Cyber-security in Defence Mission Systems

SORIN IACOB

GUEST LECTURE @UTWENTE
01.06.2023

Lecture overview

- Objectives
- Naval Mission Systems
  - Overview
  - High-Level Architecture
  - Security needs and challenges in NMS
- Architecting and Engineering Method for NMS Security
  - Requirements
  - Architectural and Engineering principles
  - Security Risk Analysis
  - Security architecture
  - Accreditability
- Quiz

Lecture Objectives

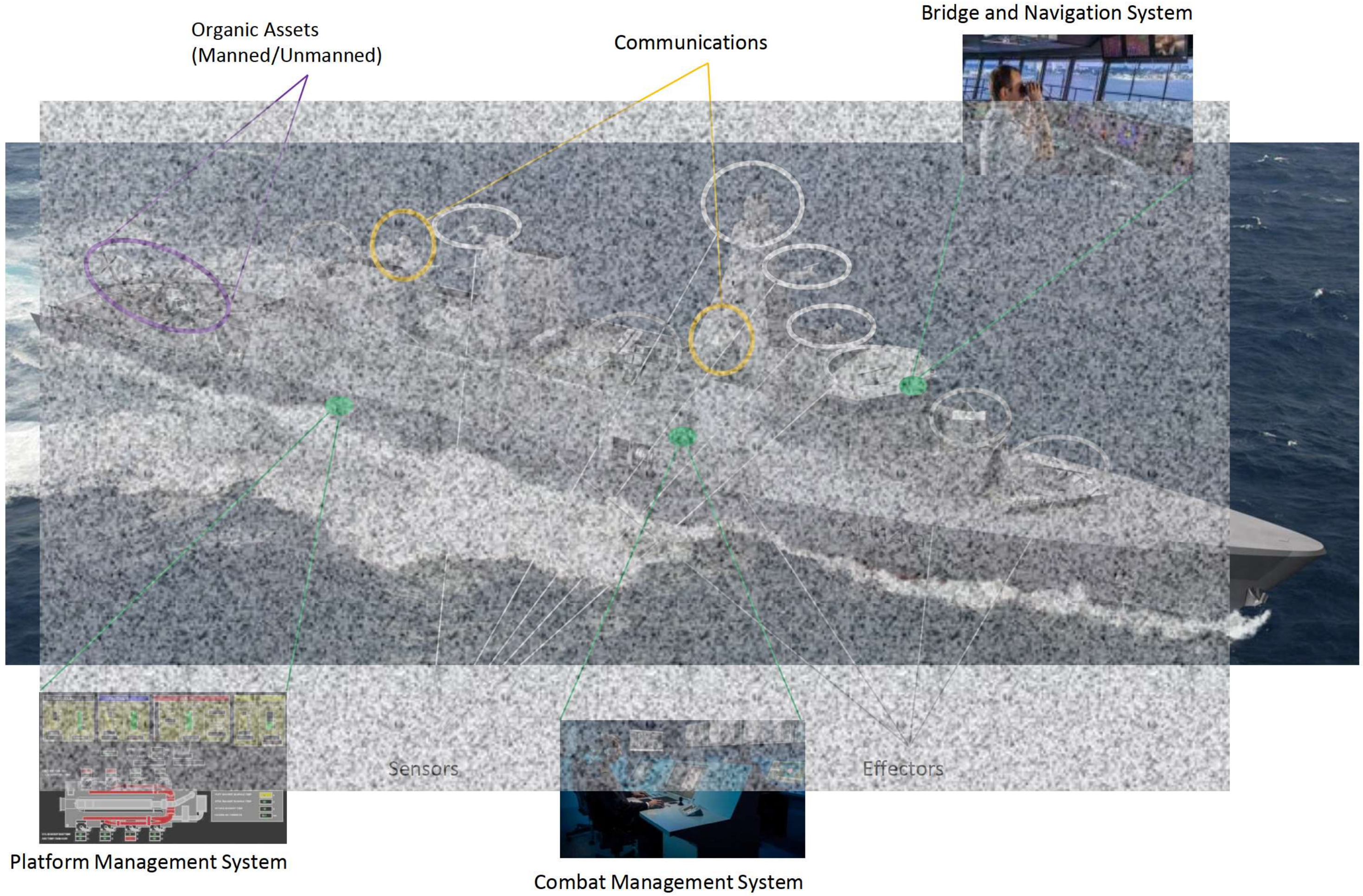
- Get a high-level understanding of what a Naval Mission System (NMS) is, and what cyber-security aspects are relevant
- Understand why and how the security requirements for a NMS are different than those for other IT/OT systems
- Know and understand the main architectural and engineering principles for building secure NMS
- Be able to identify the main elements of a security architecture for NMS

What is a Defense Mission Systems

- Safety Missions:
  - Area and border surveillance
  - Search and Rescue
  - Anti-pollution
  - Anti-terrorism
  - Anti-smuggling
  - Anti-piracy
- Defence Missions:
  - Anti-Surface Warfare
  - Anti-Submarine Warfare
  - Anti-Air Warfare
  - Electronic warfare

Main components of Naval Mission Systems

- Cyber-security protection goals
  - Classified information: tactical, intelligence, doctrines, etc.
  - Capabilities: navigation, communications, sensing, decision-making, acting, etc.

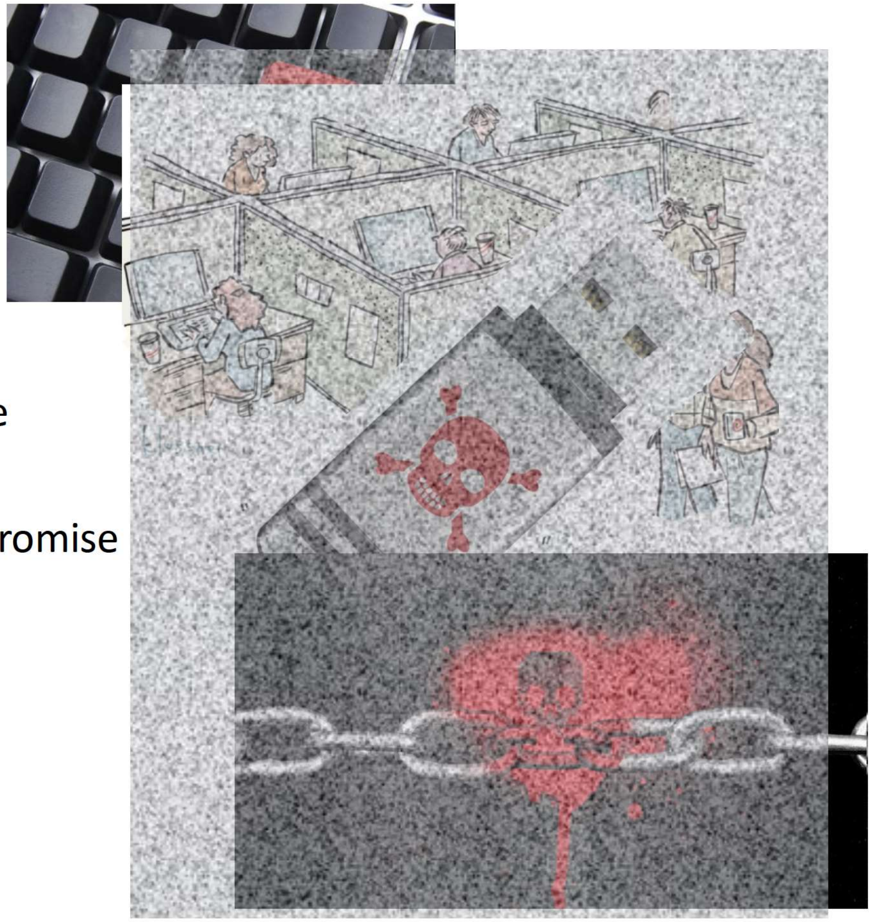


Cyber Security for Naval Mission Systems

- Why is it needed?
  - Disciplined and trained personnel
  - No connections to the internet
  - No new software may be installed
  - No attackers present on board

