

/ Cybersecurity in the context of the EU Cyber Resilience Act

Michael Roeder, CISSP, Dipl.-Ing., M.Sc. ~~LL.M.~~
Senior Manager, Software & Services EMEA



michael.roeder@avnet.eu

AVNET[®] SILICA
Software  Services



The information provided in this presentation is for informational purposes only. No guarantee is made regarding its completeness, correctness, or suitability for any particular purpose.

Therefore, the presenter and Avnet cannot be held liable for any errors, omissions, or damages arising from the use of or reliance on the information provided herein.

Any action taken based on the information in this presentation is at the sole discretion and risk of the viewer.



Agenda

- Introduction and Goals
- Basics: EU Legislation Process, Important Terms
- EU Cybersecurity Legislations Overview (excerpt)
- Network and Information Systems 2 (NIS2): Primer
- The EU Cyber Resilience Act (CRA): Overview
 - Goals
 - History
 - Products in Scope
 - Open Source Aspects
 - Classification (Product Classes)
 - Obligations
 - Security by Design
 - Vulnerability Handling
 - Documentation
 - User Instructions and Information
 - Preparing for the CRA
- Information Security Frameworks and Standards
- EU Certification
- Key Takeaways



- **Establish common ground and understanding for underlying concepts and put you in the driver's seat**
 - European Cybersecurity is work-in-progress, on many fronts
 - Valid information and suggestions today might be outdated, wrong or misleading tomorrow
- **Provide starting points and links to the actual sources.** If those are changed/obsoleted, you will know.
- **Starting on a high level of abstraction, build basic understanding of motivations, dependencies, history**
- **Principles I try to follow:**
 - **go to the source, reference the source, explain from the source. However...**
 - Legislations mostly tell you WHAT to do, not HOW to do it
 - EU Legislations are here to protect us, not to make life harder – however, nobody's perfect ☺
 - **“Make everything as simple as possible, but not simpler.” -- *Albert Einstein***
 - Don't overthink it, but keep in mind:
 - **100% secure systems are possible – with infinite cost/time investment and for an infinitesimal small timeframe**
 - **Resilience is a function of time**
 - **Security is a function of time**
 - **If someone promises you otherwise (“100% secure”, “free of errors”, ...) – RUN!**
- **#1 rule of Marketing:** „if something is for free, you are the product“

(Richard Serra, 1973)



Software&Services EMEA

Avnet Silica's EMEA-wide team of
Embedded Software Specialists and
System Architects: sas@avnet.eu



Technology Backbone

- Strategic Demand Creation
- Marketing Enablement
- Support, Training
- Topics (excerpt):
 - TSN
 - Functional Safety
 - Security
 - Image Processing and Vision

Software Expert Support

- deep-dive SoC support
- Low-Latency
- for strategic projects
- for customers, suppliers, (and partners)
- Software as protective abstraction layer

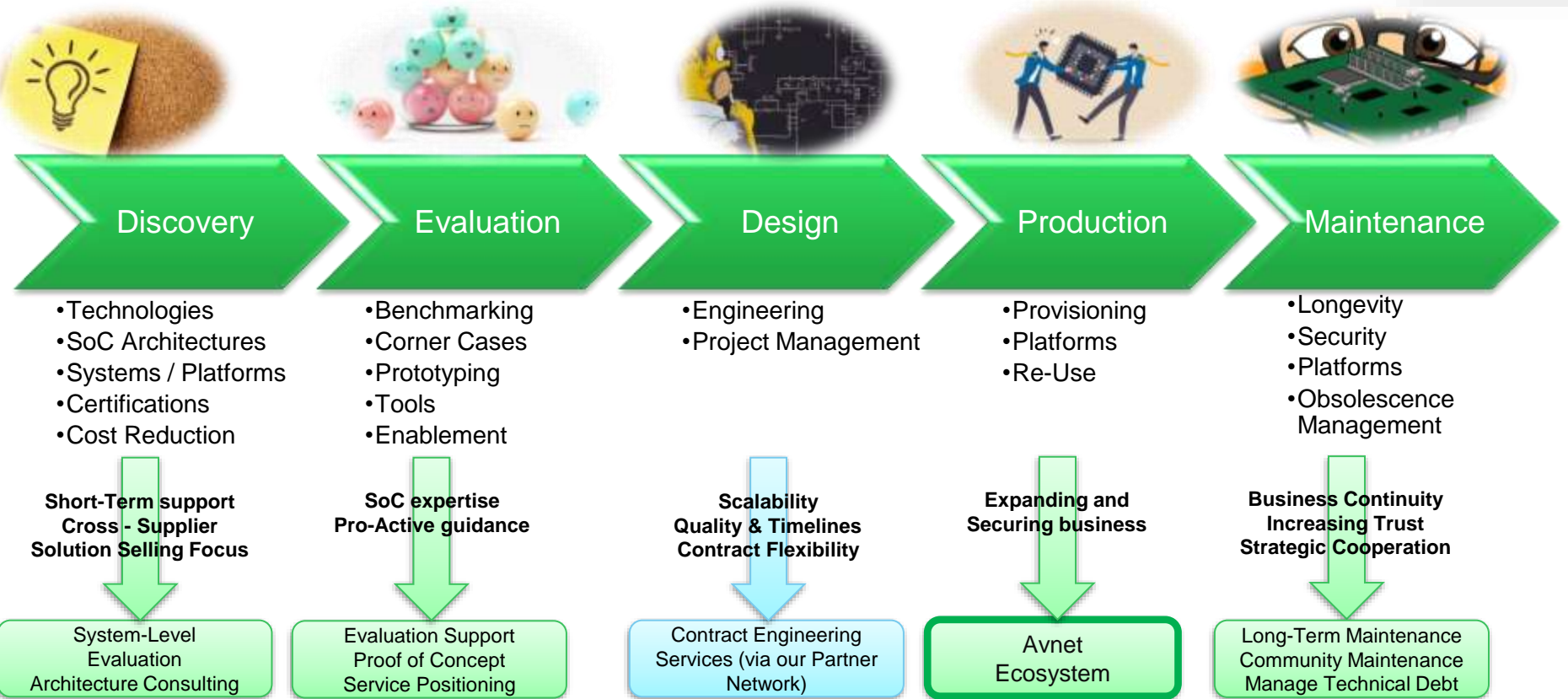
System-Level and Architecture Analysis

- Systematic Analysis of Hardware, Software, Total Cost of Ownership and Compliance
- One-Stop-Shop to access engineering partner network
- Project Management and Coordination

Partner Network Management and Coordination

- One-stop-shop for engineering services
- Open to customers and suppliers
- Qualification, Expansion, Management and Monitoring of EMEA software and technology partners
- handle all the overhead:
 - Discovery
 - Engagement Model
 - Commercial topics
 - SoW / development contract
 - Strategic Engagements

Software&Services in the Design Cycle



/ Technology Overview



System-Level and Architecture

- ✓ SoC and CPU Architectures
- ✓ Accelerators, Offloading
- ✓ Real-Time Processing Subsystems
- ✓ Move to Production
- ✓ Functional Safety according to IEC61508



Operating System and BSP

- ✓ Software Platform and Lifecycle Management
- ✓ U-Boot, TF-A, GNU/Linux, Yocto
- ✓ Zephyr, FreeRTOS, Windows 10 IoT Enterprise
- ✓ Virtualization, Real-Time



Platforms

- ✓ Platform Lifecycle and Update Management
- ✓ Total Cost of Ownership optimization, Technical Debt reduction
- ✓ Open Source: benefits, pitfalls, licensing, management
- ✓ System-on-Module: make vs. buy, multi-level abstraction



Software Architecture and Craftmanship

- ✓ Architecture Consulting, High-level decision making
- ✓ Language and library selection
- ✓ Trade-off handling
- ✓ Modern C++ on embedded devices



Security

- ✓ Security Analysis and Evaluation
- ✓ Hardware-assisted Security
- ✓ Operating System Security
- ✓ Cloud / IIOT – Security
- ✓ Security Lifecycle Management



IIoT, TSN, accelerated Ethernet

- ✓ TSN 802.1 standards
- ✓ Time Synchronisation (1588, 802.1AS-2020)
- ✓ Talkers, Listeners, Real-Time/Latency optimization
- ✓ (Automated) Configuration
- ✓ OPC/UA
- ✓ System Level integration

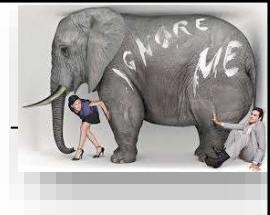


Embedded Vision and Machine Learning

- ✓ Architecture and Bottleneck Analysis
- ✓ Prototyping
- ✓ Image Sensors, Optics, Lighting
- ✓ Image Pre-Processing and Processing
- ✓ Machine Vision and Accelerators



