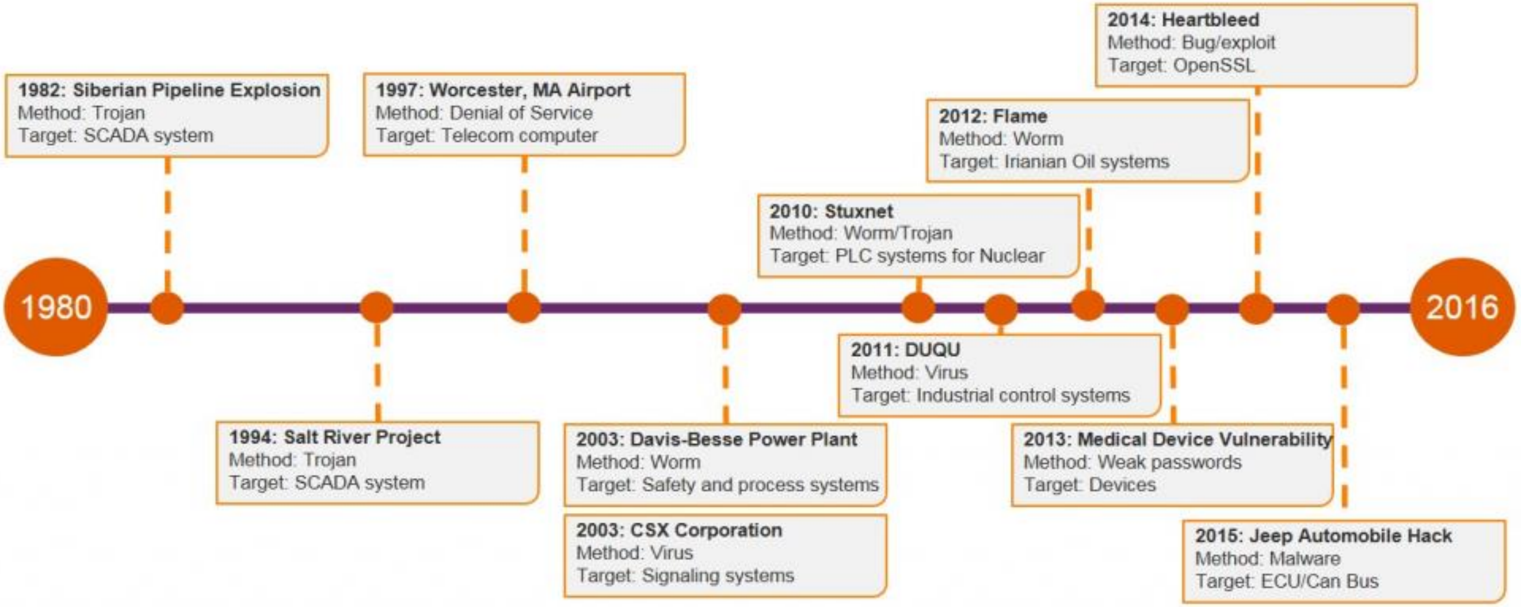
# Research Challenges at the Intersection of Cybersecurity and Safety

