

Security – An Introduction

1

Paolo PRINETTO

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



<https://cybersecnatlab.it>

License & Disclaimer

2

License Information

This presentation is licensed under the Creative Commons BY-NC License



To view a copy of the license, visit:

<http://creativecommons.org/licenses/by-nc/3.0/legalcode>

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.

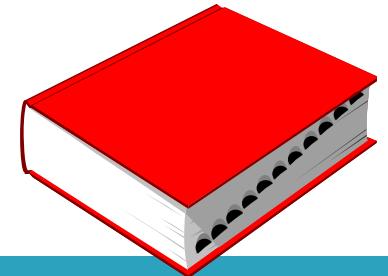
Goals

3

- Introducing the concept of Security
- Providing a taxonomy

Notation

4



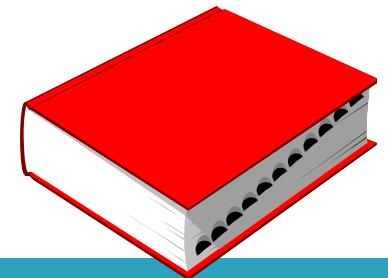
- The slides in which a dictionary is shown at the top right, as in this one, contain *definitions*.

Outline

5

- Introduction
- Dependability
- Safety
- Security
- Cybersecurity

Security



6

- 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>]

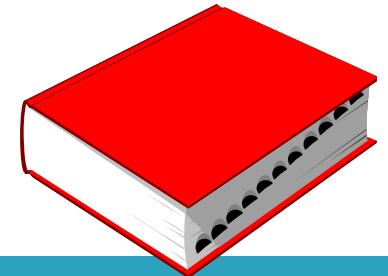
Practical implications

7

- 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

8



- 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

9

- 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).

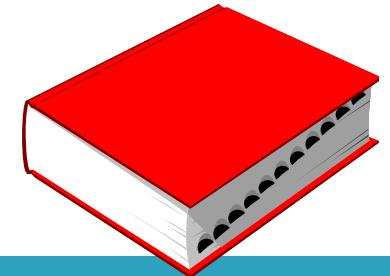
Asset consequences

10

- Assets have associated consequences of loss that determine their value, criticality, irrereplaceability, 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