/ Security Consulting



Security Analysis and Evaluation

- ✓ EU Cybersecurity Regulations, Cybersecurity Frameworks
- ✓ Risk Assessment and Threat modeling (PASTA, STRIDE+DREAD), Countermeasures
- ✓ System Security Concepts from a System (Software, Hardware and Methodology) viewpoint
- ✓ Total Cost of Ownership Analysis and Optimization
- ✓ Move to Production (system lockdown, secure deployment flows)



Hardware-assisted Security

- ✓ Integrating and combining TPMs, Secure Elements and on-chip security modules to achieve an optimal solution
- ✓ Resolving Conflicts with Free Software Licenses when using Secure or Authenticated Boot („Tivoization“)



Operating System Security

- ✓ Improving Software Security for GNU/Linux using ARM Trustzone, Containers or Trusted Hypervisors
- ✓ Trusted Computing Base optimization (RTOS, TEE-OS)



Cloud / IIOT - Security

- ✓ Secure Authentication and Connection
- ✓ Remote Attestation
- ✓ Secure Update concepts

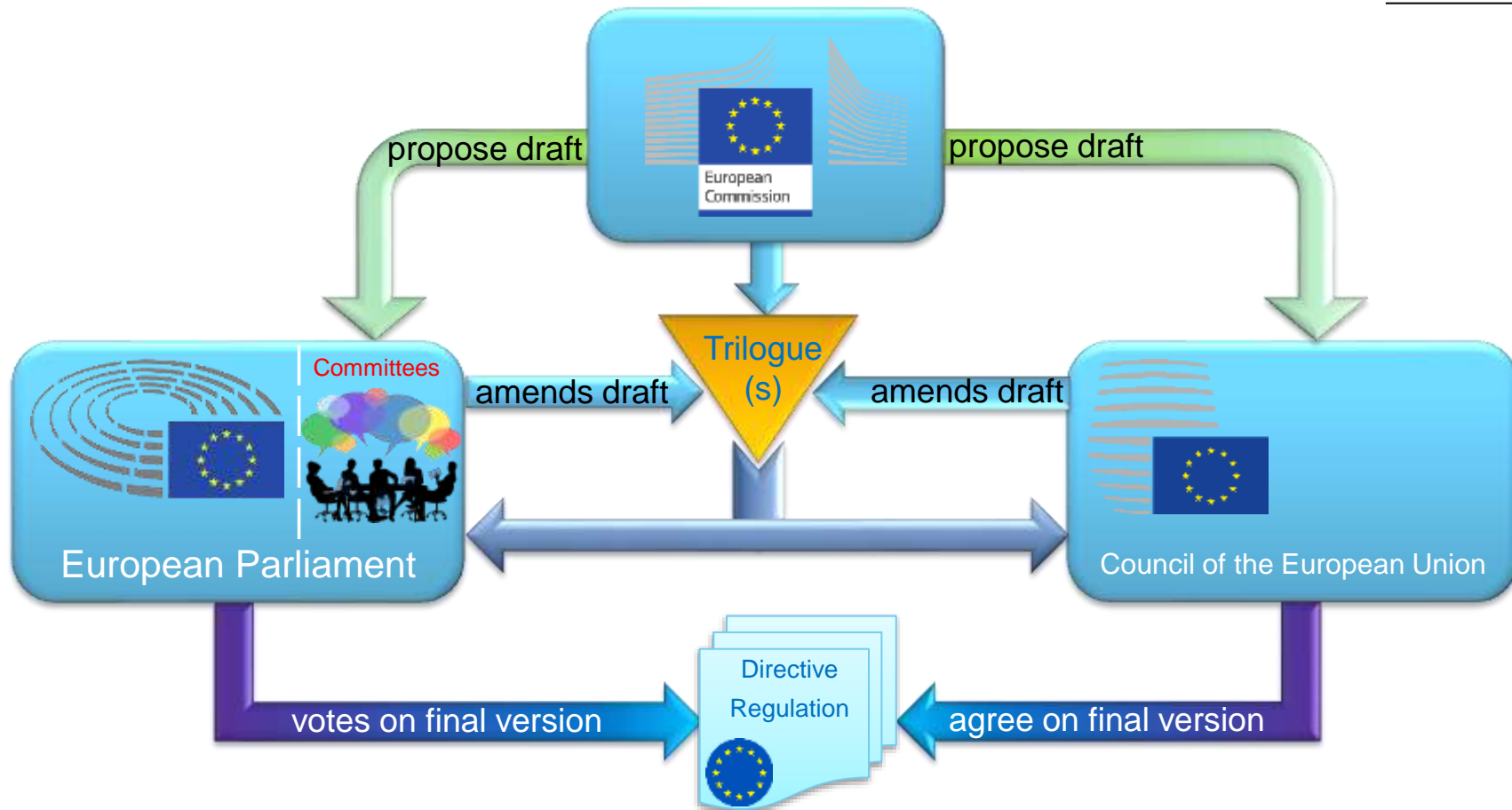


Security Lifecycle Management

- ✓ Ensuring System Security over the complete Product Lifecycle
- ✓ Common Vulnerability and Exposure tracking

- Introduction and Goals
- Basics: EU Legislation Process, Important Terms
- EU Cybersecurity Legislations Overview (excerpt)
- Network and Information Systems 2 (NIS2): Primer
- The EU Cyber Resilience Act (CRA): Overview
 - Goals
 - History
 - Products in Scope
 - Open Source Aspects
 - Product Classes
 - Obligations
 - Security by Design
 - Vulnerability Handling
 - Documentation
 - User Instructions and Information
 - Preparing for the CRA
- Information Security Frameworks and Standards
- EU Certification
- Key Takeaways

/EU Legislation Procedures Primer



/ European „Legislations“



EU Directive



usually 12..36 months

Transposition to
Local Law



short time

„Richtlinie“

EU Regulation
„Regulatory Act“



relatively relaxed
timelines, starting
from the time when
regulation is passed
and published

usually 18..36 months

„Verordnung“

<https://eur-lex.europa.eu/browse/summaries.html>

/ European Acts („Legislations“)



Type of Act	Binding force	usually adopted by...
Regulation	legally binding	Council and Parliament
Delegated Regulation	legally binding	Commission
Implementing Regulation	legally binding	Commission, Council
Directive	legally binding	Council and Parliament
Delegated Directive	legally binding	Commission
Implementing Directive	legally binding	Commission, Council
Decision	legally binding	Council and Parliament, Council, Parliament, Commission, European Council, European Central Bank
Delegated Decision	legally binding	Commission
Implementing Decision	legally binding	Commission Council
Recommendation	non-binding	Council, Commission, European Central Bank
Guideline	legally binding	European Central Bank
Opinion*	non-binding	Commission, Parliament, Council, Court of Auditors, European Central Bank

<https://eur-lex.europa.eu/browse/summaries.html>

<https://eur-lex.europa.eu/collection/eu-law/legislation/recent.html>

- **ENISA** (*European Union Agency for Cybersecurity*)
 - provides support to EU member states, businesses, and cybersecurity institutions
 - delivers solutions and improvements to the EU's cybersecurity framework.
 - support member states, businesses, and EU institutions in dealing with cyber attacks.

- **CSIRTs** (*Computer Security Incident Response Teams, CSIRTs*) and **CERTs** (*Computer Emergency Response (or 'Readiness') Teams*)
 - Respond to cybersecurity incidents on the spot and cooperate with other CSIRTs
 - Monitor vulnerable cybersecurity networks and incidents
 - Provide early warnings, alerts, predictions, and announcements about cyber risks
 - Respond to cybersecurity incidents
 - And offer dynamic risk and incident analysis and situational awareness

- **CVE** (*Common Vulnerabilities and Exposures*)
 - Reference method ("Catalog": CVE-YYYY-nnnn) for publicly known information-security vulnerabilities and exposures
 - Sponsored by U.S. Computer Emergency Readiness Team (US-CERT)
 - Operated by non-profit MITRE ("NIST Cybersecurity") www.mitre.org, cve.mitre.org, cve.org

- **CVSS** (*Common Vulnerability Scoring System*)
 - Open industry framework for rating CVEs by severity, Low (<3.9), Medium (4.0-6.9), High (7.0-8.9) and Critical (9.0-10.0)
 - "The Bogus CVE Problem": <https://lwn.net/Articles/944209/>



- Introduction and Goals
- Basics: EU Legislation Process, Important Terms
- EU Cybersecurity Legislations Overview (small excerpt)
- Network and Information Systems 2 (NIS2): Primer
- The EU Cyber Resilience Act (CRA): Overview
 - Goals
 - History
 - Products in Scope
 - Open Source Aspects
 - Product Classes
 - Obligations
 - Security by Design
 - Vulnerability Handling
 - Documentation
 - User Instructions and Information
 - Preparing for the CRA
- Information Security Frameworks and Standards
- EU Certification
- Key Takeaways

/ Issues with onboarding to EU Cyberregulations

- **Unclear EU legislation process, relevance and context**
 - will it affect me, my company, my product?
 - is it already worth my time investment?