Cyber Security for Naval Mission Systems

- Why is it needed?
  - Disciplined and trained personnel
    - … mistakes can still be made
  - No connections to the internet
    - … connections to intranet, tactical networks
  - No new software may be installed
    - … updates and external data can still contain malware
  - No attackers present on board
    - … the supply chain or 3rd party maintainers can compromise the system



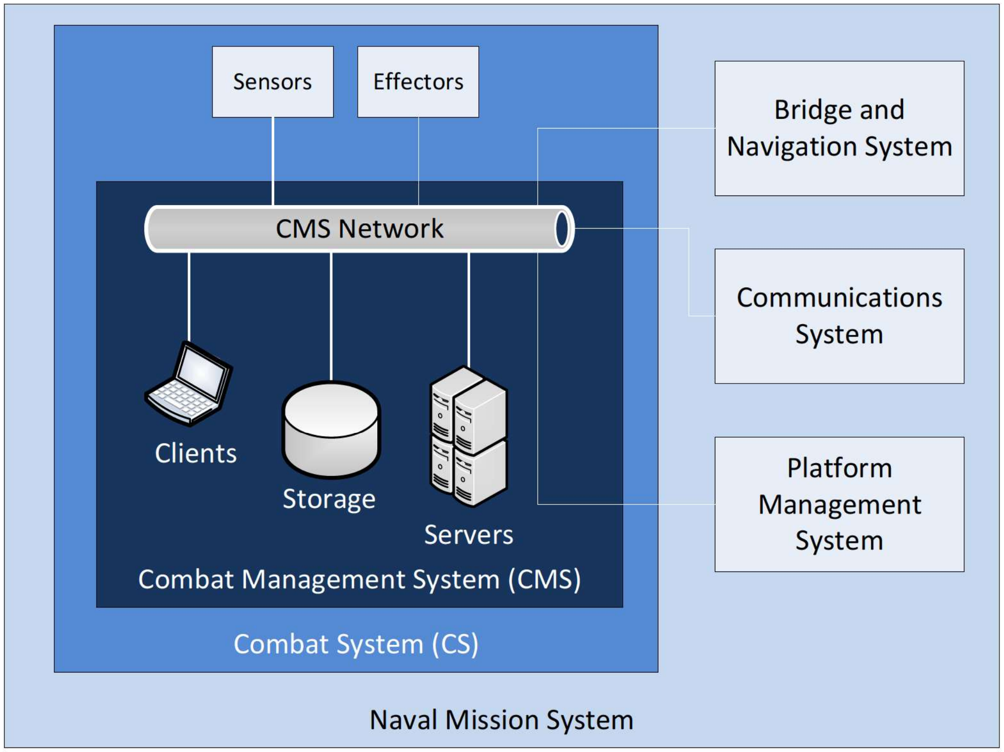
But …

Cyber Security for Naval Mission Systems

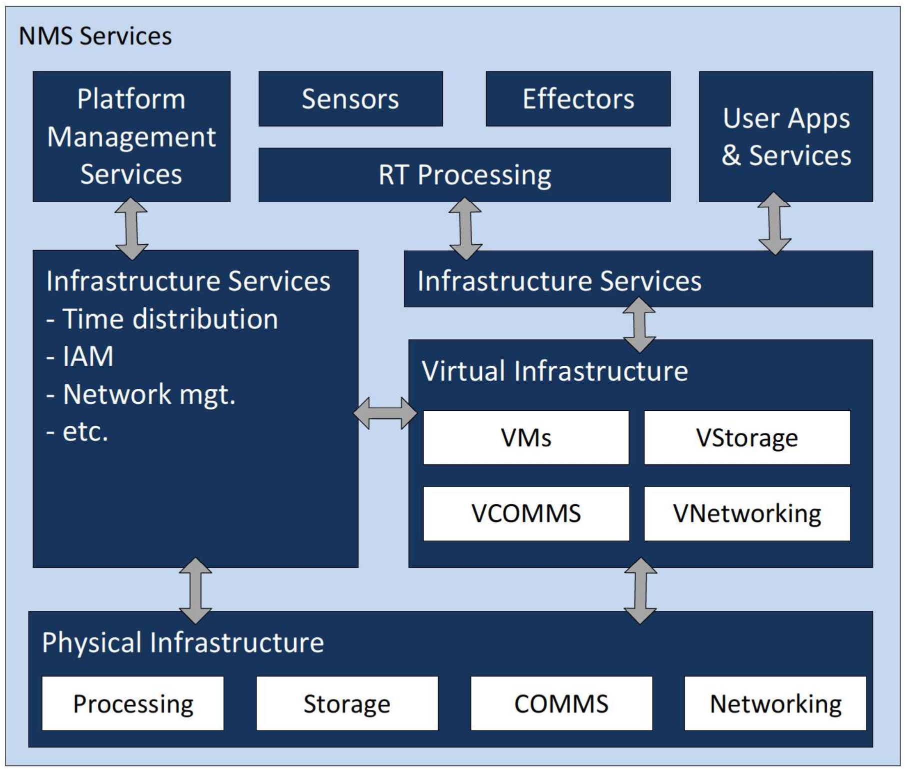
- Why is it needed?
  - … NATO Nations customers require security accreditation
  - … NATO-Partner Nations want to use NATO equipment
  - … delivering vulnerable systems can lead to reputation damage

And also because …

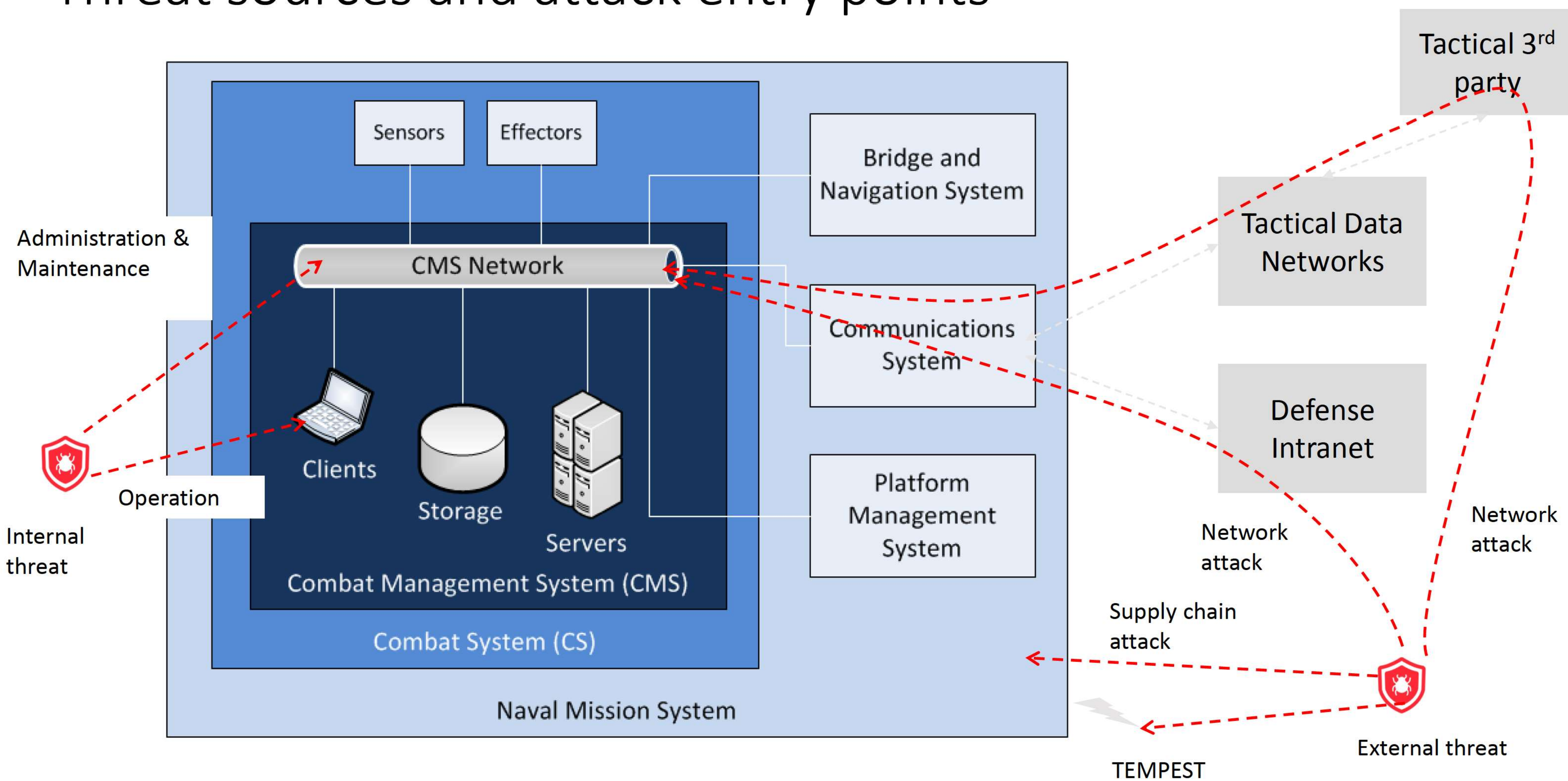
NMS Logical Architecture – Systems View (High-Level)



