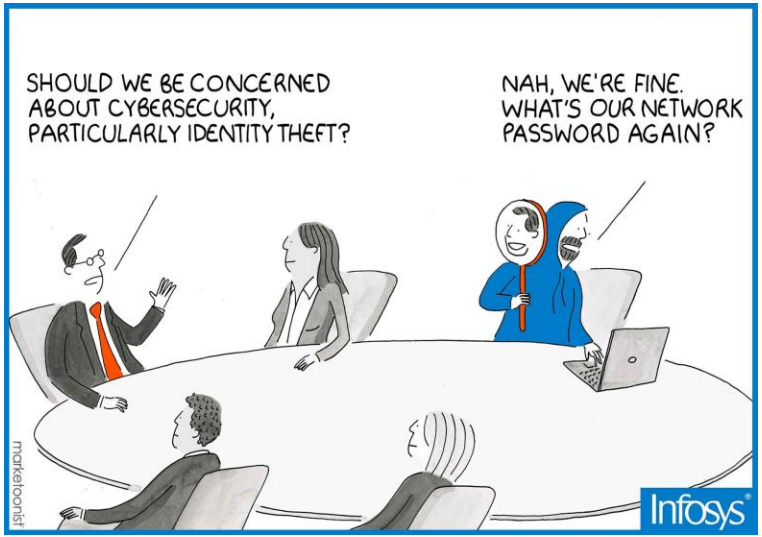


[4]

Considering potential conflicts with other discipline (e.g. FuSa)

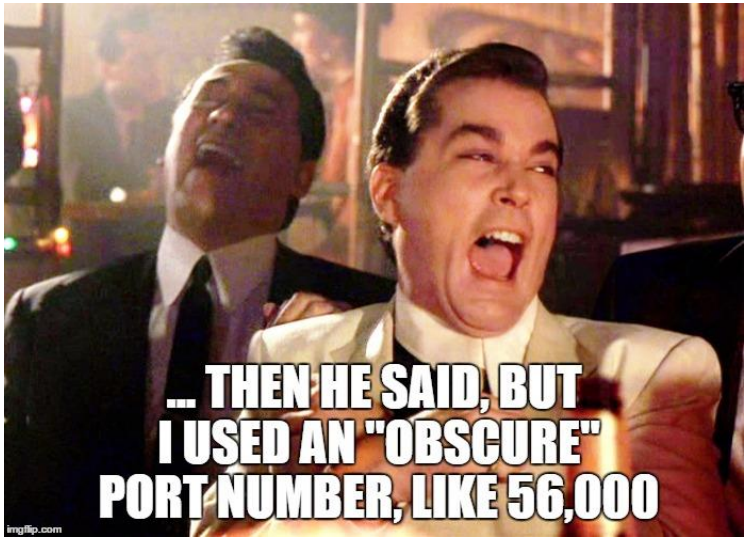
Threat Analysis & Risk Assessment – WHY

Targeted cyber security principle: Assume secrets not safe



[5]

Doing the best by assuming the worst

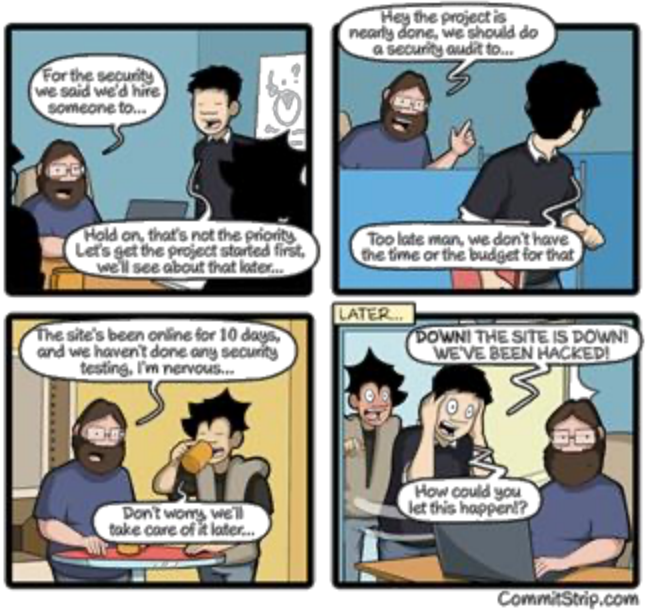


[6]