- **Information Source**
 - Source: ([T9-0130/2024](#) „Text adopted by Parliament, 1st reading/single reading”, 12/03/2024)
 - Unclear time of analysis => conflicting information
 - repeated (==copied) wrong information
 - outdated information, due to missing references to evaluated drafts and time of evaluation, resulting in wrong/conflicting information in summaries, whitepapers, ...
 - unclear motivation of authors and stakeholders involved

- **Engineers:** „legal talk“ and wording, strange „re“-definitions of terms
- **Lawyers:** „technical talk“ and wording

EU Cyber Strategy Regulations (excerpt)

Cyber Resilience Act (CRA)

- Regulation (EU 2024) – prelim. EU 2024/0130 => 2026
- Security of products with digital elements, no services
- Prerequisite for CE mark (adding security to CE)
- Conformity assessment determined by risk
- Three levels of criticality
- Highly critical will mandate certification under CSA

Annex I requirements:
up to 15M€ || 2.5% WAT
other requirements:
up to 10M€ || 2% WAT
misleading information:
up to 5M€ || 1% of WAT

Essential:
up to 10M€ || 2% WAT
Important:
up to 7M€ || 1.4% WAT

direct effect

Digital Operations Resilience Act (DORA)

- Regulation (EU 2022/2554) => 17/01/2025
- Directive (EU 2022/2556) => 17/01/2025
- Supplementing NIS2 for financial and insurance sectors
- Uniform requirements for operational resilience and security of network and information systems

ripple effect

Regulation on Machinery

- Regulation (EU 2023/1230) => 20/01/2027
- replaces EU Directive on machinery 2006/42/EC
- health and safety requirements for the design and construction of (partial) machinery placed on EU markets
- Includes security requirements with safety impacts

ripple effect

Cybersecurity Act (CSA)

- Regulation (EU 2019/881) => 05/2019 +
- ENISA – (EU Agency for Cybersecurity)
 - Permanent Mandate
 - Strengthened Power and Tasks
 - Preparation of certification schemes
 - Support preparedness and coordinated response to large-scale cyber incidents/crises across the EU
- Cybersecurity Certification Framework
 - 3 AL corresponding to different EL
 - Voluntary, except specified by law
 - Regular assessments for efficiency
 - establishes National Cybersecurity Certification Authorities, Conformity Assessment Bodies and the European Cybersecurity Certification Group (ECCG)

Network and Information Systems 2 (NIS2)

- Directive (EU 2022/2555) => 10/2024 (DE: NIS2UmsuCG)
- Entities must implement technical, operational and organizational measures to manage the risks prevent or minimize the impact of incidents on IT and OT, + services/cloud
- Reporting of Incidents (24h, 72h, 1M)
- Powerful enforcement instruments (investigations, audits, raids)

ripple effect

Critical Entities Resilience (CER)

- Directive (EU 2022/2557) => 10/2024 (DE: KritisDachG)
- Cyber und Physical Resilience of critical Infrastructure
- Critical := [NIS2 Essential] + [NIS2 Important] (exceptions!)
- Critical := serving > 0.5M people, ~2k companies in Germany

ripple effect

Artificial Intelligence Act (AIA)

- Regulation (EU 2024/0138), passed 13/03/2024
- similar to other EU product safety laws, shares concepts with GDPR
- tough compliance deadlines, +6M to 36M, 2030 based on risk assessment
- Commission can introduce secondary law (implementing and delegated acts), guidance, codes of practice, guidelines on transparency disclosure

direct effect

/ EU Cyber Strategy Regulations (excerpt)

Annex I requirements:
up to 15M€ || 2.5% WAT
other requirements:
up to 10M€ || 2% WAT
information:
up to 7M€ || 1.4% WAT

Essential:
up to 10M€ || 2% WAT
Important:
up to 7M€ || 1.4% WAT

NIS 2 (NIS2)
E: NIS2UmsuCG)
anal and
s prevent or
T, + services/cloud
ions, audits, raids)

E: KritisDachG)
ature

HOW STANDARDS PROLIFERATE:
(E: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)

14?! RIDICULOUS!
WE NEED TO DEVELOP
ONE UNIVERSAL STANDARD
FOR EVERYONE'S
USE CASES



SITUATION:
THERE ARE
14 COMPETING
STANDARDS.

SITUATION:
THERE ARE
15 COMPETING
STANDARDS.

Objective: optimal and harmonized law and guidance to manage cyber security risks across EU member states

Digital Operational Resilience

- Regulation (EU) 2016/1148
- Directive
- Supplemental
- Uniform requirements for network and information security

ripple effect

Regulation of Machinery

- Regulation (EU) 2021/1771
- replaces EU Directive 2006/42/EC
- health and safety requirements of (partial) machinery
- Includes security requirements

ripple effect

- similar to GDPR
- tough compliance deadlines, 40M to 50M, 2030 based on risk assessment
- Commission can introduce secondary law (implementing and delegated acts), guidance, codes of practice, guidelines on transparency disclosure

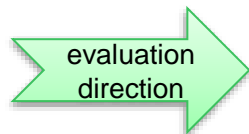
direct effect

- Introduction and Goals
- Basics: EU Legislation Process, Important Terms
- EU Cybersecurity Legislations Overview (small excerpt)
- Network and Information Systems 2 (NIS2): Primer
- The EU Cyber Resilience Act (CRA): Overview
 - Goals
 - History
 - Products in Scope
 - Open Source Aspects
 - Product Classes
 - Obligations
 - Security by Design
 - Vulnerability Handling
 - Documentation
 - User Instructions and Information
 - Preparing for the CRA
- Information Security Frameworks and Standards
- EU Certification
- Key Takeaways

- **Cybersecurity Security Directives for critical sectors (released in parallel with CER)**
- **Business Entity Classification:**
 - **Large:** > 250 employees || Annual Turnover > 50 Mio€ || Annual Balance > 43 Mio €
 - **Medium:** (> 50 employees || Annual Turnover > 10 Mio€) && ![Large]
 - **Small:** < 50 employees && Annual Turnover < 10 Mio €
- **Sector Classification:**
 - **Annex 1:** “main affected sectors”: Energy, Transport, Banking, Financial market infrastructure, Health, Drinking/Waste water, Digital infrastructure, ICT service management, Public administration, Space
 - **Annex 2:** “other affected sectors”: postal/courier services, waste management, chemicals supply, food supply, research, manufacturing of critical devices (medial, transport, ...), digital providers

- **Criticality Classification:**
simplified, details:

Article 2,
Article 3,
Article 4



Entity	listed as „Critical“ in CER (both apply!)	by national definition from Annex 1/2, NIS, national law	Trust Service Provider, DNS, Top Level Domain	listed in Annex 1	listed in Annex 2
Large	Essential	Essential	Essential	Essential	Important
Medium	Essential	Essential	Essential	Important	Important
Small	Essential	Essential	Essential	out of scope	out of scope

- **Appendix 3:** covers NIS to NIS2 migration
- NIS2 directive defines **minimum requirements**, member states are allowed to transpose with stricter implementations