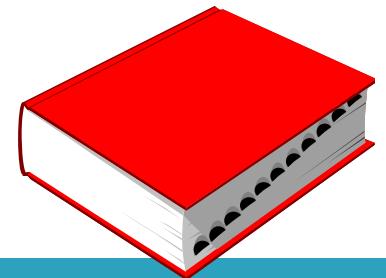
11



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

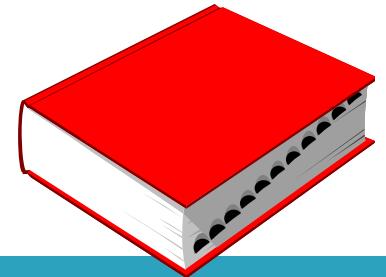
Danger

12



- The possibility of suffering harm or injury

Threat



13

- 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

14

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

IT - Information Technology

15

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

OT - Operational Technology

16

- “*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

17

Protecting what

18

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

Protecting what

19

- People
- Environment

SAFETY

- Objects
- Computers
- Information
- Cyberspace

Protecting what

20

- People
- Environment

SAFETY

- Objects
- Computers
- Information
- Cyberspace

SECURITY

Protecting what

21

- People
- Environment

SAFETY

- Objects
- Computers
- Information

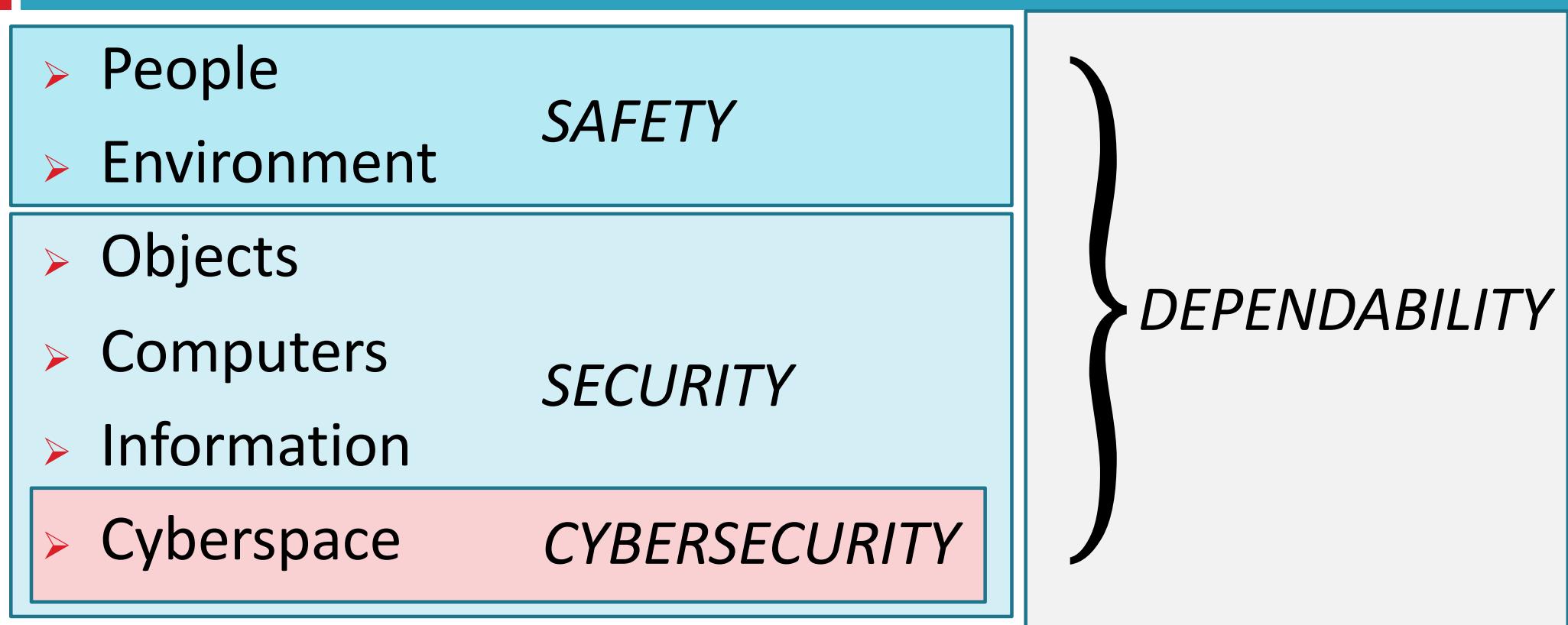
SECURITY

- Cyberspace

CYBERSECURITY

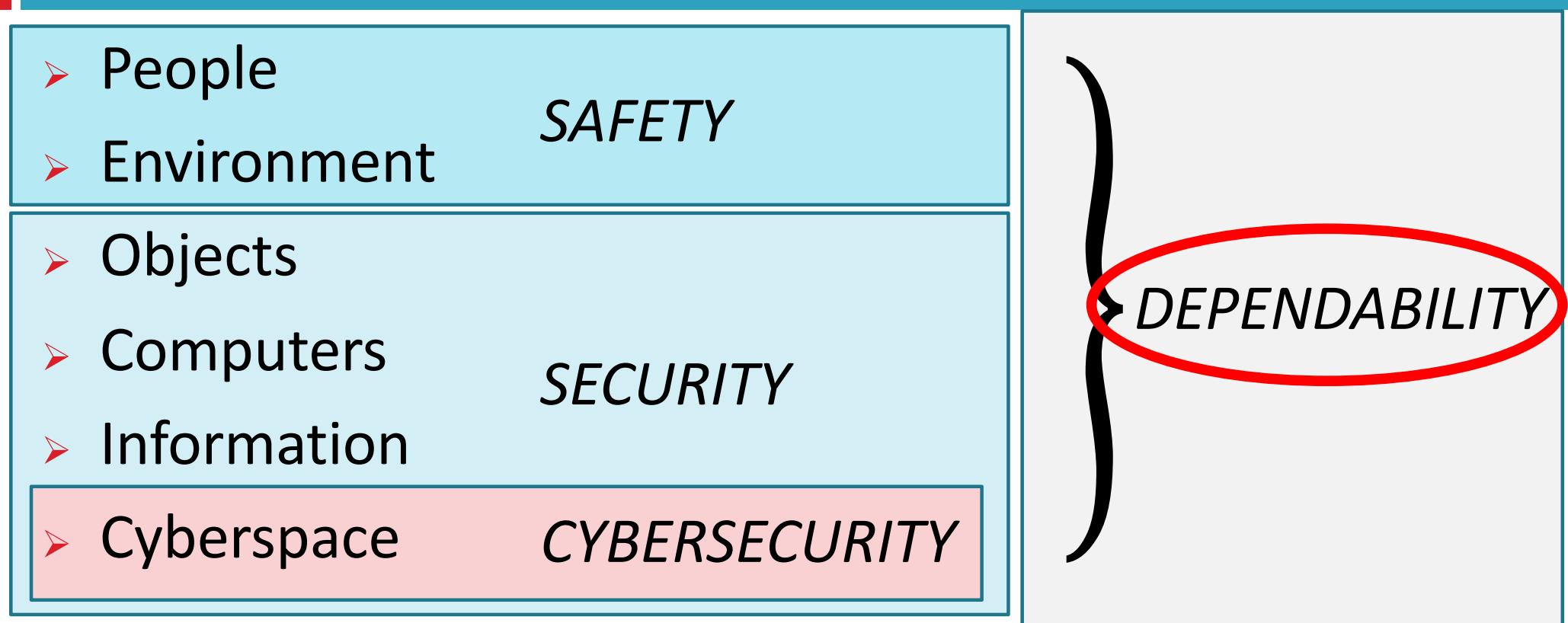
Protecting what

22



Protecting what

23



Dependability



24

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

Dependability

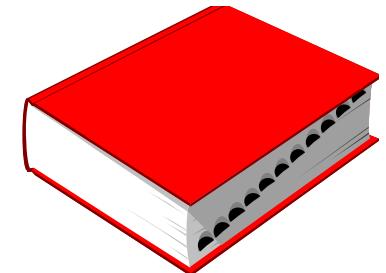


25

- 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



26

- 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

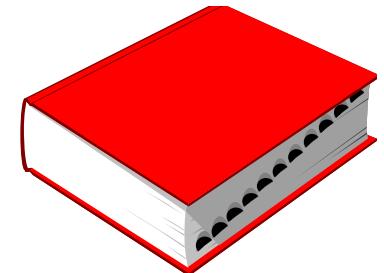


Threats (for Dependability)