NMS Logical Architecture – Services View (High-Level)



Threat sources and attack entry points



Cyber-Security in Naval Mission Systems

- Main goal of cyber-security:
  - Ensure the **operational integrity** of the NMS electronic components when these are subjected to **normal use, faults,** or **(cyber) attacks**.
  - Achieved through protection of the **confidentiality, integrity** and **availability** of **information, functionality,** and **resources**.
- Main aspects of cyber security:
  - Control of the **access to sensitive information** and its release to external systems (Information Security)
  - Control of the local and remote **access to system resources** (IT-Security)
- Accreditation
  - The security solution must be evaluated and **approved** by the National Accreditation Authority

Challenges

- Usability
  - Security may not impede usability, may not lead to lockouts, may not cause delays in operation
- Performance
  - Many real-time functional chains
  - Performance may be affected by security functions
- Conflicting requirements
  - Fail-open vs. fail-safe
    - Security functions → fail-safe
    - Functional chains → fail-open
  - Graceful shutdown vs. maximising operational time
  - User traceability vs. operational continuity

Architecting and Engineering Method for NMS Security

1. Analysis of operational context and high-level security requirements
2. Definition of architectural and engineering principles
3. Perform Security Risk Analysis
4. Define security architecture
5. Check Accreditability

Analysis of operational context and high-level security requirements

Definition of architectural and engineering principles

Perform Security Risk Analysis

Define security architecture

Check accreditability

Information Classification in Defence Systems

Security Levels and Information Domains:

- "LOW" data
- "HIGH" data

NL	FR	DE	UK	NATO
Ongerubriceerd en ongemerkt	Non Protégé	Öffentlich	Open	NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC
Ongerubriceerd	Diffusion restreinte administrateur	Offen	Official	NATO Unclassified
Departamental Vertrouwelijk	Diffusion restreinte	VS-NfD	Official-Sensitive	NATO Restricted
STG-Confidentieel	Confidentiel défense	VS-Vertraulich	UK-SECRET	NATO Confidential
STG-Geheim	Secret Défense	Geheim		NATO Secret
STG-Zeer Geheim	Très Secret Défense	Streng Geheim		Cosmic Top Secret

Convention:

- Systems and resources where "HIGH" data is processed → "RED"
- For "LOW" or encrypted data → "BLACK"

Security Modes of Operation

- Specifies the access to sensitive information
  - Based on clearance and need-to-know
  - Clearance level = the classification level up to which a user is allowed access
  - Need-to-know = information that is necessary for carrying out a task

Mode of operation	Clearance for ALL	Need to Know for ALL	Mandatory Access Control*
Dedicated	✓	✓	✘
System High	✓	✘	✘
Compartmented	✓	✘	✓
Multi-Level (Multi-Domain)	✘	✘	✘ (implicit)

* Access rights can only be granted by a Security Administrator

Security Modes of Operation - Consequences

- Most modern systems work in Compartmented or Multi-Level modes

Mode of operation	Information classes	SW & Services	HW & Facilities
Dedicated	HIGH	HIGH	RED
System High	HIGH – multiple caveats	HIGH	RED
Compartmented	HIGH and LOW	HIGH and LOW	RED and BLACK
Multi-Level (Multi-Domain)	HIGH – multiple caveats LOW – multiple caveats	HIGH and LOW	RED (different caveats) BLACK

- System architecture must reflect the differences between HIGH and LOW

Analysis of operational context and high-level security requirements

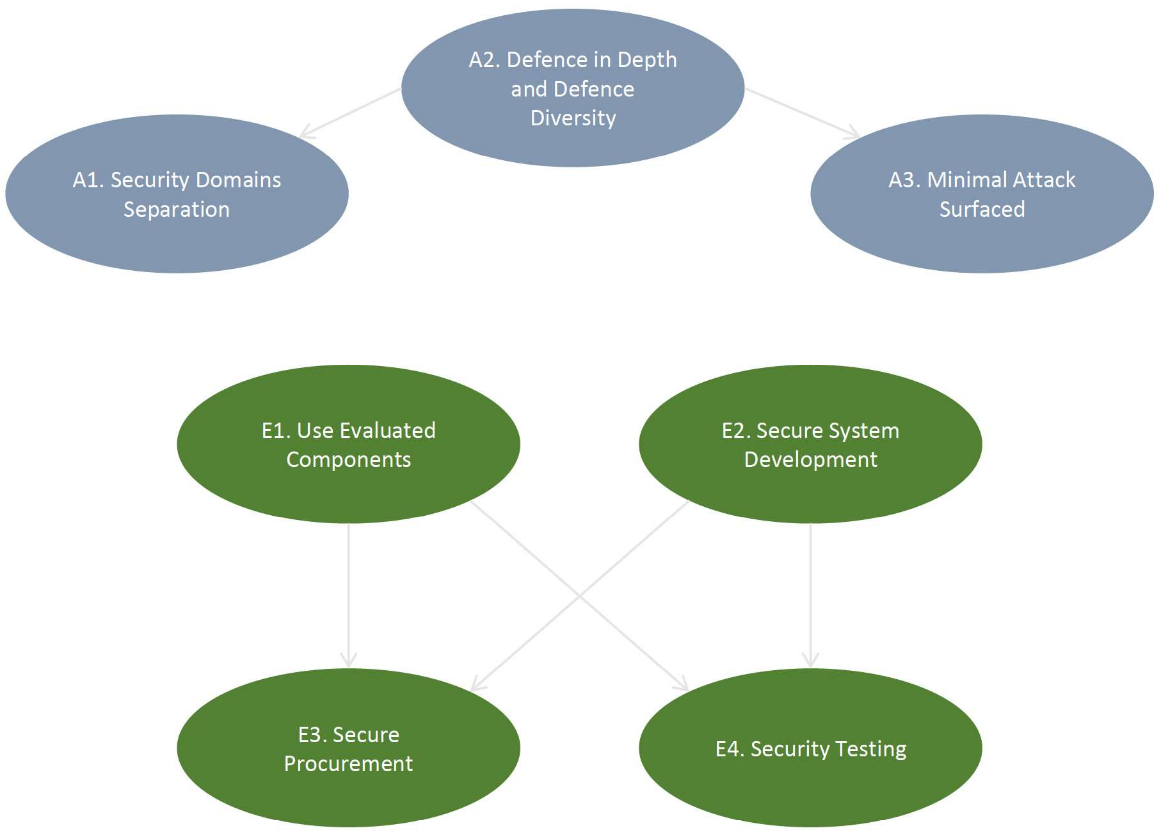
Definition of architectural and engineering principles

