MÄLARDALEN UNIVERSITY
SWEDEN

Critical Infrastructure Protection: the eternal return of dependability-related essential principles

Barbara Gallina
School of Innovation, Design and Engineering,
Mälardalen University, Västerås, Sweden
barbara.gallina@mdh.se

09th September 14, ReSA4CI (Reliability and Security Aspects for Critical Infrastructure Protection)

Talk outline

- Critical Infrastructures
  - Definitions
  - Attributes
  - Threats
  - Means
- Dependability and its eternal return
- Lessons learned and reuse perspectives

Definitions: Infrastructure

- *Def1*-the underlying foundation or basic framework (as of a system or organization).
- Def2-a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services.

- REMARK: Looks like a system of systems..

Definitions: Critical Infrastructure

- *Def1*-those infrastructure whose incapacity or destruction would have a debilitating impact on our defense and economic security.

- Categories: telecommunications, electric power systems, natural gas and oil, banking and finance, transportation, water supply systems, government services, and emergency services.

Definitions: Critical Infrastructure-EU

- *Def1*-An asset, system or part thereof located in member states that is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact on a member state as a result of the failure to maintain those functions.

(European Council Directive 2008/114/CE)

CI - attributes

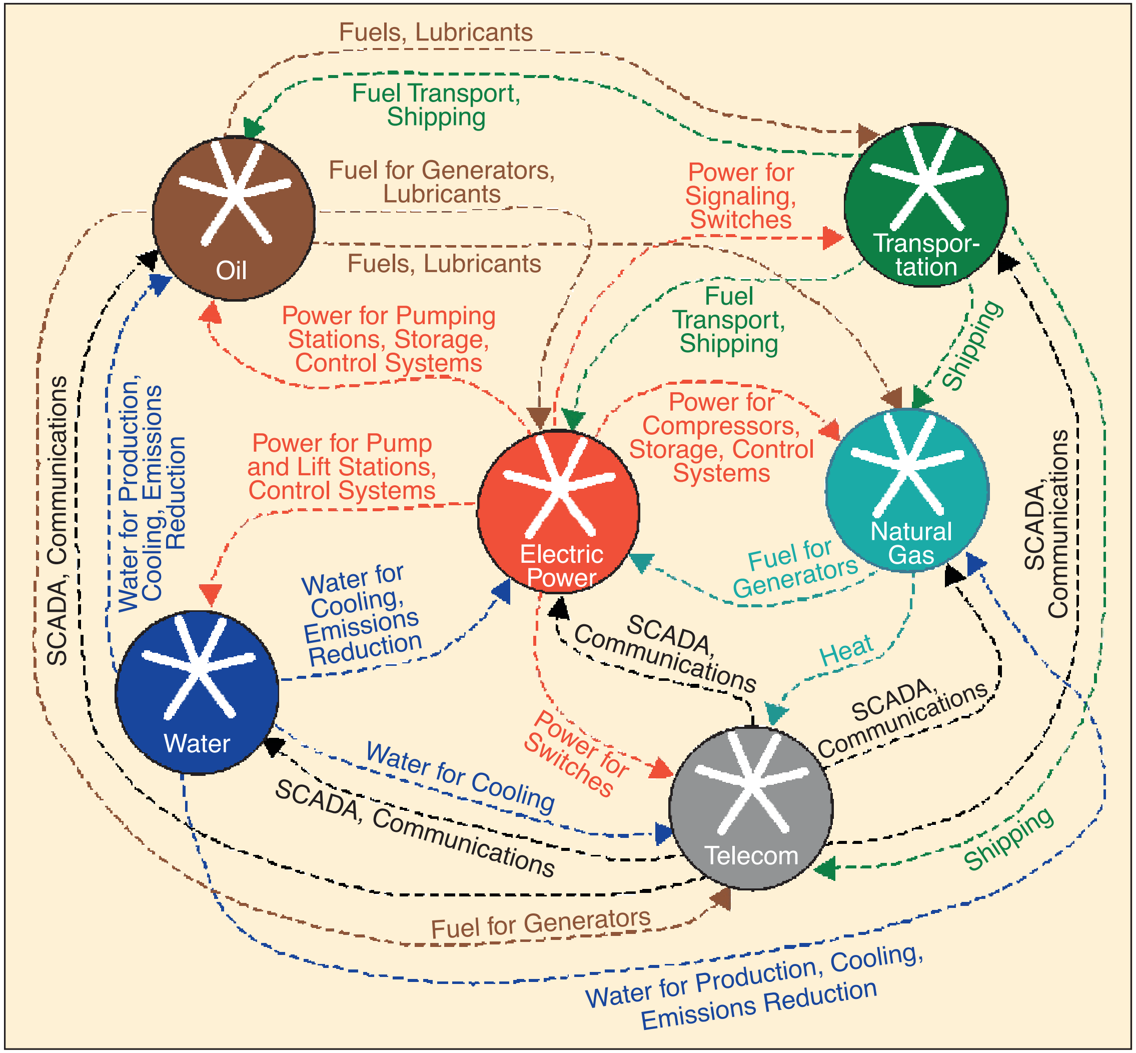
- Complex
- Heterogeneous

.. i.e., different domains, different countries, different regulations, etc.

