

TELEMETRY

Trustworthy methodologies, open knowledge & automated tools for security testing of IoT software, hardware & ecosystems

ECSCI Webinar

2026-10-26

Funded by
the European Union

TELEMETRY

Key Objectives

Develop tools & techniques for **cybersecurity testing**, security event **detection & assessment** at both ***component*** and ***system*** level

Supports ***static testing*** and ***continuous monitoring & assessment*** of IoT components and ecosystems

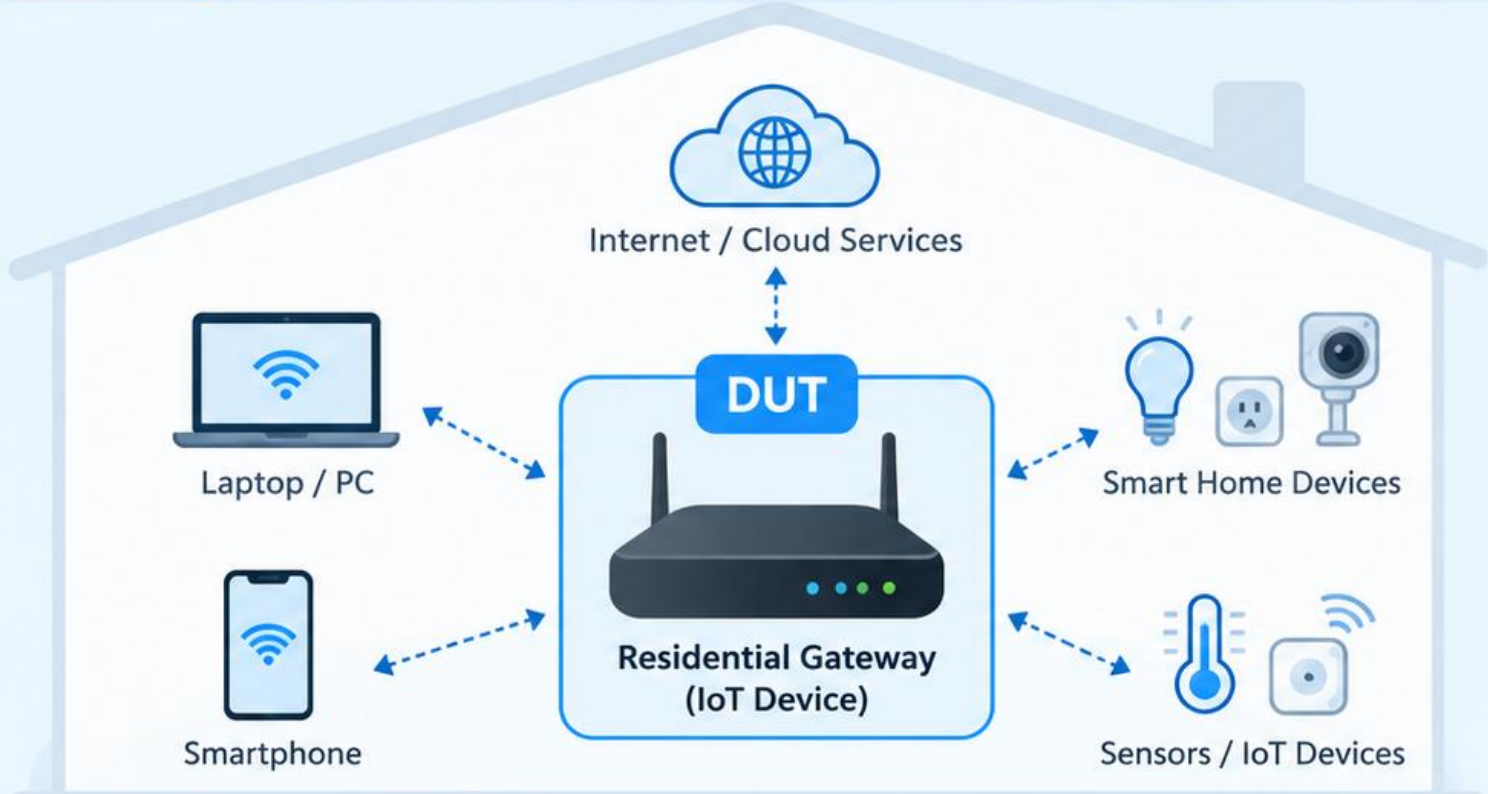
TELEMETRY

Principles, Concepts and Elements

Device Under Test vs System Under Test

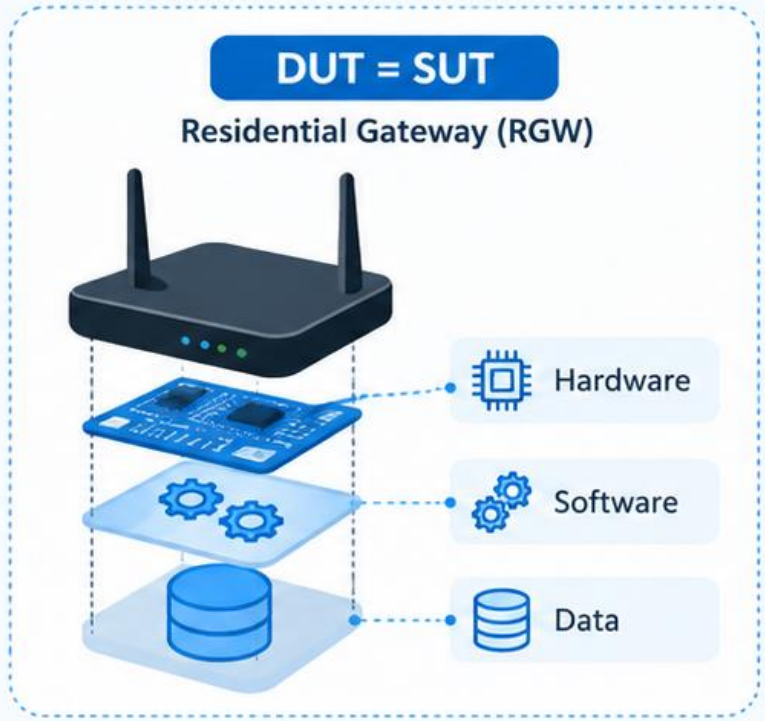
SUT — System Under Test

Complete environment including the device and its context



A DUT can itself be an SUT

Devices are complex systems on their own.
(Systems of Systems)





Example: Residential Gateway (RGW) from TIM (UC3)

- DUT integrated into a domestic environment
- RGW is a complex system of hardware, software and data

TELEMETRY

Indicators

Observable information about the Device Under Test (DUT) or System Under Test (SUT) that potentially can underpin insight on its ***cybersecurity posture***

- Generated and consumed by TELEMETRY and external tools
  - Toolchains can be built using Indicators as the interface between tools
- Displayed to human operator as alerts or insight
- Supports static and dynamic security event management
  - *Static examples:* fuzz testing results, software composition (SBOM)
  - *Dynamic examples:* device and system level AI-based anomaly detection
  - *Both static and dynamic examples:* Trust and Risk Assessment Results derived from other Indicators



