Security – An Introduction

Paolo PRINETTO
Director
CINI Cybersecurity National Laboratory
Paolo.Prinetto@polito.it
Mob. +39 335 227529

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

License & Disclaimer

License Information

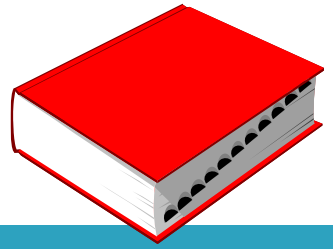
Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Goals

- Introducing the concept of Security
- Providing a taxonomy

Notation

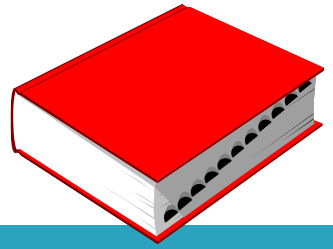


- The slides in which a dictionary is shown at the top right, as in this one, contain *definitions*.

Outline

- Introduction
- Dependability
- Safety
- Security
- Cybersecurity

Security



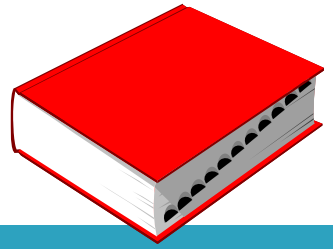
- The freedom from those conditions that can cause loss of assets with unacceptable consequences

["Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems,"
NIST, Tech. Rep. NIST.SP.800-160 Volume 1, Nov. 2016:
https://doi.org/10.6028/NIST.SP.800-160v1]

Practical implications

- It’s imperative that the specific scope of security must be clearly defined by stakeholders in terms of:
  - the *assets* to which security applies
  - the *consequences* against which security is assessed.

Assets



- The term *asset* refers to an item of value to stakeholders driven by life cycle concerns that include, but are not limited to, those concerns of business or mission.

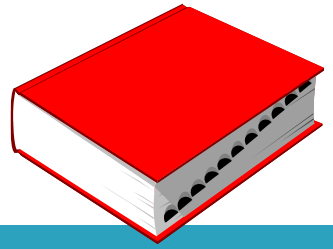
Asset classifications

- An asset may be
  - *tangible* (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component)
  - *intangible* (e.g., data, information, software, trademark, copyright, patent, intellectual property, image, or reputation).

Asset consequences

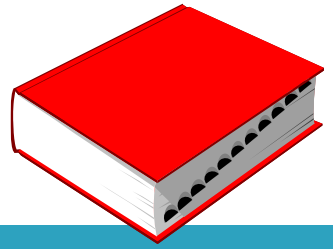
- Assets have associated consequences of loss that determine their value, criticality, irreplaceability, and the degree to which they are relied upon to achieve mission, business, or stakeholder goals and objectives.
- From these characteristics, the appropriate protections are engineered to provide for system security performance and effectiveness against asset loss and the associated consequences.

Security



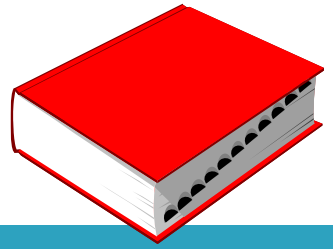
- The state of being free from *dangers* or *threats*

Danger



- The possibility of suffering harm or injury

Threat



- A statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done

Security, Danger, Threat

- They get different meanings in different domains
- In the seguel we focus on:
  - *IT - Information Technology*
  - *OT - Operational Technology,*

  only.

IT - Information Technology

- It refers to anything related to computing technology
- It focuses on the storage, recovery, transmission, manipulation and protection of data.

OT - Operational Technology

- *“Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.”*

[Gartner]

Protecting what

Protecting what

- People
- Environment
- Objects
- Computers
- Information
- Cyberspace

Protecting what

- People
- Environment

SAFETY

- Objects
- Computers
- Information
- Cyberspace

Protecting what

- People
- Environment

SAFETY

- Objects
- Computers
- Information
- Cyberspace

SECURITY

Protecting what

- People
- Environment

SAFETY

- Objects
- Computers
- Information

SECURITY

- Cyberspace

CYBERSECURITY

Protecting what

- People
- Environment

SAFETY

- Objects
- Computers
- Information

SECURITY

- Cyberspace

CYBERSECURITY

} *DEPENDABILITY*

Protecting what

- People
- Environment

SAFETY

- Objects
- Computers
- Information

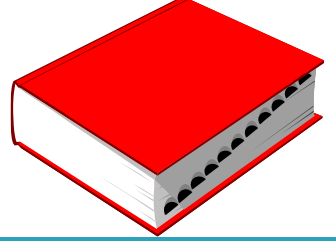
SECURITY

- Cyberspace

CYBERSECURITY

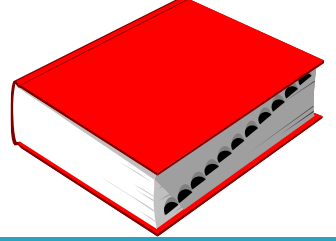
DEPENDABILITY

Dependability



- Property of a system that allows reliance to be placed justifiably on service it delivers