28

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

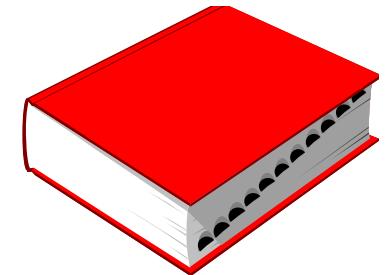
Attributes



29

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

Means

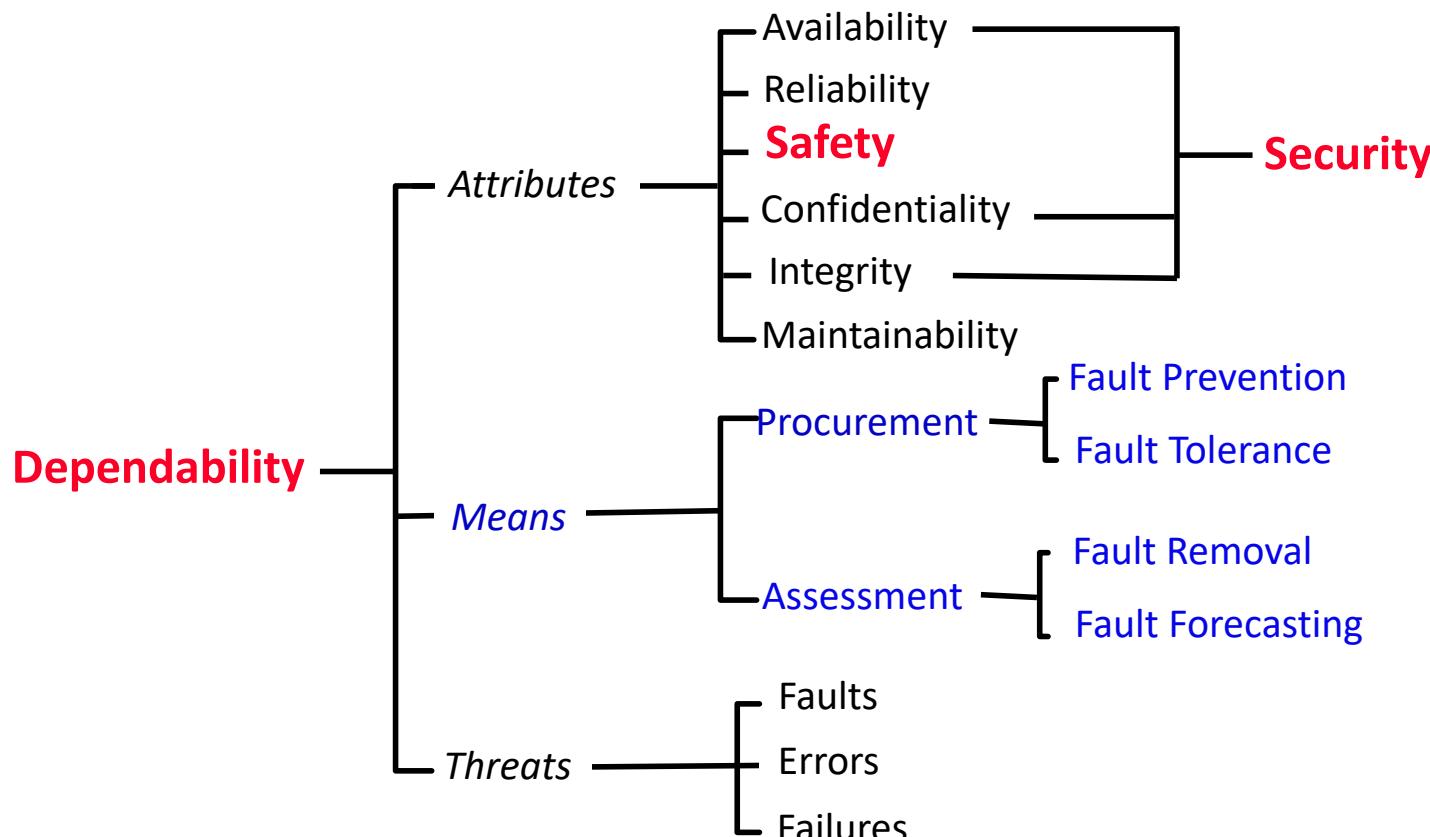


30

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