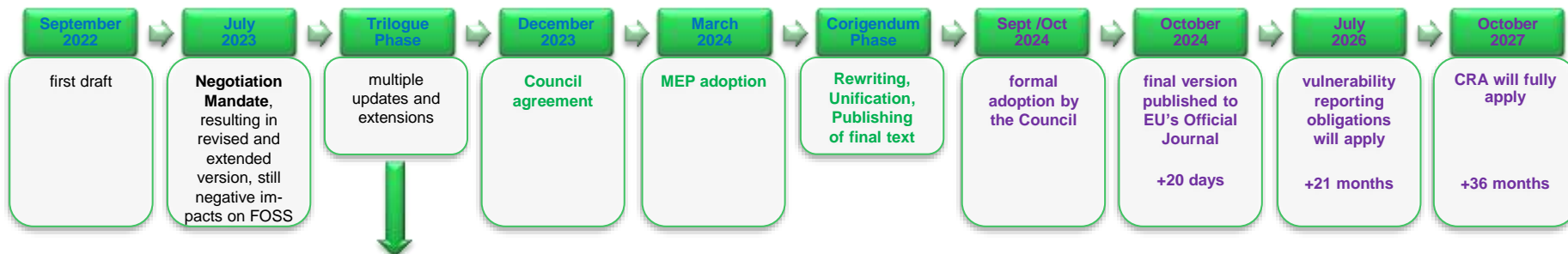
- Requirements closely aligned with ISO 27001, but also mandates a penetration test and heavy business continuity requirements
- **Minimum Measures for Essential and Important Entities (might be expanded/detailed by further jurisdiction/local transpositions)**
 - **Risk analysis and information system security policies:**
technology-based OT and ICS risk and vulnerability assessments, resulting in best practices for identifying and addressing cyber threats, implement defence in depth, physical security, human resources security, access control policies, asset management, ...
 - **Policies and procedures to assess the effectiveness of cybersecurity risk management measures:**
pen-testing, auditing, external oversight
 - **Incident handling** (prevention, detection, and response to incidents): zero trust, IDS, proactive analysis, recovery plans, ...
 - **Business continuity and crisis management:** Business Continuity Assessments, Disaster Recovery Plans, Backups, hot-sites, ...
 - **Establish cyber-hygiene practices and the use of cryptography:** encryption, multi-factor authentication, secured emergency communication
 - **Security in network and information systems acquisition, development and maintenance:** long-term strategy for CVE monitoring, vulnerability analysis, proactive patch management, pen testing,
 - **Supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers:** vulnerability handling, disclosure, quality aspects, guarantees, maintenance, ...
 - **Establish Cybersecurity / Risk Management Training:** for governing bodies and executives, managers and employees of affected entities to identify risks and to assess cybersecurity measures and their impact on their organization.
 - **Establish a chain of responsibility** (considering defined liabilities) for definition, implementation and oversight
- **The European NIS Cooperation Group will update its guidelines and clarify the practical scope of different security objectives in the Directive (current version, valid for NIS: "Reference document on security measures for Operators of Essential Services":**
https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf
- **NIS2 to KRITIS sector mapping:** <https://www.openkritis.de/eu/eu-nis-2-direktive-kritis.html>

- Introduction and Goals
- Basics: EU Legislation Process, Important Terms
- EU Cybersecurity Legislations Overview (small excerpt)
- Network and Information Systems 2 (NIS2): Primer
- The EU Cyber Resilience Act (CRA): Overview
 - Goals
 - History
 - Products in Scope
 - Open Source Aspects
 - Product Classes
 - Obligations
 - Security by Design
 - Vulnerability Handling
 - Documentation
 - User Instructions and Information
 - Preparing for the CRA
- Information Security Frameworks and Standards
- EU Certification
- Key Takeaways

Goal: **optimize and harmonize legal framework** for cybersecurity requirements for **"digital products" and "products with digital elements"** to ensure that these products are secure to use, resilient against cyber threats and provide enough information about their security properties.

product with digital elements ("PDE") := software or hardware over which access to product or network is made possible

- **NOT a consumer law**, in contrast, e.g. to Section §475a-e German Civil Code (BGB, "Waren mit digitalen Elementen")
 - **NO LIABILITY** for material defects can be derived
 - much wider scope, e.g. also affecting parts and pure software products
- Affects **all products sold in the EU** (imported or manufactured within the EU), expected to generate WW ripple effect (similar to GDPR)
- affects **Manufacturers, Dealers, Distributors and Importers**
- **Prerequisite for CE marking**
- **Ensure cybersecurity and maintain across entire product lifecycle**
 - Design PDEs to meet certain essential cybersecurity requirements through risk assessment and protection against known vulnerabilities.
 - The greater the expected damage from exploitation of a vulnerability (likelihood, damage) in a PDE, the stricter the requirements
 - Submit higher class PDEs to conformity assessments
 - Security updates to be applied automatically when technically feasible separately from functionality updates.
- **Mandatory Notification Requirements**
 - **to local authorities and ENISA**
 - **directly to users** for severe security incidents o allow users to obtain better information to make informed decisions, taking into account the cybersecurity state /features of a product.
- **Regulations for market monitoring and for Implementation of Rules for cybersecurity**
- **Reduce future costs of cyber criminality (EU commission 2021: 5.5 trillion € WW / year)**



Trilogue / MPE triggered discussions and resulting changes:

- „commerical use of a product“ and „open-source software“
- Simplified methodology to determine if product is in-scope and the categories considered „Important“ or „Critical“
- Determination of product life-time by supplier: Expectation of life-time support remains, with a minimum of 5 years, except a product is foreseen to be used for a shorter period
- Vulnerability and incident notifications: member state authorities first, who notify ENISA to assess the situation, identify systemic risks and inform other member states, therefore strengthening ENISA's influence and coordinative role
- Applicability: +3 years to provide enough time for adaptations
- Special support measures for microenterprises and SMEs, e.g. education and sensibility training programs to be offered, as well as collaborative initiatives and support for sandbox testing and conformity evaluations
- All provisions of the Cyber Resilience Act will apply 36 months after the law has passed, 21 month for reporting obligations

Thu, 6th – Sun, 9th June 2024
2024 European Union parliamentary election



This Regulation applies to products

- **with digital elements** [==software and hardware products and its remote data processing solutions]
- **made available on the market,**
- the **intended purpose** or reasonably foreseeable use of which includes a
 - **direct or indirect**
 - **logical** [==sockets, files, pipes, APIs] **or physical** [==physical interfaces]
 - **data connection** to a **device or network**.

[==all hardware and software that (could) have a data or network connection during use, including updates]


[== which communicate digitally]

Three classes of products:

- **Important** => Annex III
- **Critical** => Annex IV
- **Basic** => Essential Requirements still apply

2. (a) medical devices
(b) in-vitro diagnostics
(c) automotive
 3. civil aviation
 4. marine equipment
 6. spare parts to replace identical components within digital elements
 7. exclusively for national security, defence purposes or to process classified information.
 8. do not interfere with defense and national security interests
 5. Application **limited or excluded** to products ...
covered by other Union rules laying down ...
requirements that address all or some of the **risks covered by the essential requirements** set out in **Annex I**
IFF
 - (a) such limitation or exclusion is consistent with the overall regulatory framework that applies to those products;
and
 - (b) the sectoral rules achieve the same or a higher level of protection as that provided for by this Regulation.
- The Commission is empowered to **adopt delegated acts** ... to **supplement this Regulation** by specifying
whether such **limitation or exclusion is necessary**,
the **products and rules concerned**,
as well as the **scope of the limitation**, if relevant.

- July 2023 version still contained multiple shortcomings regarding use of FOSS
- Very wide definition of "**commercial activity**" in early drafts which could be interpreted to also including hobbyists, non-commercial organisations, public administration, and individual contributors developing open-source software
- **Revised version** after Trilogue addresses a lot of concerns raised around FOSS in **Recital 10**:
 - **development phase** is out of scope
 - for individual contributors
 - for commercial actors and organizations - both for financial support and code contributions
 - **releasing FOSS code for non-commercial reasons** (without intent to create revenue) is out of scope
 - software created by **public administrations for solely internal use** is out of scope
 - **first involvement with FOSS for commercial reasons** is in scope
 - when released as part of a commercially sold product
 - when used or supported in commercial support activities
- **Simplified Summary: first actor using FOSS in commercial context is liable, regardless of the original code author**
- **Open Source "Stewarts" := organizations, who are not software suppliers in the traditional sense, but provide FOSS services such as support, project coordination, strategies, ... (Linux Foundation, OSADL, ...)**
 - no requirement for CE label
 - responsible for due diligence and due care of establishing cyber-security in their organization, to report flaws, cooperate with public stakeholders
- **Article 10 contains an "interesting" definition of "OpenSource"**:



"Free and open-source software is understood as software the source code of which is openly shared and the licence of which provides for all rights to make it freely accessible, usable, modifiable and redistributable.

Free and open-source software is **developed, maintained, and distributed **openly**, including via online platforms."**
- **(62): if product reaches end-of-life, consider open-sourcing or escrow agreements**

Recital 10

This Regulation applies to economic operators **only** in relation to products with digital elements made available on the market, hence supplied for distribution or use on the Union market **in the course of a commercial activity**. The supply in the course of a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services when this does not serve only the recuperation of actual costs, or by an intention to monetise, for instance by providing a software platform through which the manufacturer monetises other services, by requiring as a condition for use the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software, or by accepting donations exceeding the costs associated with the design, development and provision of a product with digital elements. **Accepting donations without the intention of making a profit should not be considered to be a commercial activity.**

Recital 10c

The mere circumstances under which the product has been developed, or how the development has been financed should therefore **not be taken into account** when determining the commercial or non- commercial nature of that activity.