Forget any security-by-obscurity principles

Threat Analysis & Risk Assessment – WHY

Targeted cyber security principle: Monitor & audit

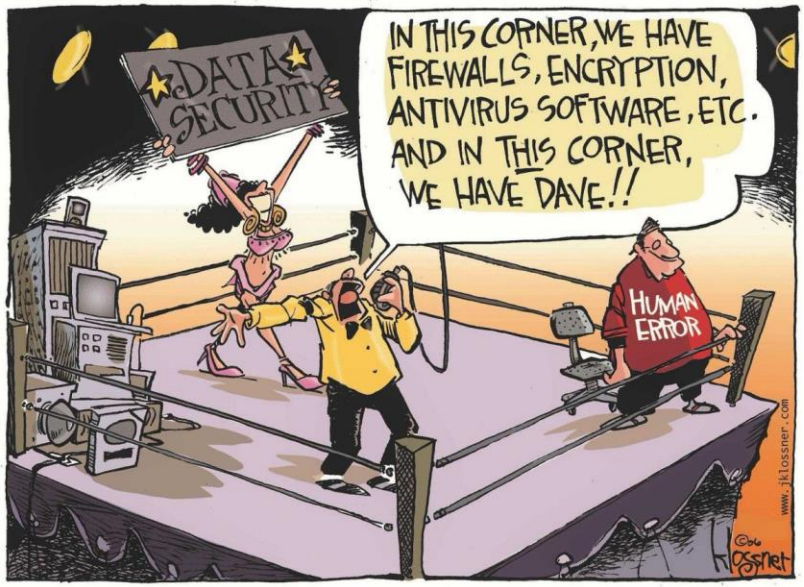


[7]

[8]

Threat Analysis & Risk Assessment – WHY

Targeted cyber security principle: Proportionality & Precautionary



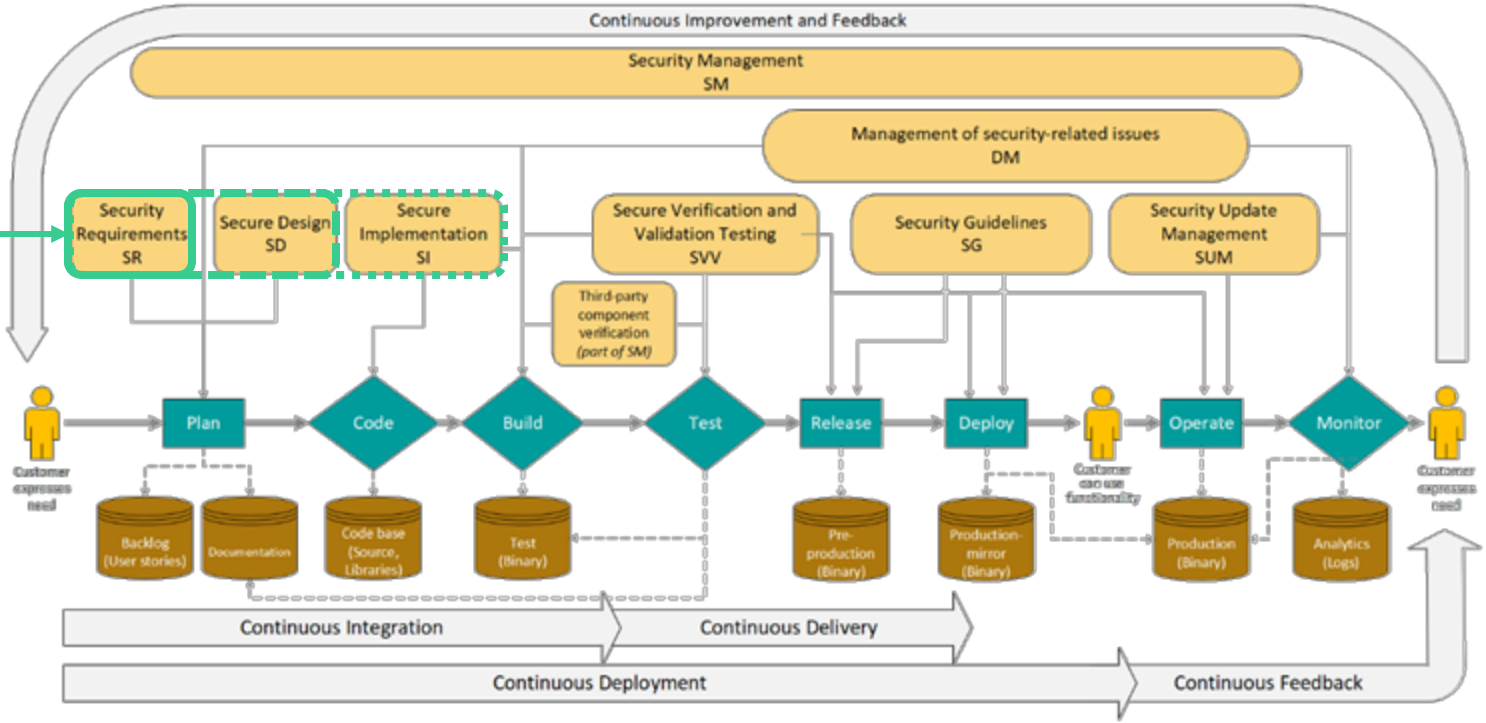
[9]