Perform Security Risk Analysis

Define security architecture

Check accreditability

Architectural and Engineering Principles for Secure NMS



A1. Security Domains Separation (I)

- Security Levels and Domains:
  - Non-sensitive
  - "Low" data
  - "High" data

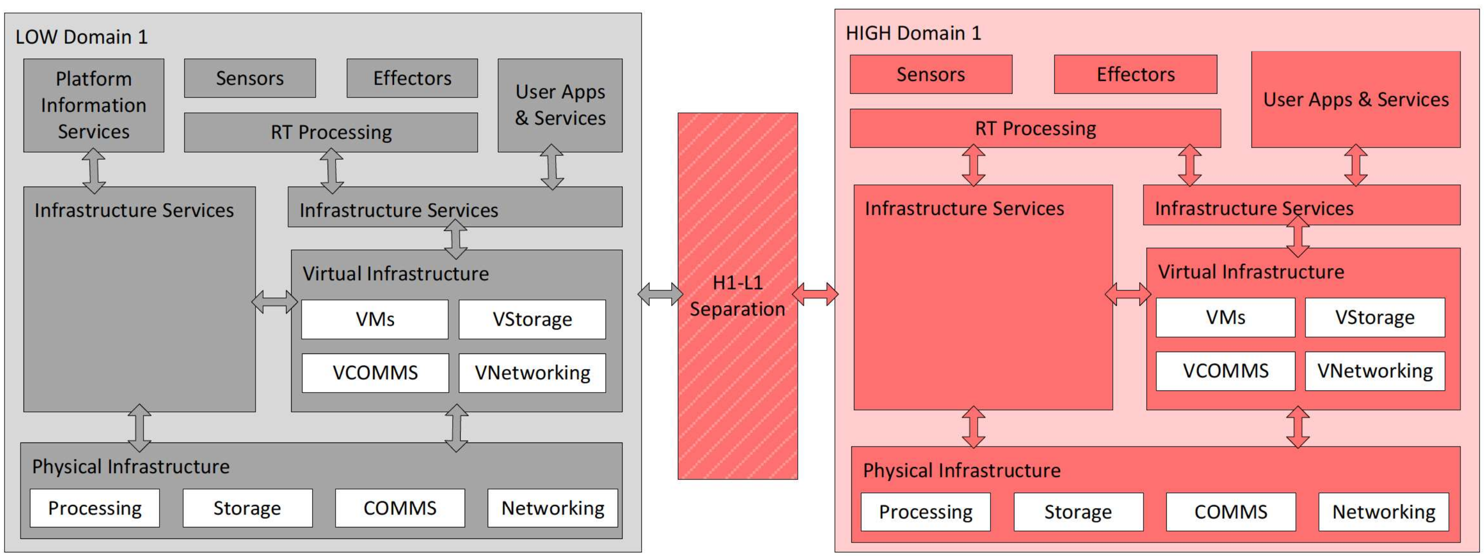
	NL	FR	DE	UK	NATO
Non-sensitive	Ongerubriceerd en ongemerkt	Non Protégé	Öffentlich	Open	NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC
"Low" data	Ongerubriceerd	Diffusion restreinte administrateur	Offen	Official	NATO Unclassified
"Low" data	Departamental Vertrouwelijk	Diffusion restreinte	VS-NfD	Official-Sensitive	NATO Restricted
"High" data	STG-Confidentieel	Confidentiel défense	VS-Vertraulich	UK-SECRET	NATO Confidential
"High" data	STG-Geheim	Secret Défense	Geheim		NATO Secret
"High" data	STG-Zeer Geheim	Très Secret Défense	Streng Geheim		Cosmic Top Secret

- 2 aspects of separation:
  - Data domains → STRONG* separation across the red lines:
    - Between HIGH and LOW
    - Between different HIGH domains
  - EM Emanations (TEMPEST)

* Strong =
- Physical separation
- High-assurance crypto
- High-assurance data exchange control

A1. Security Domains Separation (II)

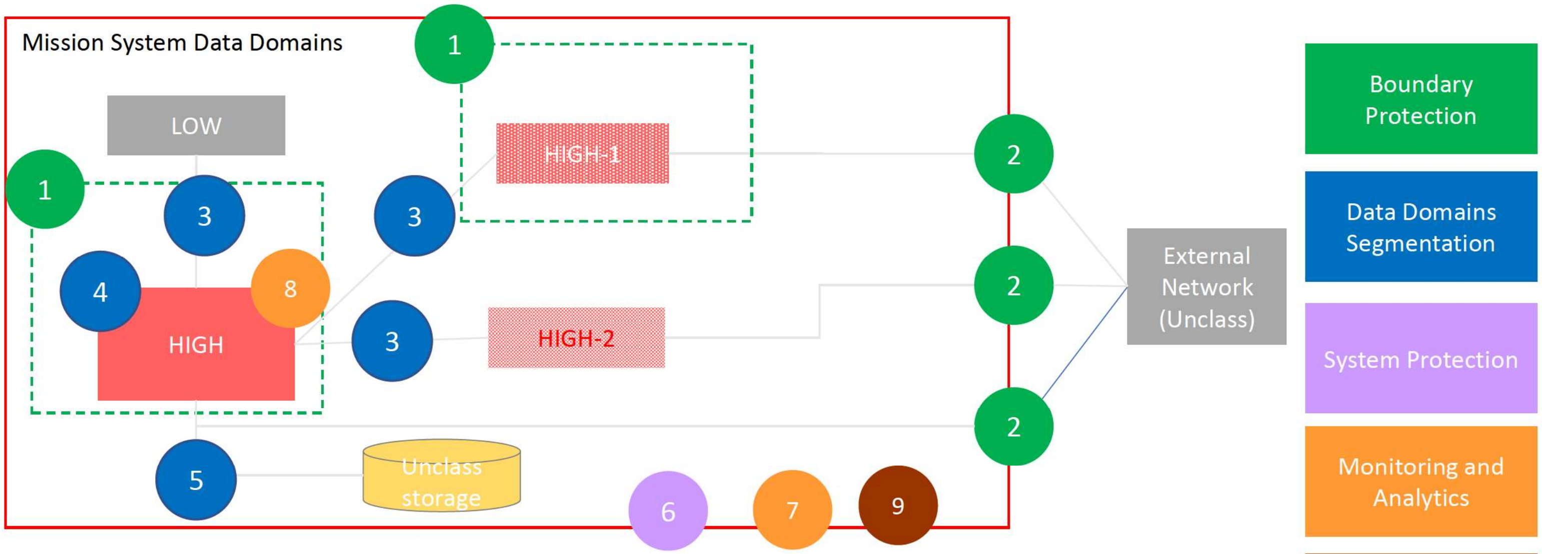
- Physically separated HW for RED and BLACK
- Controlled exchange of information between HIGH and LOW
  - From LOW to HIGH: prevent unauthorised access, check for malware
  - From HIGH to LOW: check information classification (labels, filters)



A1. Security Domains Separation (III)

- TEMPEST objectives
  - Avoid EM radiation correlated with HIGH Data
  - Avoid cross-talk between RED and BLACK cables
  - Avoid electric currents from RED to BLACK

A2. Defence in Depth



	Examples (NOT a complete list!)
1	Physical protection, TEMPEST, SecOPs
2	Data link encryption, Intrusion Prevention
3	Information Exchange Gateways, Firewalls
4	Labelling
5	Data at rest encryption
6	Hardening (HW/SW)
7	Antivirus
8	Intrusion Detection
9	Patch management and auditing