More specifically, for the purpose of this Regulation and in relation to the economic operators referred therein, to **ensure that there is a clear distinction between the development and the supply phases**, the provision of **free and open-source software products with digital elements that are not monetised by their manufacturers is not considered a commercial activity.**

Recital 10c (continued)

Furthermore, the supply of products with digital elements qualifying as free and open-source software components intended for integration by other manufacturers into their own products with digital elements should only be considered as making available on the market if the component is monetised by its original manufacturer.

For instance, the mere fact that an open-source software product with digital elements receives financial support by manufacturers or that manufacturers contribute to the development of such a product should **NOT** in itself **determine** that the activity is of commercial nature.

Finally, for the purpose of this Regulation, the development of products with digital elements qualifying as free and open-source software by not-for-profit organisations should **not** be considered a commercial activity as long as the organisation is set up in a way that ensures that all earnings after cost are used to achieve not-for-profit objectives.

This Regulation does not apply to natural or legal persons who contribute source code to free and open-source products that are not under their responsibility.

- Recital 10d Stewards
- Recital 10e Hosting
- Recital 10f Voluntary security attestation programs and financing
- Recital 10g Market surveillance authorities can request anonymized and aggregated submission of SBOMs
- Recital 62 Voluntary attestation programs

Category Important

(core functionality of a product category set out in Annex III)

CLASS I (excerpt):

- [few security related SW products], e.g. Browsers, Password Managers, SIEMs
- **Boot Managers, Operating Systems**
- **Routers, Modems, Switches, physical and virtual Network Interfaces**
- **Microprocessors, Microcontrollers, ASICs and FPGAs with security-related functionalities**
- [SMART HOME] [TOYS] [TRACKER]

CLASS II:

- **Hypervisors and container RTS**
- Firewalls, Intrusion Detection/Prevention Systems
- **tamper-resistant**
 - Microprocessors
 - Microcontrollers

Conformity Assessment using

- harmonised standards –or–
- common specifications –or–
- **European cybersecurity certification schemes at assurance level at least 'substantial' (Article 27)**

where available and applicable:

- **a European cybersecurity certification scheme pursuant to Article 27(9) at assurance level at least 'substantial' pursuant to Regulation (EU) 2019/881.**

--or--

- the EU-type examination (based on module B) (Annex VIII),
 - followed by –
- conformity to EU-type based on internal production control (based on module C) (Annex VIII)

--or--

- a conformity assessment based on full quality assurance (based on module H) (Annex VIII)

Category Critical

(product category set out in Annex VI)

- Hardware Devices with Security Boxes
- Smart meter gateways within smart metering systems
- **Other devices for advanced security purposes, including for secure cryptoprocessing;**
- Smartcards or similar devices, including **secure elements**
- **Used for Essential Entities as per Article 3(1) of NIS2 (46-49)**

Conformity Assessment using

- **a European cybersecurity certification scheme in accordance with Article 8(1);**
 - or --
- If conditions in Article 8(1) are not met, see left

Article 7, Article 8 with much more details and clarifications, e.g.:

- at latest 12 month after entry into force, there will be an implementing act specifying technical descriptions of categories in Annex III and IV
- delegated acts can create new categories within classes and move products between classes with 12 months of minimum transition period
- if element is critical in NIS2, required assurance level should be at least „substantial“ (46) (47) (48), delegated acts to follow

- Introduction and Goals
- Basics: EU Legislation Process, Important Terms
- EU Cybersecurity Legislations Overview (small excerpt)
- Network and Information Systems 2 (NIS2): Primer
- The EU Cyber Resilience Act (CRA): Overview
 - Goals
 - History
 - Products in Scope
 - Open Source Aspects
 - Product Classes
 - Obligations
 - Security by Design
 - Vulnerability Handling
 - Documentation
 - User Instructions and Information
 - Preparing for the CRA
- Information Security Frameworks and Standards
- EU Certification
- Key Takeaways

Art 10ff and Annex I/II: comprehensive obligations for products with digital elements and provides for ongoing assessment of cybersecurity risks as well as their documentation and minimization.

Manufacturers: "reasonable" minimum level of security must be achieved by

- Fulfilling Essential Requirements (for Products with Digital Elements)
- Performing Conformity Tests and EU Declaration of Conformity (with certification rules for important critical products)
- Preparing thorough Documentation, both internally and externally

Importers / Dealers

- **Importer:** only if importing other manufacturers' products. **Rebranding/Renaming: => Manufacturer, according to CRA**
- Ensure that the manufacturer conducts an appropriate conformity procedure and prepares the technical documentation
- Ensure that the product bears the CE marking and contains all required information and the instructions for use
- Attach the contact information on the product or on the packaging

Monitoring

- **Monitoring of implementation must be carried out by the Member States**
- **If national market monitoring bodies consider a product as not compliant, they can, in three steps:**
 - order elimination of the identified risks,
 - restrict or prohibit the provision of the product on the market,
 - order a product recall

1. **Decide for, adopt and Implement a fitting Secure Software Design Lifecycle Model**
2. **Loop: {**
 1. Do a **Risk Assessment** (+Threat Analysis), based on current state and requirements, e.g. using OCTAVE(-S), DREAD + STRIDE, PASTA)
 2. **Concretize attack vectors** using Attack Tree, Attack Cards, reversed confirmation bias, ...)
 3. Based on above, enter **new design requirements/changes** into SLD
 4. document (why, what, how, tests, continuous review process, exceptions, known limitations)**}**
3. **Not everything has to be done by yourself, consider Ecosystems:**
 1. adopting commercially maintained operating system MS Win IOT Enterprise LTSC 10y+
 2. switching to EU hosted cloud providers MS Azure
 3. adopting community (OSS Stewart) maintained operating systems and methodologies: Avnet Silica
 1. **Upstream** GNU/Linux (LTS: 2y+, SLTS 10y+) + Yocto: 4y+ --or-- Zephyr: 2y+
 2. permanent gap analysis (vendor patches/layers, compilers, chain of trust, apps)
 3. supplemented by:
 1. maintained distributions with security in focus Witekio Welma (Yocto Linux)
 2. CVE checking and maintenance tools Witekio CVE Check
 3. test automation and documentation Witekio Pluma
 4. remote management and update framework: Witekio Kamea
 4. Secure Hardware (leverage the CRA ☺): Avnet Silica
 1. Secure MCUs/MPUs (AMD, NXP, Renesas, ST Micro)
 2. Secure Elements (NXP SE050, NXP Secure Enclave, ST Micro TPM 2.0)



Annex I, Part 2: Vulnerability Handling Requirements => will be detailed in harmonized standards

➤ Vulnerability Management

- **identify and document vulnerabilities** and **components** contained in products with digital elements, including SBOMs in machine-readable format
- apply effective and regular **tests and reviews** of the security of the product with digital elements;
- take measures to facilitate other parties' **sharing of information** about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product including providing contact addresses

➤ Updates / Patches

- in relation to the risks posed to products with digital elements, **address and remediate vulnerabilities** without delay by providing **security updates**;
- where technically feasible, new security updates shall be provided **separately from functionality updates**;
- ensure that, where security updates are available to address identified security issues, they are disseminated **without delay and free of charge**, accompanied by advisory messages providing users with the **relevant information**, including on potential action to be taken.
- provide for mechanisms to **securely distribute updates** for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner

➤ Vulnerability Disclosure

- **share and publicly disclose information** about fixed vulnerabilities to users and public helping to remediate the vulnerabilities
- put in place and enforce a **policy on coordinated incident / exploited vulnerability disclosure**
- within 24h to local authorities and ENISA if required
- Additional reporting due according to GDPR to data protection authorities might be required

➤ **EU Declaration of Conformity** (Art 28, 32, Annex V, VI, VIII)

- Formal document, declaring that Product confirms to Essential Requirements
- Prerequisite for CE Mark
- **Self Assessment: Module A / “internal control”**
- Third-party assessments (important / critical):
 - Module H: Examination on the basis of a quality management system (Art VI)
 - Module B+C: “EU-type Examination” through an EU-appointed inspection body (Annex VIII)
 - EU Cybersecurity Certification Scheme Certificate (Art. 27(9))

EU will provide simplified formats as well as assistance for this documentation for small and medium-sized enterprises.