[10]

Threat Analysis & Risk Assessment – WHY

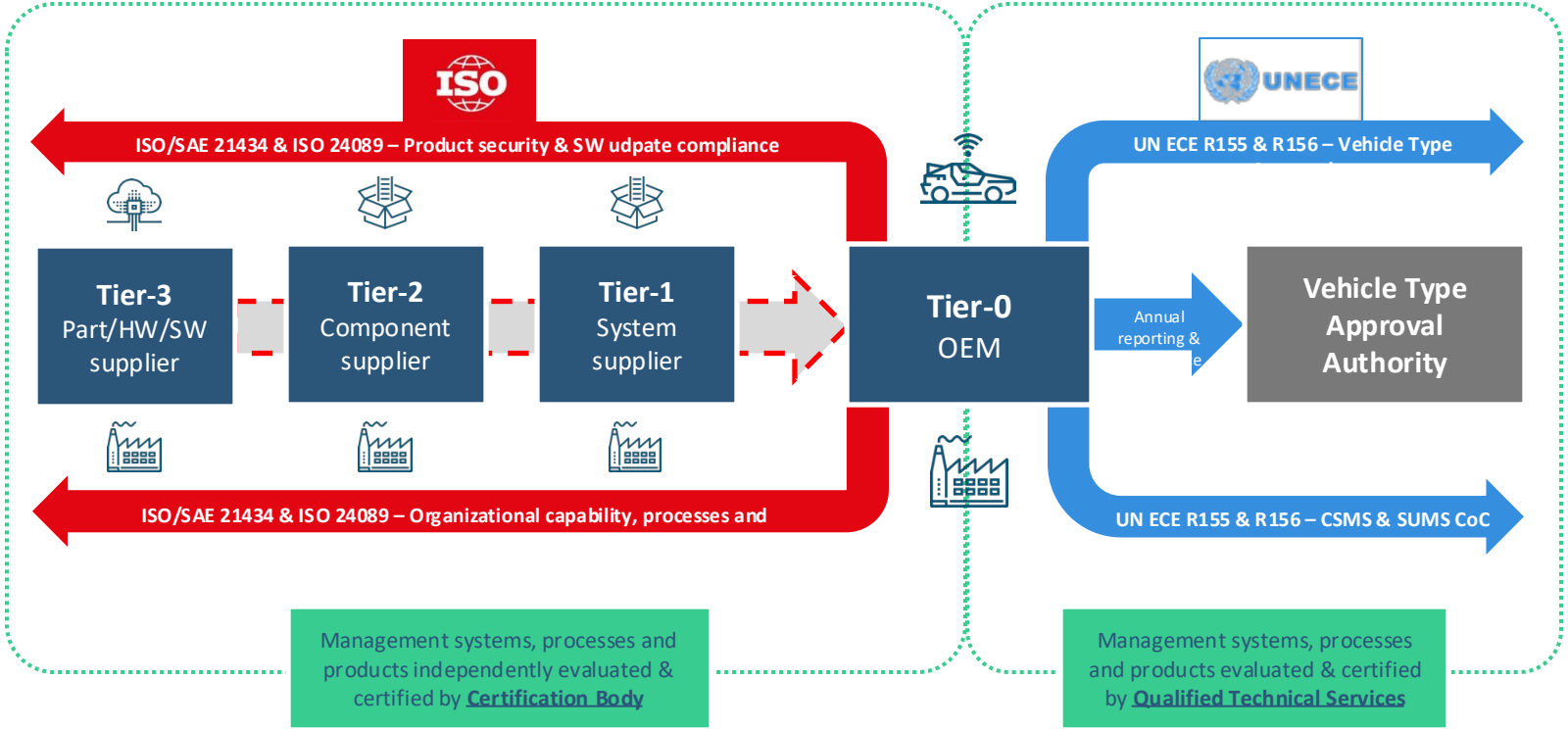
TARA
Threat Analysis & Risk Assessment

Security specs
