CYOSS

IT'S TIME TO CHOOSE: THE PERFECT SECURITY STANDARD FOR YOUR PROJECT

Stefan Unterreitmeier
Sebastian Nagel

SPEAKERS

Sebastian Nagel

Cyber Security Engineer
CYOSS GmbH

Tel: +49 89 92161-1827
Fax: +49 89 92161-61827
E-Mail: sebastian.nagel@cyoss.com

- Academic studies in cryptography
- Full-time focus on cyber security for the last four years
- Security-by-design
- Formal modelling of attack scenarios

Stefan Unterreitmeier

Senior Cyber Security Architect
CYOSS GmbH

Tel: +49 89 92161-1926
Fax: +49 89 92161-61926
E-Mail: stefan.unterreitmeier@cyoss.com

- Almost 35 years of experience in software and system development
- Including over 11 years in embedded development, in particular functional safety
- Full-time focus on cyber security for the last four years

AGENDA

- THE PROBLEM
- OUR SOLUTION
- AXIS OF COORDINATES
- THE MAPPING
- EXAMPLE

THE PROBLEM

THE PROBLEM
An abundance of standards

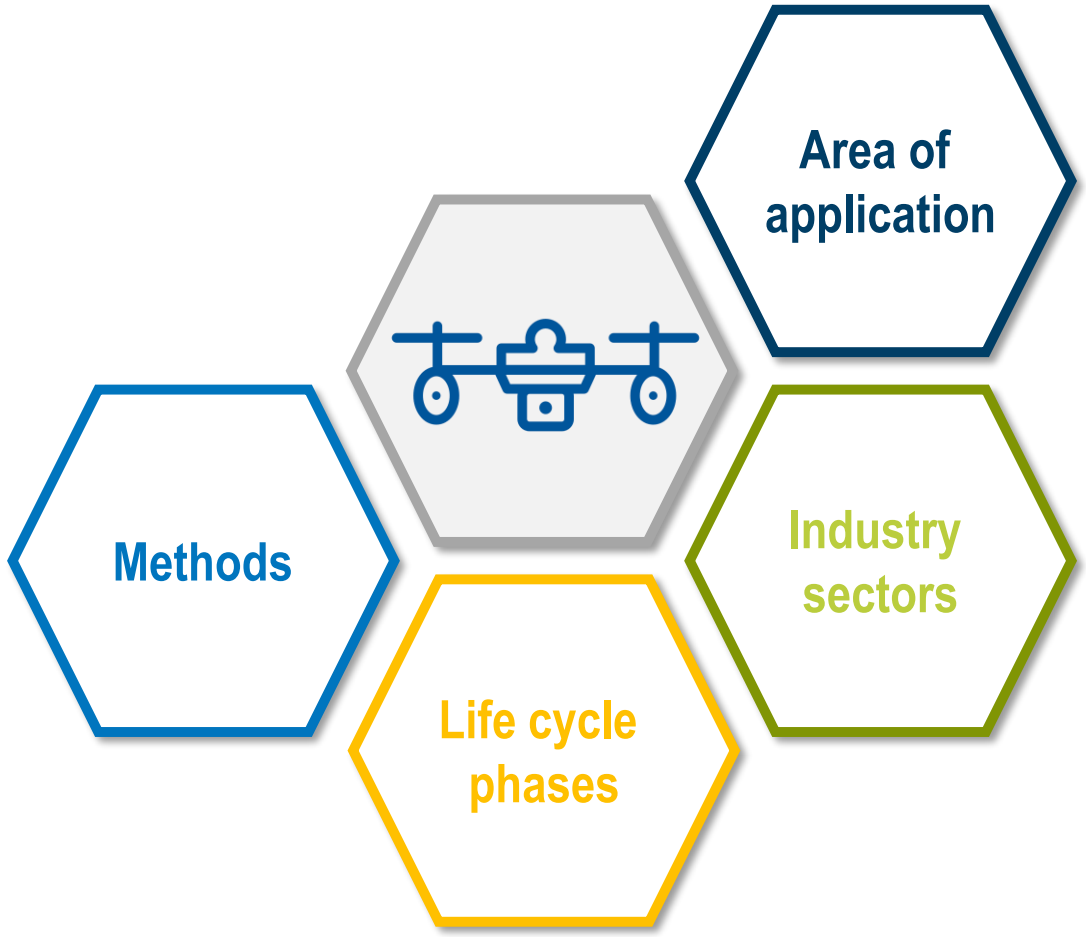
THE PROBLEM
Standards for car development

BSI IT-Grundschutz 100
ISO 15408
ED-202A
ISO/IEC 27031
ETSI TS 102 165-1
NIST 800-30
ISO 27001 Fam.
NIST 800-82
ISO/IEC 27033
DOT HS 812 333
BSI IT-Grundschutz 200
IEC TR 63069
IMO MSC-FAL.1 / Circ. 3
ED-204
ED-201
ISO/IEC 27035
ED-203
IEC 62443
MITRE SEG
SAE J3061
ISO 21434
ARINC 811
ENISA
ICT Minimum Standard
BIMCO
ISO/IEC 27032
NIST 800-160