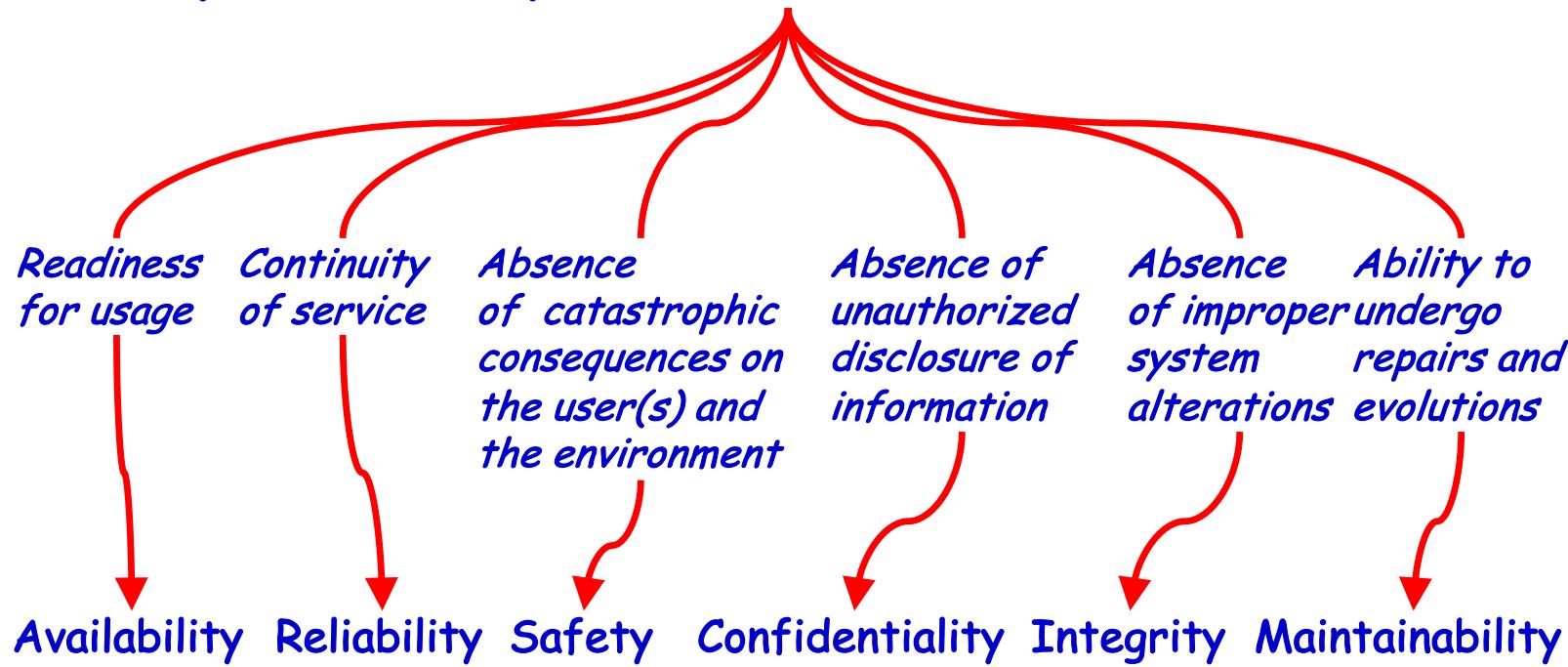
The *Dependability Tree*

31



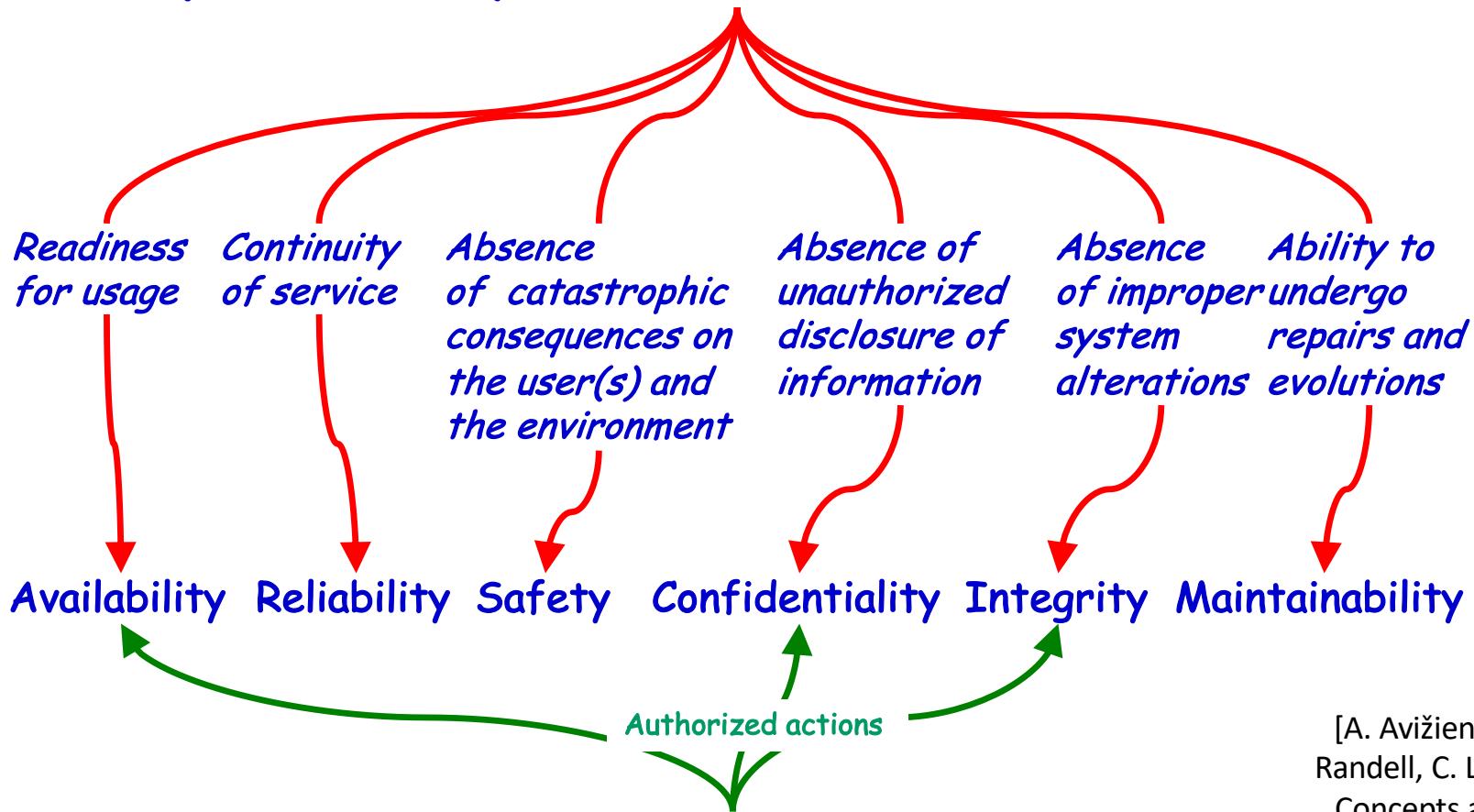
[A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr: "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE TDSC, 1 (1), pp. 11-33, Jan-Mar 2004]

