Why Safety and Security should and will merge

Andreas Pfitzmann

Dresden University of Technology, Department of Computer Science, D-01062 Dresden
Hans-Grundig-Str. 25, Room 120
Phone: 0351/ 463-38277, e-mail: pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

Structure of Talk

Safety
Security
Both needed, but limited experience

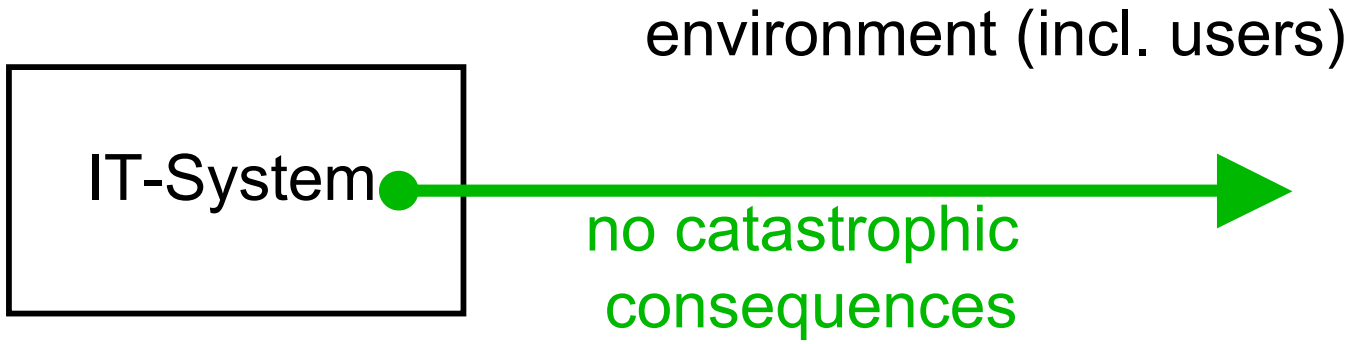
Example: Cars

Issue Warnings ... but they will be downplayed,
... so combine and integrate efforts

Embracing concepts: Dependability
Multilateral Security

Do we have a chance to successfully combine and integrate?
Properties
Methods to describe
Mechanisms

Safety

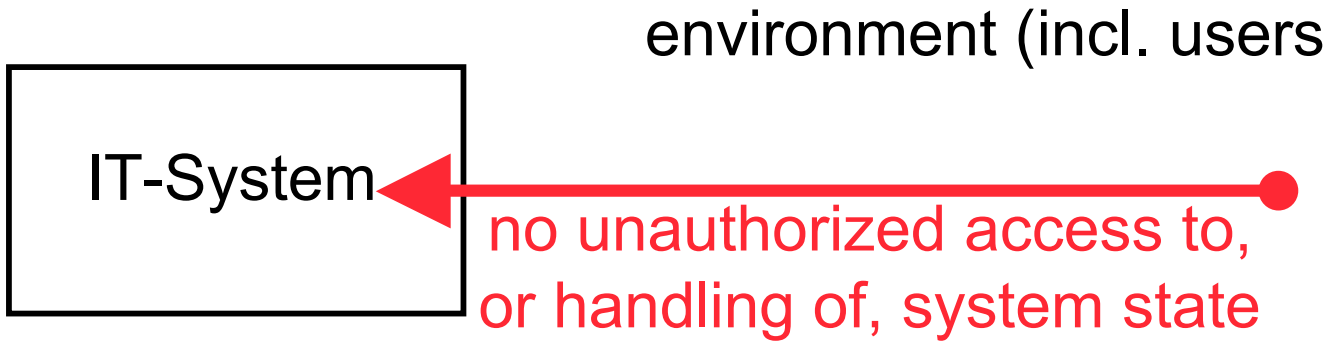


For a long time, environment regulates IT-System w.r.t. safety.

In former times:

Malicious intention of designers, builders, and operators was no issue.

Security



Only recently, environment starts to regulate networked IT-System w.r.t. security.
Causes are DDoS-attacks, spam, and worms.

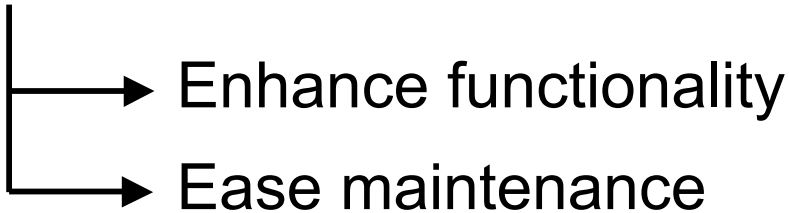
In former times:

Direct interaction with environment was no issue.

Both properties needed

In future: Both properties needed

e.g. in networked embedded systems



Limited experience:

Safety community: Attacks by terrorists

Security community: Privacy

(= direct interaction with the environment in the informational sphere)

Example: Cars

- Today: Antilock brake system → safety
- Within 5 years: Software updates for controllers via open networks → security
- Within 10 years: Driver assistance by information sent by other cars → safety and security (and privacy)

