SYSGO PRESENTATION

Thierry Maudire
Head of Technical Sales
at SYSGO

Thierry manages and coordinates a team of Solution Architects to address customers technical requirements in different industries such as Aerospace & Defense, Automotive, Railway, and Industrial.

- About 30 years of experience specifying and developing solutions for embedded systems. Prior to SYSGO, he held different positions at Wind River Systems Inc.

- Education:
  - Postgraduate Research Studies in Robotics, University of Wollongong, Australia
  - Postgraduate Degree, in Robotics, from University Pierre et Marie Curie (Paris)
  - Master of Sciences in Signal Processing and Telecommunication from University of RENNES

SYSGO
EMBEDDING INNOVATIONS

COMMON CRITERIA CERTIFICATION

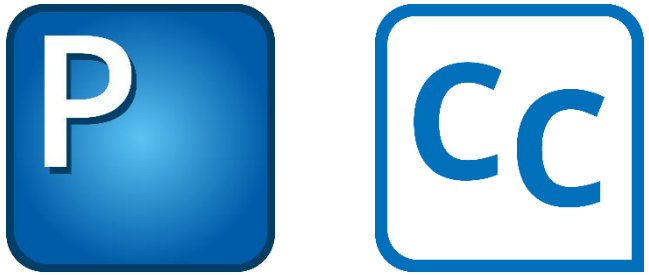
FOR REAL-TIME APPLICATIONS WITH IOT-GATEWAYS

embeddedworld
Exhibition&Conference
... it´s a smarter world

Y. Gueguen / T. Maudire - 16/03/2023

AGENDA

- SYSGO’s history in Security
- Security / Safety certification landscape
- Common Criteria overview
- PikeOS in Common Criteria
- Common Criteria vs. other Security standards
- Use cases Security gateway



SYSGO'S HISTORY IN SECURITY

- SYSGO was established in 1991
- Development of embedded software solutions
  - PikeOS, a real-time separation kernel, is widely used in highly critical cyber-physical systems used in various industries
    - E.g. Defense, Aerospace, Automotive, Railway, and Industrial Automation
- Part of the Thales group since 2012
- SYSGO has been successful in Safety certification standards, developing the expertise in real-time operation systems and developing Safety certification processes.


SYSGO Headquarters, Germany

SYSGO'S HISTORY IN SECURITY

- Even when Security was not explicitly addressed, it turns out that a product designed to achieve high Safety levels is also inherently well designed towards Security concerns.

- The artefacts generated to provide Safety assurance are also fully relevant towards Security standards. Security can be understood as a superset of Safety. Indeed, a system designed to resist intentional attacks shall also resist accidental events as these can simply be simulated by the attacker.

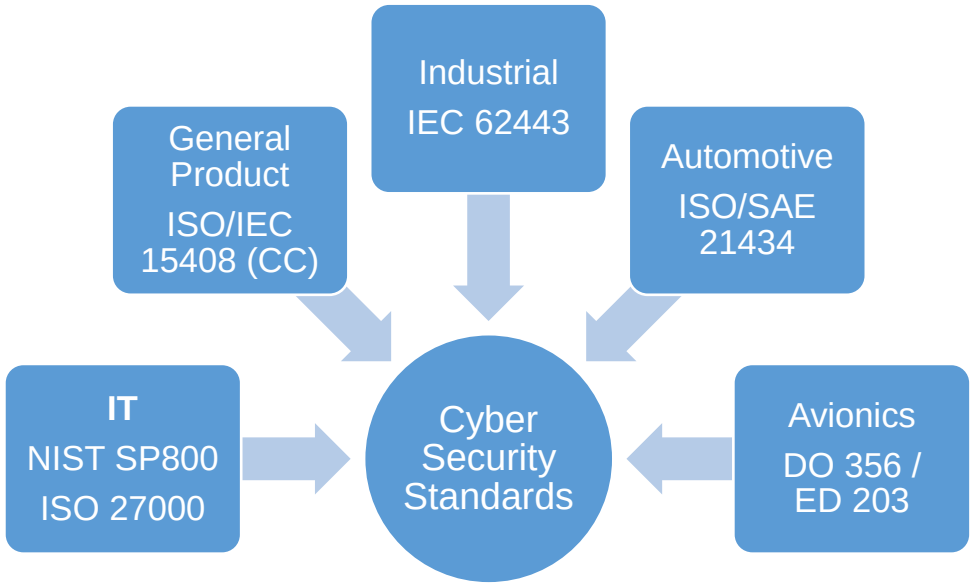
- Over the last 10 years, SYSGO has developed its expertise in Security from the certification perspective by setting up processes necessary to reach and maintain ISO 27001 and Common Criteria certifications in all company area building Security, IT, ... and from a development perspective, actively participating to the Spectre / Meltdow research, extending test coverage with fuzzer tests.

PIKEOS AND SECURITY

- Provides a separation kernel
  - For IP protection
  - For asset protection
- Support mixed criticality applications
- Small codebase → reduced surface attack
- Same product for Safety and Security

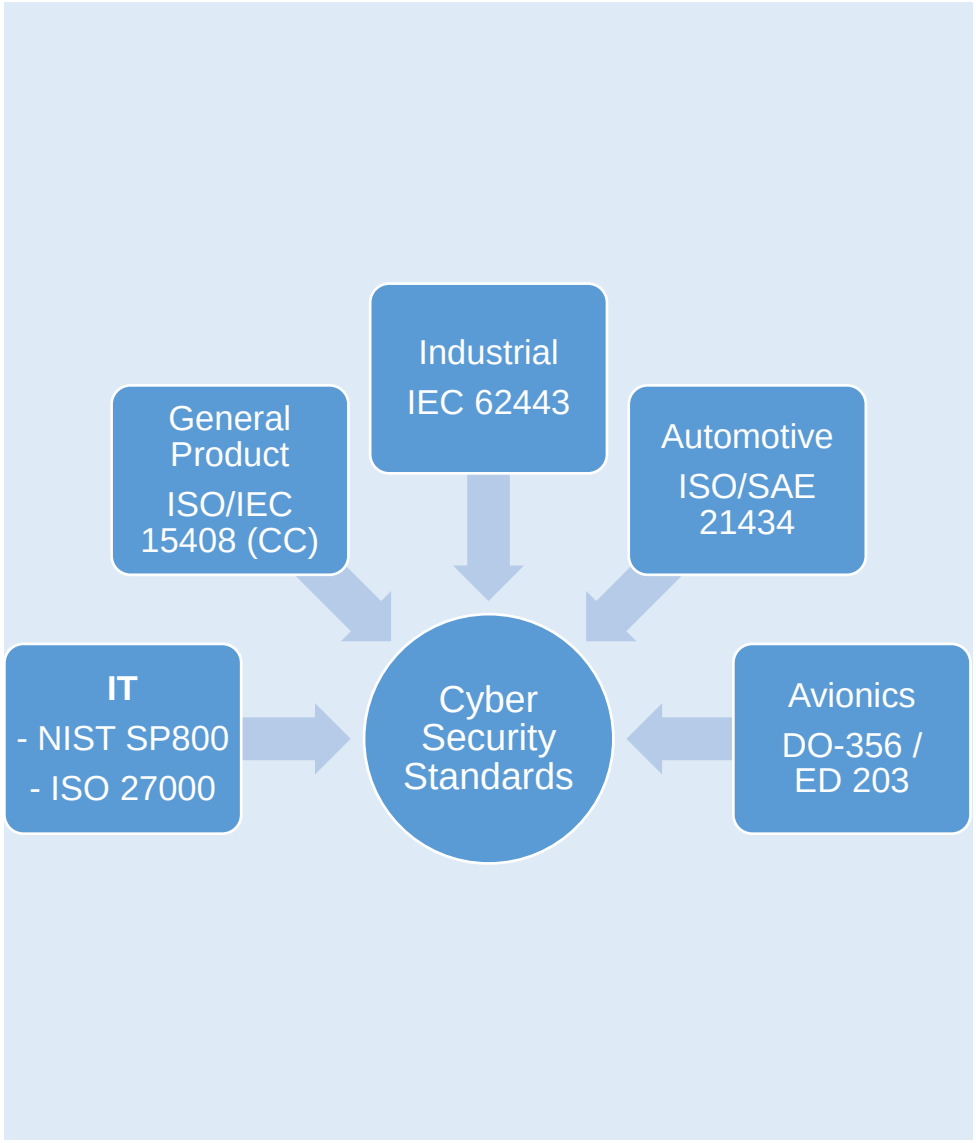
- Security features of PikeOS
  - Strong separation of partitions (spatial and temporal)
  - Controlled information flow
  - Access control to resources
  - Availability of resources
- SYSGO service expertise
  - To develop PSP and driver with Security requirements
  - To assist during Security audit and/or certification
  - To assist customer to design system architecture on top of PikeOS