Cyber security requirements & claims refined into requirements



[11]

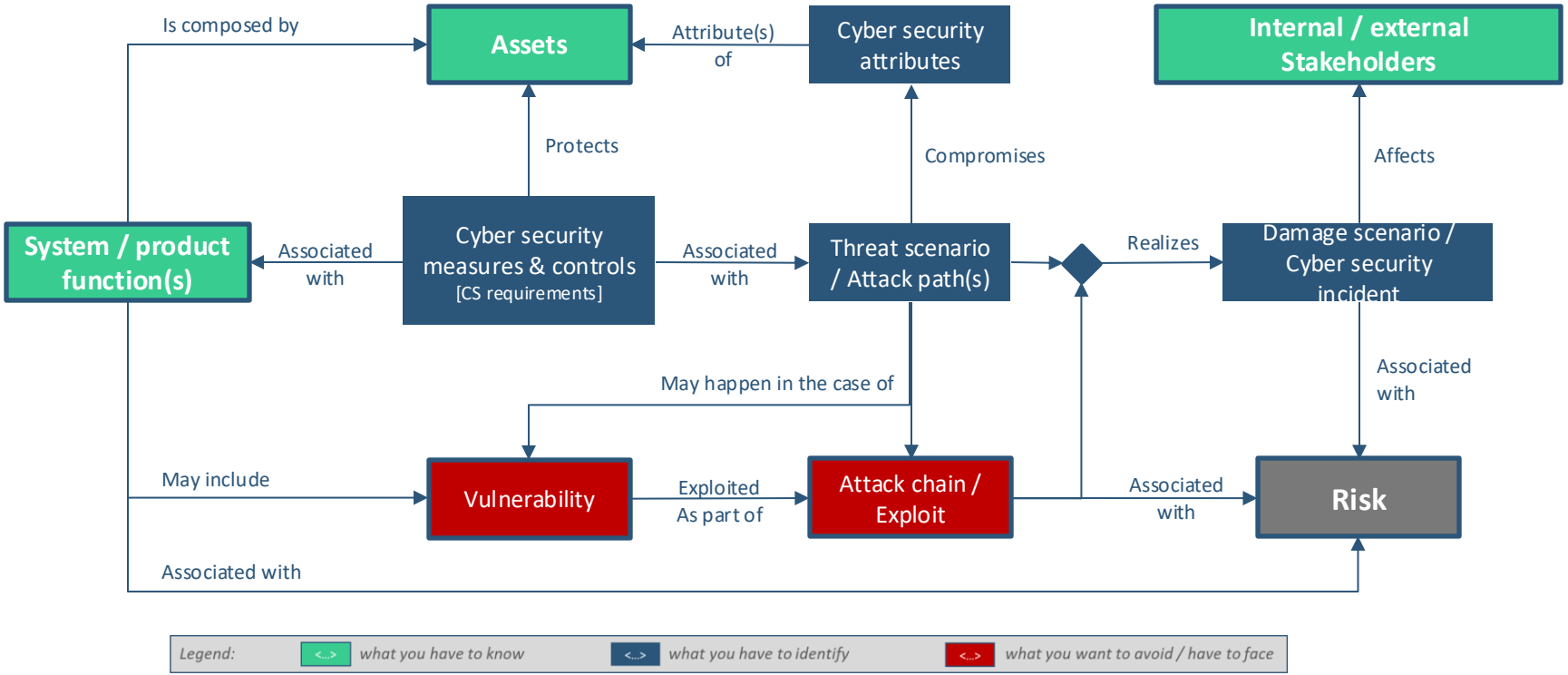
Supply chain considerations [automotive example]



