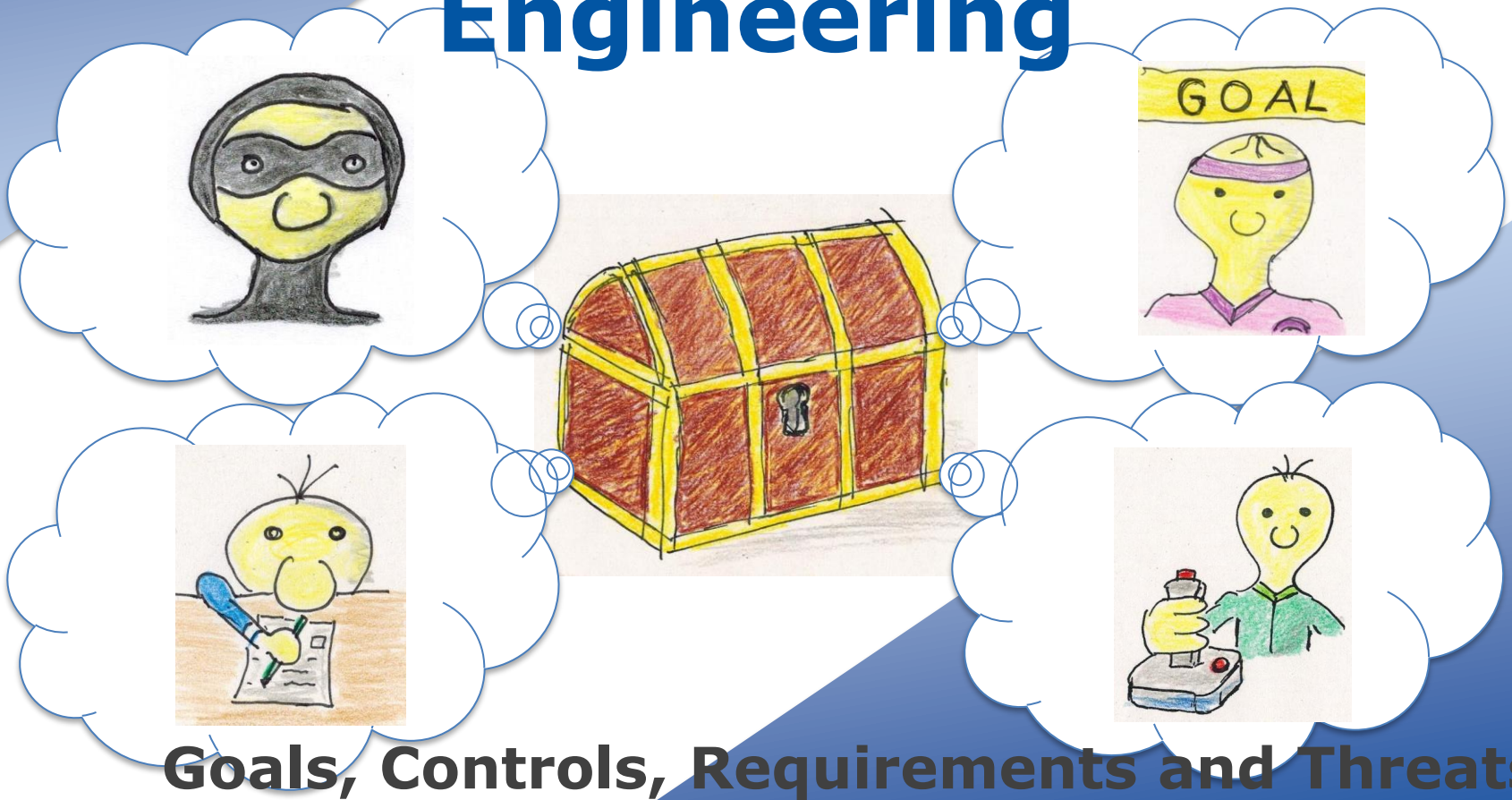
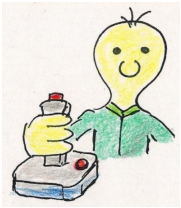
Fo(u)rces of Cybersecurity Engineering