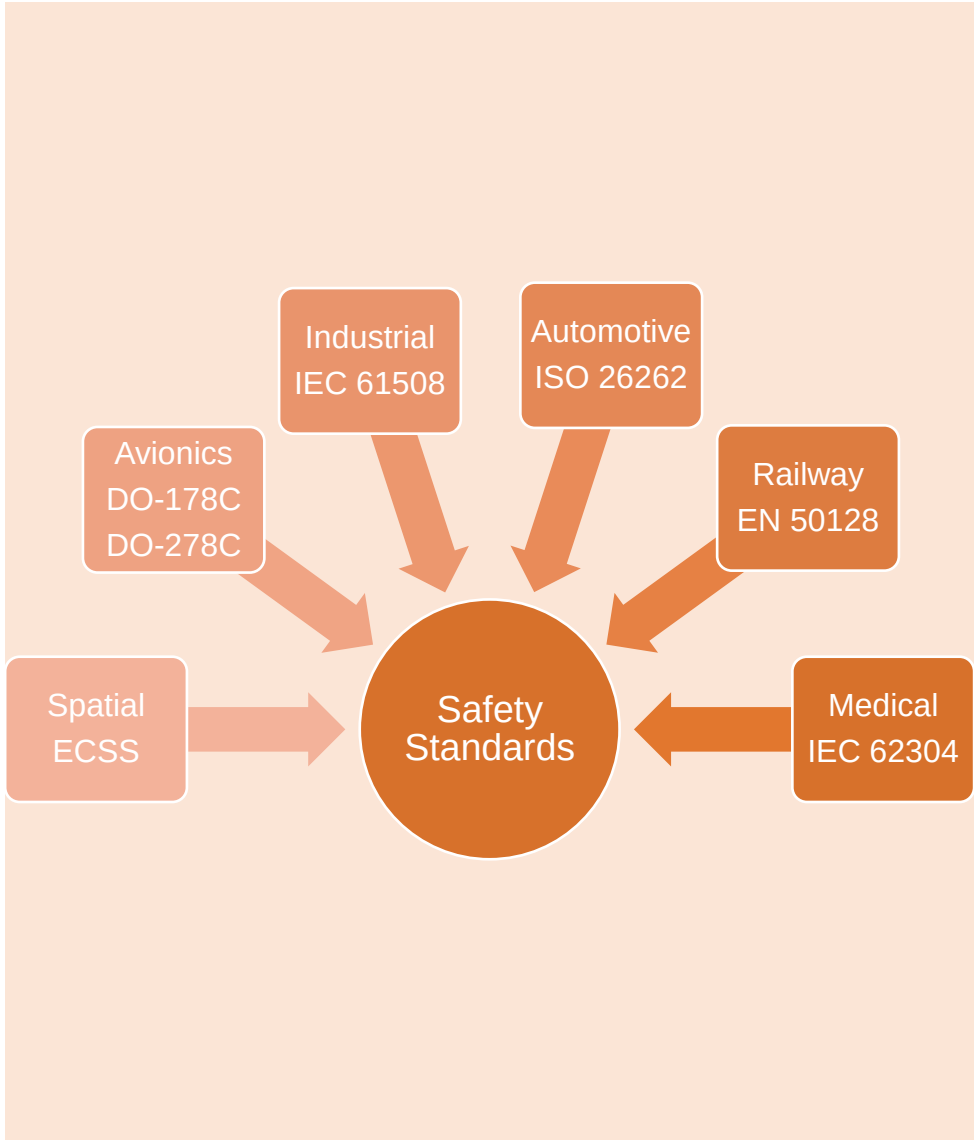
CYBERSECURITY STANDARDS LANDSCAPE



- Several (Cyber) Security standards exists, either generic or tied to specific industry:
  - Generic standards may either be corporate centric (ISO/IEC 27000) or product centric e.g. ISO/IEC 15408 (CC), or IT centric FIPS SP800 (US, NIST)
  - Industry-specific Security standards exist for e.g. Avionics (DO-356), Automotive (ISO/SAE 21434), or Industrial Automation and Control Systems (IEC 62443).

SECURITY / SAFETY CERTIFICATION LANDSCAPE





COMMON CRITERIA - OVERVIEW

The CC is presented as a set of distinct but related parts as identified below.

- **Part 1: Introduction and general model is the introduction to the CC**
  - Defines the general concepts and principles of IT Security evaluation and presents a general model of evaluation.

- **Part 2: Security functional components**
  - Establishes a set of functional components that serve as standard templates upon which to base Security Functional Requirements (SFRs) for TOEs.
  - CC Part 2 catalogues the set of functional components and organizes them in classes and families
  - SFRs specify individual Security functions which are provided by the product under evaluation, in other words the claimed Security functionalities

- **Part 3: Security assurance components**
  - Establishes a set of assurance components that serve as standard templates upon which to base Security Assurance Requirements (SARs) for TOEs
  - CC Part 3 catalogues the set of assurance components and organizes them into classes and families
  - CC Part 3 also defines evaluation criteria for PPs and STs and presents seven pre-defined assurance packages which are called the Evaluation Assurance Levels (EALs).

COMMON CRITERIA - GENERAL MODEL (PART 1)