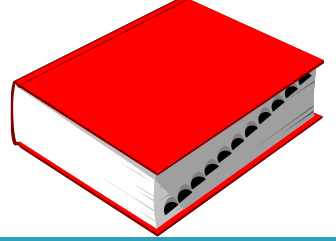
Dependability



- The collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance

["Quality Concepts and Terminology," part 1: Generic Terms and Definitions, Document ISO/TC 176/SC 1 N 93, Feb. 1992]

Dependability



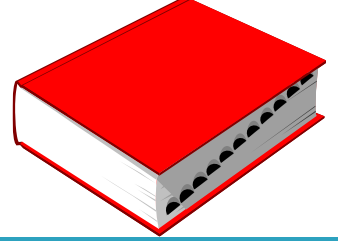
- The extent to which the system can be relied upon to perform exclusively and correctly the system task(s) under defined operational and environmental conditions over a defined period of time, or at a given instant of time

["Industrial-Process Measurement and Control - Evaluation of System Properties for the Purpose of System Assessment", Part 5: Assessment of System Dependability, Publication 1069-5, Int'l Electrotechnical Commission (IEC) Secretariat, Feb. 1992]

The Dependability Tree

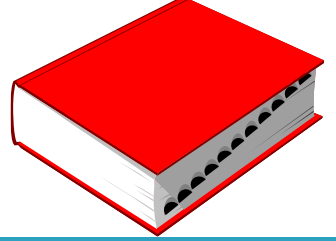
- A systematic exposition of the concepts of dependability consists of three parts:
  - the *threats* to
  - the *attributes* of
  - the *means* by which dependability is attained

Threats (for Dependability)



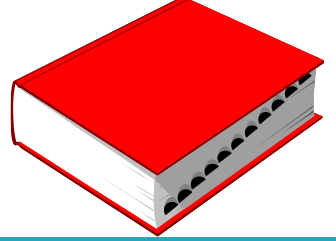
- Undesired (not unexpected) circumstances causing or resulting from undependability (reliance cannot or will not any longer be placed on the service)

Attributes



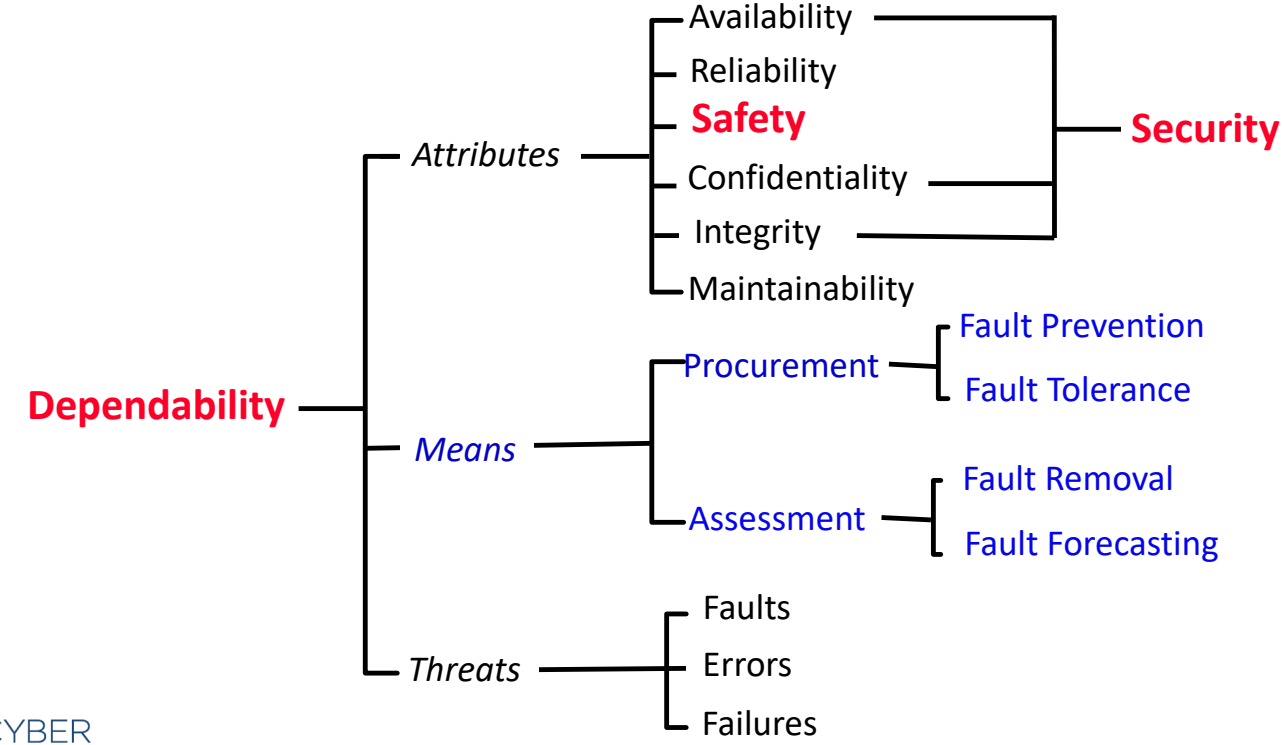
- Properties expected from the system and according to which assessment of service quality resulting from threats and means opposing to them is conducted