Goals, Controls, Requirements and Threats

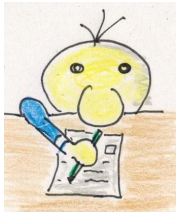
Agenda and Purpose

1. Cybersecurity Threat



3. Cybersecurity Control

2. Cybersecurity Goal



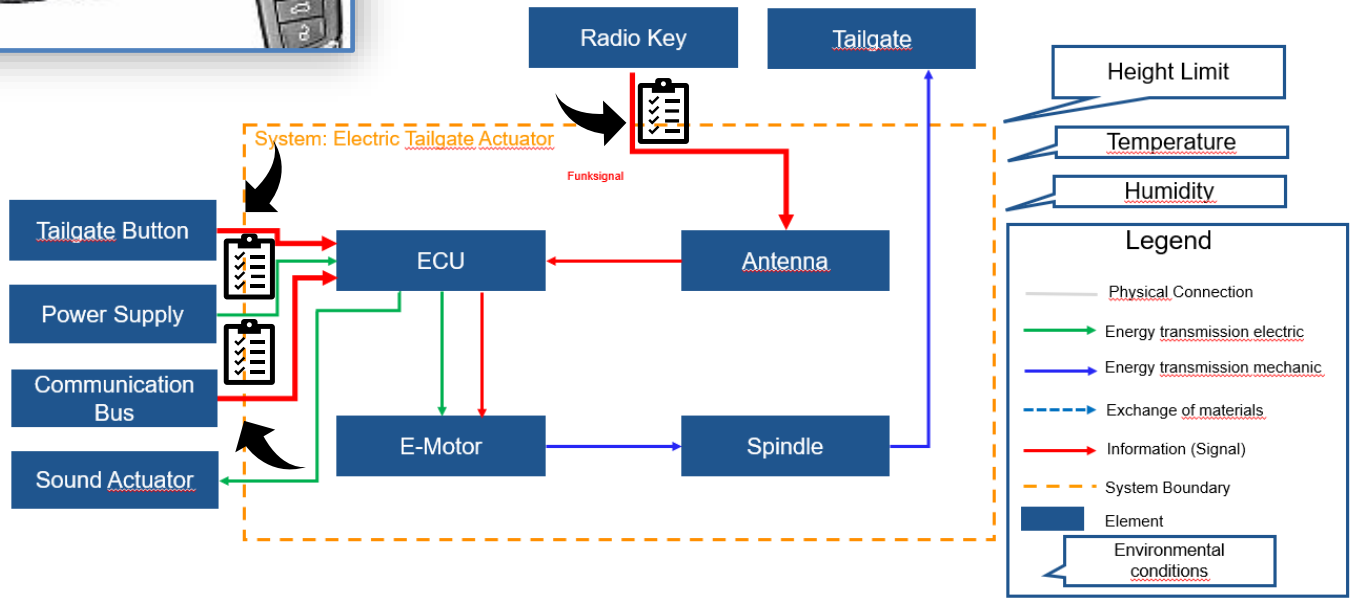
4. Cybersecurity Requirement

Purpose

Our purpose is to explain the **connection** between these four Cybersecurity topics.
Therefore, we will use an easy **example**!