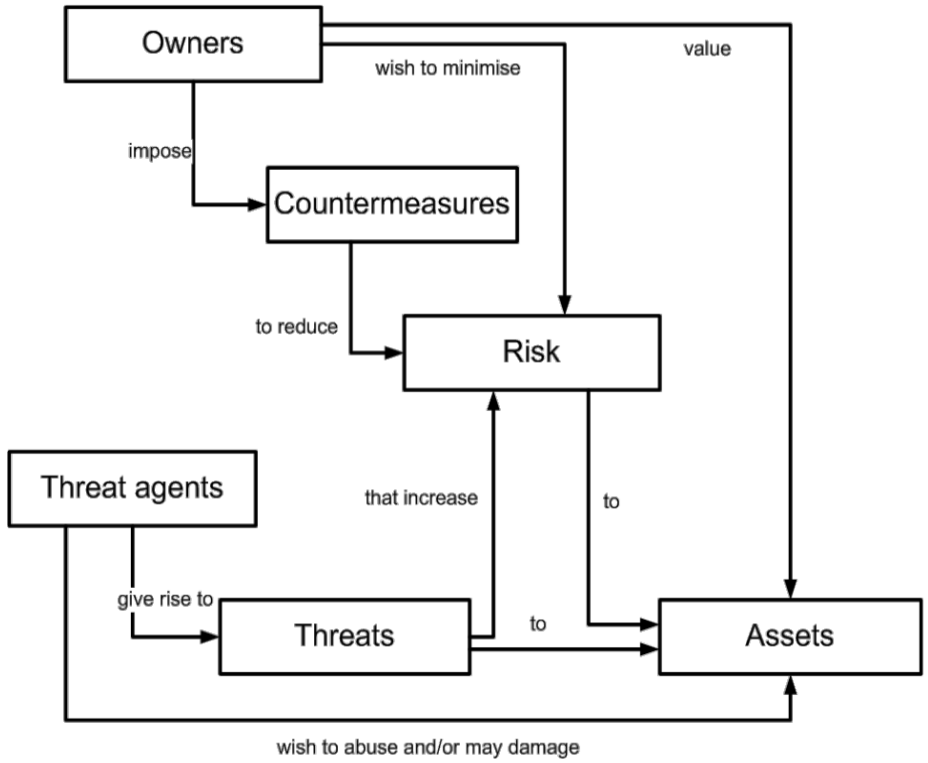


Figure 2 - Security concepts and relationships

Security Model

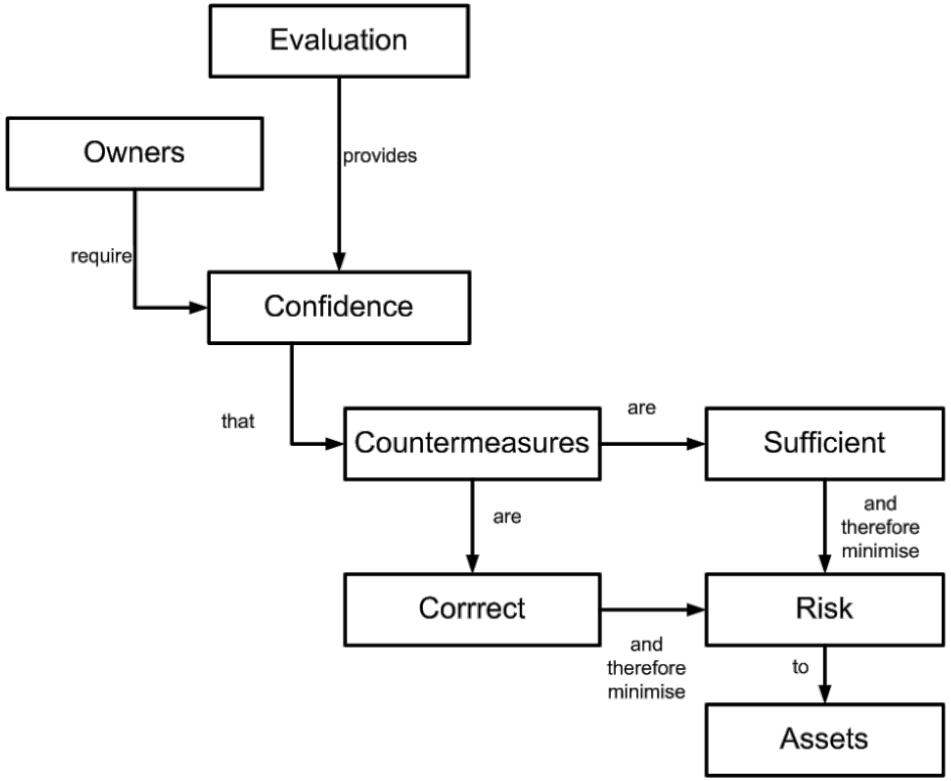


Figure 3 - Evaluation concepts and relationships

Security Evaluation Model

COMMON CRITERIA - SECURITY FUNCTIONAL COMPONENTS (PART 2)

- Security functional components are classified in classes:
  - Class FAU: Security audit
  - Class FCO: Communication
  - Class FCS: Cryptographic support
  - Class FDP: User data protection
  - Class FIA: Identification and authentication
  - Class FMT: Security management
  - Class FPR: Privacy
  - Class FPT: Protection of the TSF
  - Class FRU: Resource utilization
  - Class FTA: TOE access
  - Class FTP: Trusted path/channels

- Each class is refined in families

COMMON CRITERIA - SECURITY ASSURANCE COMPONENTS (PART 3)

- Levels EAL 1 to 7
  - Increasing rigor and formalism from 1 to 7

- Classes are addressed for each levels:
  - Development
  - Guidance Documents
  - Life cycle support (including Configuration management, Delivery, operation and maintenance)
  - Security Target evaluation
  - Testing
  - Vulnerability analysis

- Classes are refine in families
  - See next slide

COMMON CRITERIA EVALUATION ASSURANCE LEVELS PART 3)

Assurance Class	Assurance Family	Assurance components	Assurance Components by Evaluation Assurance Level						
			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC	Security Architecture		1	1	1	1	1	1
	ADV_FSP	Functional specification	1	2	3	4	5	5	6
	ADV_IMP	Implementation representation				1	1	2	2
	ADV_INT	TSF internals					2	3	3
	ADV_SPM	Security policy modelling						1	1
	ADV_TDS	TOE design		1	2	3	4	5	6
Guidance Documents	AGD_OPE	Operational user guidance	1	1	1	1	1	1	1
	AGD_PRE	Preparative procedures	1	1	1	1	1	1	1
Life Cycle Support	ALC_CMC	CM capabilities	1	2	3	4	4	5	5
	ALC_CMS	CM scope	1	2	3	4	5	5	5
	ALC_DEL	Delivery		1	1	1	1	1	1
	ALC_DVS	Development security			1	1	1	2	2
	ALC_FLR	Flaw remediation							
	ALC_LCD	Life cycle definition			1	1	1	1	2
	ALC_TAT	Tools and techniques				1	2	3	3
Security Target Evaluation	ASE_CCL	Conformance claims	1	1	1	1	1	1	1
	ASE_ECD	Extended components definition	1	1	1	1	1	1	1
	ASE_INT	ST introduction	1	1	1	1	1	1	1
	ASE_OBJ	Security objectives	1	2	2	2	2	2	2
	ASE_REQ	Derived security requirements	1	2	2	2	2	2	2
	ASE_SPD	Security problem definition		1	1	1	1	1	1
	ASE_TSS.	TOE summary specification	1	1	1	1	1	1	1
Tests	ATE_COV	Coverage		1	2	2	2	3	3
	ATE_DPT.	Depth			1	1	3	3	4
	ATE_FUN	Functional tests		1	1	1	1	2	2
	ATE_IND	Independent testing	1	2	2	2	2	2	3
Vulnerability Assessment	AVA_VAN	Vulnerability analysis	1	2	2	3	4	5	5

COMMON CRITERIA SECURITY TARGET DOCUMENT

- *an ST introduction* containing three narrative descriptions of the TOE on different levels of abstraction;
- *a conformance claim*, showing whether the ST claims conformance to any PPs and/or packages, and if so, to which PPs and/or packages;
- *a security problem definition*, showing threats, OSPs and assumptions;
- *security objectives*, showing how the solution to the security problem is divided between security objectives for the TOE and security objectives for the operational environment of the TOE;
- *extended components definition* (optional), where new components (i.e. those not included in CC Part 2 or CC Part 3) may be defined. These new components are needed to define extended functional and extended assurance requirements;
- *security requirements*, where a translation of the security objectives for the TOE into a standardized language is provided. This standardized language is in the form of SFRs. Additionally this section defines the SARs;
- *a TOE summary specification*, showing how the SFRs are implemented in the TOE.