➤ **Technical Documentation** (Art. 31, Annex VII)

- *“all data and details of the means used to ensure conformity with essential requirements”.*
- Not Public, but must be disclosed upon request to (also local) Market Surveillance Authorities
- Content:
 - **Description and Intended Purpose**
 - **Risk Assessment**, analyzing in particular the applicability of the essential requirements for the product (new!)
 - **Documentation of the vulnerability management process** in accordance with “essential requirements Part II”; including SBOM,
 - **Design Information** to document the “essential requirements Part I”: system architecture, interactions of system components, production process, monitoring process
 - **Test reports** from the conformity assessment procedure
 - **List of the harmonized standards** applied
 - **Way of Determination for Support Period**

Art 13; Annex II: Information and Instructions to Users

➤ Product Information

- Manufacturer Name, Trademark, Address, Contact Information
- single point of contact to receive and submit vulnerability information and where to find supplier coordinated vulnerability disclosure policy
- Information to allow unique identification of product

➤ Security Information

- **Intended purpose** of product including security environment information
- **essential properties** and **security properties**
- **Known and foreseeable circumstances that might lead to a cybersecurity risk** when using the product, including reasonably foreseeable misuse
- Link to **EU declaration of conformity** (if applicable)
- Type of **technical security support** offered by the manufacturer
- **End-Date of the support period**

➤ Advanced Information: detailed instructions or link to detailed instructions

- Required measures during commission (installation) and over lifetime to **ensure secure use of product**
- How **changes** to the product can **affect the security of data**
- How security relevant **updates** can be installed
- Secure **decommissioning** of product including deletion of user data
- How to **turn off the default automatic security updates**
- **Integrator information**, if appropriate
- Access to SBOM, if desired

- Introduction and Goals
- Basics: EU Legislation Process, Important Terms
- EU Cybersecurity Legislations Overview (small excerpt)
- Network and Information Systems 2 (NIS2): Primer
- The EU Cyber Resilience Act (CRA): Overview
 - Goals
 - History
 - Products in Scope
 - Open Source Aspects
 - Product Classes
 - Obligations
 - Security by Design
 - Vulnerability Handling
 - Documentation
 - User Instructions and Information
 - Preparing for the CRA
- Information Security Frameworks and Standards
- EU Certification
- Key Takeaways

T0

➤ **Clarify Scope and Timelines (First Assessment)**

- EU and National Cybersecurity and Safety Frameworks: Full Picture
 - Will CRA be relevant for my products? If so, Class, Assessment Requirements?
 - By which OTHER Regulatory Frameworks are / will my products be affected?
 - CRA dependencies in my supply chain? What is mentioned in the CRA regarding the other regulatory frameworks?
- Read Full Article 69 ("Transitional Provisions"): T0 := date of entry into force
 - EU Type Certification will remain valid until T0 + 42 months
 - CRA does not apply to products before T0 + 36 months, except for Reporting Obligations according to Article 14

T0

T0

➤ Analyze (and Optimize) **Supply Chain** (BOM, SBOM) and establish supply chain monitoring and management process based on due diligence

T0+6M

➤ **Establish Security Processes and Security Working Group / Competence Centre**, clarify continued funding (process!!!!)

- C-Level endorsement, top-down
- Classify your products, analyze resulting obligations, and determine product lifetimes
- Implement responses to findings based on due diligence and due care throughout all processes and departments:
C-Level, Management, Purchasing, Design Engineering, Testing, Manufacturing, Sales, Documentation, Legal, Marketing

T0+6M

➤ Prepare fulfillment of **reporting obligations** for products already released to the market:

- Analyze and monitor existing (and to be continued) products in terms of cybersecurity and vulnerabilities and prepare documentation / incident reporting process
- Check Reporting Obligations for security incidents and put into place (need to be up and running by ~Q1/2026)
- First working testcase for Competence Center

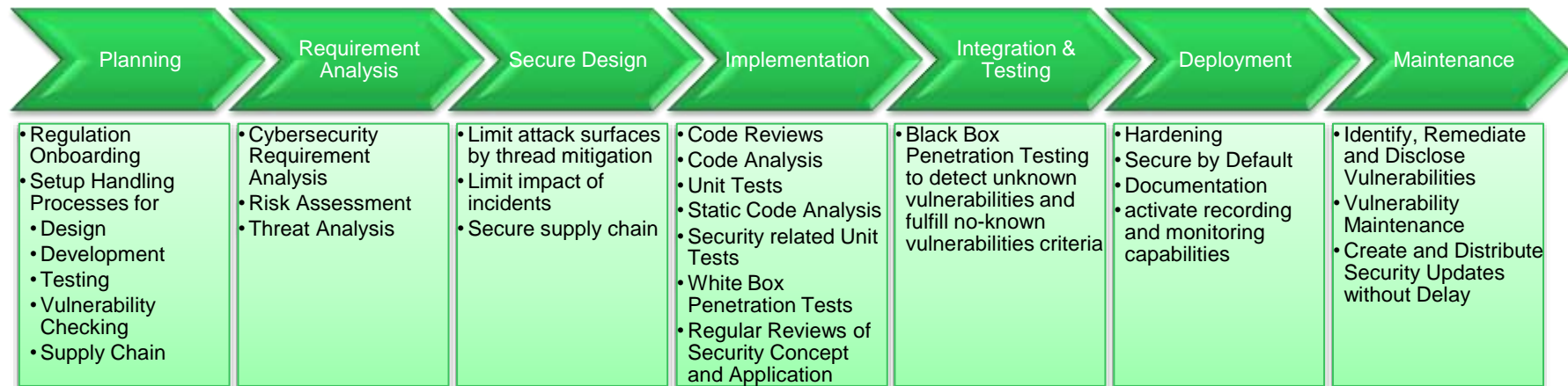
T0+1Y

➤ Adjust **Process for New Developments** (and functional derivative updates):

- Implement / Adapt **Secure Product Design Lifecycle** or adopt a fitting **Cybersecurity Framework** into product development process
- Establish a process for product monitoring over the entire lifecycle and to provide / facilitate required security updates
- Select appropriate process for Conformity Assessment
- if mandated, make necessary preparations (e.g. create the basis for the EU type-testing, ...) - reach out to partners for guidance

- Introduction and Goals
- Basics: EU Legislation Process, Important Terms
- EU Cybersecurity Legislations Overview (small excerpt)
- Network and Information Systems 2 (NIS2): Primer
- The EU Cyber Resilience Act (CRA): Overview
 - Goals
 - History
 - Products in Scope
 - Open Source Aspects
 - Product Classes
 - Obligations
 - Security by Design
 - Vulnerability Handling
 - Documentation
 - User Instructions and Information
 - Preparing for the CRA
- Information Security Frameworks and Standards
- EU Certification
- Key Takeaways

Secure Software Design Lifecycle with CRA Application



Alternatively: Manage using Information Security Standards Frameworks

- What to certify? Systems, **Components**, Processes. Always choose Framework aligned to industry and processes

ISO/IEC 27001:2022

- quite formalized
- addresses
 - people,
 - processes and
 - technology



EN IEC 62443:

- Group of Standards
- Industrial Products

	IEC 62443-1-1	IEC 62443-1-2	IEC 62443-1-3	IEC 62443-1-4
General	Foundational security requirements	Foundational security requirements	Foundational security requirements	Foundational security requirements
Policies & Procedures	Foundational security requirements	Foundational security requirements	Foundational security requirements	Foundational security requirements
System	Foundational security requirements	Foundational security requirements	Foundational security requirements	Foundational security requirements
Component	Product development requirements	Product development requirements	Product development requirements	Product development requirements

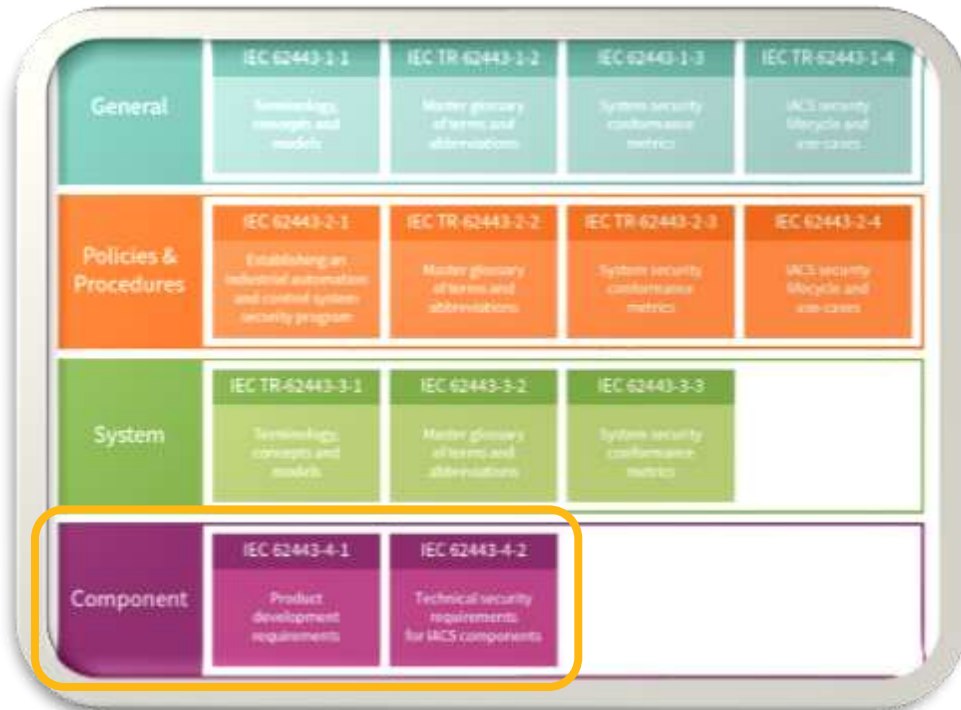
ETSI EN 303 645:

„Cyber Security for Consumer Internet of Things: Baseline Requirements“

ETSI TS 103 701:

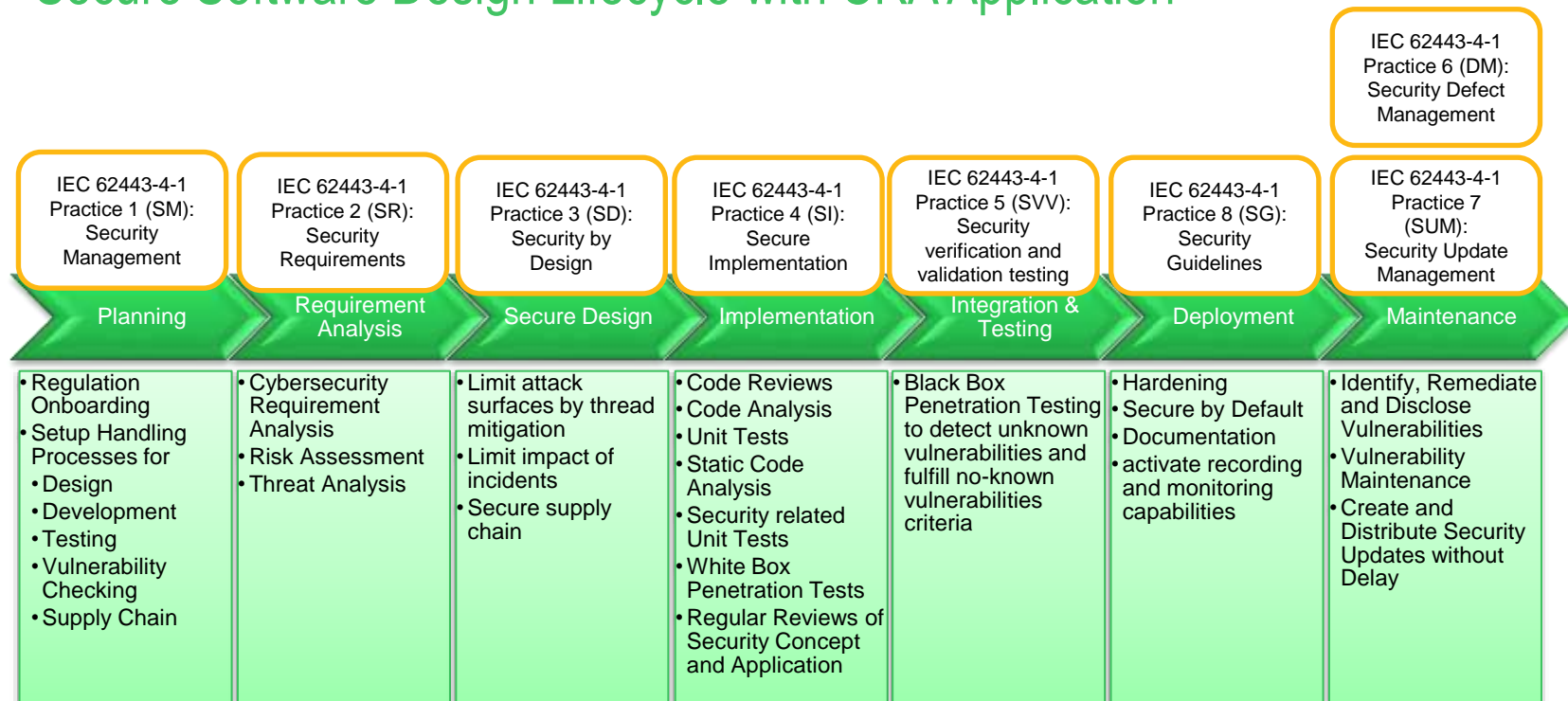
„Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements (Evaluation Specification)“

- Group of Standards
- Addresses Industrial Products (IACSs)
- Mitigate current and future security vulnerabilities
- Collection of requirements that industrial products should meet
- No evaluation methodology issued by IEC, but available, e.g. from Teletrust or ISA Secure



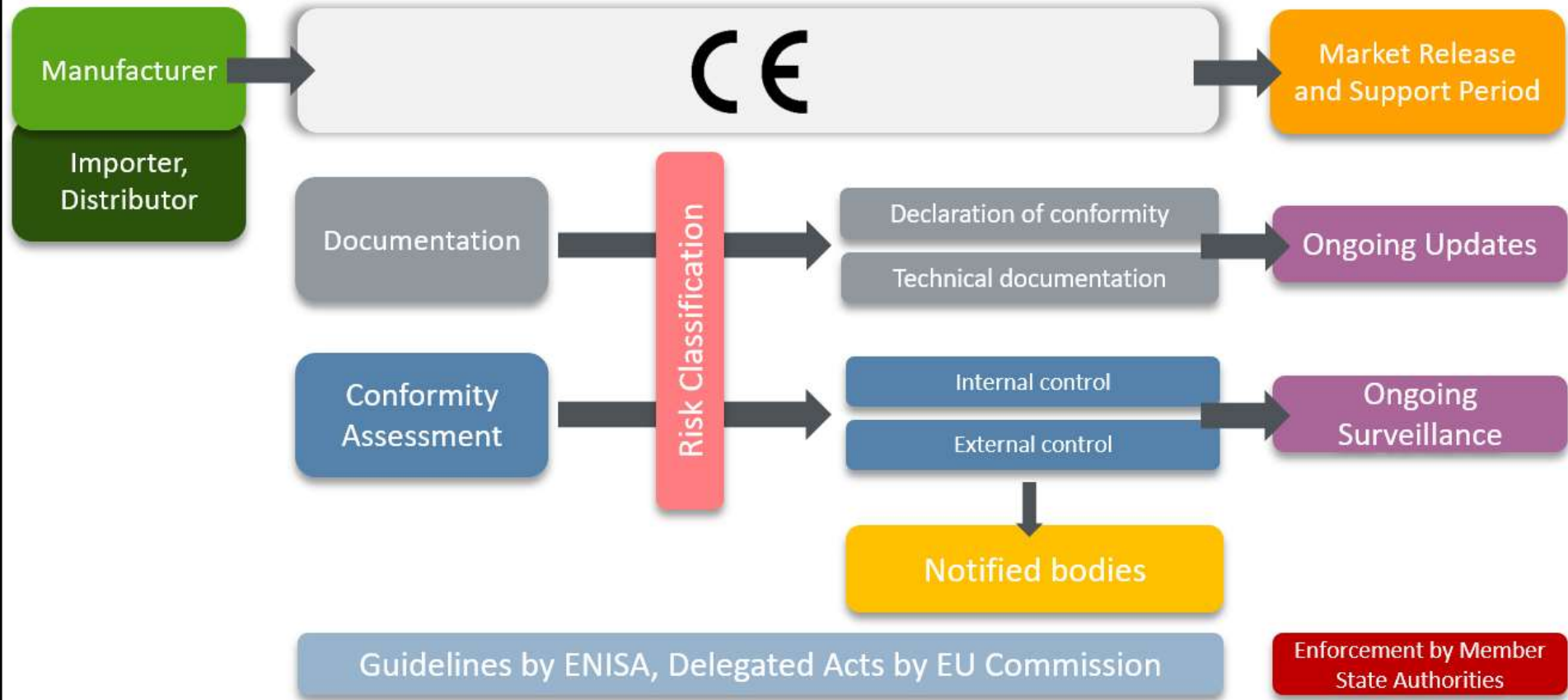
Security Level	Attack Type
SL-1	Protection against casual or coincidental violation.
SL-2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation.
SL-3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation.
SL-4	Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation.