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



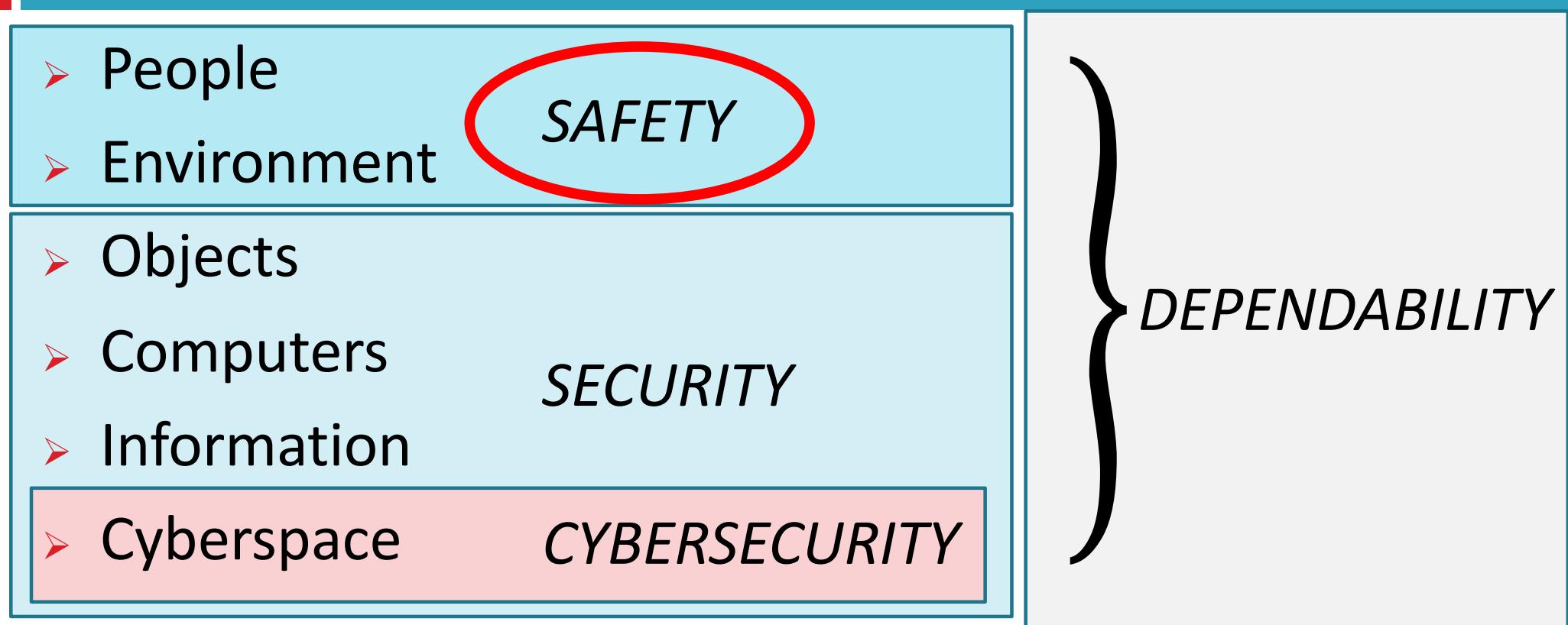
Security

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]