TARA Primitives – Terminology

Assets & cyber security attributes	Threat scenarios	Damage scenarios
Key components (hardware, software, data) and their security attributes (confidentiality, integrity, availability) that has a value for product / system stakeholders. *Examples: confidentiality of user data, integrity of new SW package…*	High-level & realistic attack situations describing how adversaries could target system vulnerabilities to compromise security *Examples: Denial-of-service of logging function, GPS Spoofing, tampered data…*	Impact and/or consequences of successful cyber attacks, including safety, financial, operational, and legal harm amongst other dimensions (up to company risk mgmt.) *Examples: Loss of personal data (PII) leading to GDPR penalty and reputational damage…*
Cyber security measures & controls	**Vulnerabilities**	**Exploits / attack chains**
Technical and organizational safeguards to reduce risk and protect assets from cyber threats *Examples: Secure boot mechanisms, Secure SW OTA deployment, SecOC over CAN…*	Real weaknesses in a product / system that could be exploited by a threat actor, implementing a threat scenario *Examples: Buffer overflows, Remote Code Execution, non-sanitized inputs handling…*	Step-by-step methods attackers use to leverage vulnerabilities and achieve malicious objectives. *Examples: Phishing campaign, credential retrieval, communication message forging…*

TARA Primitives – Relationships



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 – 1st step – System definitions

Objective: Clarify following elements to drive TARA process with relevant inputs

- product / system function: What are functions provided to customer and any other stakeholder during all phases of product lifecycle ?
  - Examples: sensor measurement, safe-mode enablement, system diagnostic, SW update, data logging…
- Assets & cyber security attributes relevance: What matters in the case of compromission ?
  - Examples: confidentiality of user data, integrity of SW update, availability of Safety function…
- Assumptions: What pre- / environmental / adversarial conditions impact the system / product ?
  - Examples: running in a protected / restricted environment, trained stakeholders, centralized authentication servers provided by hosting environment…
- Architecture: What are product / system sub parts ?
- communications (dataflows, technologies): What information exchanges between product / system parts & towards external parties ?
- trust boundaries: What is under company's control ?

See DFDs on next slide

TARA Process – 1st step – System definitions

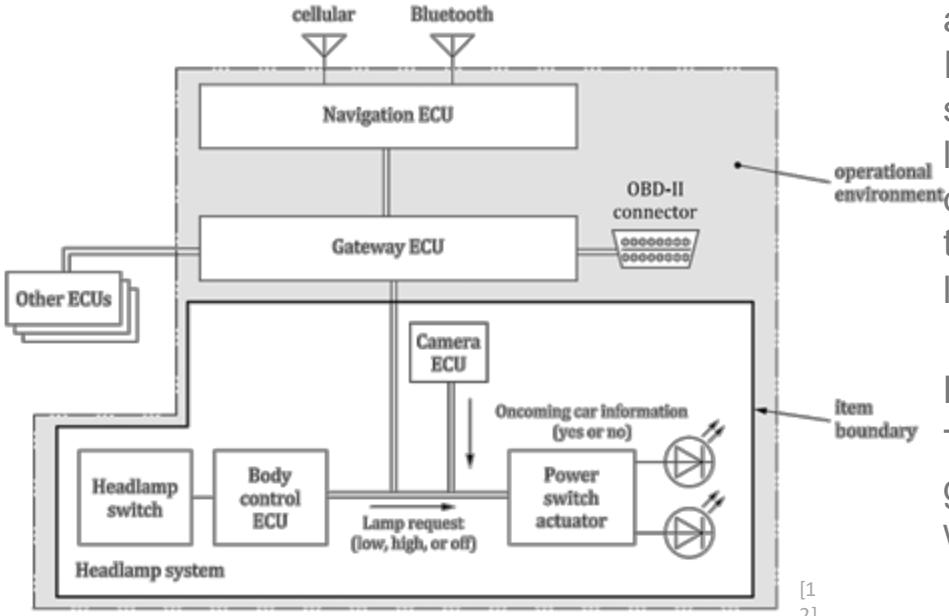
Data Flow Diagrams (DFDs) A way to help visualize the system that is being threat modeled. At a high level, DFDs are a way to represent the entities involved within the functioning of the system / product, how those entities are related, and the assumed trust boundaries between them