TELEMETRY

Key Elements



Semi-static analysis

Software Bill of Materials (SBOM) -> vulnerability indicators -> prioritisation

Network Fuzz Testing



Dynamic Event Detection

ML-based detectors of device and network anomalies

Redundant anomaly detection using different methods for consensus



Auditable data infrastructure

Data exchange and storage via immutable Distributed Ledger for audit



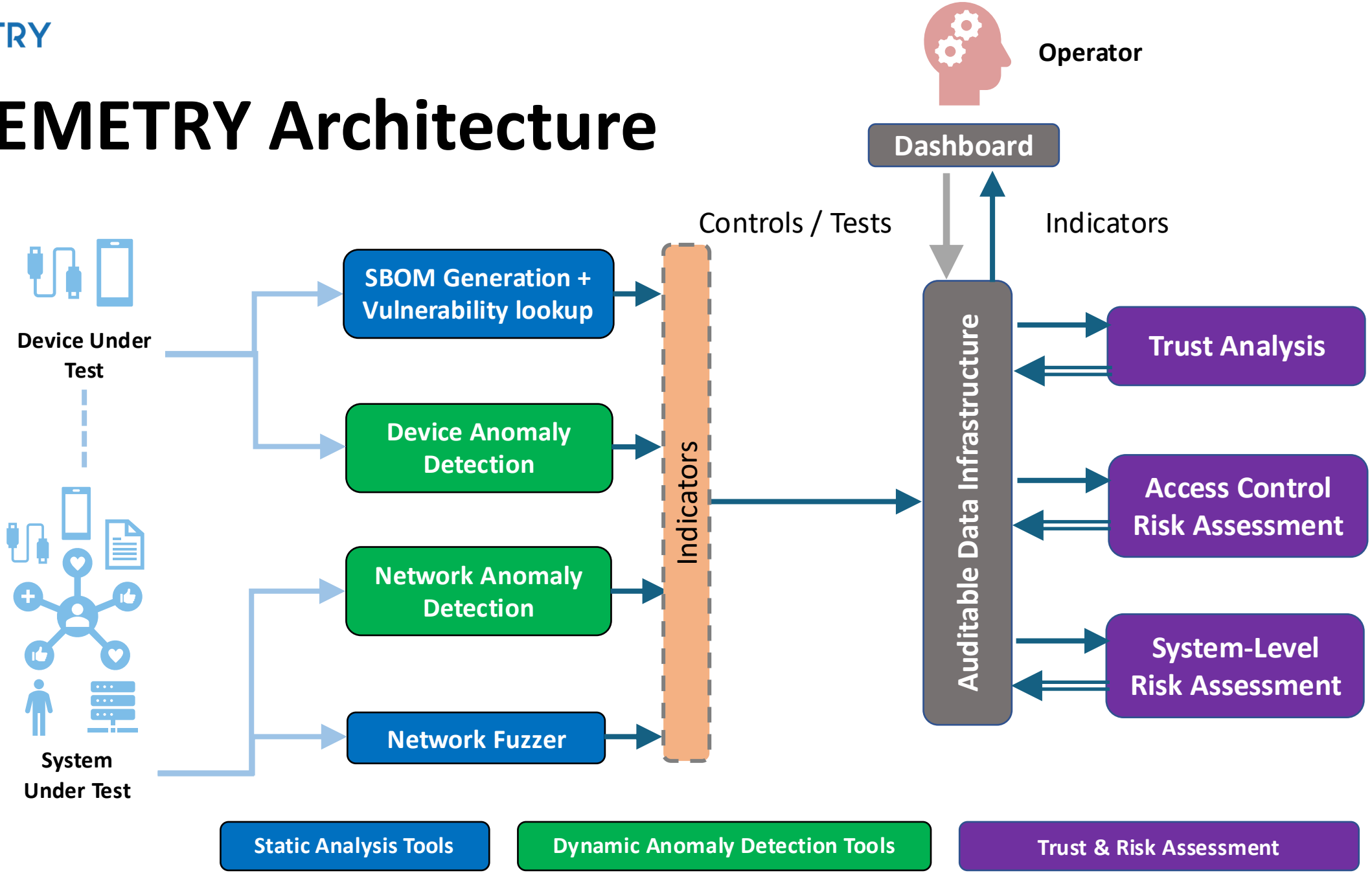
Trust & Risk Assessment

Automatic tools analysing Indicator Consequences via Likelihood & impact

Informed by testing tools or dynamic anomaly detection indicators

TELEMETRY

TELEMETRY Architecture



Use Cases



UC1: Aircraft

Upgrade of critical aerospace systems in Antonov aircrafts

UC2: Manufacturing

Security and trust in software and hardware components

UC3: Telecommunications

Security testing for Residential Gateway and IoT Devices

TELEMETRY

Case Study: Common Vulnerabilities and Exposures (CVE) Prioritisation for Residential Gateways