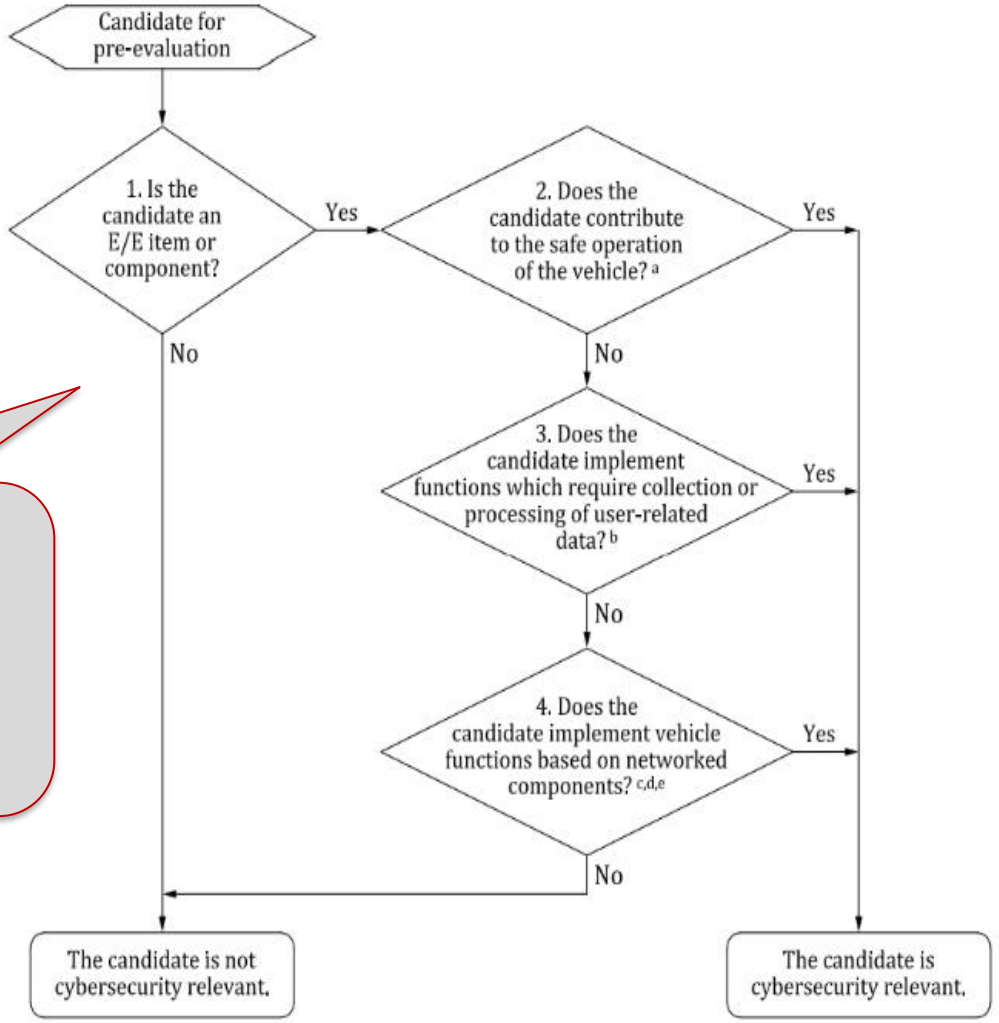
Our product

- **Electric Tailgate Actuator System**



Is our product cybersecurity-relevant?

- ISO 21434:2021 Annex D



Every system, that is **safety** relevant, is as well **security** relevant!
Safety Goals are the most popular attack paths!

Let us analyze our assets: Example

Primary stake-holder	Asset	CS property	Damage scenario	Impact rating: SFOP				Justification
				S	F	O	P	
Car user	Communi-cation interface radio key – antenna	Confi-dentiality	Cryptographic key for communication channel is made publicly available due to unauthorized disclosure	0	0	0	1	- no direct impact for car user
		Integrity	Unexpected opening of ETG due to tampered message	2	0	3	0	- severe safety impact if it happens while driving - severe operational impact for the service provider of a fleet
		Availabi-lity	Remote opening does not work due to non-functioning of communication channel, caused by a transmission outage	0	0	2	0	- only impact for the one attacked car