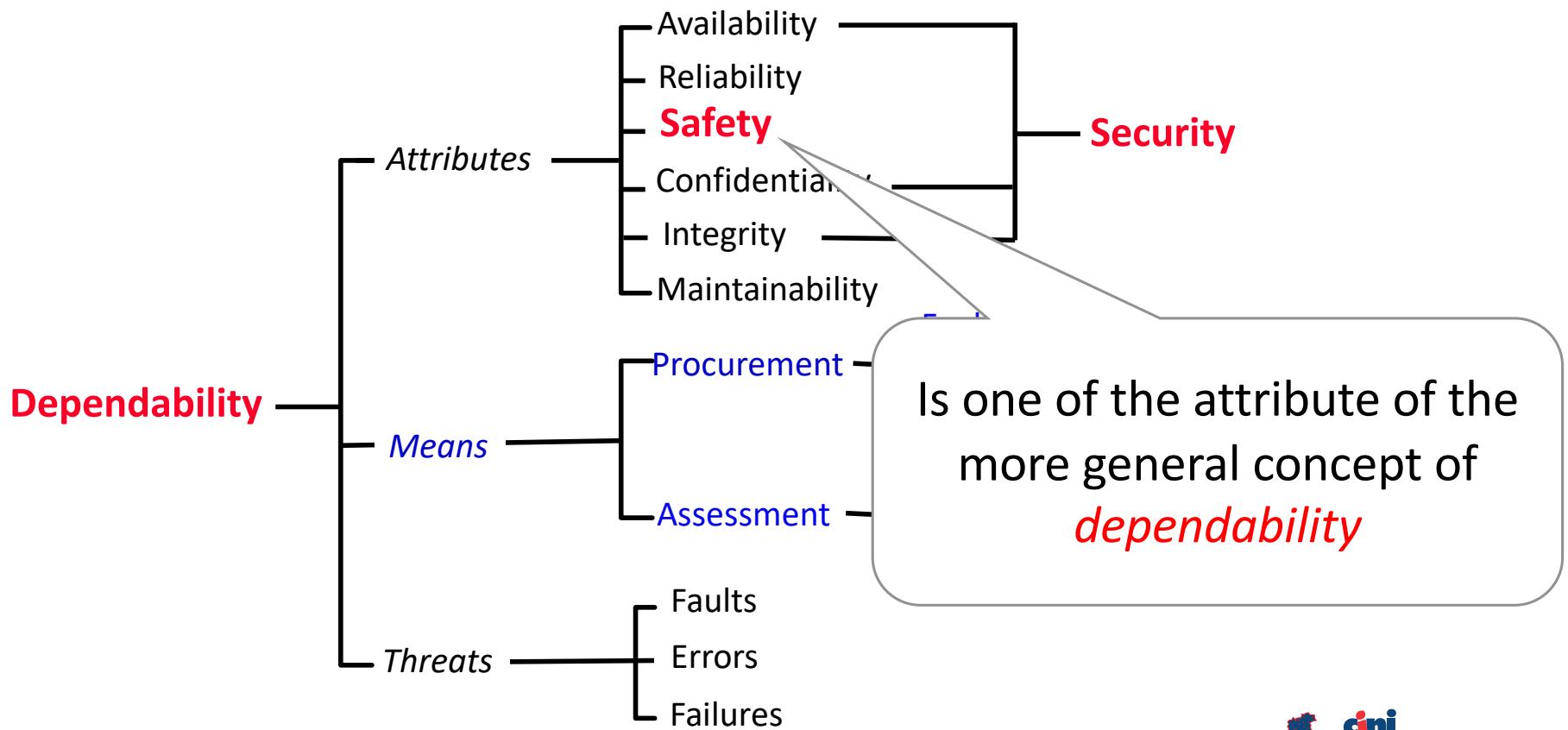
Protecting what

34

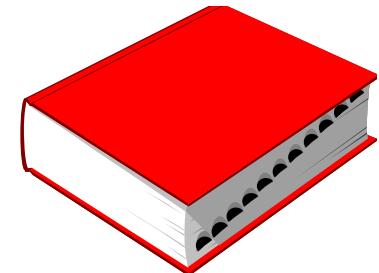


The *Dependability Tree*

35



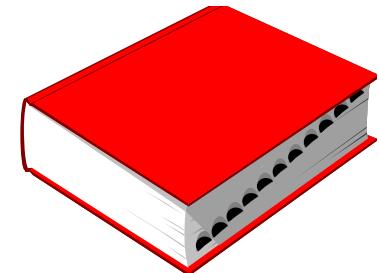
Safety



36

- 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

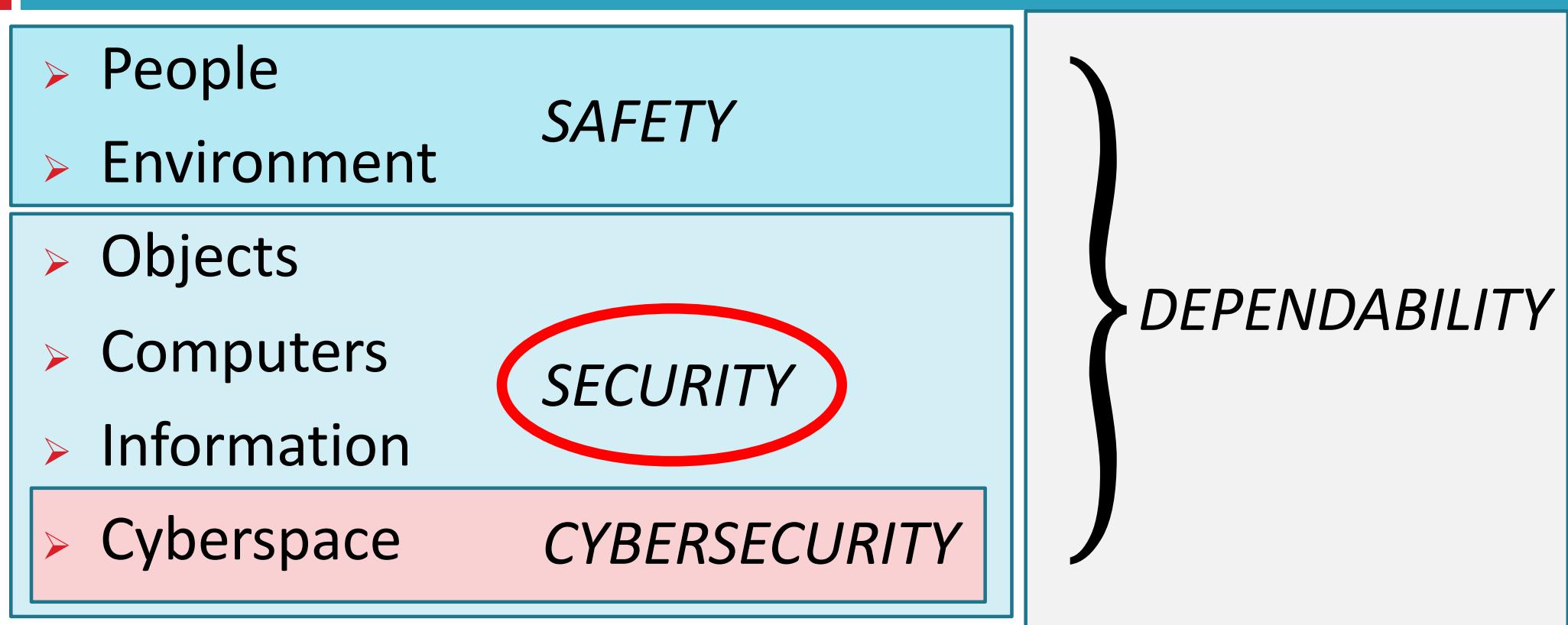


37

- 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

38



Computer security



39

- 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



40

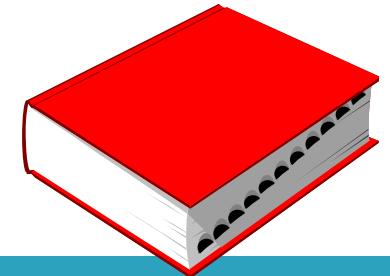
- Deals with the prevention and detection of **unauthorized** actions by users of a computer system