OUR SOLUTION

OUR SOLUTION
The security standards map

- Create a landscape map of all the standards
- Define a coordinate system for the standards
- Properties as index

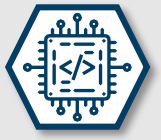


AXIS OF COORDINATES
Areas of application

IT systems

OT systems

Internet of things



Embedded systems

AXIS OF COORDINATES
Industry sectors

- Aviation
- Marine technology
- Governmental affairs (forceless)
- Military, police & intelligence
- Energy
- Chemical industry
- Automotive
- Railway
- Water systems
- Telecommunications
- Finance & banking
- Food & beverage

AXIS OF COORDINATES
Lifecycle phases

AXIS OF COORDINATES
Methods

Methods Groups

- Processes
- Operations
- Requirement engineering
- Security risk assessment
- Implementation
- Testing

AXIS OF COORDINATES
Methods – processes & operations

Processes


Security awareness


Security policies and procedures


Build and train a cross-functional team


Auditing

Operations


Security Operations Centre (SOC)


Incident detection and response


Security updates


Supply chain risk management

AXIS OF COORDINATES

Methods – concepts / specification & assessment

Requirement engineering

- Security requirement engineering
- Feature definition
- Business, use, and mis-use Cases
- High level system requirements
- Secure environment and interfaces
- Network architecture

Security risk assessment

- Security assessments
- Security analysis catalogues
- Security analysis metrics

AXIS OF COORDINATES
Methods – implementation & testing

Implementation

Coding guidelines for secure programming

Secure code reviews

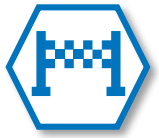
Hardening

Testing

Fuzzing

Functional and non-functional testing

Penetration testing



End of line testing

THE MAPPING

Ref.	ID	Org	Typ	Nummer	Version	Postfix	Title	Security Relevant	Veröffentlicht?
[01]	ISO 15408-1:2009	ISO		15408-1	2009		Evaluation criteria for IT security (Common Criteria) – Part 1: Introduction and general model	x	x
[02]	ISO 15408-2:2008	ISO		15408-2	2008		Evaluation criteria for IT security (Common Criteria) – Part 2: Security functional requirements	x	x
[03]	ISO 15408-3:2008	ISO		15408-3	2008		Evaluation criteria for IT security (Common Criteria) – Part 3: Security assurance requirements	x	x
[04]	ISO 27000:2018	ISO		27000	2018		Overview and vocabulary	x	x
[04]	ISO 27000:2020 (D)	ISO		27000	2020	(D)	Überblick und Terminologie	x	x
[05]	ISO 27001:2013	ISO		27001	2013		Information technology - Security techniques - Information security management systems - Requirements	x	x
[06]	ISO 27002:2013	ISO		27002	2013		Information technology - Security techniques - Code of practice for information security controls	x	x
[07]	ISO 27003:2010	ISO		27003	2010		Information technology - Security techniques - Information security management system implementation guidance	x	x
[08]	ISO 27004:2016	ISO		27004	2016		Information technology - Security techniques - Information security management – Monitoring measurement analysis and evaluation	x	x
[09]	ISO 27005:2011	ISO		27005	2011		Information technology - Security techniques - Information security risk management	x	x
[10]	DOT HS 812 333:2016	NHTSA	HS	812 333	2016		Cybersecurity Best Practices for Modern Vehicles	x	x
[11]	ENISA:2017	ENISA			2017		Cyber Security and Resilience of smart cars - Good practices and recommendations	x	x
[12]		Microsoft			2012		Security Development Lifecycle	x	x
[13]	IMO MSC-FAL.1/Circ.3:2017	IMO		MSC-FAL.1/Circ.3	2017		Guidelines on maritime cyber risk management	x	x
[14]	ARINC 811:2005	ARINC		811	2005		Commercial Aircraft Information Security Concepts Of Operation And Process Framework	x	x
[15a]	IEC 62443	IEC		62443-1-1	2009		Industrial automation systems and integration – Industrial communication networks – Network and system security - Part 1-1: Terminology, concepts and models	x	x
[15b]	IEC 62443-2-1:2010	IEC		62443-2-1	2010		Industrial automation systems and integration – Industrial communication networks – Network and system security - Part 2-1: Establishing an industrial automation and control system security program	x	x
[15c]	IEC 62443-2-3:2015	IEC		62443-2-3	2015		Industrial automation systems and integration – Industrial communication networks – Network and system security - Part 2-3: Patch management in the IACS environment	x	x
[15d]	IEC 62443-2-4:2017	IEC		62443-2-4	2017		Industrial automation systems and integration – Industrial communication networks – Network and system security - Part 2-4: Security program requirements for IACS service providers	x	x
[15e]	IEC 62443-3:2008	IEC		62443-3	2008		Industrial automation systems and integration – Industrial communication networks – Network and system security - Part 3: Security for industrial process measurement and control - Network and system security	x	
[15f]	IEC 62443-3-1:2009	IEC		62443-3-1	2009		Industrial automation systems and integration – Industrial communication networks – Network and system security - Part 3-1: Security technologies for industrial automation and control systems	x	x
[15g]	IEC 62443-3-3:2013	IEC		62443-3-3	2013		Industrial automation systems and integration – Industrial communication networks – Network and system security - Part 3-3: System security requirements and security levels	x	x
[15h]	IEC 62443-4-1:2018	IEC		62443-4-1	2018		Industrial automation systems and integration – Industrial communication networks – Network and system security - Part 4-1: Secure product development lifecycle requirements	x	x
[16]	SAE J3061:2016	SAE		J3061	2016		Cybersecurity Guidebook for Cyber-Physical Vehicle Systems	x	x
[17]	EUROCAE ED-201:2015	EUROCAE		ED-201	2015		Aeronautical Information Systems Security	x	x
[18]	EUROCAE ED-202A:2014	EUROCAE		ED-202A	2014		Airworthiness Security Process Specification	x	x
[19]	EUROCAE ED-203:2018	EUROCAE		ED-203	2018		Airworthiness Security Methods and Considerations	x	x