Bruno Crispo

Unversity of Trento

UNIVERSITY
OF TRENTO

Breaches of Industrial Control Systems: 1980-2016



**1982: Siberian Pipeline Explosion**
Method: Trojan
Target: SCADA system

**1994: Salt River Project**
Method: Trojan
Target: SCADA system

**1997: Worcester, MA Airport**
Method: Denial of Service
Target: Telecom computer

**2003: Davis-Besse Power Plant**
Method: Worm
Target: Safety and process systems

**2003: CSX Corporation**
Method: Virus
Target: Signaling systems

**2010: Stuxnet**
Method: Worm/Trojan
Target: PLC systems for Nuclear

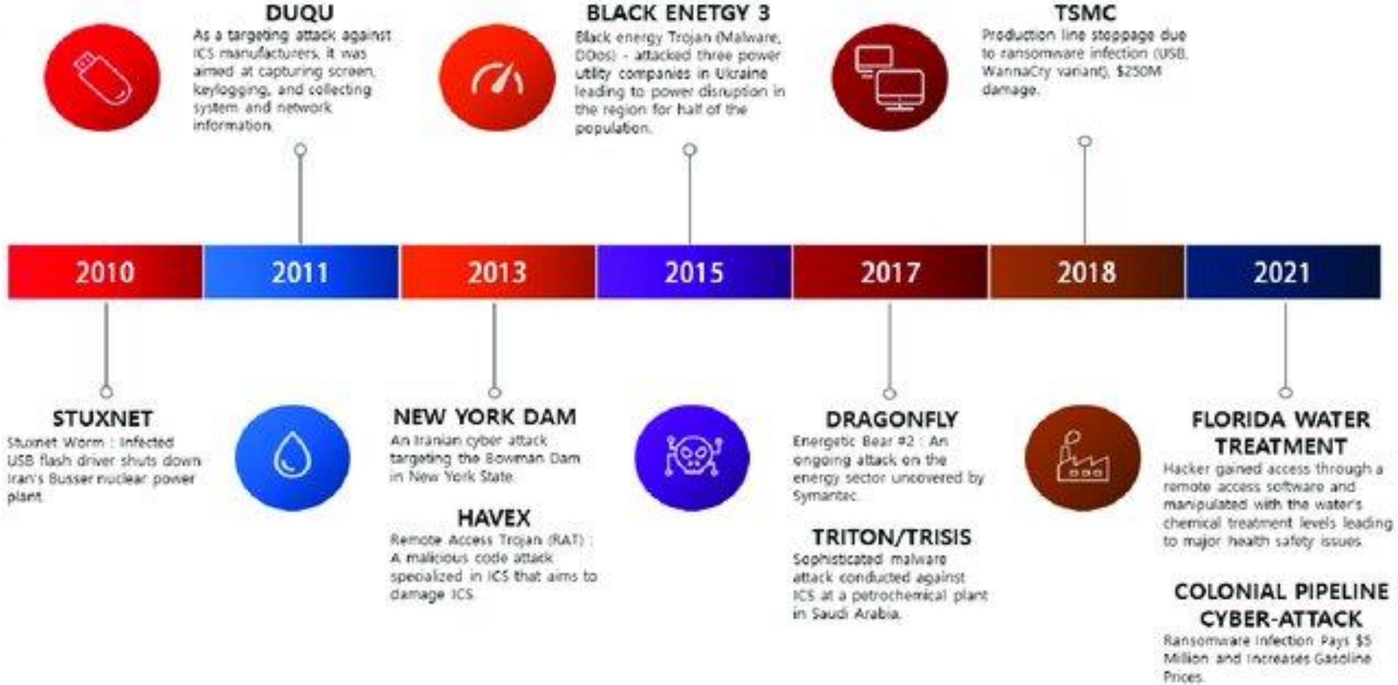
**2011: DUQU**
Method: Virus
Target: Industrial control systems

**2012: Flame**
Method: Worm
Target: Irianian Oil systems

**2013: Medical Device Vulnerability**
Method: Weak passwords
Target: Devices

**2014: Heartbleed**
Method: Bug/exploit
Target: OpenSSL

**2015: Jeep Automobile Hack**
Method: Malware
Target: ECU/Can Bus



**STUXNET**
Stuxnet Worm : Infected USB flash driver shuts down Iran's Busser nuclear power plant.

**DUQU**
As a targeting attack against ICS manufacturers, it was aimed at capturing screen, keylogging, and collecting system and network information.

**NEW YORK DAM**
An Iranian cyber attack targeting the Bowman Dam in New York State.

**HAVEX**
Remote Access Trojan (RAT) : A malicious code attack specialized in ICS that aims to damage ICS.

**BLACK ENETGY 3**
Black energy Trojan (Malware, DDos) - attacked three power utility companies in Ukraine leading to power disruption in the region for half of the population.