(From CC Part 1: Introduction and general model)

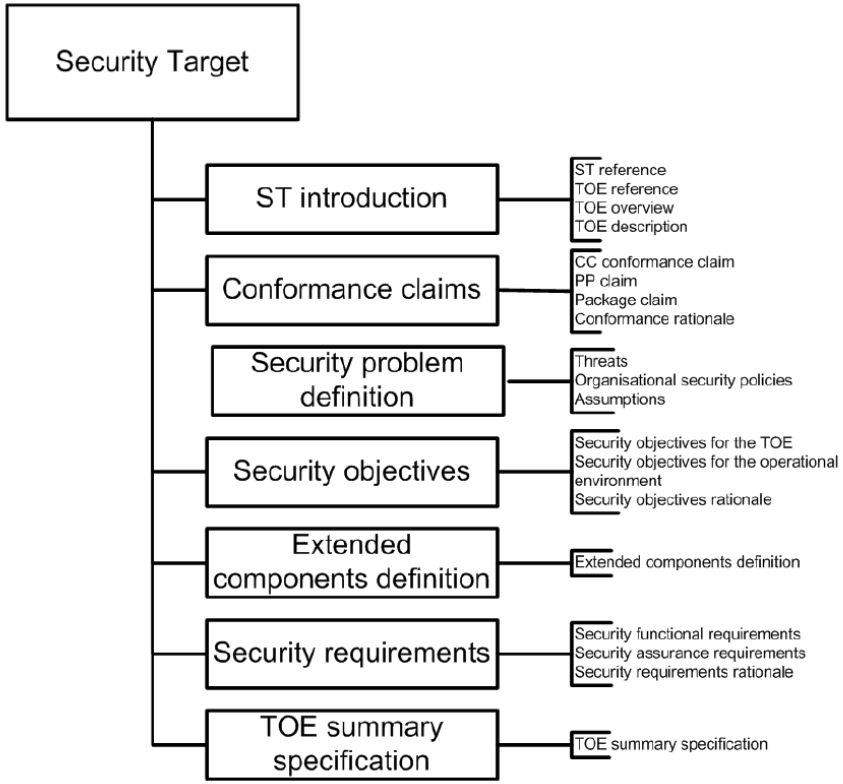
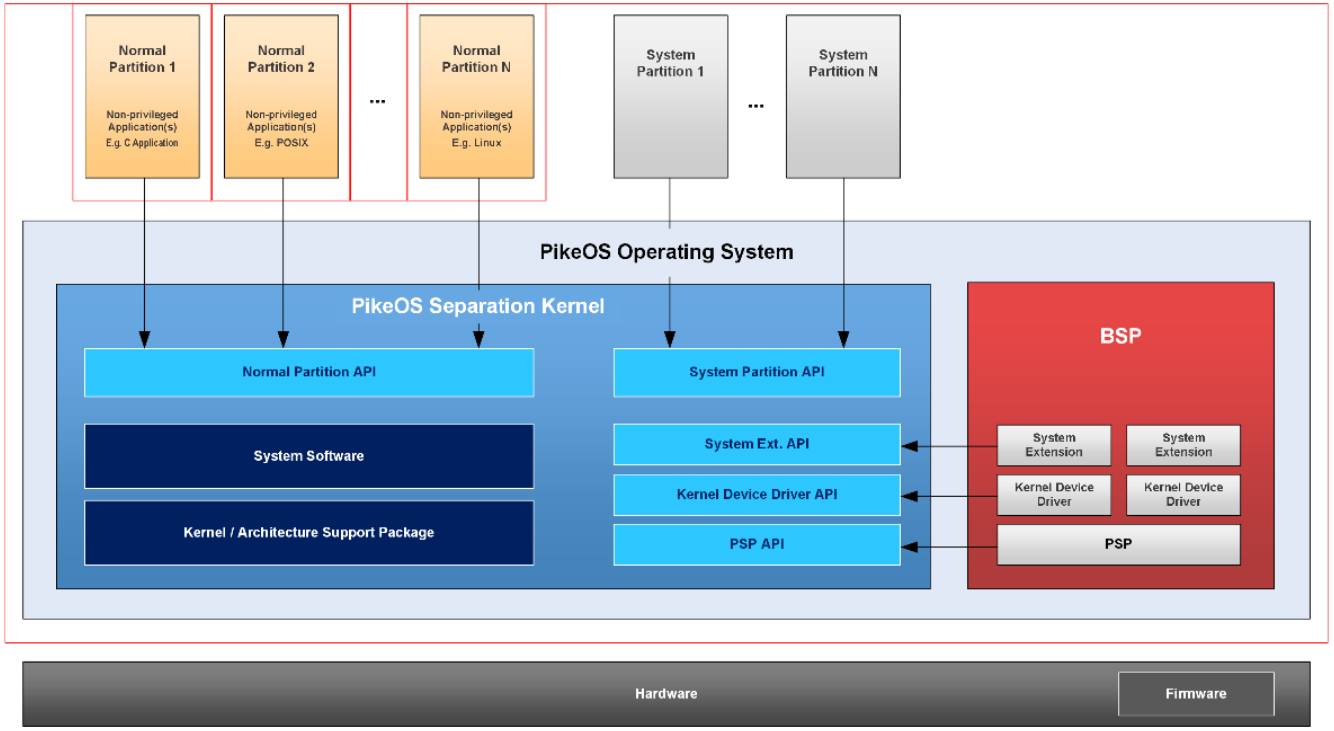


Figure 5 - Security Target contents

PIKEOS SCOPE IN COMMON CRITERIA

- The criteria to choose the Common Criteria for PikeOS certification are
  - A well-recognized international standard
  - An independent evaluation from a specialized and recognized certification laboratory (atsec)
  - A national Security agency certificate with international agreement (BSI)
  - The ability to define a PikeOS Security Target (ST) dedicated to hypervisor and real-time OSs

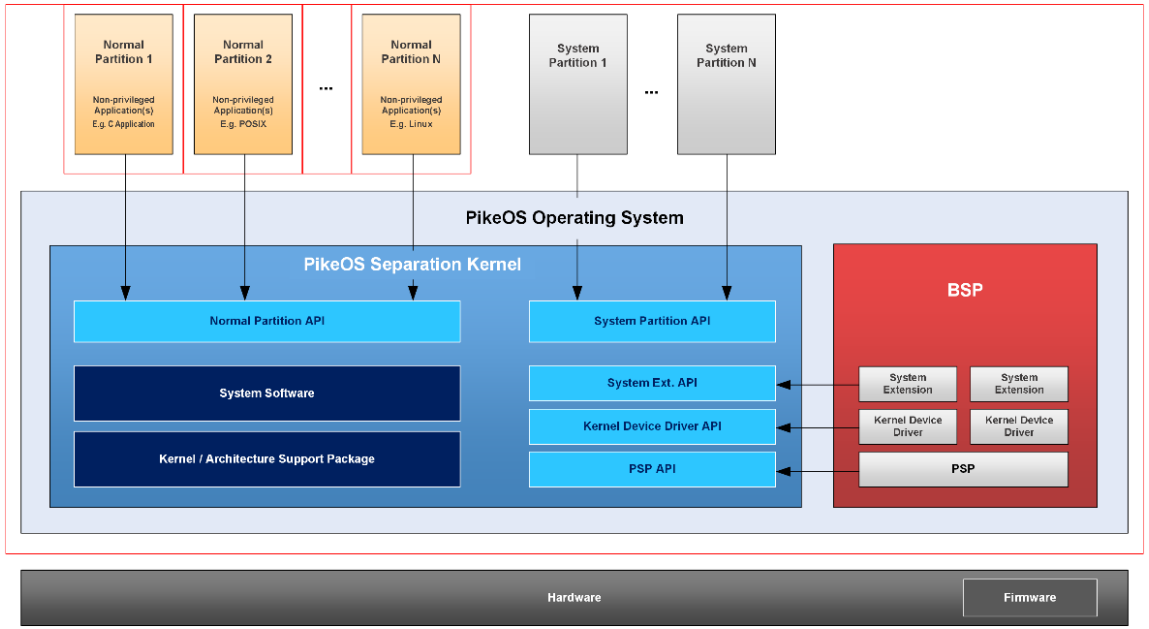


- As there is no existing Separation Kernel Protection Profile (SKPP), the Security scope is fully defined in the Security Target
- The Security scope is different from one product to the other.
- The scope of the TOE is the complete “PikeOS Separation Kernel” including multicore support.