A3. Minimimal Attack Surface

- Least privilege, need-to-know
  - Access rights to information and system resources
    - Only for the necessary tasks
    - Only for the necessary time
- Minimize the extent of the HIGH domain
  - Avoid “classification creep”
- Network choke points
  - Minimize interfaces with external networks
- Minimize the SW footprint
  - Remove all unused functions and SW packages

Engineering Principles (I)

- E1. Use Evaluated Components
  - Certified security components
    - Security properties proven by a certification body (national, NATO, international)
    - → Simplify the accreditation process
  - Whenever possible choose components from an approved list:
    - E.g., Common Criteria (https://www.commoncriteriaportal.org/products/)
    - NATO, US: NIAP (https://www.niap-ccevs.org)
- E2. Secure System Development
  - Model-based engineering
  - Configuration tools
  - Static code analysis

Engineering Principles (II)

- E3. Secure Procurement
  - Downflow of Cyber-security requirements
  - Certified suppliers
- E4. Security Testing and Qualification
  - Specific tests must be developed for Cyber-security
    - In general: “Negative testing”
  - Tools
    - SW configuration testing tools
    - Dynamic program analysis
    - Network security analysis
    - Penetration testing
    - Cyber range testing

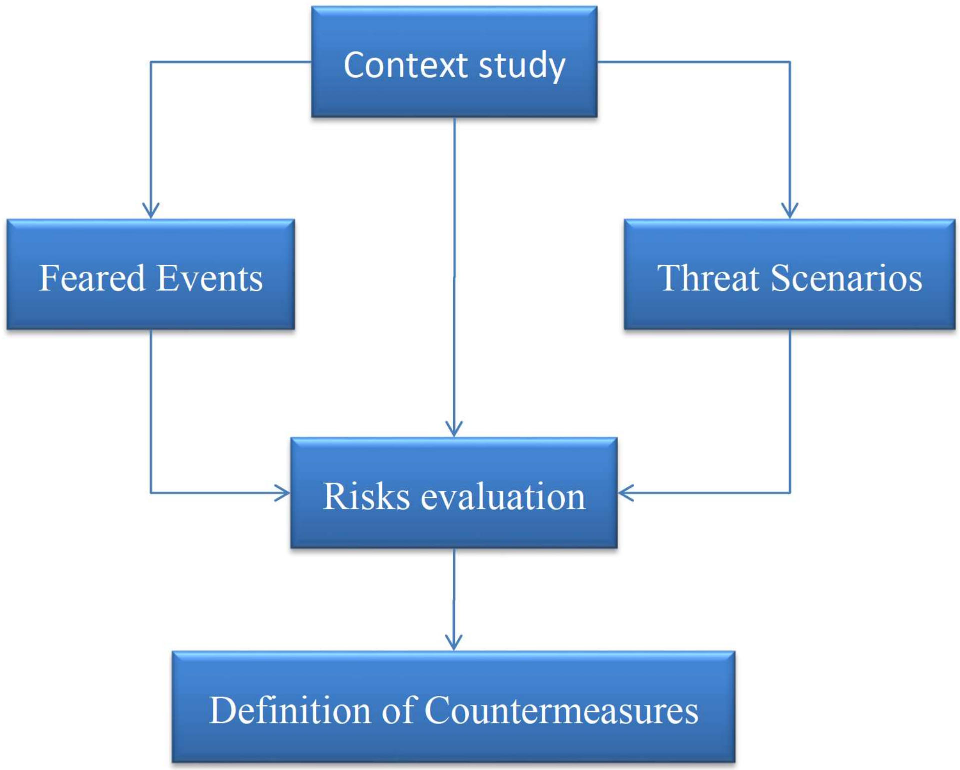
Analysis of operational context and high-level security requirements
Definition of architectural and engineering principles
Perform Security Risk Analysis
Define security architecture
Check accreditability

Acceptable Security Risk Analysis Methods (examples)

- ISO-27001 (Risk assessment) + ISO-27005 (Risk treatment)
  - https://en.wikipedia.org/wiki/ISO/IEC_27001
  - https://en.wikipedia.org/wiki/ISO/IEC_27005
- NIST 800-30
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- NL: VIR E&E
  - https://nl.wikipedia.org/wiki/Voorschrift_Informatiebeveiliging_Rijksdienst
- FR: EBIOS
  - https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/
- GE: BSI 200-3
  - https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard203/ITGStandard203_node.html
- UK: IS1&2 Information Risk Management and Technical Risk Assessment
  - https://en.wikipedia.org/wiki/HMG_Infosec_Standard_No.1

SRA Example: EBIOS

- Overview



SRA Example: EBIOS – Context Study (I)

- The scope of the SRA
  - Internal and external contexts, system boundaries
  - Assumptions
- Risk evaluation approach
  - Threat sources: internal/external, intent, capability
  - types of threats, and impacts
  - Definition of risk metrics
    - Risk = Severity x Likelihood
    - Risk = *f*(Severity, Likelihood), for any arbitrary *f*

Risk level		Severity			
		0	1	2	3
Likelihood	0	0	0	0	0
	1	0	1	1	2
	2	0	1	2	3
	3	0	1	3	3

  - Risk appetite
    - What is the maximum acceptable risk

SRA Example: EBIOS – Context Study (II)

- The target system
  - **Primary (Business) Assets (PA)**: immaterial assets, which are essential for the execution of the main operational flows.
    - Capabilities
    - Information
  - **Supporting Assets (SA)**: physical or functional components that enable, implement, store, or otherwise support a primary asset
    - Computers, networks
    - Sensors, effectors
  - **Links** between primary and supporting assets: show the dependencies between these two categories
- The list of existing controls
  - Most of the supporting assets have their main vulnerabilities already protected with standard controls
  - There are three categories of controls: prevention, protection, and restoration

SRA Example: EBIOS – Feared Events (FE)

- Describe what can go wrong with the PA
- FEs result in loss of PA value
- E.g.:
  - Loss of Availability and/or Integrity for capabilities
  - Loss of Confidentiality of communications
- Quantified in severity levels

SRA Example: EBIOS – Threat Scenarios (TS)

- Describe how FE can happen
- TS Result from SA vulnerabilities
- E.g.:
  - DoS
  - Inadvertent release or intentional exfiltration of confidential data
  - Fire in server room
- Quantified in likelihood levels