Means



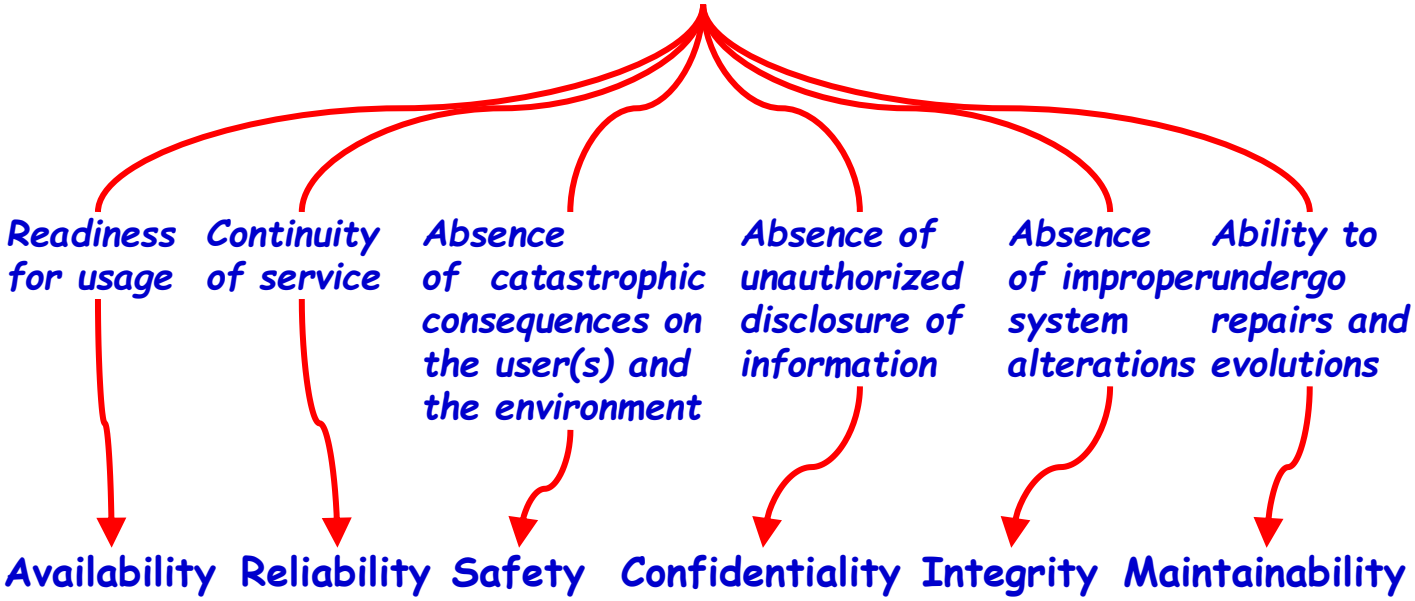
- Methods and techniques enabling:
  - to provide service on which reliance can be placed
  - to have confidence in its ability