TOE: Target of Evaluation

PIKEOS SCOPE IN COMMON CRITERIA

- PikeOS provides platform level properties (Security functional requirements) that have been evaluated in the scope of CC certification.
- Platform Level Properties provided by PikeOS are:
  - Separation in time and space of user applications hosted in different user partitions from each other and from the TSF (PikeOS kernel)
    - Separation of partitions/VM
    - Controlled information flow
    - Access control to resources
    - Availability of resources
    - White list security policy
  - Confidentiality of per-partition resource usage
  - Absence of residual information flow on partition switch
  - Management of TSF and TSF data
  - Access to TSF and TSF data
  - TSF self-protection and accuracy of Security functionality



- The Platform Level Properties provided by PikeOS are in the following CC classes:
  - Class FDP: User data protection
  - Class FIA: Identification and authentication
  - Class FMT: Security management
  - Class FRU: Resource utilization

PIKEOS EVALUATION ASSURANCE LEVELS

Assurance Class	Assurance Family	Assurance components	Assurance Components by Evaluation Assurance Level						
			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC	Security Architecture		1	1	1	1	1	1
	ADV_FSP	Functional specification	1	2	3	4	5	5	6
	ADV_IMP	Implementation representation				1	1	2	2
	ADV_INT	TSF internals					2	3	3
	ADV_SPM	Security policy modelling						1	1
	ADV_TDS	TOE design		1	2	3	4	5	6
Guidance documents	AGD_OPE	Operational user guidance	1	1	1	1	1	1	1
	AGD_PRE	Preparative procedures	1	1	1	1	1	1	1
Life Cycle Support	ALC_CMC	CM capabilities	1	2	3	4	4	5	5
	ALC_CMS	CM scope	1	2	3	4	5	5	5
	ALC_DEL	Delivery		1	1	1	1	1	1
	ALC_DVS	Development security			1	1	1	2	2
	ALC_FLR	Flaw remediation					3	3	3
	ALC_LCD	Life cycle definition			1	1	1	1	2
	ALC_TAT	Tools and techniques				1	2	3	3
Security Target Evaluation	ASE_CCL	Conformance claims	1	1	1	1	1	1	1
	ASE_ECD	Extended components definition	1	1	1	1	1	1	1
	ASE_INT	ST introduction	1	1	1	1	1	1	1
	ASE_OBJ	Security objectives	1	2	2	2	2	2	2
	ASE_REQ	Derived security requirements	1	2	2	2	2	2	2
	ASE_SPD	Security problem definition		1	1	1	1	1	1
	ASE_TSS.	TOE summary specification	1	1	1	1	1	1	1
Tests	ATE_COV	Coverage		1	2	2	2	3	3
	ATE_DPT.	Depth			1	1	3	3	4
	ATE_FUN	Functional tests		1	1	1	1	2	2
	ATE_IND	Independent testing	1	2	2	2	2	2	3
Vulnerability Assessment	AVA_VAN	Vulnerability analysis	1	2	2	3	4	5	5

- PikeOS is certified EAL5+
- Assurance level for each component is highlighted in green
- EAL 5: Semi-formally designed and tested plus the
  - + ALC_FLR.3
  - + AVA_VAN.5
  - + ADV_IMP.2
  - + ALC_DVS.2
  - + ALC_CMC.5
- EAL5+ includes the ANSSI French scheme “Qualification renforcée”

CYBERSECURITY STANDARDS LANDSCAPE

- As industry-specific standards more or less explicitly relate to the CC, compliance matrices can be built to map most requirement between CC and those industry-specific standards

- For a product as PikeOS such compliance matrices show that only a very limited set of the industry-specific requirements are not directly covered by CC evaluation
  - For these requirements, compliance can be established by producing dedicated additional evidences or by adjusting slightly the product life cycle activities as mandated by the industry-specific standard
  - The main deviations to the standards are system / equipment level requirements stated as “Not applicable” or “Partially compliant” in the table below

Standard	Compliant	Partially compliant	Not applicable	Total
DO-356A / ED-203A	29	3	7	39
IEC 62443	39	2	2	43
ISO / SAE 21434	87	6	9	102