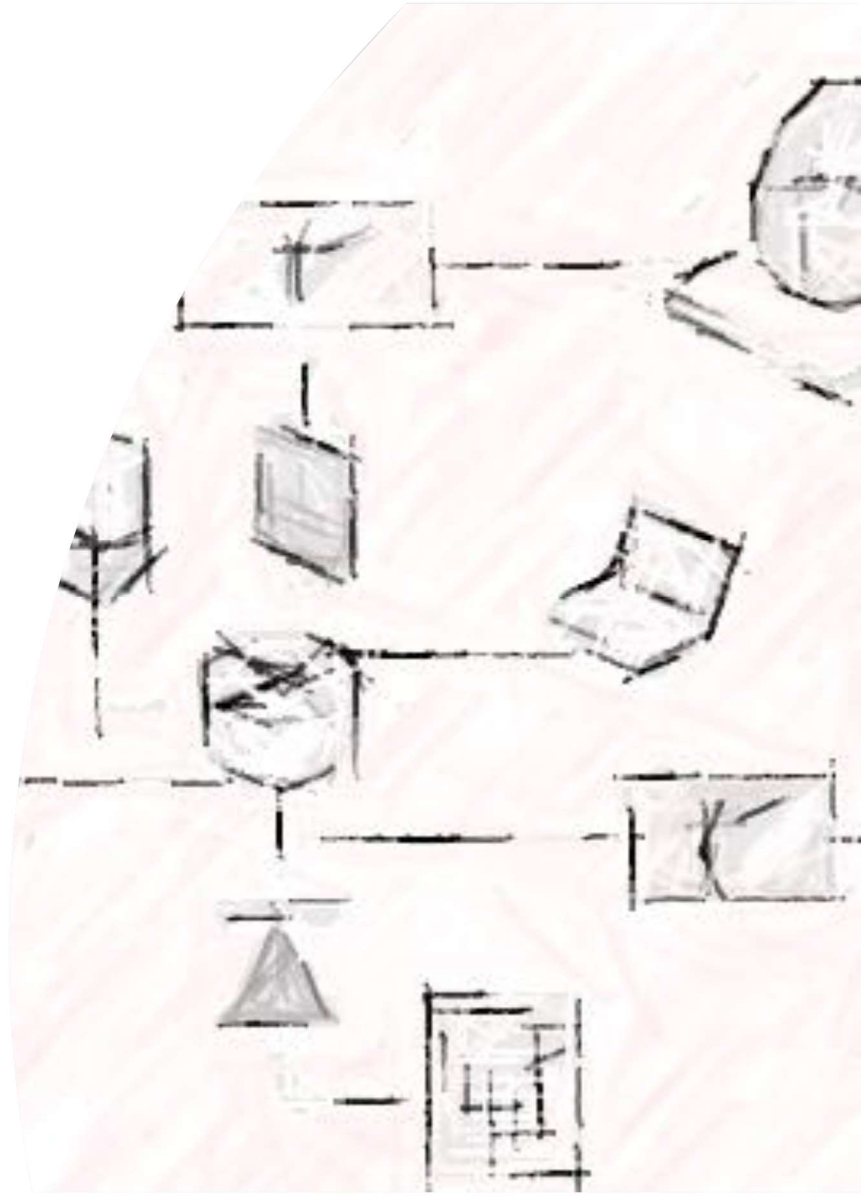
SRA Example: EBIOS – Risk Evaluation

- Quantify each risk based on the risk metric, severity, and likelihood
- Check risk appetite
  - If **Estimated_Risk** > **Risk_Appetite** then apply **Risk_Treatment**
- Risk Treatment:
  - Reduce
  - Avoid → not always possible
  - Accept
  - Transfer → not really applicable in defence systems

SRA Example: EBIOS – Definition of countermeasures

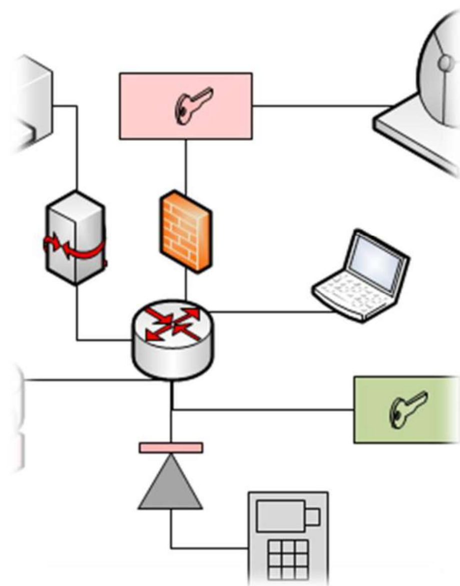
- For all risks which need to be reduced
- Targets:
  - Reduce impact of FE (examples):
    - Confidentiality → segmentation of data domains
    - Integrity → backups
    - Availability → redundancy
  - Reduce likelihood of TS (examples):
    - Confidentiality: encryption, access control
    - Integrity: error detection and correction (e.g. RAID)
    - Availability → (network) access control

Analysis of operational context and high-level security requirements
Definition of architectural and engineering principles
Perform Security Risk Analysis
Define security architecture
Check accreditability



Boundary Protection

- Encryption
  - Bitstream, tunnel, payload, message, file
  - Key storage
- Data flow control & network separation
  - Data Diodes: prevent flows from HIGH to LOW
    - Logical, Physical
    - Support for 2-way protocols?
  - Data Filters
    - Label-based
      - unstructured data
      - Label definition and binding
    - Value-based
      - Structured data
      - Payload values check
  - Firewalls, DMZ, Intrusion detection/prevention

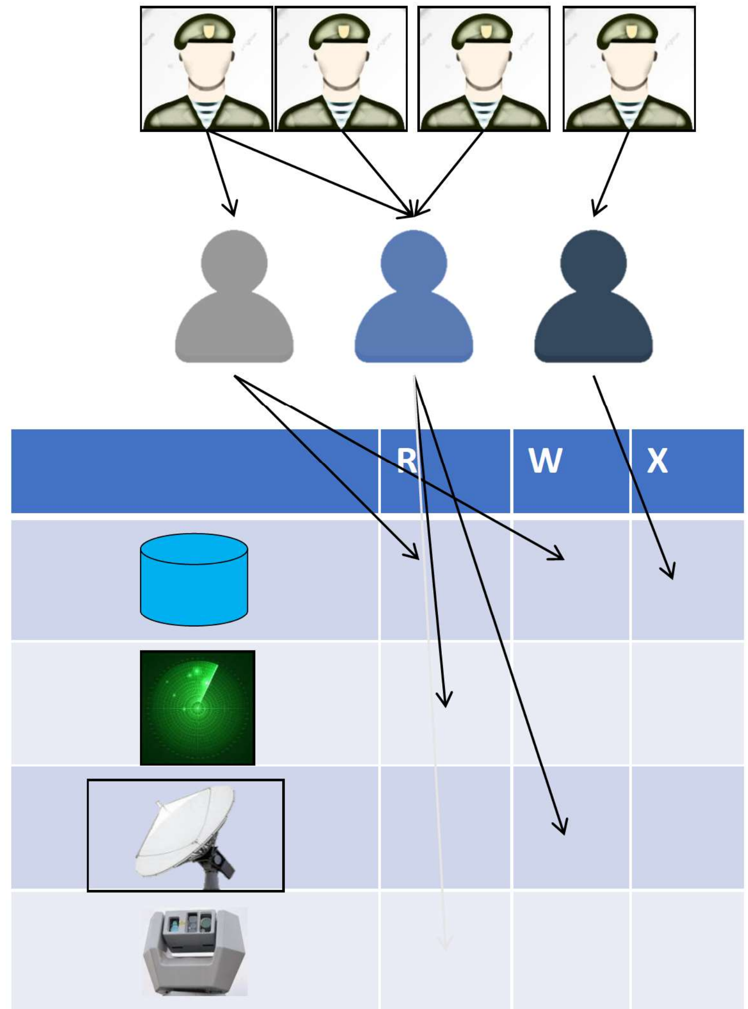


Endpoint Protection

- Computing Platform Security
  - Hardening
  - Anti-malware
- Data at rest protection
  - Confidentiality: Disk/file encryption
    - Mobile systems
    - Removable media
  - Integrity: RAID
- Secure virtualisation
  - All relevant countermeasures as for native
  - Note: Type 2 virtualisation is more vulnerable – limited use in NMS

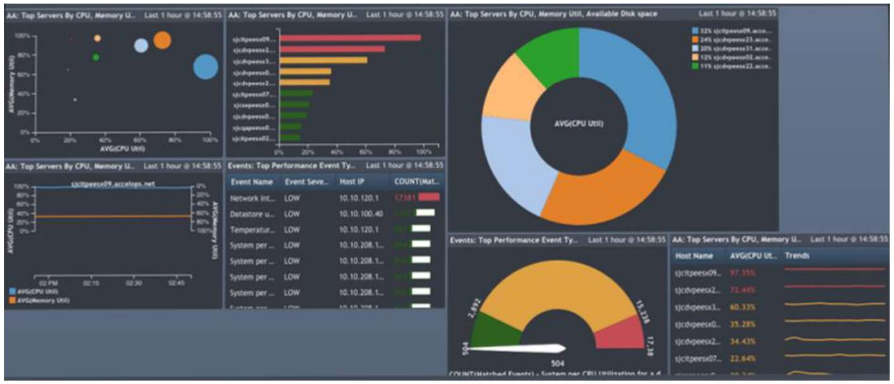
Identity and Access Management

- Identification
  - Directory services
- Authentication
  - Single factor and 2-factor,
  - Centralised
- Authorisation
  - Role-Based
  - Mandatory Access Control
  - Separation of concerns
  - Least privilege
- Accountability
  - Auditing of security events
  - Attention point on GDPR