Impact rating is based on: Damage scenario

And now we attack the assets

Damage scenario

Unexpected opening of ETG due to tampered message

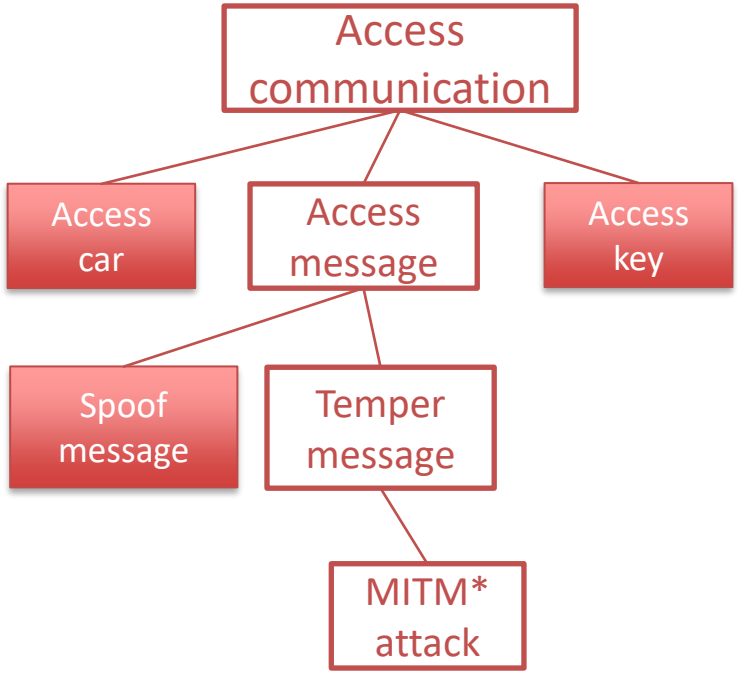
Threat Scenario

tampered messages may lead to messages at the wrong time

Attack Path Analysis

- **get access** to the communication channel
- **intercept** message flow
- **perform a MITM*** attack to tamper the communication

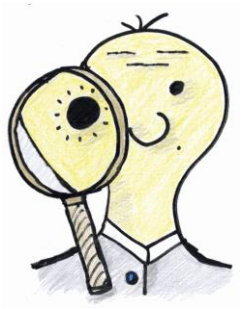
Attack tree:



*MITM: Man in the middle

But how feasible is this attack?

Attack Path Analysis	Elapsed Time	Specialist Expertise	Knowledge of the item	Window of opportunity	Equipment required
• gets access to the communication channel • intercept message flow • performs a MITM attack to tamper the communication	≤ 1 week	Proficient	Confidential information	Easy	Standard



Elapsed Time	Specialist Expertise	Knowledge of the item	Window of opportunity	Equipment required	Total Value	Attack feasibility Value
1	3	7	1	0	12	High

Used method:
attack potential-based approach

Risk value: combine attack feasibility & impact ratings

Integrity	Unexpected opening of ETG due to tampered message	2	0	3	0	- severe safety impact if it happens while driving - severe operational impact for the service provider of a fleet

Impact Rating

Risk Value

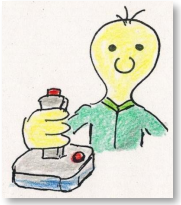
Attack Feasibility Rating

Elapsed Time	Specialist Expertise	Knowledge of the item	Window of opportunity	Equipment required	Total Value	Attack feasibility Value
1	3	7	1	0	12	High

Risk Value < step 6 >			
Stakeholder: Road User			
S	F	O	P
4	1	5	1

Risk value: combine attack feasibility & impact ratings

Risk value high → Risk Treatment Decision: Reduce the risk → Implement Controls



Security Goal

Trustable signal needs to be ensured by authentication of signal

ISO 21434, Clause 15, RQ-15-17:
For each threat scenario, considering its risk values, one or more of the following risk treatment options shall be determined:

a) Avoiding
b) Reducing
c) Sharing
d) Retaining

We select a Cybersecurity Control

Attack

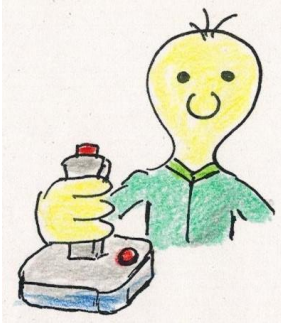
Modifying data or code

Cybersecurity Property

Integrity

Attack Example

Modifying configuration files or firmware storage devices or modify messages as they traverse the network.