TIM

TELEMETRY

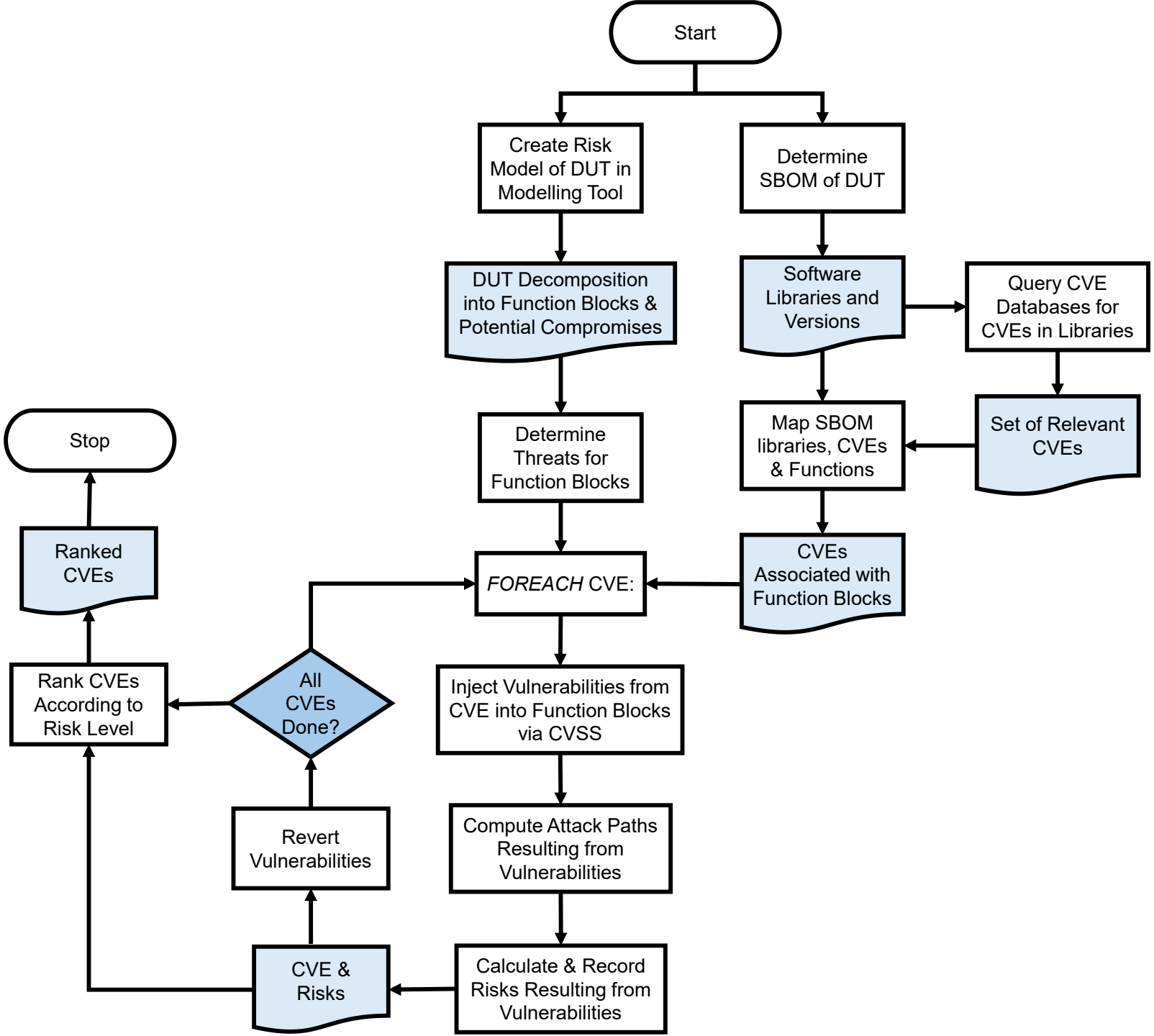
Residential Gateway Vulnerability Prioritisation