The *Dependability Tree*



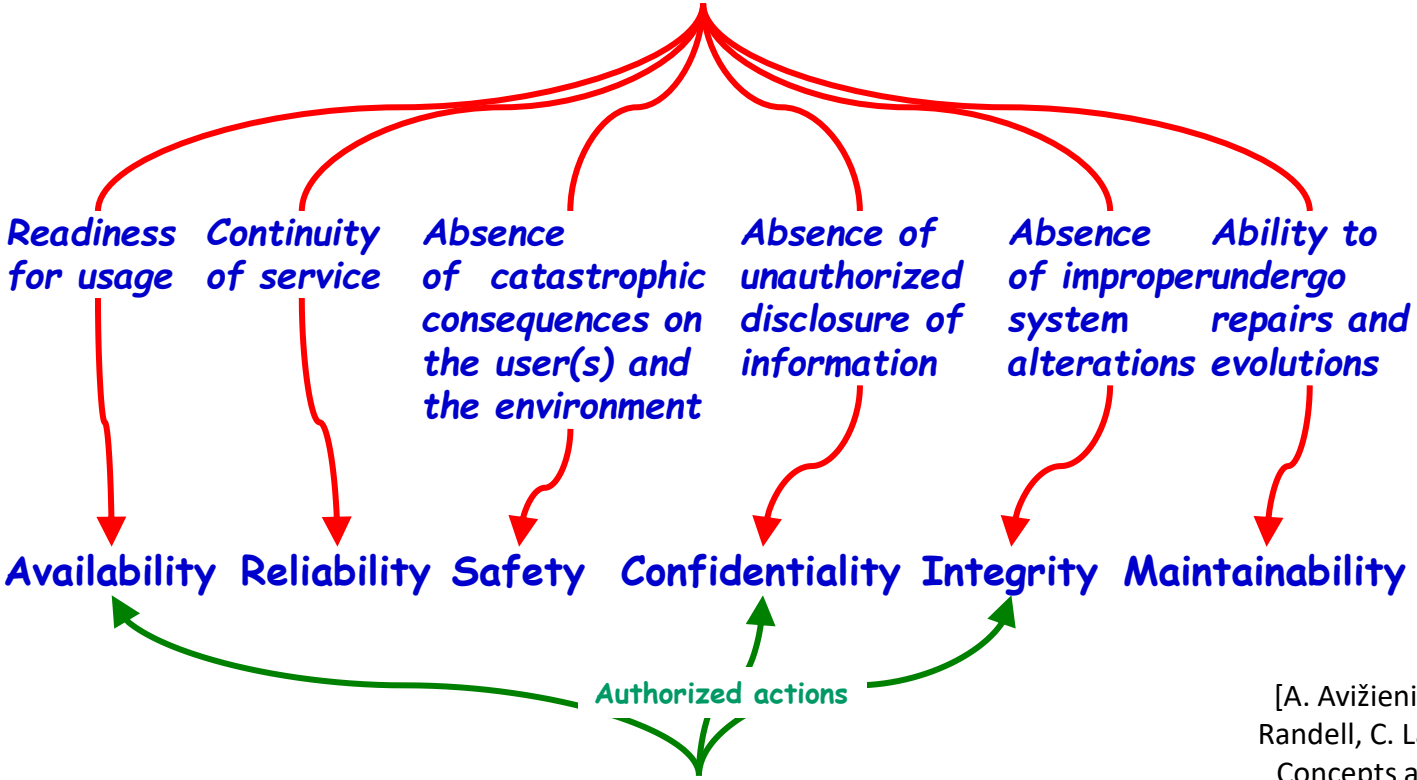
[A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr: "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE TDSC, 1 (1), pp. 11-33, Jan-Mar 2004]

Dependability



[A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr: "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE TDSC, 1 (1), pp. 11-33, Jan-Mar 2004]

Dependability



Security

Absence of unauthorized access to, or handling of, system state

[A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr: "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE TDSC, 1 (1), pp. 11-33, Jan-Mar 2004]