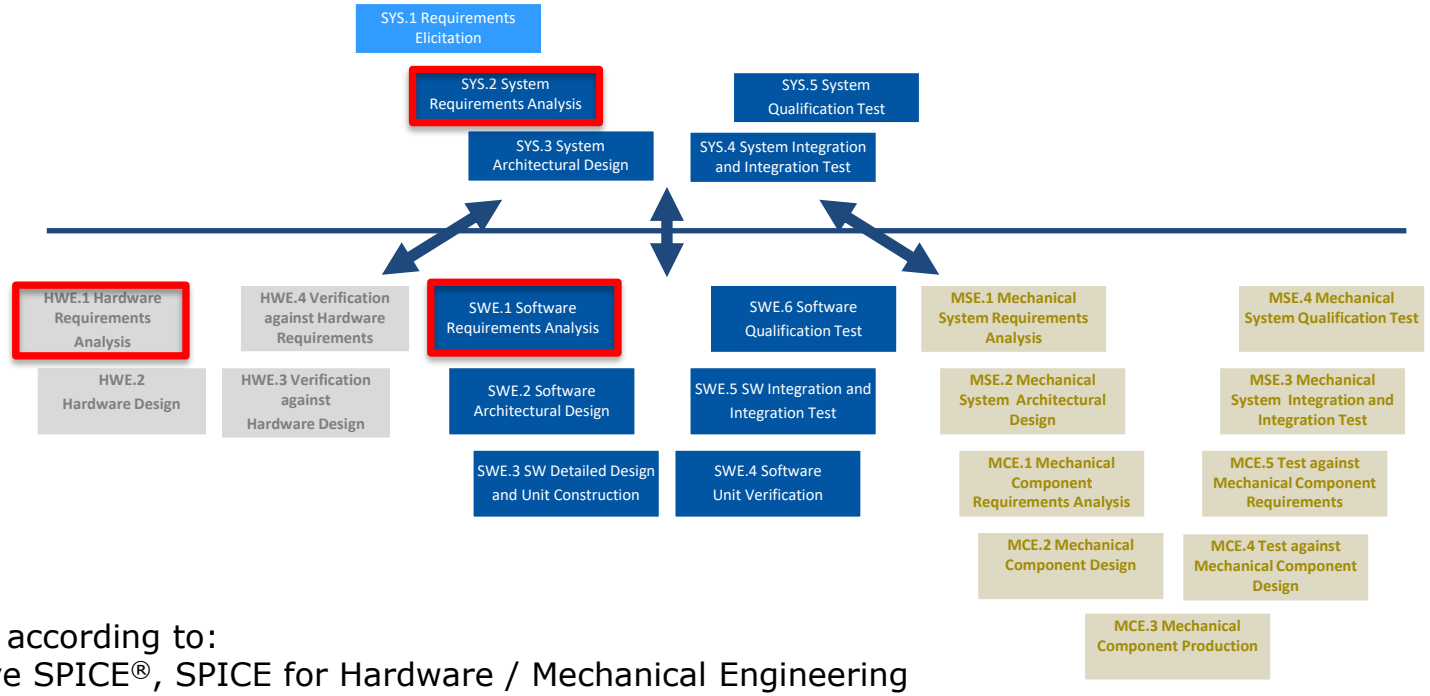
Cybersecurity Control

Hash and CRC

- A **Hash** is a digital fingerprint of a binary input.
- Cyclic Redundancy Check (**CRC**) is a method of checking information for errors during data transmission.

Derive Cybersecurity Requirements

- Cybersecurity Requirements shall be defined based on the identified Cybersecurity Goals
- Typically, they will be reflected on
  - **System** Requirements Specification
  - **Software** Requirements Specification
  - **Hardware** Requirements Specification



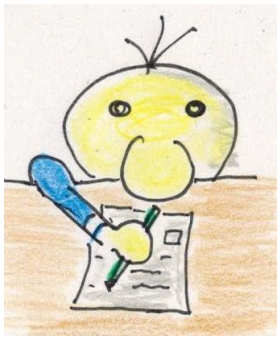
Processes according to:
Automotive SPICE®, SPICE for Hardware / Mechanical Engineering