- TIM Provides Residential Gateways (RGWs) to subscribers – router / modem devices that provide link to ISP and home network
- RGWs manufactured by third party providers
- RGWs are deployed in domestic environments and connect to ISP but are systems in their own right (DUT is SUT)
- Many security vulnerabilities (CVEs) published for RGWs – which ones to prioritise?

TELEMETRY

Approach

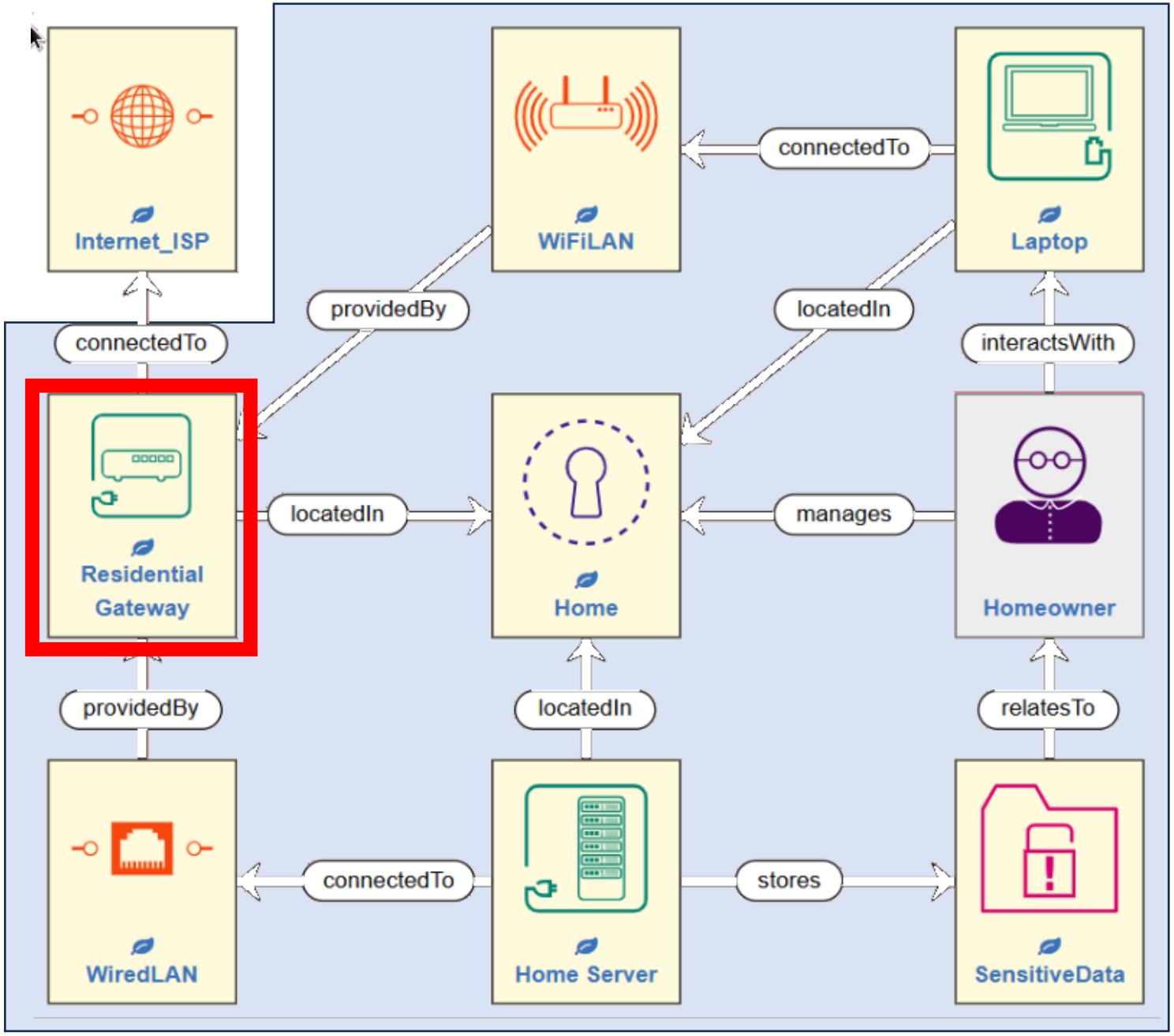
- Use **SBOM Generation + Vulnerability lookup** to identify packages on device & lookup relevant CVEs
- Use **System-Level Risk Assessment** to determine risks resulting from each CVE of device in its deployment context
- Once setup, can be rerun frequently to automatically assess new CVEs and new builds