Computer security

41

- 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



42

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

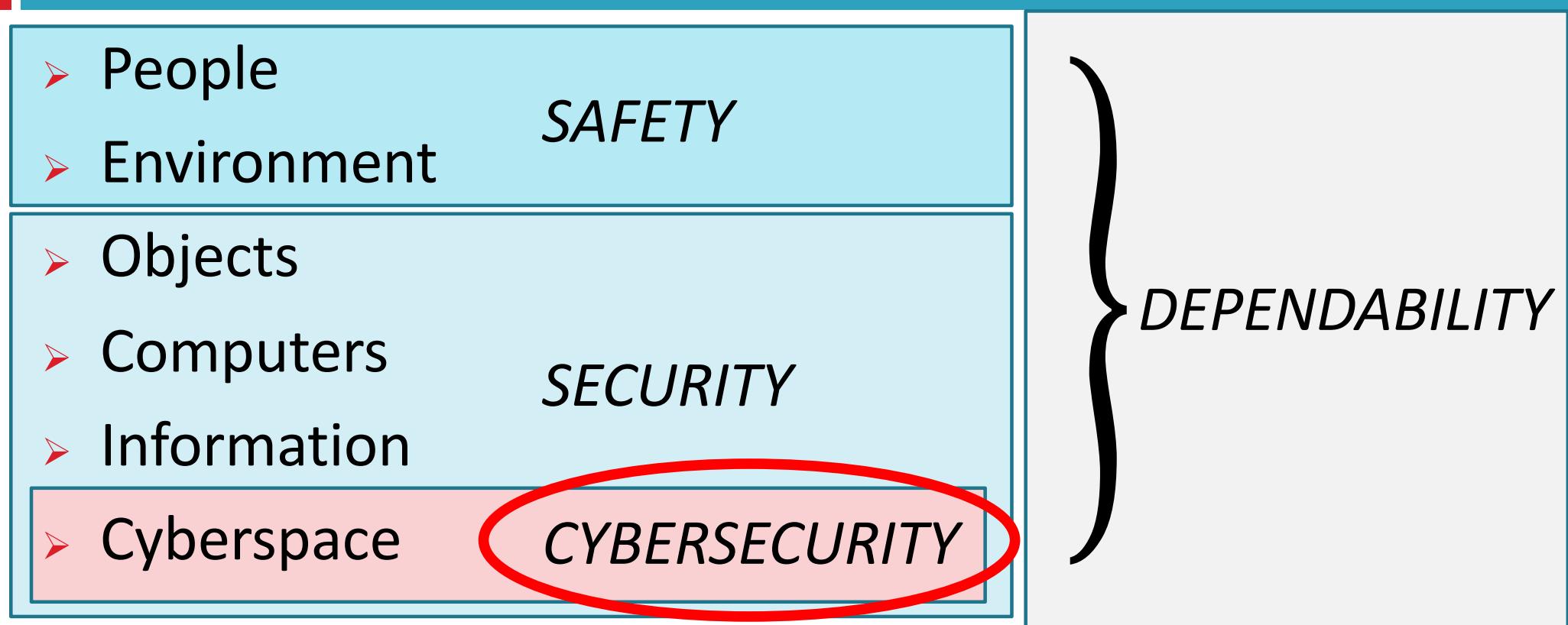
Information security - Remark

43

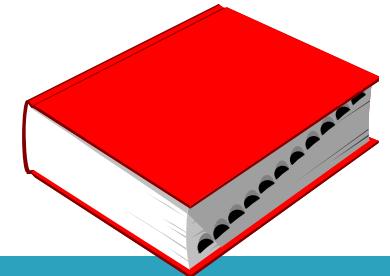
- Information is more general than data
- Data convey information
- But information may also be revealed, without revealing data, e.g., by statistical summaries
- Constitutes a basic right: protection of self (possessions, ...)

Protecting what

44



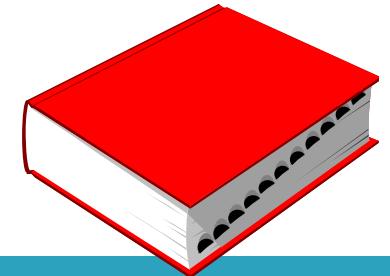
Cybersecurity



- 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]

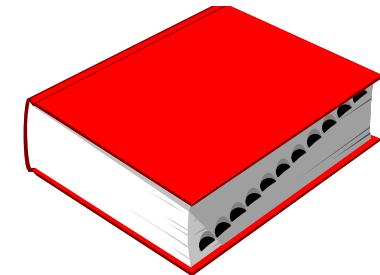
Cybersecurity



- 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*

47

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

The concept of Failure

48

- 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

49

- 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”

50

- 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”

52

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

Different “perceptions”

IEEE Standard Glossary of
Software Engineering
Terminology

53

- 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

54

- 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

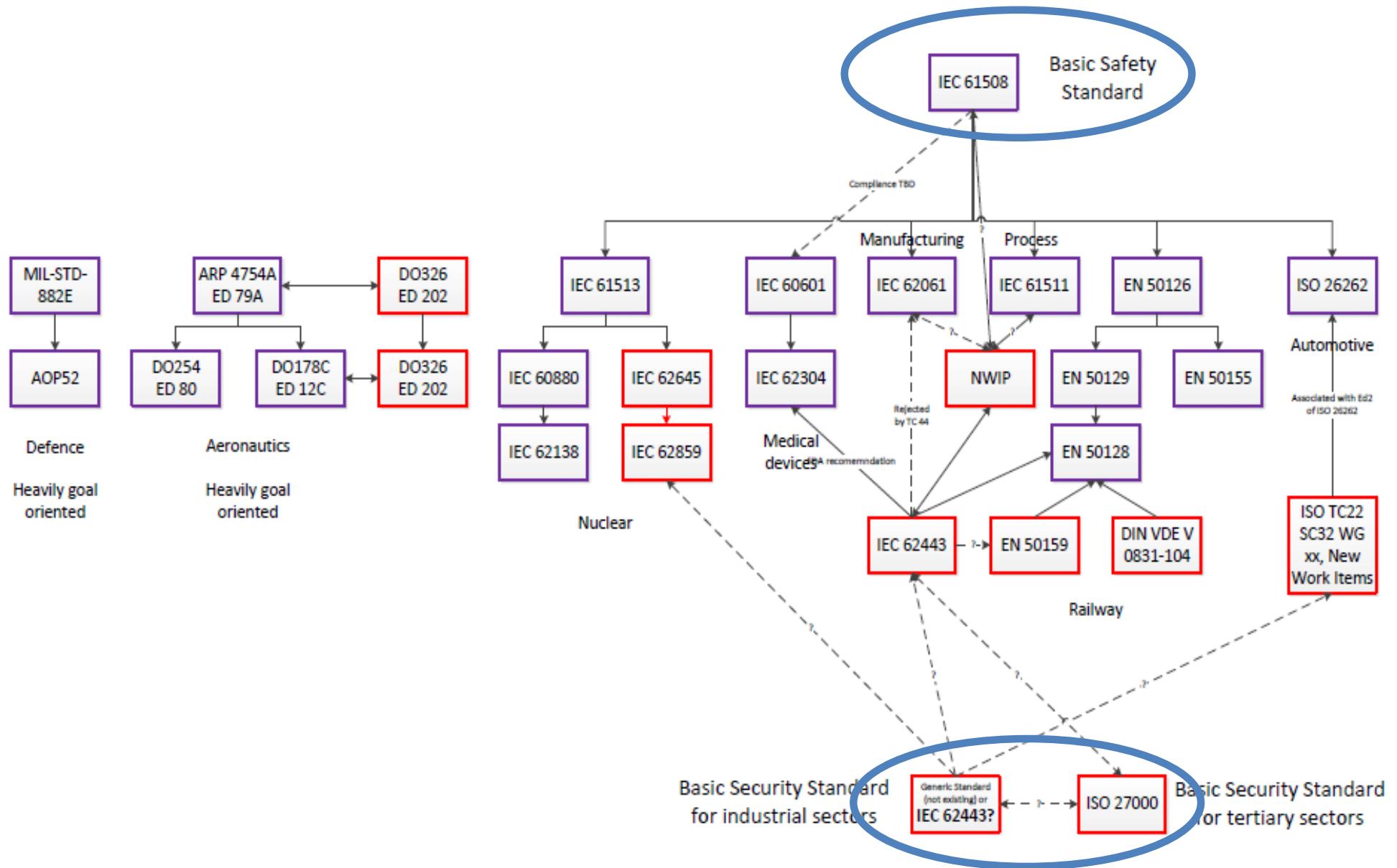
Unauthorized entry by jumping on the car.