**DRAGONFLY**
Energetic Bear #2 : An ongoing attack on the energy sector uncovered by Symantec.

**TRITON/TRISIS**
Sophisticated malware attack conducted against ICS at a petrochemical plant in Saudi Arabia.

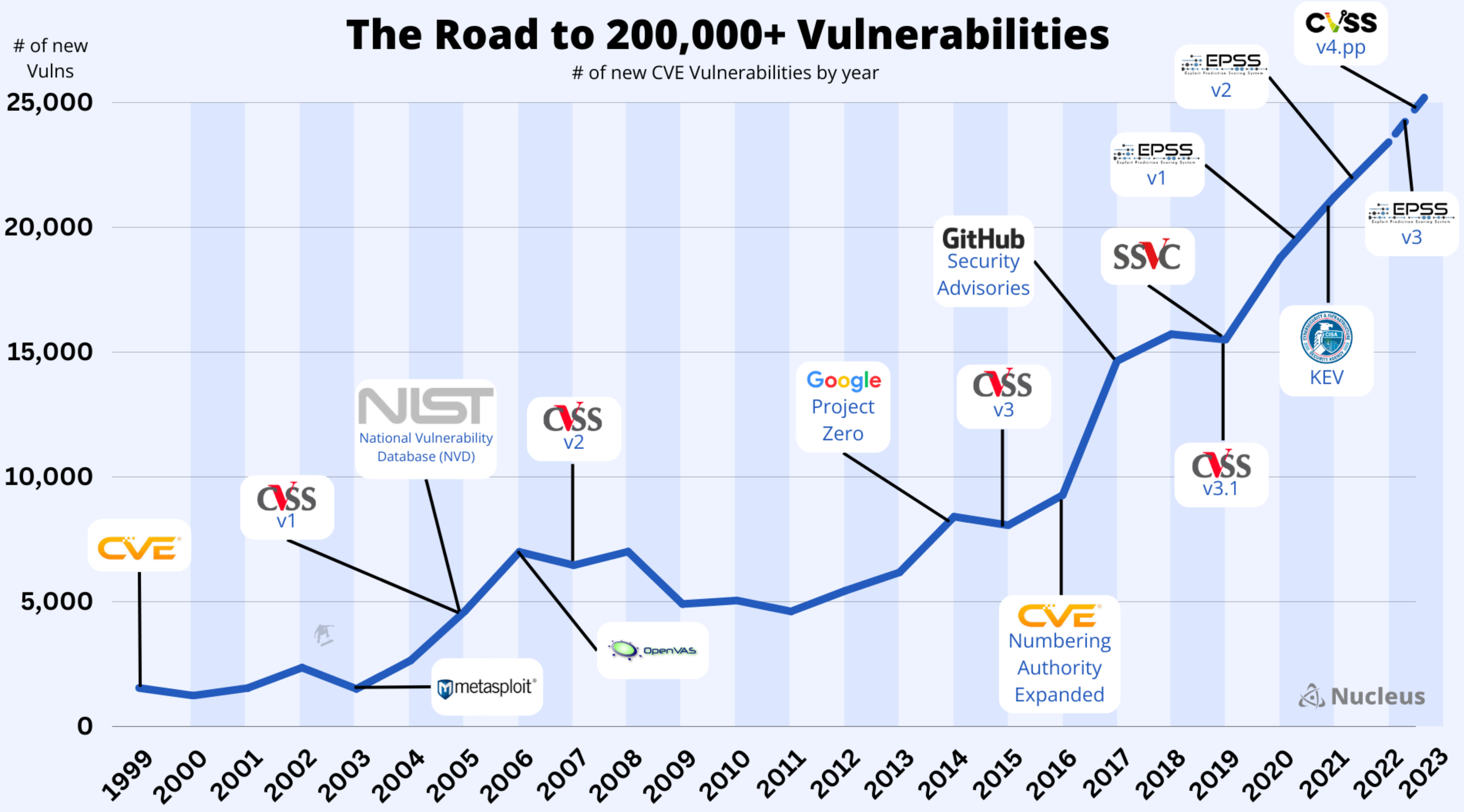
**TSMC**
Production line stoppage due to ransomware infection (USB, WannaCry variant), $250M damage.

**FLORIDA WATER TREATMENT**
Hacker gained access through a remote access software and manipulated with the water's chemical treatment levels leading to major health safety issues.

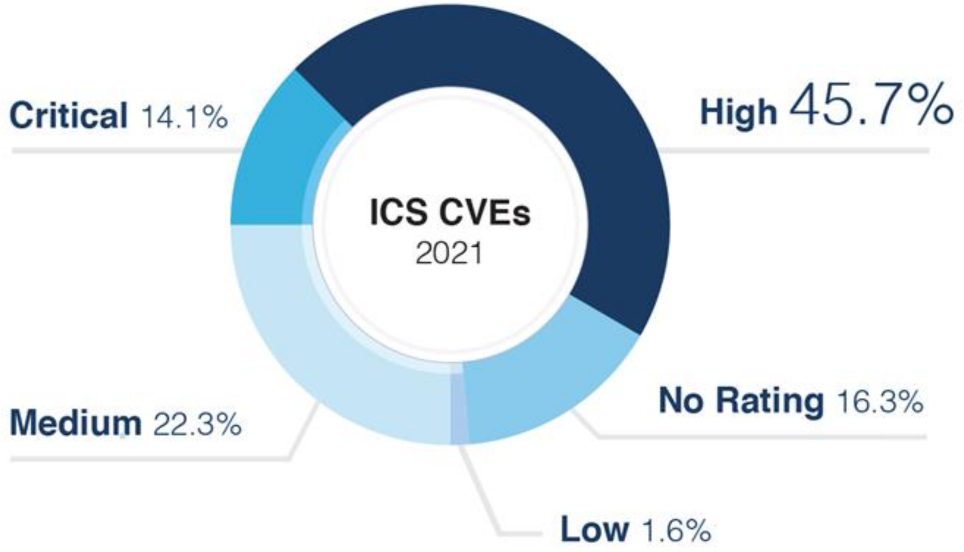
**COLONIAL PIPELINE CYBER-ATTACK**
Ransomware Infection Pays $5 Million and Increases Gasoline Prices.