TELEMETRY

SUT + DUT

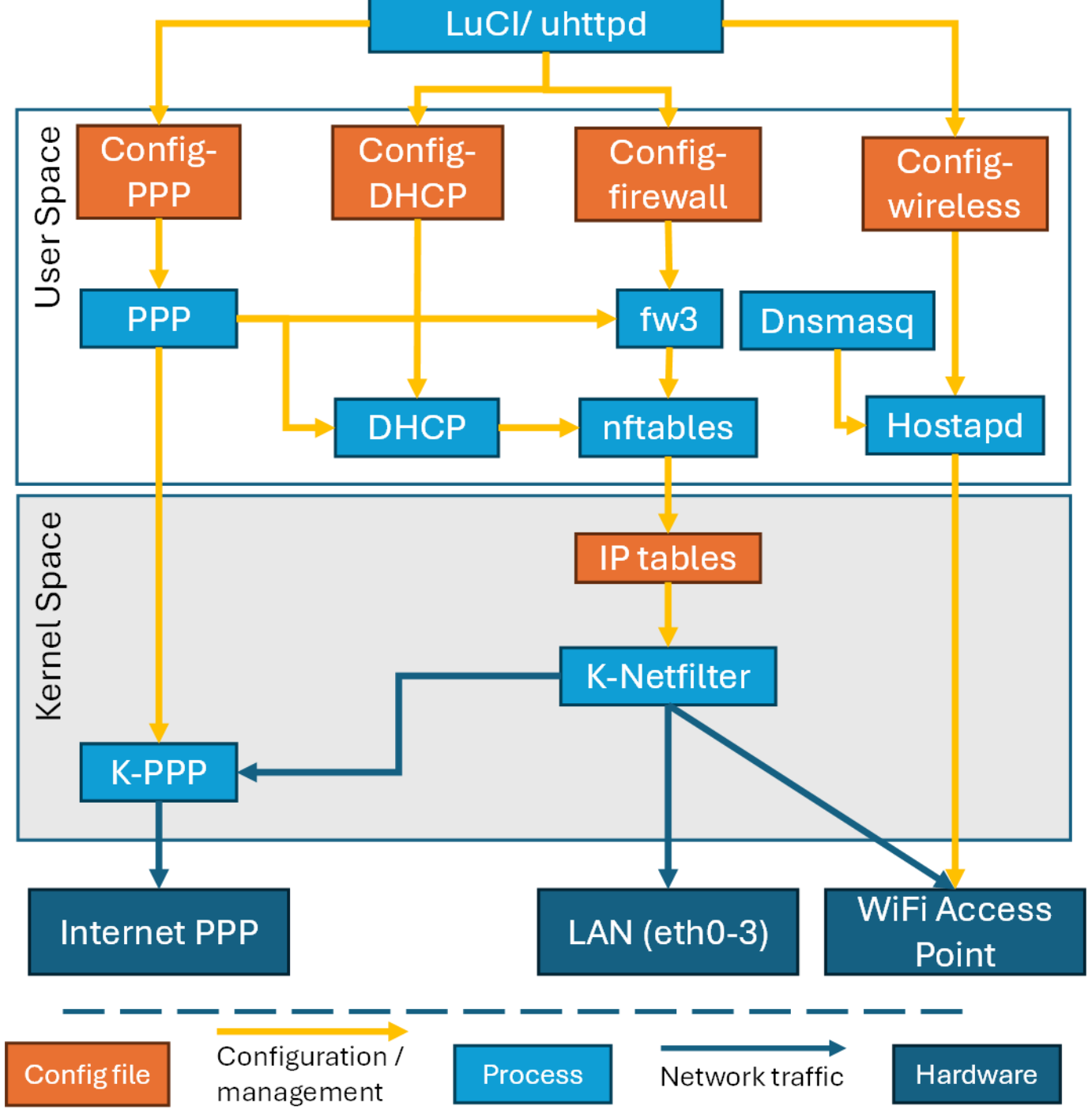
- System = Domestic Context + ISP
- RGW is interface between WAN + private WiFi & LAN
- Typical domestic equipment on LAN including sensitive data