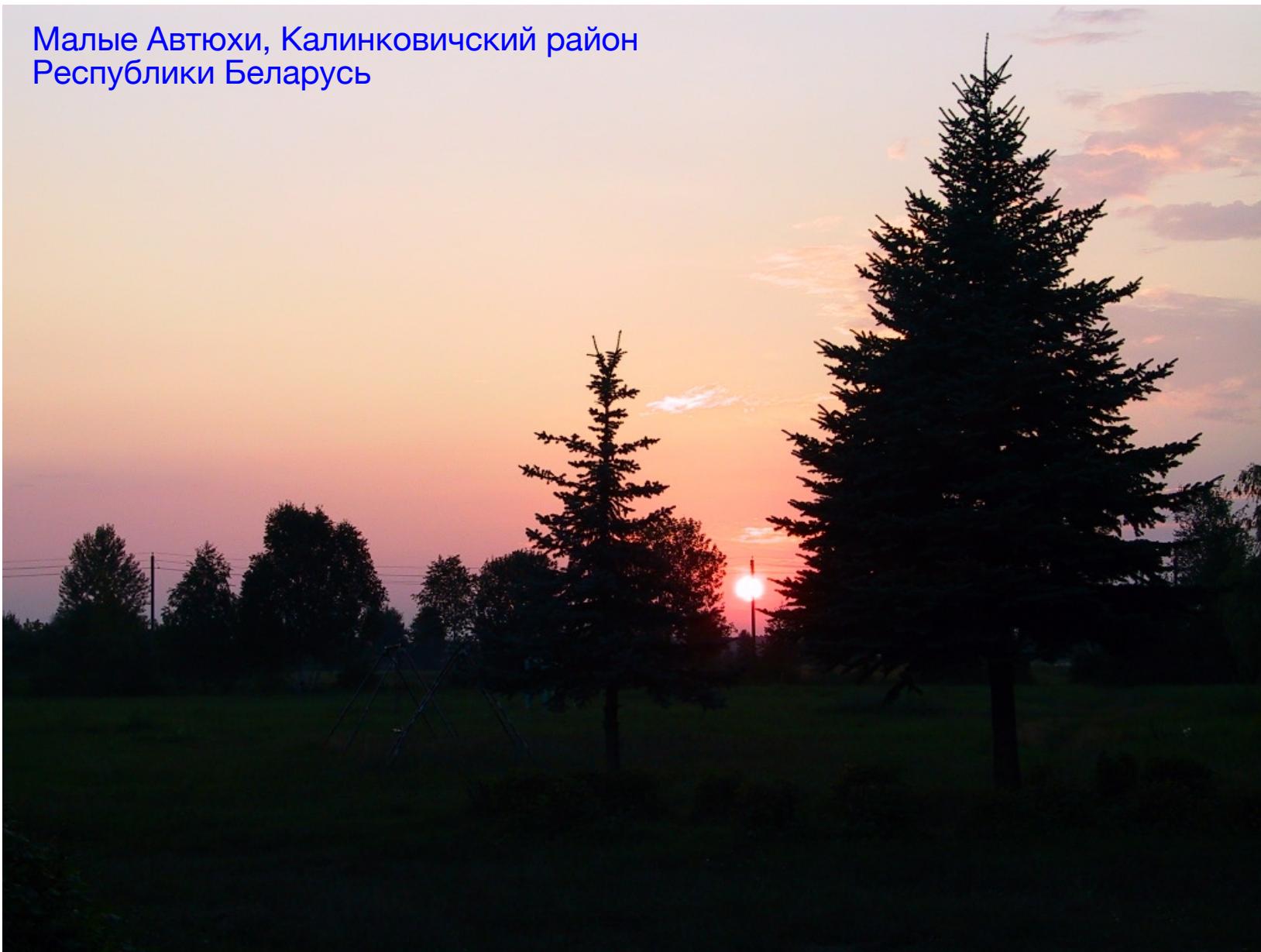
The role of Standards

58

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



Малые Автюхи, Калинковичский район
Республики Беларусь



Paolo PRINETTO

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



<https://cybersecnatlab.it>