- *Several notation languages exist for DFDs – DFD3 is used here for simplification purposes (only 5 symbols)*

Elements	Symbol	Definitions
External Entity		Anything outside your control. Examples include people and systems run by other organizations or even divisions.
Process		Any running code, including compiled, scripts, shell commands, Structured Query Language (SQL) stored procedures…
Data Store		Anywhere data is stored, including files, databases, shared memory, cloud storage services, cookies…
Data Flows		All the ways that processes can talk to data stores or each other. If a conversation is only initiated by one side, you can represent the initiating side as an empty arrow
Trust boundaries		A way to display different trust levels between objects

TARA Process – 1st step – System Definitions

Automotive example



[12]

Example of Item functions descriptions

the headlamp system turns on/off the headlamp in accordance with the switch by demand of the driver. If the headlamp is in high-beam mode, the headlamp system switches the headlamp automatically to the low-beam mode when an oncoming vehicle is detected. It also returns the headlamp automatically to the high-beam mode if the oncoming vehicle is no longer detected.

Example of operational environment descriptions

The item (headlamp system) is connected with the gateway ECU, and the gateway ECU is connected with the navigation ECU by data communication.

Ass-1: gateway ECU has strong security controls including a firewall function

TARA Process – 1st step – Cyber security attributes

Damage scenarios are consequences of compromissions of cyber security properties of assets

Major cyber security properties

- Authentication – The asset must be linked with its author / editor over its entire lifecycle
- Integrity – The asset is accurate and complete (= unaltered) over its entire lifecycle.
- Confidentiality – The asset is not made available or disclosed to unauthorized individuals, entities, or processes.
- Availability – The asset must be available when it is needed

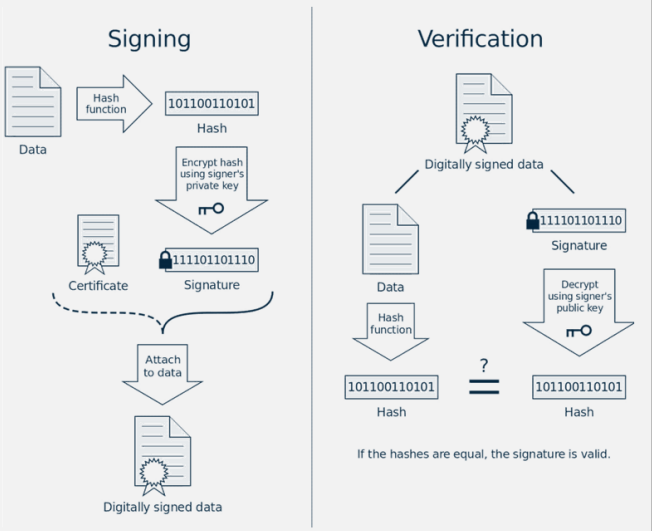
Some well-known triads:

- CIA – Confidentiality, Integrity and Availability, a model designed to guide policies for information security within an organization.
- AAA – Authentication, Authorization and Accounting, a model for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security.

TARA Process – 1st step – Cyber security attributes

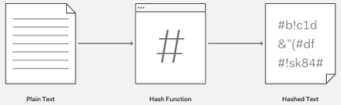
Authentication

Usually mitigated using identifiers in conjunction with integrity checks or digital signatures



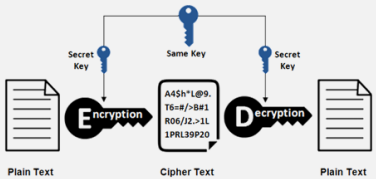
Integrity

Usually mitigated using hashing schemes and fingerprinting / signature



Confidentiality

Usually mitigated using encryption schemes (e.g. symmetric, asymmetric, hybrid)



Availability

Usually mitigated using redundant architectures, degraded mode handling and elastic capabilities

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**

Identify how feasible compromissions are

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

swissuniversities

TARA Process – 2nd step (a) – Damage scenario

Damage scenarios shall be assessed against potential adverse consequences for stakeholders in, at least, the independent impact categories of safety, financial, operational, and privacy (or legal)

- So-called SFOP impacts

If further impact categories are considered beyond S, F, O and P, then those categories shall be documented.