TELEMETRY

RGW Decomposition

- RGW (DUT) as System in its own right
- Kernel Processes control Internet connection, LAN, WIFI
- Kernel processes managed by user processes & configured by files
- Orange routes = potential attack paths
- ***CVEs mapped into key processes via SBOM packages and CVSS vector***



Example 1 - CVE-2020-8597: Buffer overflow vulnerability in pppd (Point-to-Point Deamon)

- CVSSv2 vector: AV:N/AC:L/Au:N/C:P/I:P/A:P
- Remote code execution network based attack (AV:N), Low complexity (AC:L), Does not require authentication (Au:N)
- Could result in partial compromise of C, I and A of the pppd process
- CVSS score 9.8 Critical
- System context-aware risk score: Very High
  - May enable a remote anonymous exploit on PPP to open a path between the Internet and the private WiredLAN, thus allowing untrusted users onto the WiredLAN
- ***Conclusion – CVSS and system context-aware risk assessment agree***

• Example 2 - CVE-2021-23017 Buffer Overflow in nginx (web server used for RGW admin)

- CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L
- Network attack, High Complexity, No Privileges resulting in potential Confidentiality and Integrity compromise in nginx
- Severity CVSS score: 7.7 (high)
- System context-aware risk score: Low
  - Significant vulnerability that has consequences that the nginx web server is made insecure and gain admin access to the RGW
  - ***But* nginx is only accessible from internal private networks and so there is no route for untrusted users to access it**
- ***Conclusion: CVSS and system context-aware risk assessment disagree***
- *However! If untrusted users get access to LAN (e.g. via Example 1) context score would be Very High*
  - *Therefore combined analysis of CVEs is also important*

Conclusion

- TELEMETRY supports testing and dynamic analysis of Devices and Systems together
  - Devices can be Systems in their own right
- Indicators are key concepts
  - Information and insight for operator
  - Output from and consumed by TELEMETRY tools
  - Stored in Auditable Data Infrastructure
- Example use case of vulnerability assessment and prioritisation
  - CVSS scores independent of deployment system
  - System context is important in CVE assessment
  - Combined CVEs in system may have significant consequences

TELEMETRY

Thank you

info@telemetry-project.eu

NOKIA

SINTEF

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Ideas for Research & Innovation

ATC
ATHENS TECHNOLOGY CENTER

KU LEUVEN

TIM

eng

WRCVE

ANTONOV AIRLINES

University of Southampton

Funded by the European Union

Grant agreement ID 101119747