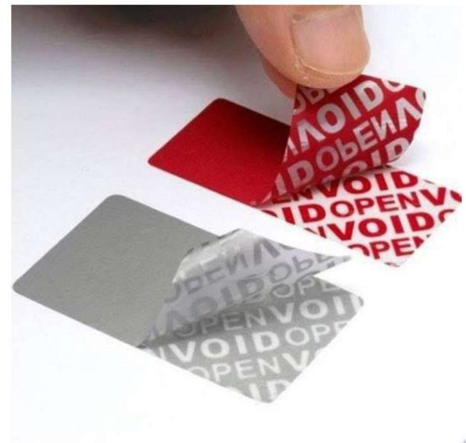


Cyber Incident Maangement

- Logging
  - Events
    - Operational events: who did what
    - Technical information: e.g. system faults
    - Security relevant events: e.g. failed logon attempts, sudo, indicators of compromise
  - Raw traffic
- Monitoring and auditing
- Analytics
  - Rule-based
  - Anomaly detection

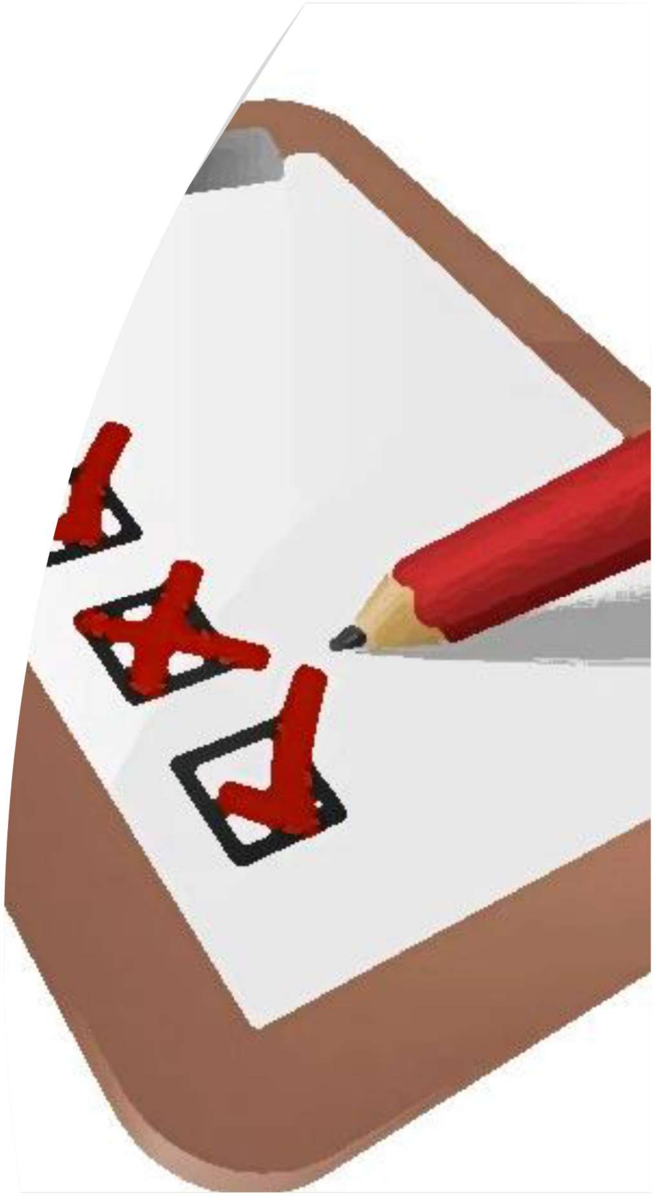


Physical Protection



- Often underestimated
- Locks, alarms, CCTV
- Tamper evident seals
- Storage media destruction
- TEMPEST
  - = unintended emanation of signals correlated with classified data
  - Through EM radiation or electric currents in cables or metallic ducts
  - Countermeasures
    - Shielding
    - Filtering, media conversion
    - Distance

Analysis of operational context and high-level security requirements
Definition of architectural and engineering principles
Perform Security Risk Analysis
Define security architecture
Check accreditability



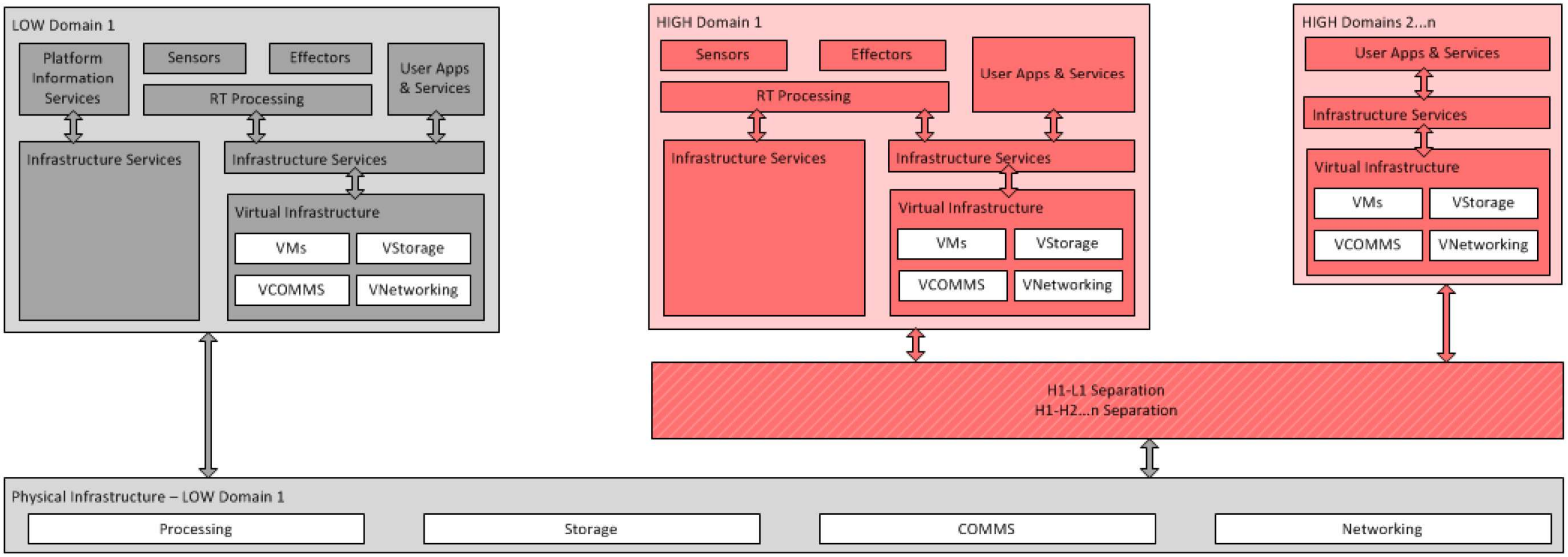
Final steps

- Check and document compliance with relevant regulations
  - National
  - International: EU, UN, NATO (depending on the intended missions)
- Define Security Operating Procedures (SecOPs)
  - User on- and off-boarding
  - Backup storage
  - Updating process
  - Regular checks
  - …
- Document residual risks
  - No security solution is perfect
  - The users must be aware of these risks and <u>accept</u> them