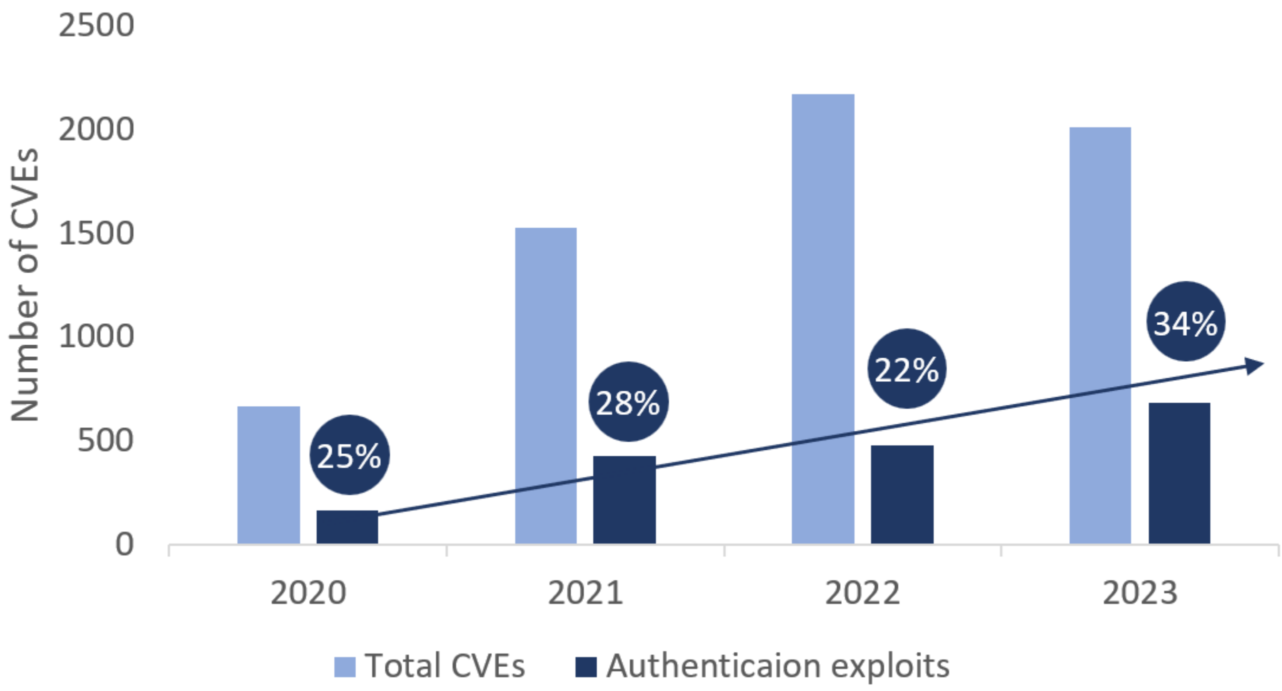
# The Road to 200,000+ Vulnerabilities

# of new CVE Vulnerabilities by year



# CVEs related to OT





# Assumptions

- Devices will get more and more powerful so likely to run complex features-rich applications
- Devices will be connected…to Internet

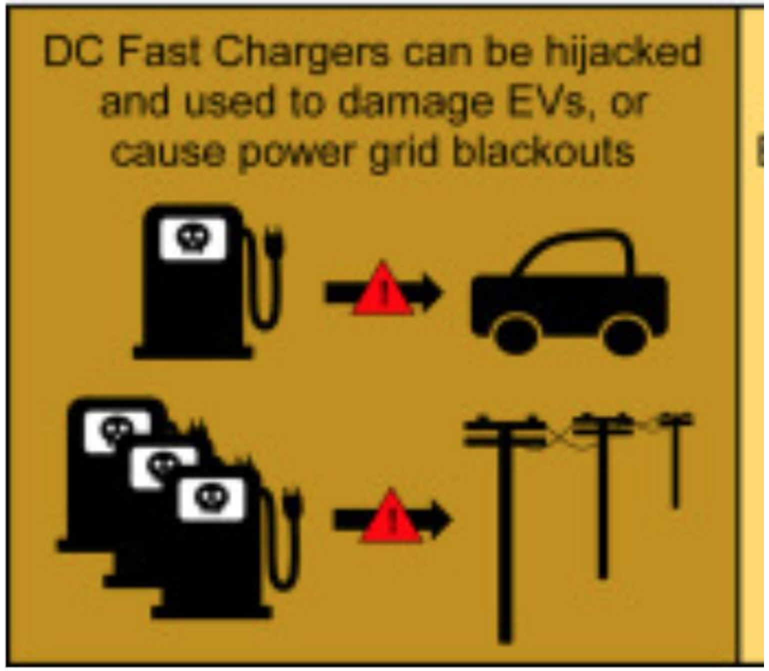
# Security solutions

- Authentication
- Encryption
- Key management
- Secure communications
- Intrusion detection
- .....

- Beware to choose the one that fit your security requirements.
- The threat model underlying secure protocols and security solitions is not always explicit, so what can be secure in a context may be unsecure in a different one!

