

Safety and Security



Odd Nordland,
Maria Bartnes Line, Lillian Røstad, Inger Anne Tøndel

SINTEF ICT
Trondheim
Norway

SINTEF



■ Largest independent R&D organisation in Scandinavia

■ Located in Trondheim (HQ) and Oslo

- offices in Bergen, Stavanger, Ålesund, Houston (TX), Warsaw, Skopje...

■ 7 divisions

- Information and Communication Technology
- Technology and Society
- Health
- Oil and Energy
- Materials and chemistry
- Marine
- Building technology



Safety and Security



■ Introduction

- The concepts of safety and security have a lot in common
- But there are communication problems between them
 - Terminology is not agreed
 - Safety: 4 different definitions in 7 sources
 - Security: 6 different definitions in 6 sources!
 - Many languages have one word for both
 - Germanic languages
 - Romanic languages
 - Chinese
- So what are safety and security?



Safety and Security

- A “working definition”:
 - We have a “system” in an “environment”
 - The system can have an undesirable effect on its environment
 - The environment can have an undesirable effect on the system
- SAFETY:
 - The inability of the system to have an undesirable effect on its environment
- SECURITY
 - The inability of the environment to have an undesirable effect on the system



Safety and Security

■ Terms: Hazard vs. Threat

- Hazard – a situation that can result in undesirable effects for health, life or assets (i.e. the environment)
- Depending on likelihood, an associated risk can be defined
 - risk also includes the severity of the “undesirable effects”
- Safety measures concentrate on reducing risk, i.e. reducing the likelihood of a hazard, its severity, or both
- Threat – a situation that can result in undesirable effects for the system
 - E.g. integrity, functionality, dependability...
- Likelihood can be 100% (intentional attacks)
- Security measures concentrate on reducing the consequences

Safety and Security



■ Terms: Failure vs. Incident

- Failure – a safety measure does not function correctly
 - Probability can be calculated from technical properties (MTBF etc.)
 - Will not always result in loss of safety: “permissible” failures are undesirable, but can be accepted
 - e.g. emissions within legal limits
- Incident – any event that can “*have a significant probability of compromising ... security*”
 - Probability assumed to be 100% - incidents happen!
 - Can be intentional
 - Configuration changes
 - Modifications
 - ...

Safety and Security



■ Terms: SIL vs. EAL

- SIL – Safety Integrity Level
 - please do not say “SIL level”!
- Based on failure rates of safety functions
 - Not on the failure rates of the equipment that implements the function
- Generally 5 SILs
 - 4=high, 1=low, 0=no safety relevance
- EAL – Evaluation Assurance Level
 - Defined in the Common Criteria
- 7 EALs
 - 7=high, 1=low, no 0



Safety and Security

- Techniques: Risk analysis
 - HAZOP
 - ETA
 - FTA
 - FMEA
 - FMECA
 - Threat modelling
 - Attack trees
 - Misuse cases

Safety and Security



- Techniques: Barriers vs. Perimeter protection
 - (Safety) Barriers from the middle outwards
 - Integrated safety functions
 - Redundancy/diversity
 - Time control
 - Watch dogs
 - Perimeter protection
 - Access control
 - Intrusion detection
 - Zones/Islands



Safety and Security

- Techniques: Safety and Security Testing
 - Safety Qualification Testing
 - Field trials / provisional operation
 - Supplement to analyses and calculations
 - Security testing
 - Black box attacks
 - White box attacks
 - Penetration testing

Safety and Security



- Techniques: Self-test vs. Integrity protection
 - Safety related systems perform self-tests to ensure their own correct functionality
 - Self-correction can also be applied
 - e.g. use checksums and parity to determine data errors and correct modified data
 - e.g. use self-sealing tyres to avoid punctures
 - Integrity protection
 - Continuous monitoring of status/modifications
 - Generation of alarms when unauthorised changes are detected

Safety and Security



■ Techniques: Logging

- Safety logs are used to be able to reconstruct the series of events that led to an incident
- Used after the fact
 - Corrupted data does not compromise safety
- Security logs can also be used to detect attacks
- Used during attacks
 - Corrupted data can compromise security

Safety and Security



- Techniques: Software development
 - Safety related standards contain detailed prescriptions and recommendations
 - e.g. IEC 61508 identifies “*mandatory*”, “*highly recommended*”, “*recommended*” and “*not recommended*”(!) measures and techniques
 - Security related standards are less specific on software
 - Security is to be considered in all phases of the life cycle
 - No explicit recommendations
 - Include “patch management” vs. “new issue”

Safety and Security



■ Certification

- Safety certification is performed by an Independent Safety Assessor (ISA) according to the applicable safety standard
 - The certification process is independent of the targeted SIL
 - A higher SIL cannot be achieved by a renewed certification, the system has to be modified
- Security certification is performed according to the Common Criteria (CC) and the Common Evaluation methodology (CEM)
 - The certification process depends on the targeted EAL
 - A higher EAL can be achieved by a renewed certification without modifying the system

Safety and Security



■ Differences

- Direction of focus
 - Safety protects the environment
 - Security protects the system
- Assets
 - Safety addresses health, life and the natural environment
 - Security addresses financial assets, confidentiality, privacy, rights
- Terminology
 - Some terms are used differently, some different terms mean the same
- Testing
 - Safety testing cannot always be done on the full scale system
 - Security testing can



Safety and Security

■ Potential synergy

- Safety techniques are “proven in use”
 - Many can be adapted to security
- Testbeds
 - Safety is often tested with simulators
 - Simulator technology can be extended to security
- SILs and EALs
 - SILs define requirements on the system, EALs define requirements on the assessment
 - Define “Security Requirement Levels” and “Safety Assessment Procedures”
- Security breaches can compromise safety, safety breaches can compromise security
 - Mutual standards, procedures etc. needed