EQUIPMENT: ISO/SAE 21434 SECURITY MODEL

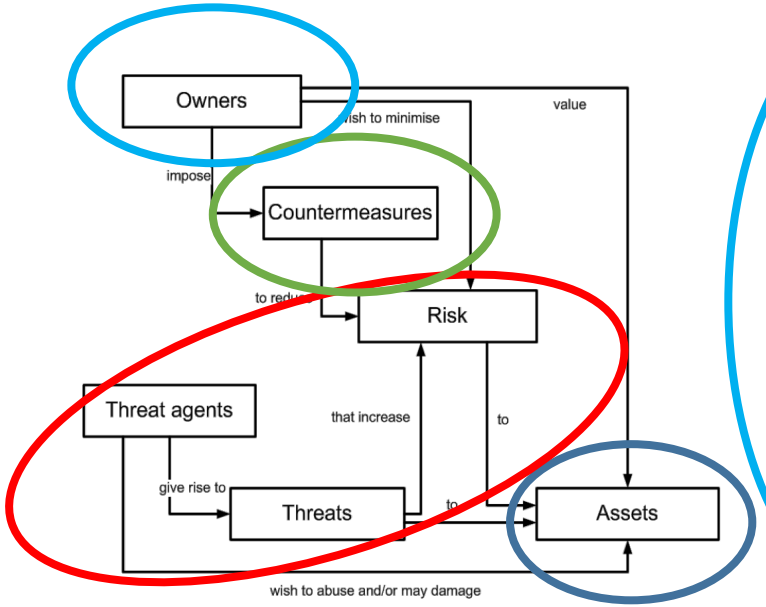


Figure 2 - Security concepts and relationships

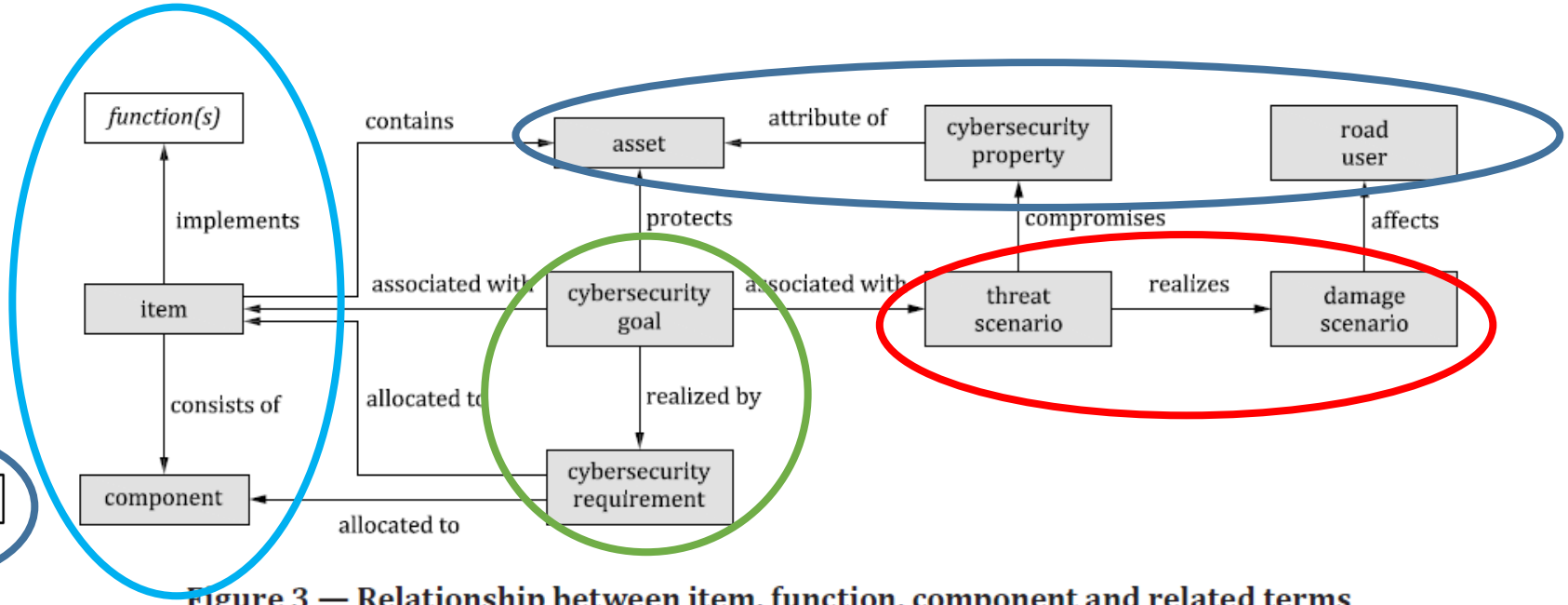


Figure 3 — Relationship between item, function, component and related terms

CC Security Model

ISO / SAE 21434 Security Model

SECURITY LIFE CYCLE

Automotive (ISO/SAE 21434)

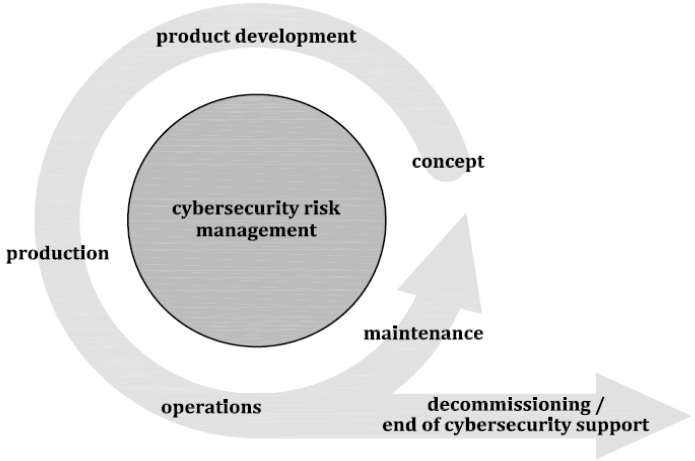


Figure 2 — Overall cybersecurity risk management

Avionics (ED-202A / DO-326A)

- **Product Life Cycle Context:**
  - Airworthiness Security during the Aircraft product life cycle **from project initiation until the aircraft Type Certificate is issued** for the aircraft type design, including afterwards the issuance of STCs and ATCs.
  - In addition, it includes the handover of information about the type design that is necessary to ensure continuing airworthiness with respect to unauthorized interaction.
  - **For the other stages of the product life cycle (operation, support, maintenance, administration, and disposal) guidance may be found in a companion document** ED-204 / DO-355 "Information Security Guidance for Continuing Airworthiness".

Industrial (IEC 62443-4-1)

- The primary goal of these requirements is to provide a framework to address **a secure by design, defense in depth approach to designing, building, maintaining and retiring products** used in industrial automation and control products and systems.
- Application of the framework is intended to provide confidence that the component, product or system has security commensurate with its expected level of risk throughout the product's life cycle.

- **Common Criteria Classes covers the full product life cycle**
  - ASE : Security Target evaluation
  - ADV : Development
  - ATE : Testing
  - AGD : Guidance Documents
  - ALC : Life Cycle support (including Configuration management, Delivery, operation and maintenance)
  - AVA : Vulnerability analysis

SECURITY LIFE CYCLE

- All standards assume that the system will be certified from conception, based on a top-down strategy from the system level to the lowest sub-components
  1. Identifying the assets to be protected, threats, vectors of threats associated at the level of the system
  2. Decline these elements on the components of their systems to implement countermeasures that reduce risks