# Example: ISO 15118 about charging plug

- The charging plug as intrusion point
- CHAdeMO standard widely used in Japan, relies on a CAN bus connection to the vehicle for the communication
- Mounting man-in-the-middle attacks attaching a connector between the charging plug of the car and the charging station, might allow criminals to modify packet and reprogram ECUs through the charging plug.
- To protect the vehicle against attacks through the charging plug, the upcoming ISO 15118 standard suggests the Transport Layer Security (TLS) protocol

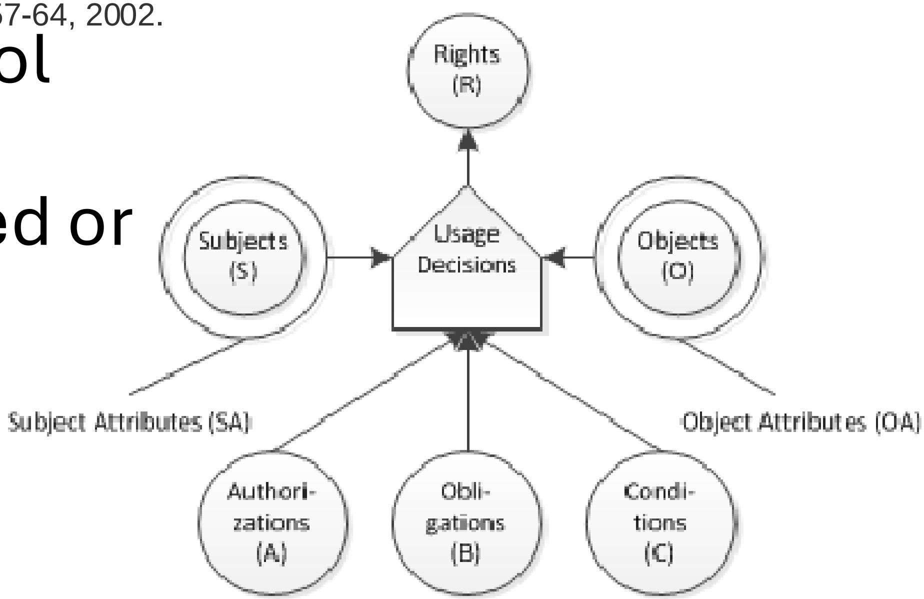

DC Fast Chargers can be hijacked
and used to damage EVs, or
cause power grid blackouts

Its important to identify the security correctly. This is not a problem of message integrity or authentication or confidentiality  but rather of access control!

# Access control is an opportunity

J PARK and R SANDHU, "Towards Usage Control Models:Beyond Traditional Access Control", *California USA Proceedings of the 7th ACM Symposium on Access Control Models and Technologies*, pp. 57-64, 2002.

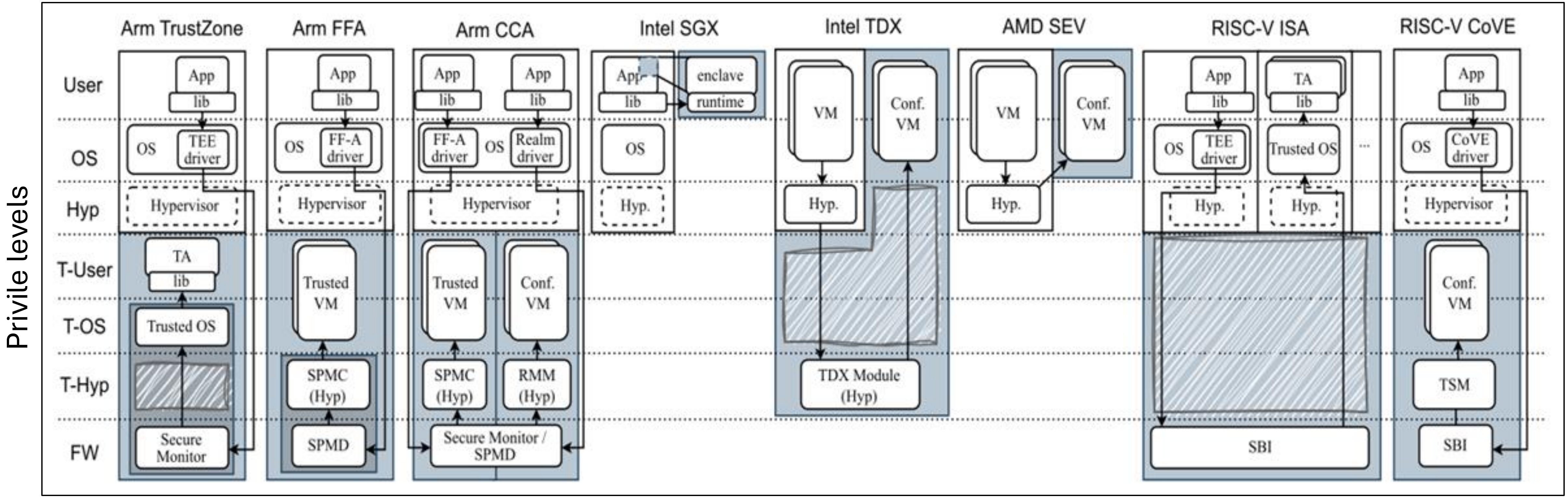
- MAC/DAC/RBAC/ABAC. Classical Access control models regulate only the access to information/services.How the function is invoked or if it is executed correctly is out of scope