Secure Software Design Lifecycle with CRA Application



- Introduction and Goals
- Basics: EU Legislation Process, Important Terms
- EU Cybersecurity Legislations Overview (small excerpt)
- Network and Information Systems 2 (NIS2): Primer
- The EU Cyber Resilience Act (CRA): Overview
 - Goals
 - History
 - Products in Scope
 - Open Source Aspects
 - Product Classes
 - Obligations
 - Security by Design
 - Vulnerability Handling
 - Documentation
 - User Instructions and Information
 - Preparing for the CRA
- Information Security Frameworks and Standards
- EU Certification
- Key Takeaways

The EU CE process



- **Common Goal:** apply the European cybersecurity certification framework (CCF) concepts ...
 - through implementations for different product categories, such as
 - EUCC (Information and Communication Technologies),
 - EUCS (cloud services),
 - EU5G (5G Network Services)
 - to create tailored EU cybersecurity certification schemes for above product categories, specifying:
 - the categories of products and services covered;
 - the cybersecurity requirements, such as standards or technical specifications;
 - the type of evaluation, such as self-assessment or third party;
 - the intended level of assurance.
 - that are valid across the EU
- EU Cybersecurity Certification Scheme (EUCC): <https://certification.enisa.europa.eu/#documentation>
 - 31/01/2024: EU 2024/482 “[Commission Implementing Regulation about adoption of the European Common Criteria-based cybersecurity certification scheme](#)”
 - Defines Roles, Rules, Implementations, Technical References, ...
 - Relies heavily on ISO 15408 (CC) and Common Evaluation Methodology (ISO 18045)
 - Assurance levels are aligned to CC vulnerability assessment families components 1-5
 - Certification bodies shall issue EUCC certificates at assurance level ‘substantial’ or ‘high’.
 - ‘high’ correspond to certificates that cover AVA_VAN level 3, 4 or 5.
 - ‘substantial’ correspond to certificates that cover CC AVA_VAN level 1 or 2
 - ‘basic’ out of scope, self-certification
 - EUCC certificates have a lifetime of < 5 years, exceptions can apply
 - Lists specific evaluation criteria for protection profiles using
 - applicable elements of the standards referred to in Article 3;
 - level of risk associated with the intended use of the ICT product
 - applicable state-of-the-art documents technical listed in Annex I.
- **Recital (92): Manufacturers should choose an applicable harmonized standard, common specification or European cybersecurity certification scheme.**



/ Key Take-Aways

- **The EU Cybersecurity Regulation Frameworks will affect everyone, mostly positively. Understand the overall picture, interdependencies and legislation process – and see it as an opportunity to differentiate.**
- **CRA requires the due diligence and due care that you should do anyway to build good products – and it supports you by forcing your supply chain to provide what you need to do the right thing.**
- **Act now, but don't panic: select scope and frameworks, understand obligations, follow releases and updates on harmonized standards, supplements and national supplemental legislation**
- **Beware of outdated or 2nd/3rd source information – always check the source and date**
- **(Recommended / Fitting) formalized frameworks can help to implement and follow process automatically and provide many more benefits**
- **Start Analysis and Optimization of Supply Chain (BOM/SBOM) now – CRA (and Avnet Silica) is your friend here**
- **Reporting Obligations are in critical timing path and relevant for ALL PRODUCTS**
- **Establish competence center and create formalized processes (due diligence), minimally for all Essential Requirements**
- **Documentation is key – start now and integrate dynamically into processes**
- **Reach out for help and collaborate**

/ Questions?



Avnet Silica Software&Services:

sas@avnet.eu

Michael Roeder

michael.roeder@avnet.eu

/ System-Level and Architecture Consulting



SoC Architecture

- ✓ Analysis and Benchmarking of different implementation approaches on hardware, software and system level
- ✓ Mapping applications/algorithms to SoC architectures, optionally including FPGA SoC
- ✓ Bottleneck / Throughput / Latency Analysis



Total Cost of Ownership

- ✓ Optimizing Maintenance and Service Costs over Product Lifetime
- ✓ Proactive Lifecycle and Obsolescence Management (Hardware and Software)
- ✓ Technical Dept analysis and control
- ✓ Legal and Maintenance Cost-Management for Open Source Software
- ✓ Make vs Buy (Hardware and Software)
- ✓ Re-Use of Platforms
- ✓ Leveraging System-on-Modules to optimize costs without sacrificing independence



Move to Production

- ✓ Build System, BSP Adaptions, Continuous Integration
- ✓ Maintenance, Patching
- ✓ Hardware and Software Longevity (LTS, CIP, strategic mainlining)
- ✓ Licensing and Legal Aspects



Functional safety according to IEC61508 (2 TÜV-Sued certified FSE/FSP embedded specialists)

- ✓ Architecture Analysis and Discussions
- ✓ Functional Safety Enablement and Process on various SoC architectures

/ Operating System / BSP Consulting



Operating Systems / GNU/Linux / RTOS

- ✓ U-Boot, TF-A, TEE OS, GNU/Linux, Zephyr, FreeRTOS
- ✓ Yocto / OpenEmbedded BSP development and build system integration into development flow
- ✓ Realtime analysis and optimization
- ✓ moving from Supplier BSP to Production BSP
- ✓ Board bringup and BSP porting
- ✓ Footprint and Boot-Time Optimization
- ✓ Software Platform and Lifecycle Management



Virtualization / Realtime

- ✓ Security, Safety and Realtime using GNU/Linux, Containers or a Trusted Hypervisor / Isolation
- ✓ ROS / ROS2 enablement
- ✓ Offloading: FPGA Fabric, Realtime-Subsystems (Cortex-M, Cortex-R, RISC-V, Softcores)

Software Architecture and Craftmanship



Software Architecture

- ✓ Modern architectures for highly distributed (embedded) systems
- ✓ Architectural patterns
- ✓ Architecture review and consulting
- ✓ Interplay hardware selection and software architecture
- ✓ Trade-off handling, constraint management
- ✓ Change management for existing/legacy architectures
- ✓ Library evaluation and selection
- ✓ Usage of off-the-shelf components
- ✓ Architecture documentation



Software Craftmanship

- ✓ Modern C++ on embedded devices
- ✓ Safe resource management
- ✓ Languages beyond C
- ✓ Testing strategies and HIL-Integration
- ✓ Customized workshops addressing issues raised by code analysis and in-depth discussions

/ IIoT / TSN / accelerated Ethernet



TSN Standards

- ✓ Training and Consulting
- ✓ Usecase Evaluation



Time Synchronization (1588, 802.1AS(-rev))

- ✓ Configuration optimization for specific setups, including latency analysis and optimization
- ✓ Protection of PTP/AS traffic from best-effort traffic



TSN Communication

- ✓ VLAN aware TSN talkers and Listeners
- ✓ Realtime and flow optimization (PREEMPT_RT, Xenomai, separated core)



(Automated) Configuration

- ✓ Configuration of Systems using NETCONF/YANG
- ✓ Configuration / Data Flow isolation
- ✓ Setup and optimization of L2/L3 traffic paths using qdisc schedulers or side injection



OPC/UA

- ✓ OPC/UA enablement of devices
- ✓ OPC/UA pub/sub based control



System Level integration

- ✓ IEEE/IEC60802 industrial usecases, ProfiNet over TSN
- ✓ Complex node/switch infrastructure concept planning and evaluation

accelerated SoCs:
DPAA, DPAA2,
Felix, Sparx5
AMD/Xilinx TSN IP

switches in
GNU/Linux
(DSA, SwitchDev)



System-Level Architecture / Bottleneck Analysis

- ✓ Application definition, analysis and feasibility checks
- ✓ Target system hardware capabilities: NXP, AMD/Xilinx, Renesas, Intel, STM
- ✓ Software package options on target system
- ✓ Technical implementation alternatives and options



Prototyping

- ✓ Proof-of-concept
- ✓ Discussing minimal and optimal requirements
- ✓ Determine paths from prototype to final product (production, maintenance)
- ✓ Discussing available hard- and software for rapid prototyping



Image Sensors

- ✓ Basics: Types, characteristics, limitations
- ✓ Feature discussion
- ✓ Optical and Physical Considerations: Optics, housing, cooling, lighting
- ✓ Production requirements, "Make vs. Buy"
- ✓ Sensor tuning and image quality improvement: Sensor parametrics, tuning, calibration flow
- ✓ Interfaces: MIPI-CSI2, FPD-LINK, GMSL2, USB



Pre-Processing

- ✓ Image pre-processing requirements for subsequent image processing
- ✓ Analysis of required pre-processing steps: Demosaicing, dead pixel correction, HDR, etc.
- ✓ ISP image sensor calibration process



Image Processing

- ✓ Discussion and evaluation of processing architectures
- ✓ Optimization: Processing steps, modules, alternatives
- ✓ Latency and throughput analysis



Machine Vision

- ✓ Discussion and evaluation of possible machine vision approaches
- ✓ Feature extraction, labeling/decision making, good/bad detection, VSLAM
- ✓ Total-Cost-of-Ownership and maintenance
- ✓ Hardware acceleration/support: NPU, FPGA, GPU, ASSP