Protecting what

- People
- Environment

SAFETY

- Objects
- Computers
- Information

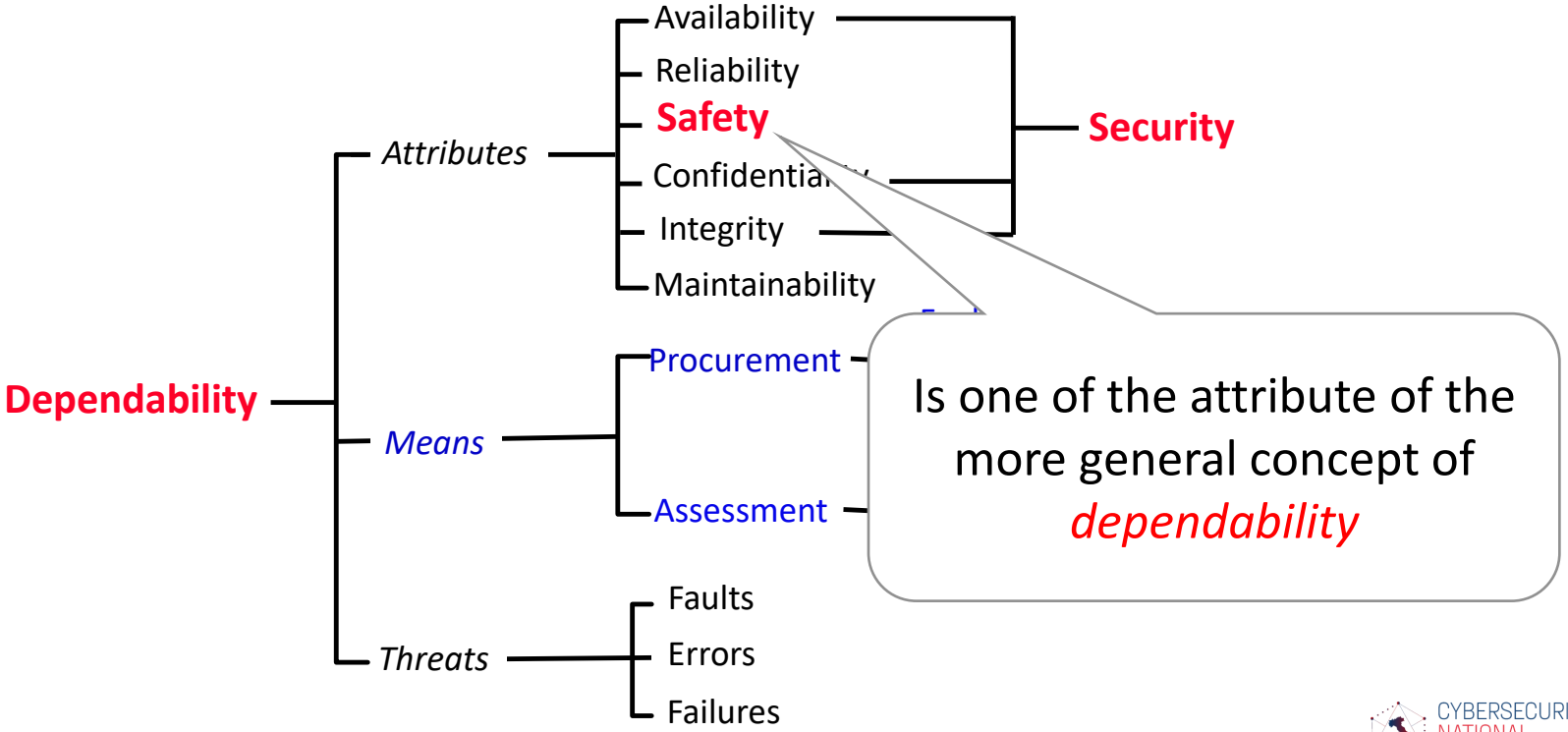
SECURITY

- Cyberspace

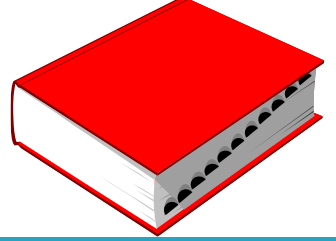
CYBERSECURITY

} *DEPENDABILITY*

The *Dependability Tree*

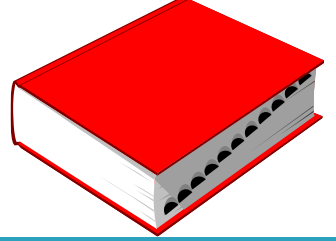


Safety



- Property of a system that reflects the system's ability to operate, normally or abnormally, without danger of causing human injury or death and without damage to the system's environment

Safety



- The probability, S(t), that a system will either perform its function correctly or will discontinue its function in a manner that does not disrupt the operation of other systems or compromise the safety of any people associated with the system

Protecting what

- People
- Environment

SAFETY

- Objects
- Computers
- Information

SECURITY

- Cyberspace

CYBERSECURITY

} *DEPENDABILITY*

Computer security

- Measures and controls that ensure *confidentiality*, *integrity*, and *availability* of information system assets including hardware, software, firmware, and information being processed, stored, and communicated