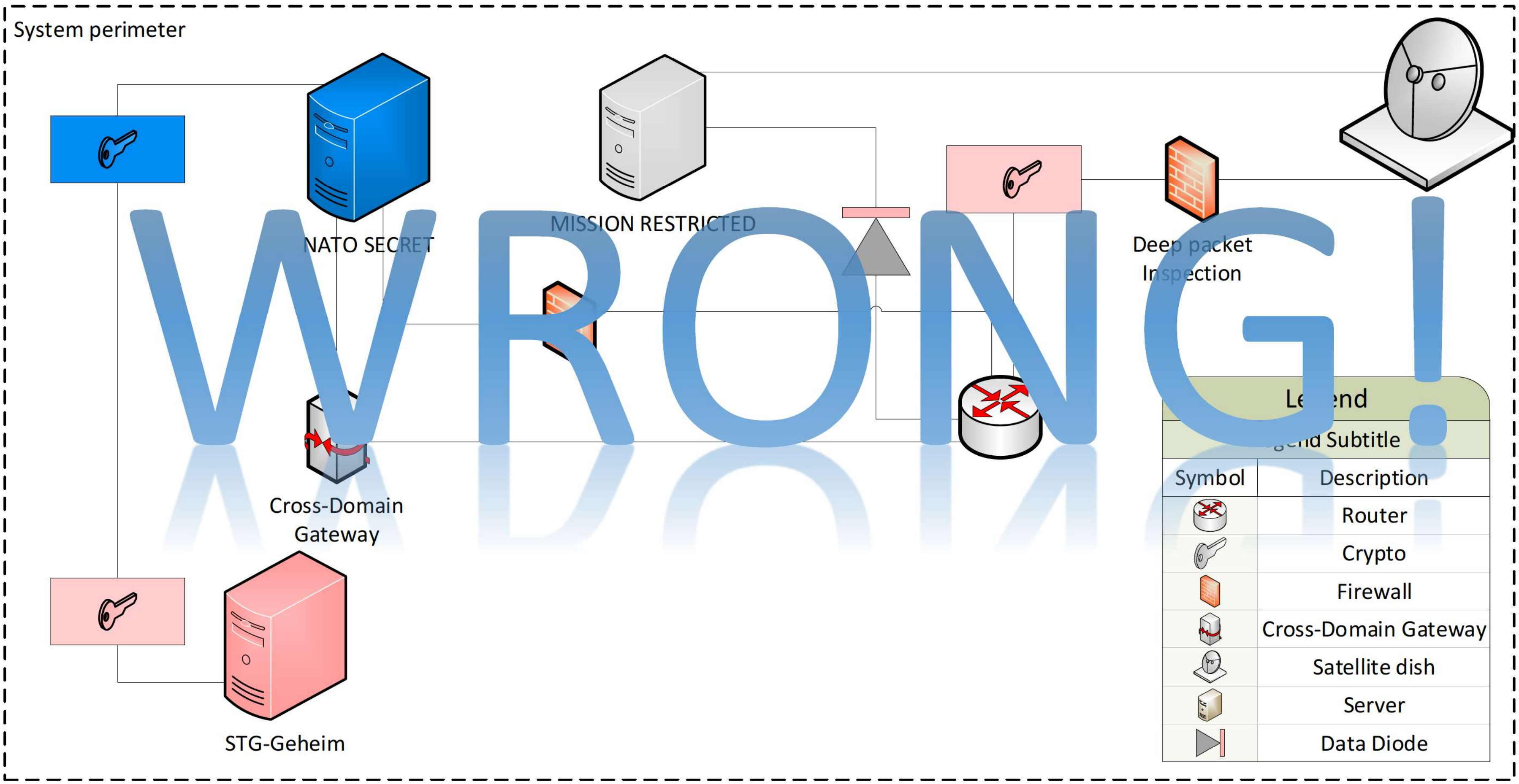
Quiz

Virtualisation

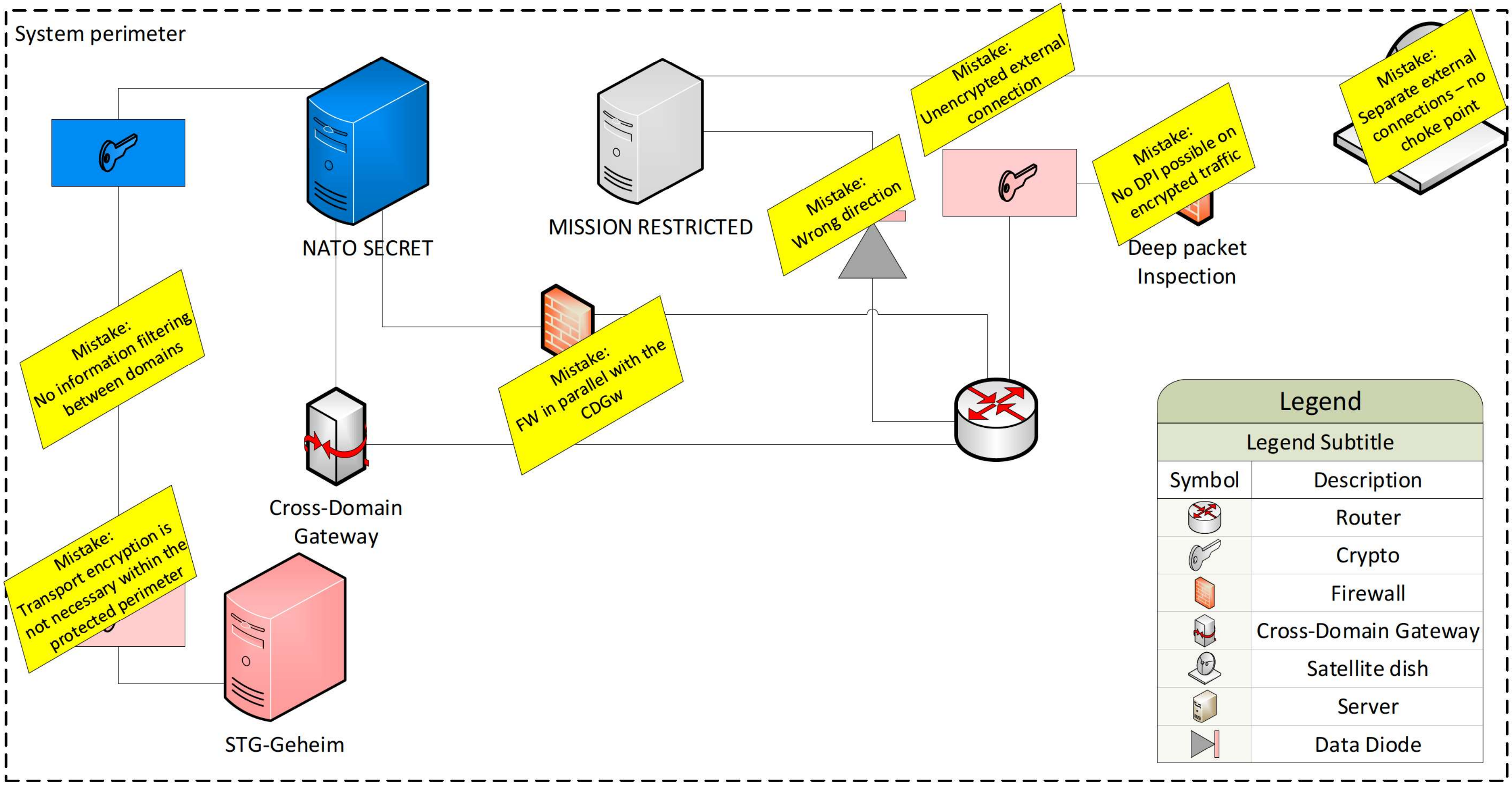
- Is this architecture accreditable?
  - Yes/No?
  - Why?



What’s wrong with this picture?



What’s wrong with this picture?



Name 2 reasons why:

- DevOps methodology is (not) applicable for NMS
- Cloud and Edge paradigms are (not) practical
- Account lockout after *n* unsuccessful logon attempts is (not) desirable
- Discretionary Access Control policies are (not) adequate
- Biometrics-based access control for the CMS is (not) convenient
- Quantum computing will (not) have a big impact on NMS security