- Highly interconnected
- Highly distributed-complex topology

CI - interdependecies

- Physical
- Logical
- Geographical
- Cyber



Fuels, Lubricants
Fuel Transport, Shipping
Fuel for Generators, Lubricants
Fuels, Lubricants
Power for Signaling, Switches
Oil
Transportation
Power for Pumping Stations, Storage, Control Systems
Fuel Transport, Shipping
Shipping
Power for Compressors, Storage, Control Systems
Power for Pump and Lift Stations, Control Systems
Electric Power
Natural Gas
SCADA, Communications
Water for Production, Cooling, Emissions Reduction
SCADA, Communications
Fuel for Generators
Water for Cooling, Emissions Reduction
SCADA, Communications
Heat
SCADA, Communications
Water
Power for Switches
Water for Cooling
SCADA, Communications
Telecom
Shipping
Fuel for Generators
Water for Production, Cooling, Emissions Reduction

CI - interdependecies

- Physical

→material link (physical commodity flow)

CI - interdependecies

- Geographical

→spatial proximity

CI - interdependecies

- Cyber

→informational links

CI - interdependecies

- Logical

Critical infrastructure?

	Linear interaction	Complex interaction
High coupling	E.g.: Dams	E.g.: Nuclear plant
Low coupling	E.g.: Most manufacturing	E.g.: Military operations

Charles Perrow, http://en.wikipedia.org/wiki/Normal_Accidents

Critical Infrastructure: Threats

- *Failures*
  - *Common cause failures*
  - *Cascading failures (domino effect..)*
  - *Escalating failures*

Critical Infrastructure: Threats

- *…cyber attack …*
- *…vulnerabilities…*
- *…disruption…*

Any association?