[The NIST Internal/Interagency Report NISTIR 7298
- Glossary of Key Information Security Terms, May 2013
(**NIST** = U.S. National Institute of Standards and Technology)]

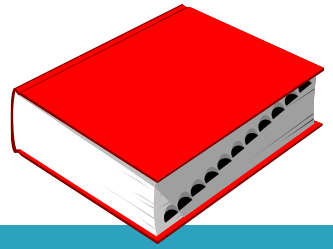
Computer security

- Deals with the prevention and detection of unauthorized actions by users of a computer system

Computer security

- Deals with the prevention and detection of unauthorized actions by users of a computer system
- *Authorization* is central to definition
- Sensible only relative to a *security policy*, stating who (or what) may perform which action

Information security



- It deals with information, independently of the underlying computer systems

Information security - Remark

- Information is more general than data
- Data convey information
- But information may also be revealed, without revealing data, e.g., by statistical summaries
- Constitutes a basic right: protection of self (possessions, ...)

Protecting what

- People
- Environment

SAFETY

- Objects
- Computers
- Information

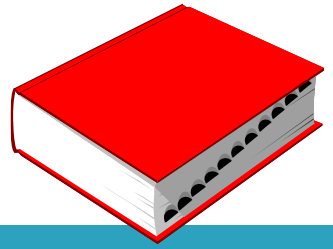
SECURITY

- Cyberspace

CYBERSECURITY

} *DEPENDABILITY*

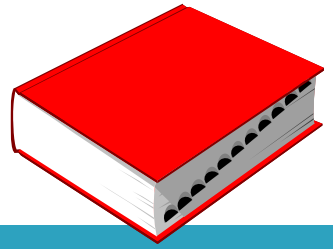
Cybersecurity



- That practice that allows an entity (organization, citizen, nation, ...) to protect its physical assets and confidentiality, integrity and availability of its information from threats that come from *cyberspace*

[standard ISO/IEC 27000:2014 & ISO/IEC 27032:2012]

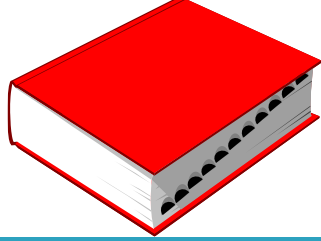
Cybersecurity



- That practice that allows an entity (organization, citizen, nation, ...) to protect its physical assets and confidentiality, integrity and availability of its information from threats that come from *cyberspace*

See lecture:
CS_1.2 - Cybersecurity – Definition & relevance

The concept of *Failure*



- In general, failure is defined as not meeting a specified requirement, objective, or performance measure.

The concept of Failure

- With respect to complexity, uncertainty, and security being an emergent property of a system, failure can be defined in terms of:
  - the *behavior* exhibited by the system
  - the *interactions* among the elements that compose the system
  - the *outcomes* produced by the system.

System security failure

- A system security failure is defined as not meeting the security-relevant requirements, objectives, and performance measures, to include exhibiting unspecified behaviour, exhibiting unspecified interactions, or producing unspecified outcomes, where there is security-relevance.

[NIST, Tech. Rep. NIST.SP.800-160 Volume 1, Nov. 2016: https://doi.org/10.6028/NIST.SP.800-160v1]

Different “perceptions”

- The “Dependability community” usually refers to the so called *3-universe model* to outline the *threat chain* that can lead to a failure:

3-universe threat model

- If, during the design phase, appropriate tolerance mechanisms have not been foreseen and introduced in the system, a *fault* may lead to an *error* which, in turn, may lead to a *failure*

Different “perceptions”

- The “Software community” usually resort to other definitions:

Different “perceptions”

IEEE Standard Glossary of Software Engineering Terminology

- The “Software community” usually resort to other definitions:
  - *Bug*: an error or a fault that causes a failure.
  - *Error*: a human action that produces an incorrect result.
  - *Fault*: an incorrect step, process, or data definition in a computer program.
  - *Failure*: the inability of software to perform its required functions within specified performance requirements.

Concluding remark

- The various dependability dimensions can have conflicting requirements...

Door opening mechanism

Safety Requirement

Doors shall open when car is flipped.

Door opening mechanism

Safety Requirement

Doors shall open when car is flipped.

Solution

Install pressure sensor at the roof of the car.

Door opening mechanism

Safety Requirement

Doors shall open when car is flipped.

