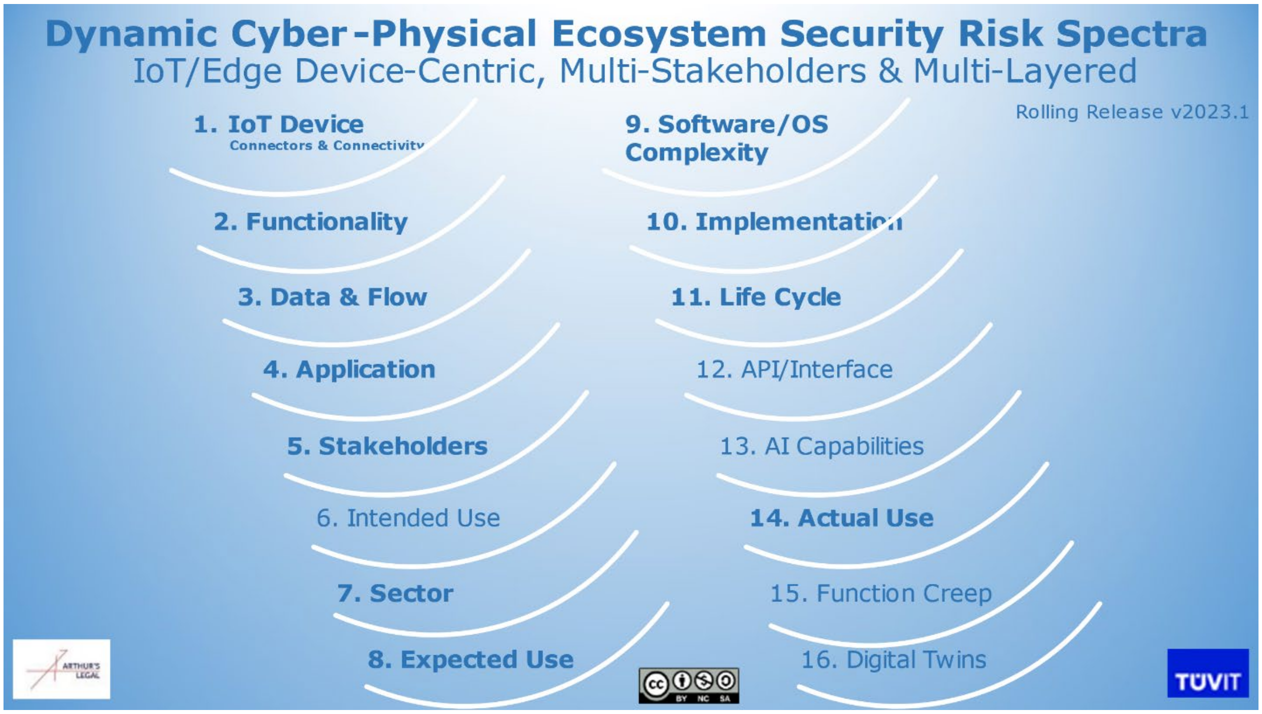
How to use the Device-Centric IoT Security Risk Spectra

The Seven Step Protocol

1. Check the various Spectra, from upstream/left to downstream/right
2. Do the current Risk Classification for Spectrum 1
3. Do the current Risk Classification for subsequent Spectra
4. Combine Outcome
5. Mitigate: Consider & Organise Technical & Organisational Security Measures
6. Double-loop Measures
7. Double-loop Changes



Dynamic Cyber -Physical Ecosystem Security Risk Spectra

IoT/Edge Device-Centric, Multi-Stakeholders & Multi-Layered

Rolling Release v2023.1

1. IoT Device
Connectors & Connectivity

2. Functionality

3. Data & Flow

4. Application

5. Stakeholders

6. Intended Use

7. Sector

8. Expected Use

9. Software/OS Complexity

10. Implementation

11. Life Cycle

12. API/Interface

13. AI Capabilities

14. Actual Use

15. Function Creep

16. Digital Twins

Description per Each of the Seven Steps:

1. Check the various Spectra, from upstream/left to downstream/right

Especially more downstream there may be Spectra that may not be relevant; however, if such Spectrum may become relevant later in the life cycle of the IoT device it is recommendable to keep it in and already do the Spectrum Risk Classification.

2. Do the current Risk Classification for Spectrum 1

The Risk Classification shall be done on each Risk Layer, meaning 'in General' as well as in relation with Hardware, Connectivity, Data, Platform/OS, Functionality/ Application, Financial Impact, Ecosystem and Other. Each such Layer in the well-known three Risk Levels: Low, Medium and High.

3. Do the current Risk Classification for subsequent Spectra

After doing a Risk Classification for Spectrum 1, please do a Risk Classification for Spectrum 2, and so forth.

4. Combined Outcome

Based on the outcome of (i) a Risk Classification for each Spectrum, and (ii) the combined outcome of the various Risk Classifications, the Combined Risk Classification can be established.

5. Mitigate: Consider & Organise Technical & Organisational Security Measures

Based on the Combined Risk Classification one can consider & organise technical & organisational security and related measures. The Device-Centric IoT Security Risk Spectra is to get you started with that; it however does not give any recommendations or guidance about those.

6. Double-loop Measures

Measures by itself can include, cause or otherwise trigger risk. It is therefore recommended to double-loop the particular set of measures, for once to initially assess whether these could result to achieving and sustaining the appropriate level of trust and assurance. For instance in Clause 32 GDPR, this contextual level is defined as the state-of-the-art continuous appropriate dynamic accountability (‘*Dynamic Level*’).

Therefore, it is recommended to double-loop the above until that Dynamic Level has been met, and to continuously double-loop thereafter to keep the security measures up to date and resilient.

7. Double-loop Changes

As per the dynamics of IoT and IoT security, any of the Spectra notable changes are expected to trigger, change or otherwise show relevant dynamics, such as for instance (A) technical or other threats and vulnerabilities, (B) actors and other stakeholders anomalies, updates or upgrades in code, datasets or attributes, or (C) changes in regulatory standards, policies or other relevant best practices, it is recommended to double-loop as well, including those Spectra that are or may be related or otherwise are (inter)depended on the particular Spectra.

Therefore, it is recommended to continuously monitor the risks, and where necessary or otherwise double-loop thereafter to keep the security measures up to date and resilient.

Reminder

As a reminder please do note that this is the Device-Centric IoT Security Risk Spectra Protocol, focussing from a single device. Hence, when more devices, systems and services are relevant – which is generally the case in deployed IoT ecosystems – it is recommended to also run this Seven Step Protocol, in a layered way, with multiple devices and related technical stack, stakeholders and the like. Layered, as with that one can both better identify and address the dependences, risk aggregators and risk mitigators, as well as later on better identify and pinpoint threats and vulnerabilities and its potential impact thereof. It also demonstrates that manufacturers and operators of (parts of) IoT ecosystems – and customers and other demand side of (parts of) IoT ecosystems – might have different results in their risk classification of selected IoT devices.