- Usage Control (UCON). Put guards in the execution of the process. Can be extended to inlcude safety conditions. Process must not be hardcoded but configurable

Possibility to specify UCON policy that encompass secure and safe conditions. Operational conditions under which an authorized entity must operate the system → this can be considered a form of *Intrusion Prevention System*

# TEE technology landscape

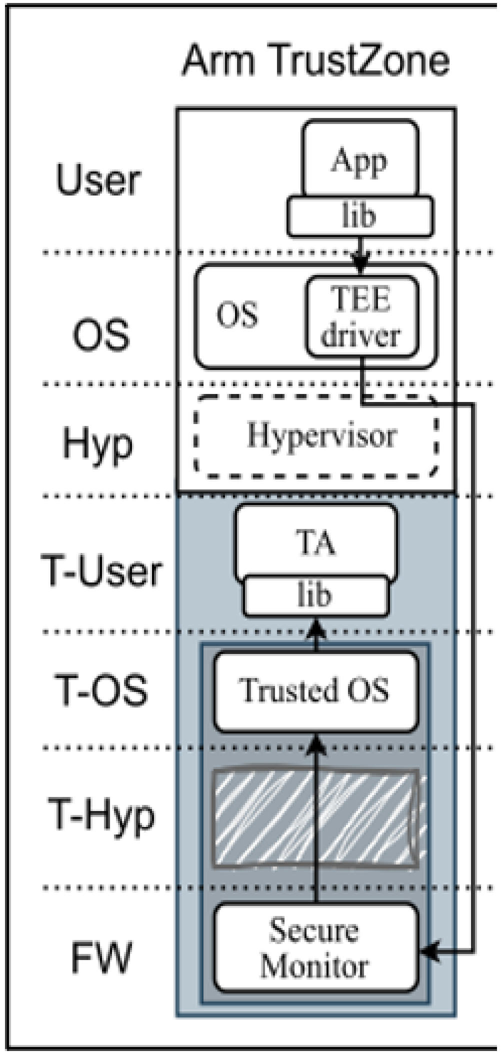


- Big issues with interoperability
- Proprietary solutions. API restricted ⇢ RISC V is an opportunity
- What to store in the protected part (*safe state to recover to?*)

# Assurance issues

- Software and architectural vulnerabilities

- CVE-2015-6639, CVE-2016-8754
- CVE-2016-2431, CVE-2017-18655, CVE-2017-18657, CVE-2020-10848
- *"Kinibi TEE: Trusted Application exploitation"*
- *War of the Worlds - Hijacking the Linux Kernel from QSEE"*
- *"Breaking Samsung's Root of Trust - Exploiting Samsung Secure Boot"*
- *"Extracting Qualcomm's KeyMaster Keys - Breaking Android Full Disk Encryption"*
- *"Exploiting Trustzone on Android"*
- *"Breaking Samsung's ARM TrustZone"*



# Monitor and intrusion detection

- A lot of work to detect failures of the preventive security solutions. Example, plenty of work on intrusion detection applied to the CAN bus.

Pros

- Most approach are based on anomalous detection
- Advance in the use of ML classifier so higher accuracy
- A lot of automation in the detection

Cons

- Monitoring introduce new code that need to be validated for safety not only for security
- Good to stop most attacks and large scale campaign, less for target attacks
- Difficult to profile legitimate behaviour. Dealing with false alarms

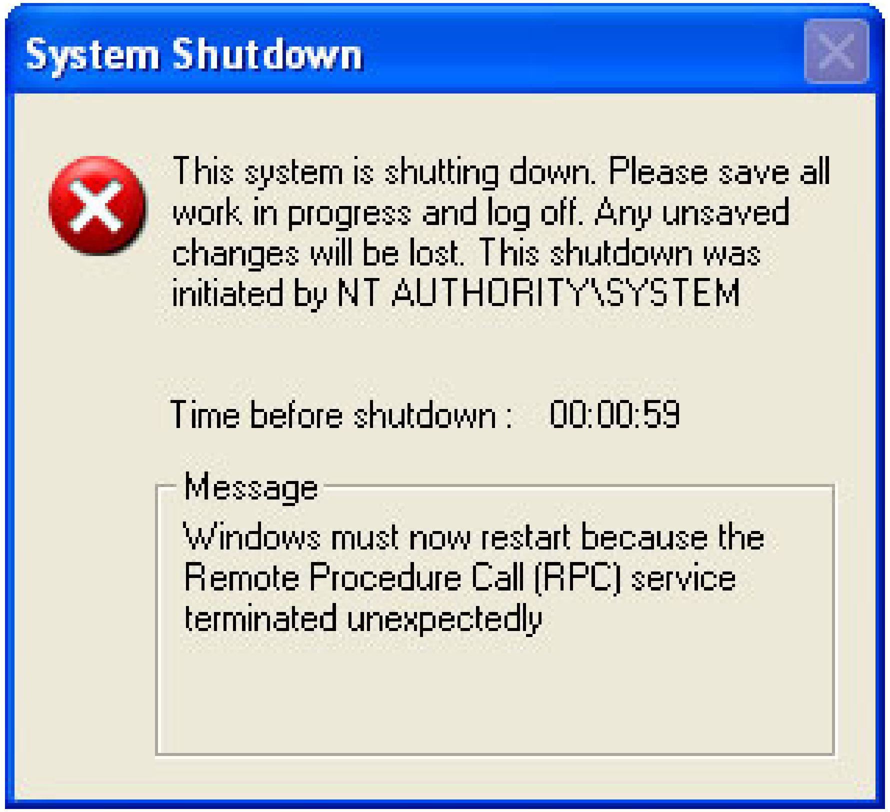
# The open problem is the recovery...