Solution

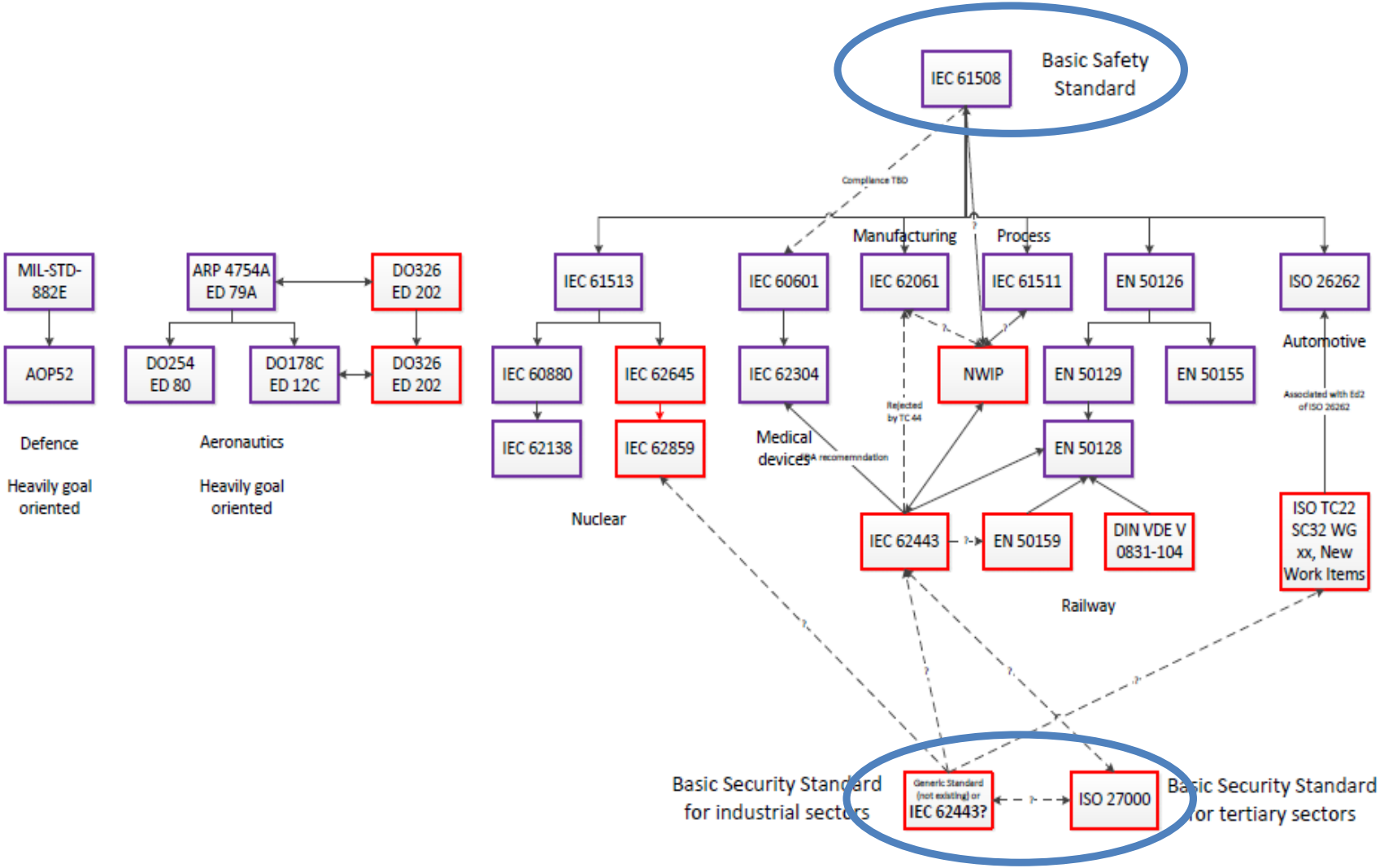
Install pressure sensor at the roof of the car.