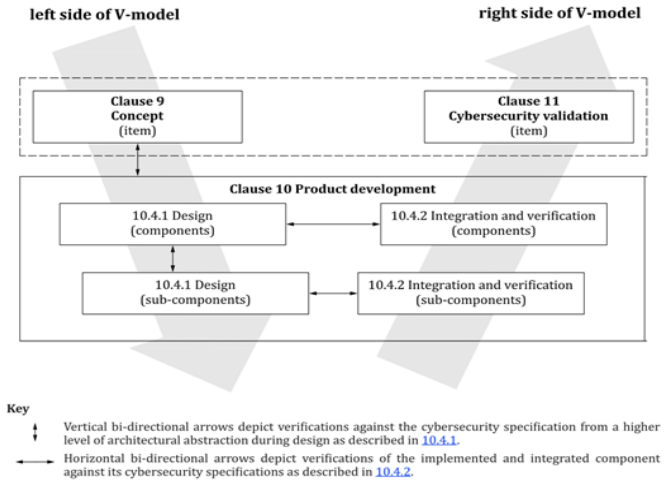


Figure 9 — Example of product development activities in the V-model

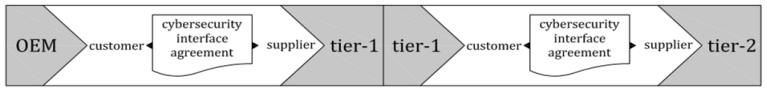


Figure 8 — Use cases for customer/supplier relationships in the supply chain

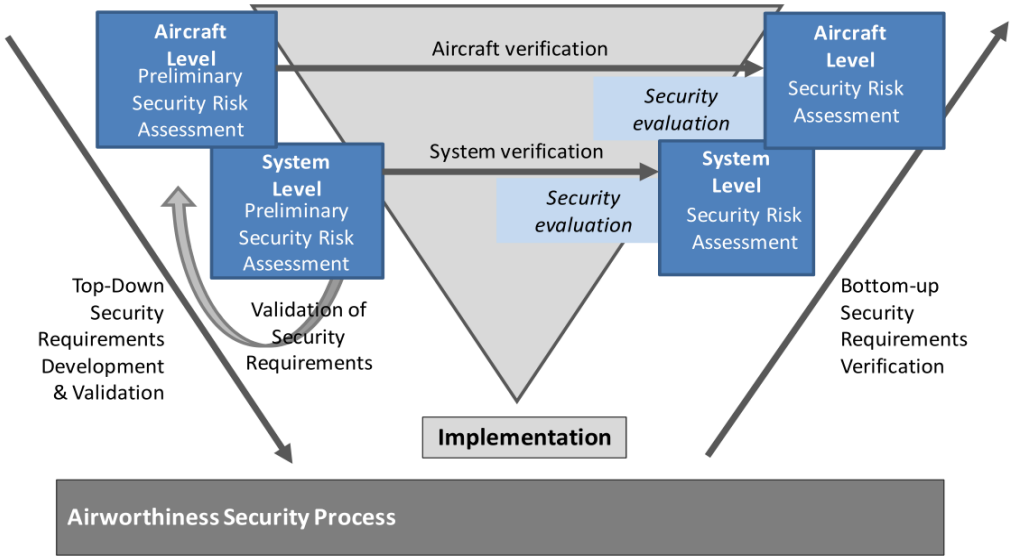
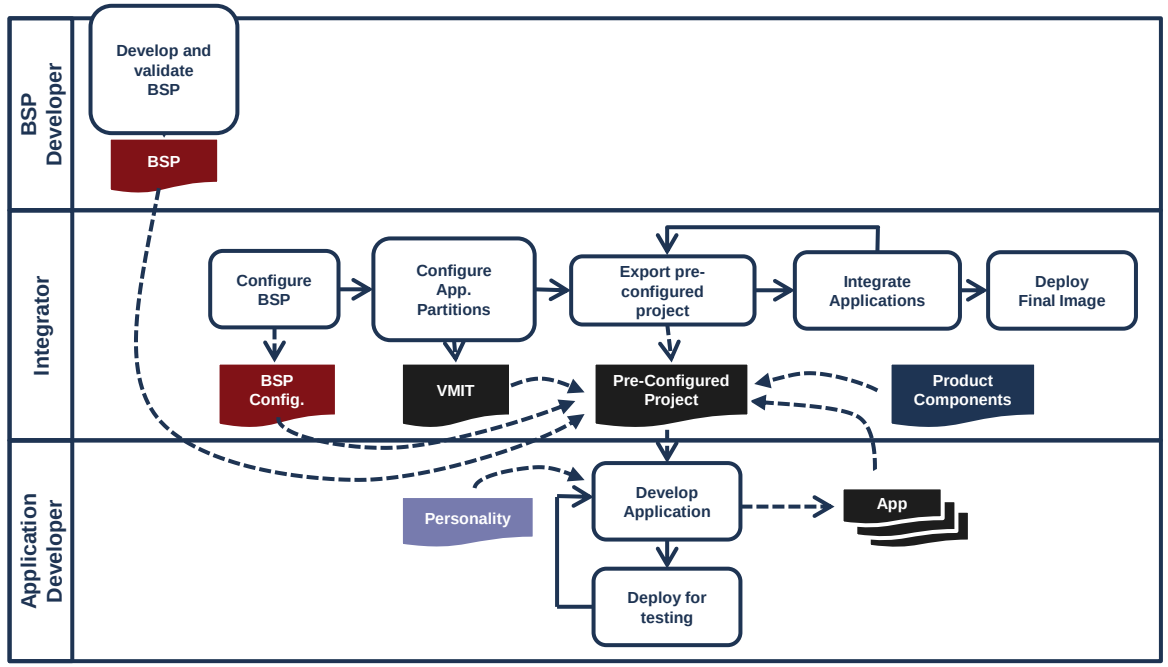


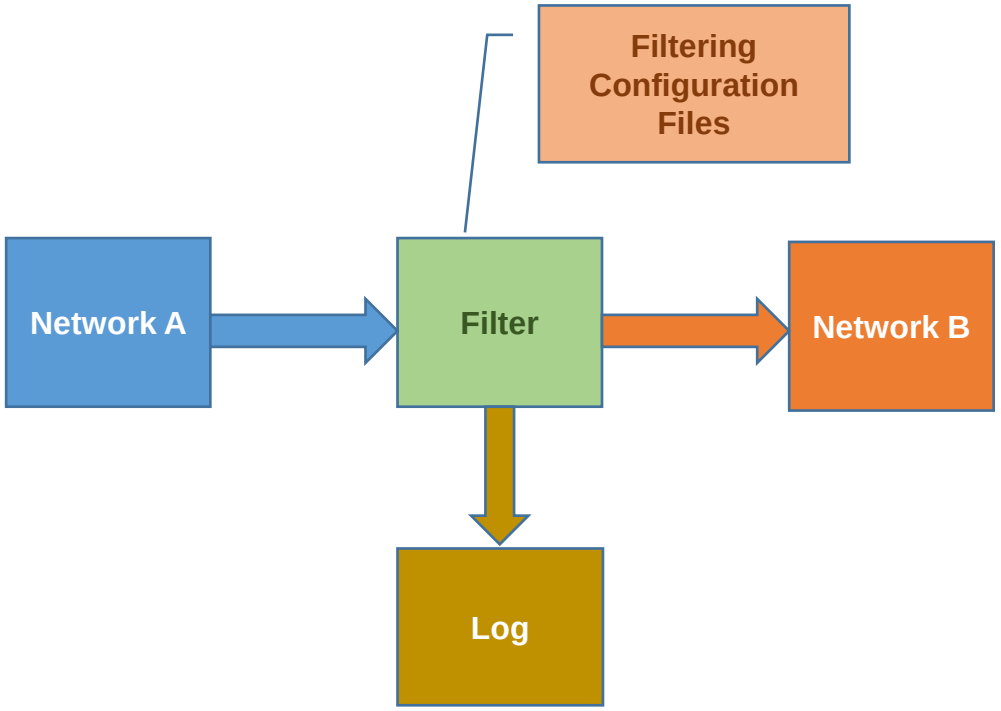
FIGURE 2-2: SECURITY RISK ASSESSMENT RELATED ACTIVITIES IN THE DEVELOPMENT PROCESS V-MODEL

SECURITY LIFE CYCLE

- Based on its Common Criteria certification, PikeOS provides proven properties allowing these countermeasures to be implemented at the component level.
- Based on the Role definition defined in PikeOS, a bottom-up approach makes it possible to take advantage of PikeOS properties by defining an appropriate system architecture.
- Customer (Integrator) performs a top-down threat analysis / risk assessment on its system (using a generic or industry-specific method)
- Customer can rely on the BSP components (including PikeOS) to support its Security demonstration



USE CASE: SECURE GATEWAY BASED ON PIKEOS



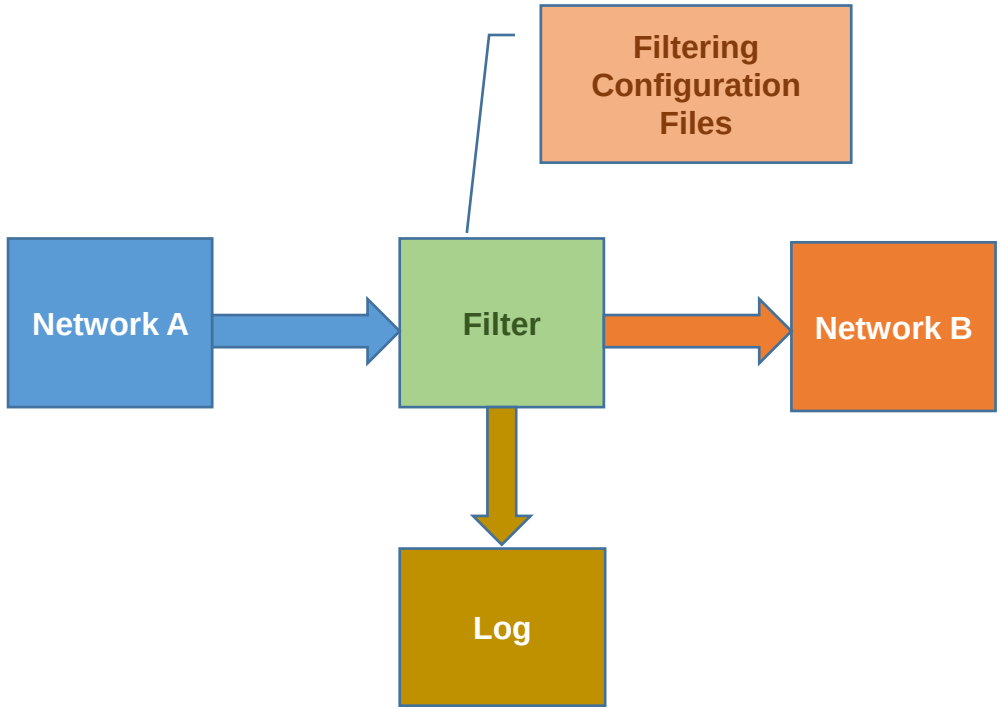
- The TOE offers generic filtering functionality. It is configured by means of a filtering configuration file