- The recovery is where safety and security really diverge because concerns like operational continuity or functional safety are not explicitey considered. Security react to the "attack" with the aim of preserving or mitigating the loss of the affected security properties that relates to information
- An intrusion has been detected, then what? Call the operator
- Difficult to automate the recovery for general purpose interactive systems, can be different for special purpose deterministic systems.

# Example of how NOT to Automate a  Response

- Welchia (anti-worm)
  - Removes Blaster infection, patches the vulnerability
  - Used the same Microsoft RPC bug as Blaster
  - Deletes itself after January 1, 2004

*While the idea of a good worm is certainly a worth while venture to be explored (and could be quite profitable to the programmer that develops it), any such venture would have to have security restrictions to ensure it does not leave the intended network. Welchia demonstrates what happens when these little monsters escape. …… At the very least, with 2004 approaching rapidly, Welchia will soon be a distant, bad memory.*



System Shutdown

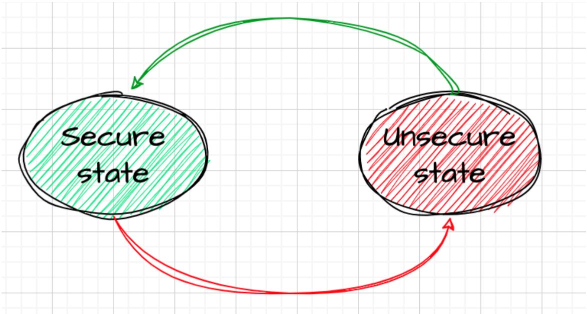
This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM

Time before shutdown : 00:00:59

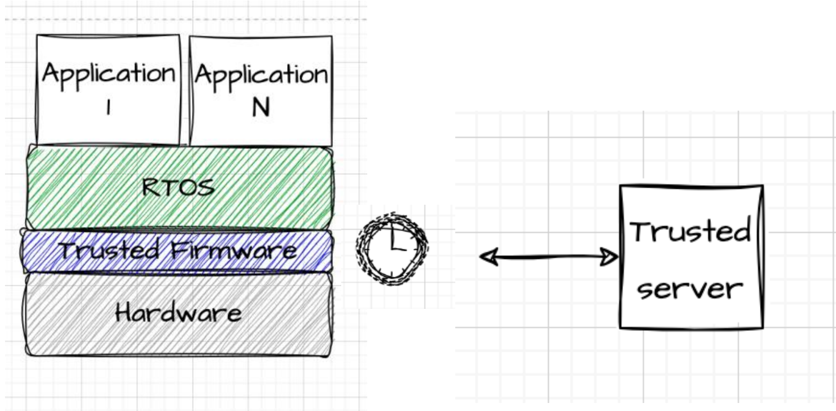
Message

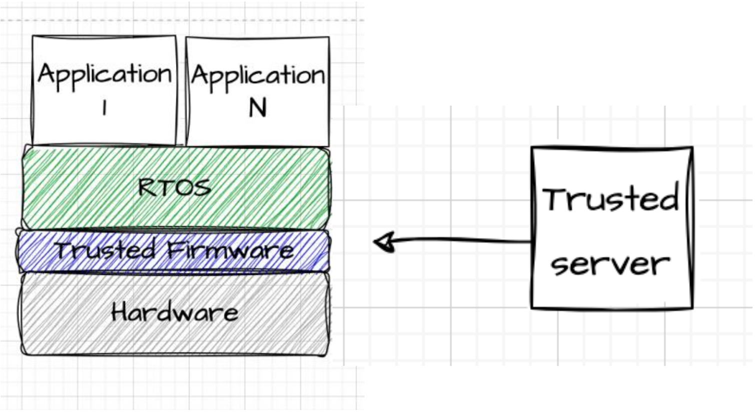
Windows must now restart because the Remote Procedure Call (RPC) service terminated unexpectedly