- Examples of other / more specific categories : loss of intellectual property, financial losses to business, loss of brand image or reputation

The impact rating of the damage scenario shall be determined to be one of the following: Severe, Major, Moderate or Negligible.

Impact Rating	Criteria for Financial Impact Rating
Severe	The financial damage leads to catastrophic consequences which the affected stakeholder might not overcome.
Major	The financial damage leads to substantial consequences which the affected stakeholder will be able to overcome.
Moderate	The financial damage leads to inconvenient consequences which the affected stakeholder will be able to overcome with limited resources.
Negligible	The financial damage leads to no effect, negligible consequences or is irrelevant to the stakeholder.

[12]

TARA Process – 2nd step (a) – Impact analysis

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

Impact Rating	Criteria for Operational Impact Rating
Severe	The operational damage leads to a vehicle not working, from non-intended operation up to the vehicle being non-operational.
Major	The operational damage leads to the loss of a vehicle function.
Moderate	The operational damage leads to partial degradation of a vehicle function or performance.
Negligible	The operational damage leads to no effect or indiscernible degradation of a vehicle function or performance.

[12]

Impact Rating	Criteria for Privacy Impact Rating
Severe	The privacy damage leads to significant or even irreversible impact to the road user. In this case, the information regarding the road user is highly sensitive and easy to link to a PII principal.
Major	The privacy damage leads to serious impact to the road user. In this case, the information regarding the road user is: a) highly sensitive and difficult to link to a PII principal, or b) sensitive and easy to link to a PII principal.
Moderate	The privacy damage leads to significant inconveniences to the road user. In this case, the information regarding the road user is: a) sensitive but difficult to link to a PII principal, or b) not sensitive but easy to link to a PII principal.
Negligible	The privacy damage leads to no effect or can create few inconveniencies to the road user. In this case, the information regarding the road user is not sensitive and difficult to link to a PII principal.

[12]

Impact Rating	Criteria for Safety Impact Rating
Severe	S3: Life-threatening injuries (survival uncertain), fatal injuries
Major	S2: Severe and life-threatening injuries (survival probable)
Moderate	S1: Light and moderate injuries
Negligible	S0: No injuries

Safety impact rating criteria are taken from ISO 26262-3:2018.

[12]

TARA Process – 2nd step (b) – Threat scenario

Threat scenario identification is a key intermediate step to identify relevant high-level scenario an attack may exploit to compromise assets, and therefore force the system / product to lead to damage scenario

- STRIDE is an acronym. It stands for

Accr.	Threat	Desired property	Description
S	Spoofing	Authenticity	Impersonating something of someone else
T	Tampering	Integrity (C**I**A)	Modifying data or code
R	Repudiation	Non-repudiation	Claiming to have not performed an action
I	Information disclosure	Confidentiality (**C**IA)	Exposing information to someone not authorized to see it
D	Denial of service	Availability (CI**A**)	Deny or degrade service to users
E	Elevation of privilege	Authorization	Gain capabilities/rights without proper authorization

TARA Process – 2nd step (b) – Threat scenario

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

Damage Scenario No.	Damage Scenario	Threat Scenario	Threat Scenario No.
:	:	:	:
D.x	Unintended headlamp's turn off during night driving resulting from loss of integrity of CAN signal	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU potentially causing unintended headlamp's turn off during night driving resulting from loss of integrity of CAN signal	T.x
		Tampering of a signal sent by Body Control ECU leads to ….	T.y
		….	…
:	:	:	:

[12]

Use case based exercises - guidance

Part I
[in-class]

Domestic medical device
- System understanding & asset identification
- Threat scenario identification
- Impact rating

Part II
[in-class]

Domestic medical device
- Attack path analysis
- Attack feasibility rating
- Risk calculations & treatment decisions

Homework
[optional]

Professional medical device

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