- The filtering algorithm is the following:

1. The **Filter** component obtains the data from the **Network A**
2. The **Filter** component verifies the data content according to a configurable filter rules defined in the configuration file (e.g. structure, content, sizes, elements, attributes, …)
3. If the filter rules are met, the **Filter** passes the data on to **Network B**
4. If the filter rules are not met, the TOE immediately rejects the message and creates an audit record to the **Log interface**

USE CASE: SECURITY PROBLEM DEFINITION

- Assets of the secure gateway:
  - Filtering rules
  - System configuration
  - Software implementing TOE Security functions
  - Logging data
  - Traffic data sent from one network to the other



USE CASE: SECURITY PROBLEM DEFINITION

- The threat agents are
  - a user accessing through its filter interfaces attempting to leak transferred data
  - a user that gain physical or logical access to the TOE

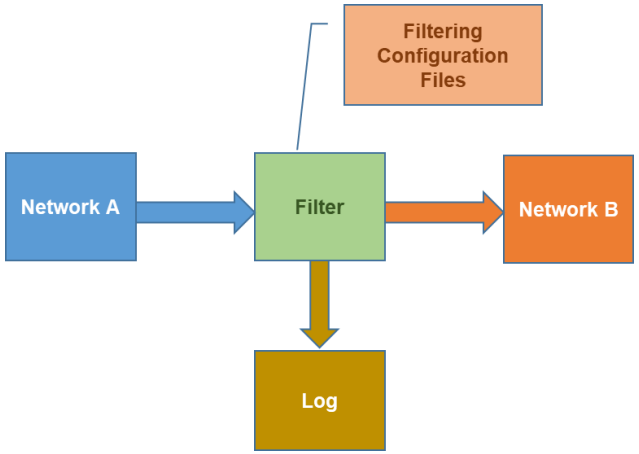
- The possible threats are
  - the leak of the traffic data
  - an illegal configuration
  - the manipulation of the data logged
  - attempt to send unauthorized data through the filter interfaces or attempts to manipulate the TSF data by introducing malicious code.

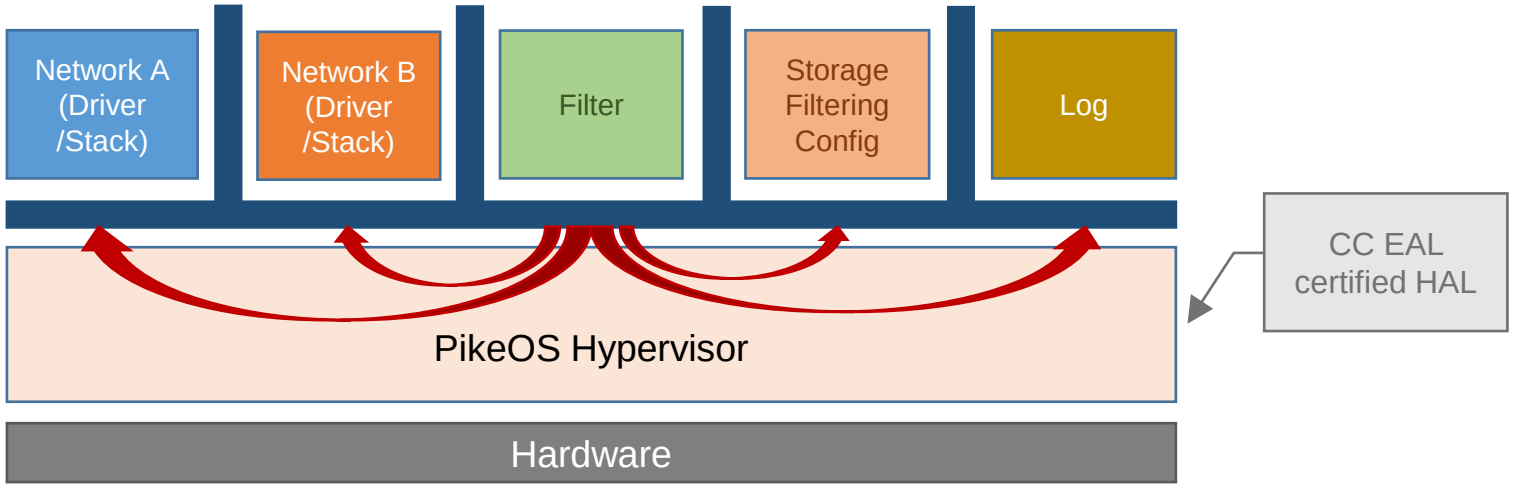
- *Note: The list of threat agents and threats is not exhaustive but just identified to support the use case example.*

USE CASE: ARCHITECTURE

- The secure gateway runs on a single physical server.

- The secure gateway will have the following number of physical network interfaces:
  - Two network interfaces per filtering gateway, each connected to one of the operational network segments (**Filter interfaces**);
  - One network interface per server to an optional external system for audit trail management (**Log interface**);
  - All external network interfaces are Ethernet (IEEE 802.3) compatible.



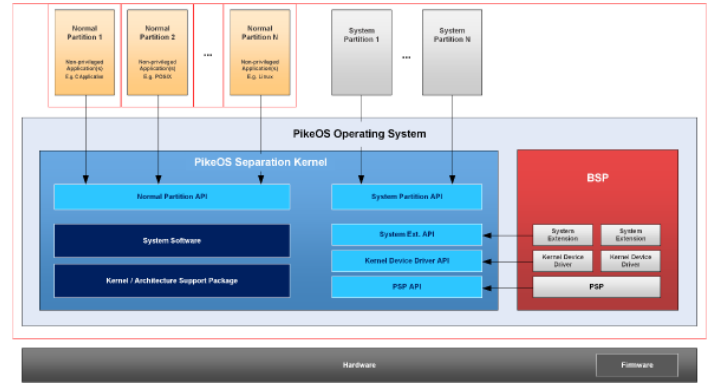


USE CASE: TOE ENVIRONMENT SECURITY OBJECTIVES

- All industry-specific Security standards have the concept of environment and assumptions
  - TOE environment can be called Security context, Security environment, can be introduced by an out-of-context component

- These assumptions based on the TOE environment Security objectives are the PikeOS Security objectives, evaluated in the scope of the PikeOS CC evaluation:

  - Separation in time and space of user applications hosted in different user partitions from each other and from the TSF (PikeOS kernel)
  - Confidentiality of per-partition resource usage
  - Absence of residual information flow on partition switch
  - Management of TSF and TSF data
  - Access to TSF and TSF data
  - TSF self-protection and accuracy of Security functionality



SUMMARY

- Using PikeOS as part of a CC EAL5+ certified HAL split the Security scope:
  - **System / Equipment Level:**
    - The scope of the evaluation is limited to the system / equipment level Security objectives. The architecture of the system can take advantage of PikeOS separation properties to isolate logical components and efficiently achieve Security goals
  - **Platform Level (PikeOS, BSP):**
    - The platform evaluation can be efficiently obtained by extending the PikeOS CC certification to the BSP. The Cybersecurity claims and assumptions of the platform will be validated by means of compliance matrix to the CC standard and minimal extra activities
- The existing Common Criteria EAL 5+ certificate on PikeOS reduces the Security certification effort, complexity and time-to-market of an embedded system built on PikeOS