# No-man land



- Remote operator.
- Problem: Restore a secure state in a compromised unattended remote device where all software but some small trusted firmware is malicious.
- How to design such a trusted firmware is an open problem

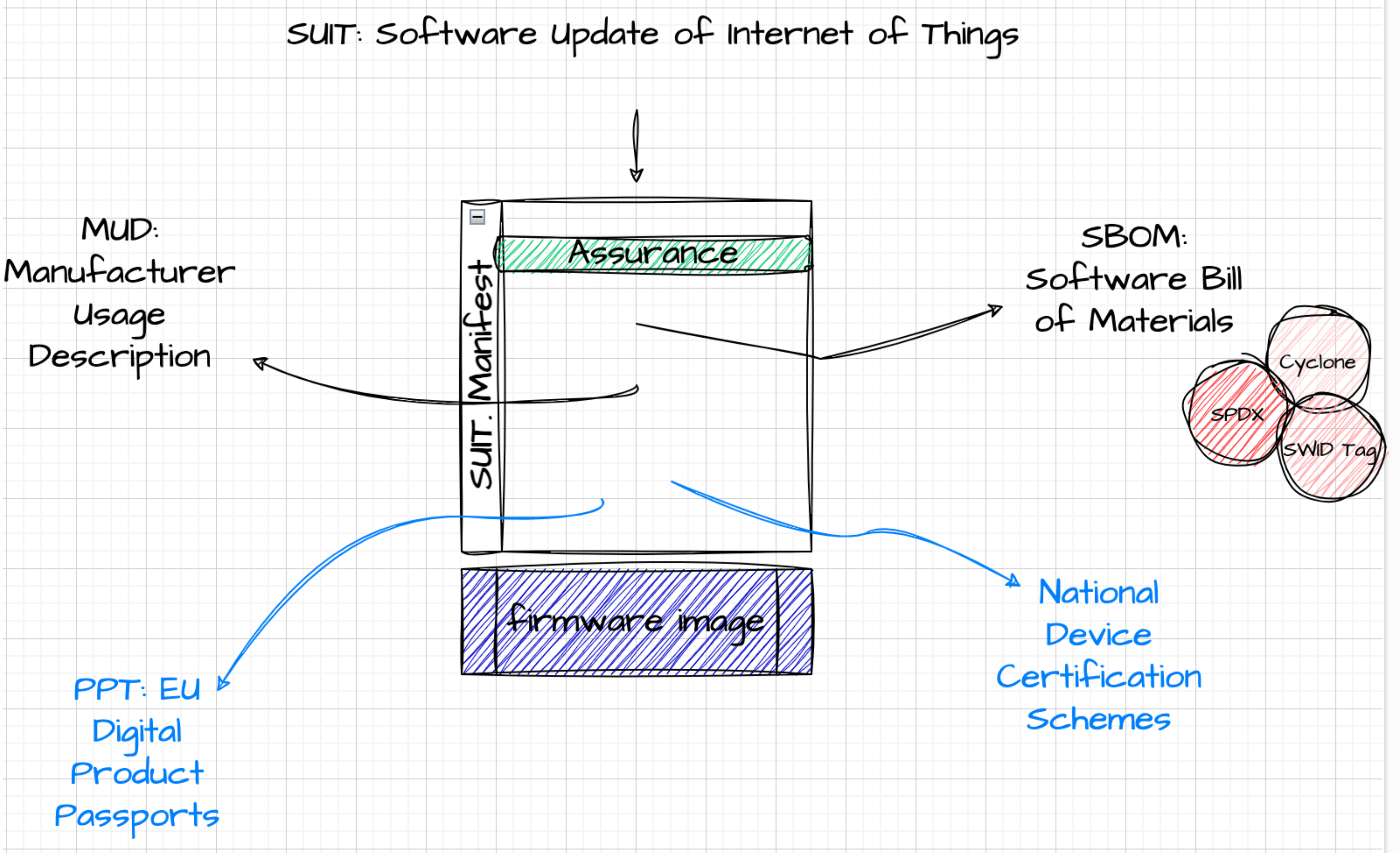




# Supply-chain:   firmware secure updates

- Need for a standard.  Good candidate SUIT (RFC 9019, RFC 9124)

- Need to create a link with other regulations, standards, certification, etc. in order to have a complete up to date picture of the SW that is going to be installed


SUIT: Software Update of Internet of Things
Assurance
SUIT. Manifest
MUD: Manufacturer Usage Description
SBOM: Software Bill of Materials
Cyclone
SPDX
SWID Tag
firmware image
PPT: EU Digital Product Passports
National Device Certification Schemes

# Conclusions

These are just few of the research challenges that lie at the intersection of security and safety. More can be added. Much more exist if looked from the safety prespective

There is room for impact if a real multidisciplinary approach is used
This implies learning something about the other discipline rather than demanding to the other discipline what yours did not manage to solve.