Issue Warnings

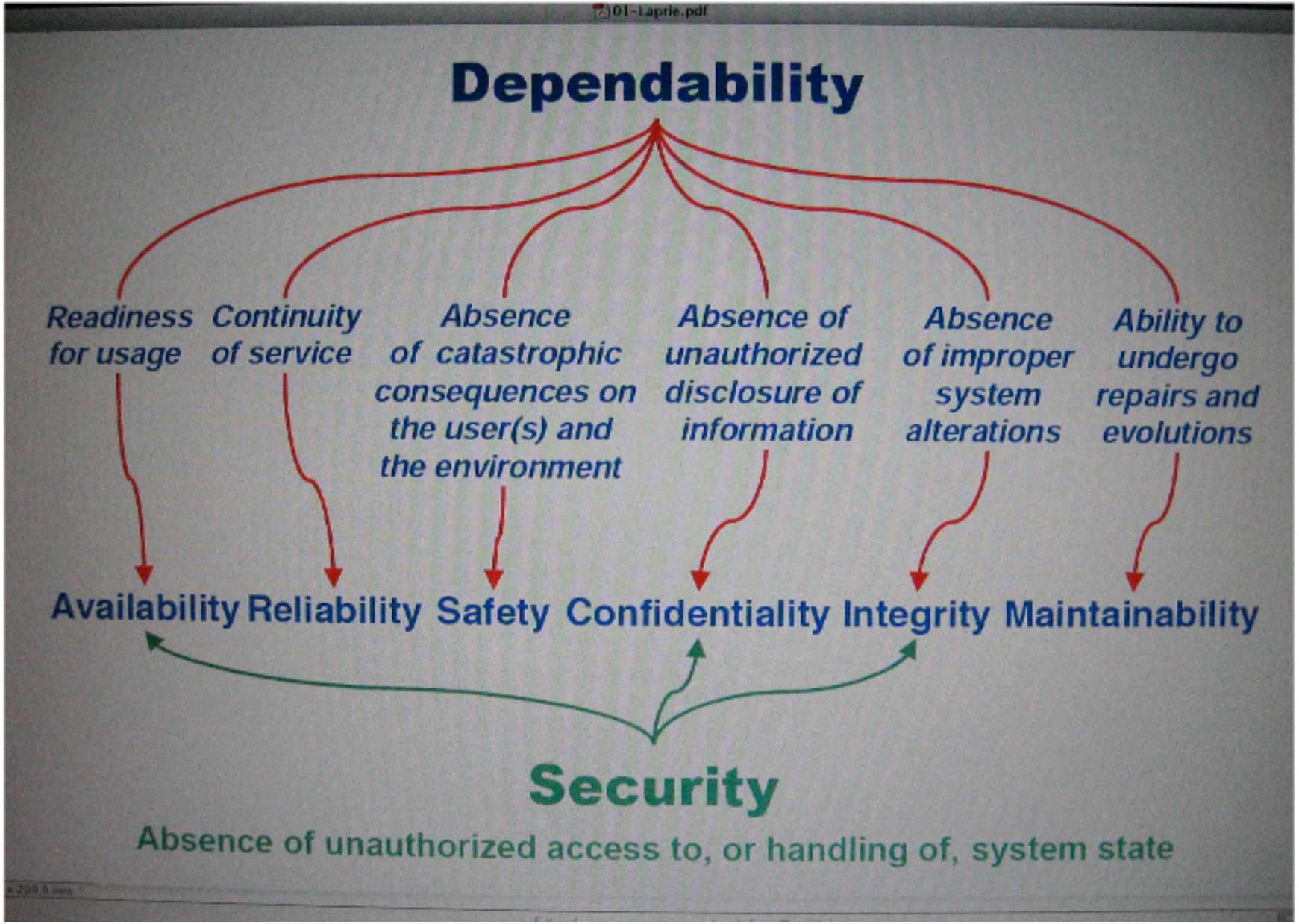
Our warnings will not be heard or downplayed

- Safety and security communities should combine and integrate efforts to design,
  build,
  operate/use
  the networked embedded systems as secure and safe as possible.
  Constraints: Legacy systems to be used and functionality deemed necessary for the end-users.

- Concept embracing safety and security is needed.
  I don't care much about words, so call the embracing concept
  dependability (construction and maintenance-oriented view)
  multilateral security (user-centric view)
  or whatever you like.

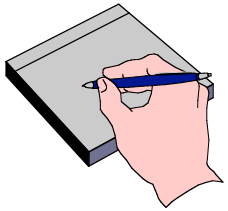
Dependability

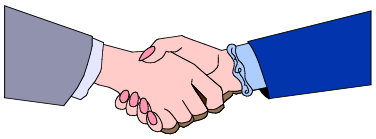
Picture taken from first figure in: Jean-Claude Laprie: Dependability vs Survivability vs Trustworthiness, 42nd 10.4 meeting

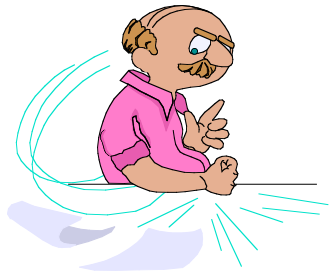


Multilateral security

- Each party has its particular protection goals.
- Each party can formulate its protection goals.
- Security conflicts are recognized and compromises negotiated.
- Each party can enforce its protection goals within the agreed compromise.







Security with minimal assumptions about others

Do we have a chance to successfully combine and integrate?

1. Properties

Safety properties	Security properties
Fail-safe	Confidentiality, comprising data avoidance (anonymity) and data scarcity (pseudonymity)
Gracefully degraded service	Availability

Do we have a chance to successfully combine and integrate?

2. Methods to describe

Fault tolerance	Security
Fault trees	Attack trees

Do we have a chance to successfully combine and integrate?

3. Mechanisms

Fault tolerance	Security
Checksums	Cryptographic checksums, e.g. digital signatures

End-to-end arguments in system design suggest to understand fault tolerance mechanisms as efficiency improvements of the security mechanisms needed anyway.

Outlook

- I am sure,
  - there is a need.
  - in building systems in the future, combination and integration of safety and security will be tried.
- I believe,
  - combination and integration is at least to some degree possible and worthwhile.
- I can‘t say,
  - how fast,
  - at what levels (system specification, system architecture, mechanisms)

safety and security will merge ...

but I am eager to discuss this with you.