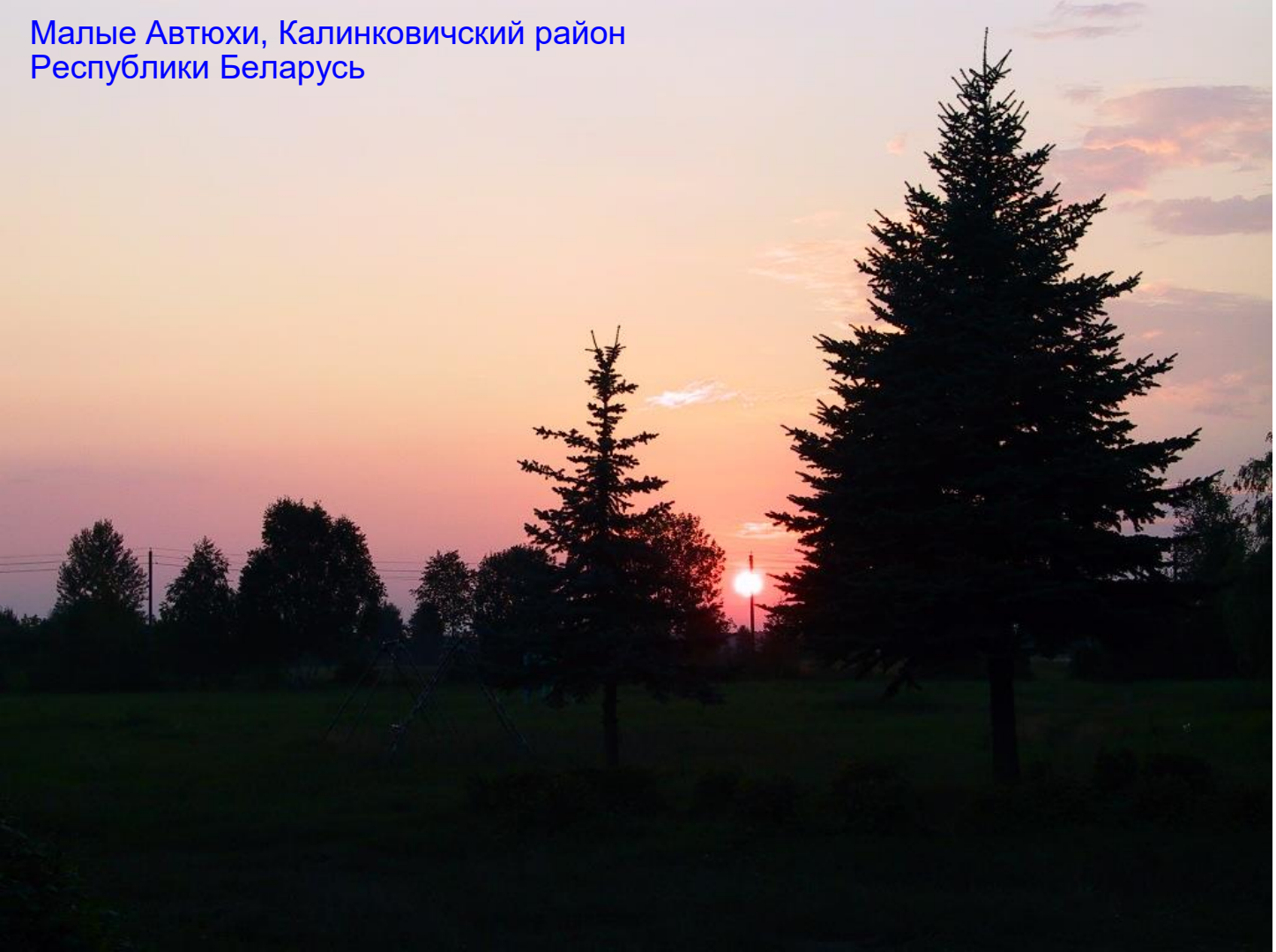
Solution has serious security consequences

Unauthorized entry by jumping on the car.

The role of Standars

- Nevertheless, a significant convergence of standards has been achieved…


IEC 61508
Basic Safety Standard
Compliance TBD
Manufacturing
Process
MIL-STD-882E
AOP52
Defence
Heavily goal oriented
ARP 4754A ED 79A
DO326 ED 202
DO254 ED 80
DO178C ED 12C
DO326 ED 202
Aeronautics
Heavily goal oriented
IEC 61513
IEC 60880
IEC 62645
IEC 62138
IEC 62859
Nuclear
IEC 60601
IEC 62304
Medical devices
IEC 62061
IEC 61511
NWIP
Rejected by TC 44
EA recommendation
IEC 62443
EN 50126
EN 50129
EN 50155
EN 50128
EN 50159
DIN VDE V 0831-104
Railway
ISO 26262
Automotive
Associated with Ed2 of ISO 26262
ISO TC22 SC32 WG xx, New Work Items
Basic Security Standard for industrial sectors
Generic Standard (not existing) or IEC 62443?
ISO 27000
Basic Security Standard for tertiary sectors



Paolo PRINETTO

Director
CINI Cybersecurity National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it