We implement the Cybersecurity Control

Purpose of Cybersecurity Requirement

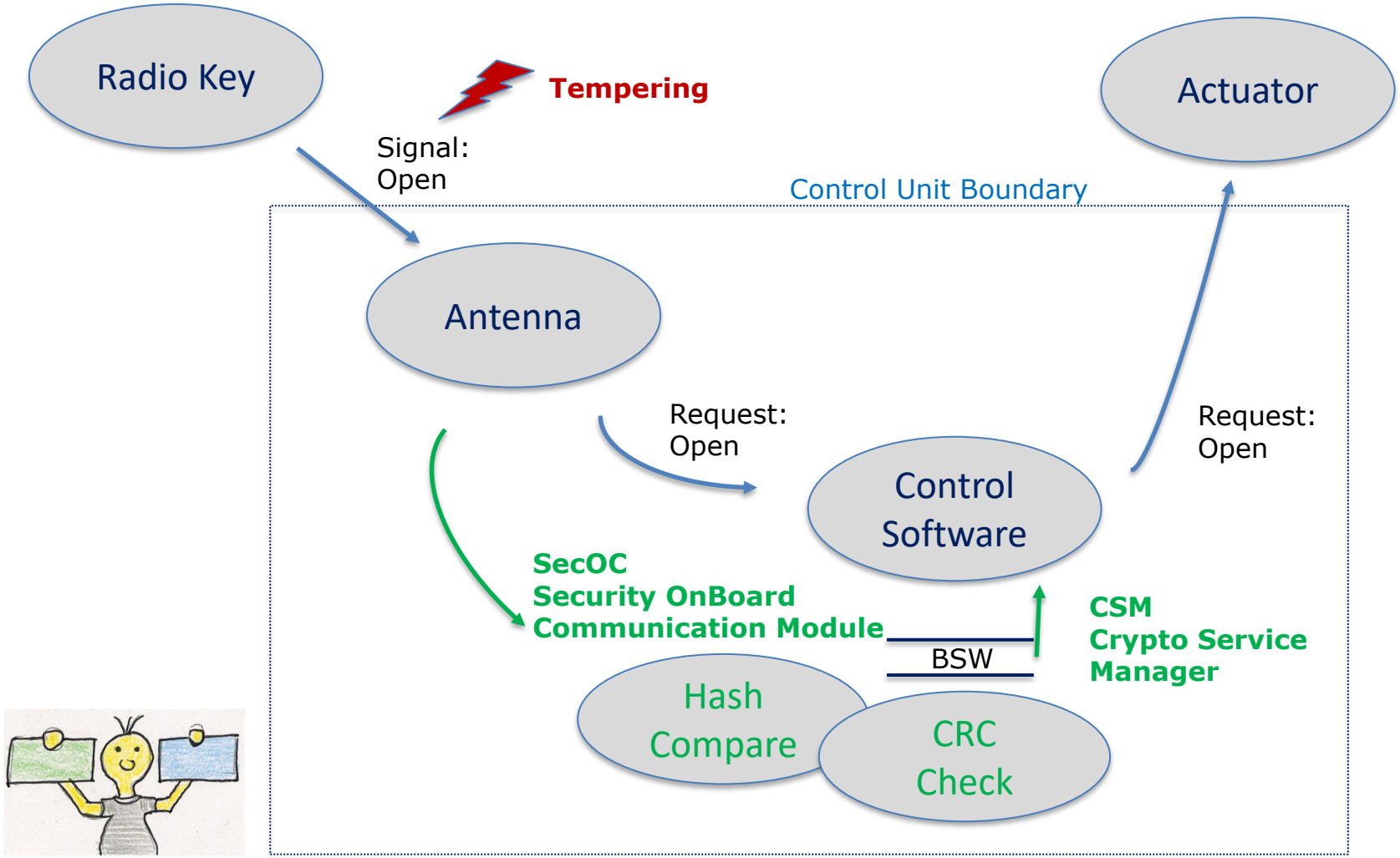
Implement a communication protocol including hash/CRC checks to protect the integrity of radio communication.

System Requirement	Allocated to
The system shall ensure that key is sending “Hash” and “CRC” information.	External
The system shall be able to check Hash and CRC information.	System
The software shall read Hash and CRC information.	Software
The software shall be implemented on an HSM.	Hardware



Software Requirement	Allocated to
The software shall read information on radio key interface.	SecOC
The software shall compare sent Hash.	CSM
The software shall check sent CRC.	CSM
If hash and CRC checks are okay, the software shall call „open“ command.	CSM

Analysis in our Threat Model



We deliver to testing

Security Goal

Trustable signal needs to be ensured by authentication of signal

Threat Scenario

tampered messages may lead to messages at the wrong time

Cybersecurity Requirement

Implement the selected Cybersecurity Control, to protect the mentioned Cybersecurity Property.

Cybersecurity Validation

Try to attack the system, to compromise the goal!

Interface Testing

Check the effectiveness of the control by sending a tempered message!

Verification

Check the correct implementation of the Control!

Conclusion

- The development **challenge** may not be that big. Many activities are already known and established!
- But it is important to know and understand the **dependencies** in these development tasks!