WHITEPAPER

Comparison of Cyber Security Standards

- Dive into over 40 different standards

For each standard

- Short summary and reasoning of the standard
- Locating it on the axis
- Our subjective opinion about the usefulness of the standard
- List of pros and cons

cyoss.com

WHITEPAPER
Example – ISO 21434

The ISO/SAE 21434 is an upcoming automotive security standard that, for the moment (02.02020) remains in the draft status. This document is intended to provide an encompassing guideline to integrate cyber security in the development process of the automotive domain, acknowledging that newly developed (E/E) systems within road vehicles are increasingly endangered by outside cyber attacks that will change in used technology and methods.

Therefore the ISO/SAE 21434 concentrates on the procedural approach to establish and keep up the cyber security of road vehicles:

1. Abbreviations and definitions are introduced to establish a common domain language for all participants in providing cyber security of road vehicles.
2. The ISO/SAE 21434 recognizes the fact, that cyber security has be engrained in the culture of the producing organization. To do so a set of formal requirements are introduced whose adherence has to be proven with documents called working products.
3. Providing and tailoring of the cyber security integration process to the concrete development project at hand like for example: responsibilities in the project team; cyber security relevance of the system in question; tracking of cyber security activities; or the reuse of an old cyber security analysis, because of a further development of an already existing system. All requirements are provided in a formal manner that must be proven with working products.
4. Project independent cyber security activities: tracking and monitoring of cyber security incidents, triage or assessment of cyber security events. The results of these activities can be mirrored into concrete development projects. All requirements are provided in a formal manner that must be proven with working products.
5. Defining and justifying the necessity to identify assets, threat scenarios, damage scenarios for the system. All requirements are provided in a formal manner that must be proven with working products.
6. Integration of cyber security into the different development stages: “concept phase”, “product development”, “validation phase”, “production”, “operation and maintenance” and “decommissioning”. For each of these phases formal requirements are given, that must be proven in working products.
7. Defining of requirements for the integration of cyber security in the relationship and project related communication between different organizations like customers and suppliers, that share the responsibility for said project. Formal requirements and work products are defined.
8. The Annex provides practical examples for the theoretical descriptions of the previous chapters like: good and bad cyber security company culture; cyber security assurance levels; an example use case with the corresponding work products and asset and attack ratings.

WHITEPAPER
Example – ISO 21434 – pros and cons

✔ Pros	✗ Cons
• Encompassing “How-To”-Integration guide • Checklist in form of requirements and work products • Practical examples for different concepts of the standard • Acknowledging the need for coordination between customers and suppliers	• Still in the draft phase and not finalized • Only for the automotive domain

QUESTIONS?


BSI IT-Grundschutz 100
ISO 15408
ED-202A
ISO/IEC 27031
ETSI TS 102 165-1
NIST 800-30
ISO 27000 Fam.
NIST 800-82
ISO/IEC 27033
DOT HS 812 333
BSI IT-Grundschutz 200
IEC TR 63069
IMO MSC-FAL.1 / Circ. 3
ED-204
ED-201
ISO/IEC 27035
ED-203
IEC 62443
MITRE SEG
SAE J3061
ISO 21434
ARINC 811
ENISA
ICT Minimum Standard
BIMCO
ISO/IEC 27032
NIST 800-160

THANK YOU FOR YOUR ATTENTION

We look forward to working with you

CYOSS
AN ESG GROUP COMPANY

CYOSS GmbH
Ganghoferstraße 66
80339 München

Tel.: +49 89 92161 - 4600
Fax: +49 89 92161 - 2909

cyoss.com

All icons from https://thenounproject.com