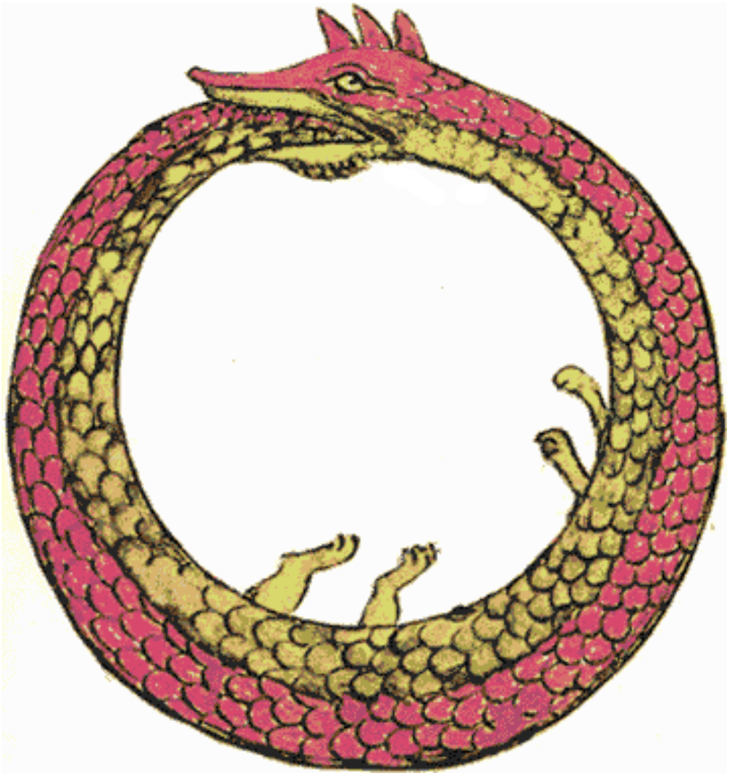
Critical Infrastructure: Means

- *Prevention: risk-driven cyber security-oriented processes*
- *Fault tolerance: monitoring/detection/recovery*
  - *Power grid example*
- *Fault forecasting: means to assess the exposure of CIs to escalating and cascading failures .. due to accidental and/or malicious faults*
  - *Qualitative/quantitative analysis*

Talk outline

- Critical Infrastructures
- Dependability concepts
  - Definitions
  - Attributes
  - Threats
  - Means
- Lessons learned and reuse perspectives

Dependability



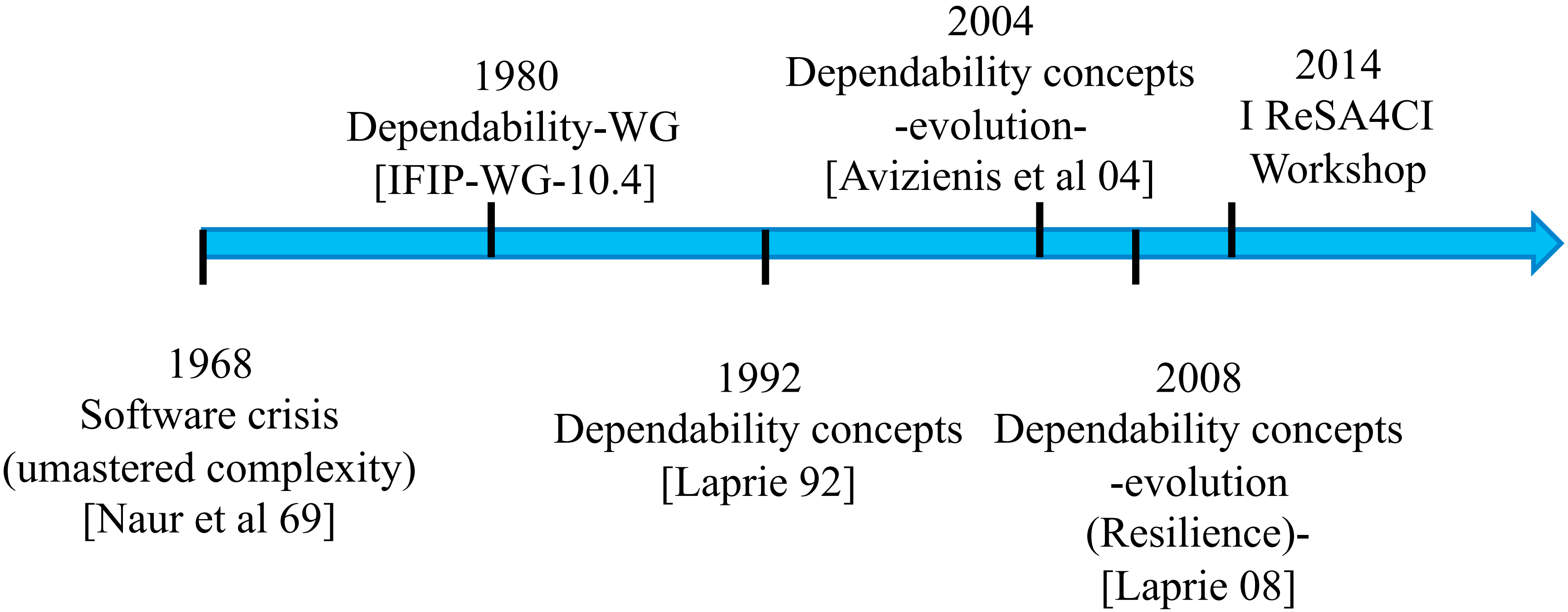
Dependability Context/Motivation/ Historical evolution

There are of course many good systems, but
are any of these good enough to have human life tied on-line to them,
in the sense that if they fail for more than a few seconds,
there is a fair chance of one or more people
being killed?

1968
Software crisis
(unmastered complexity)
[Naur et al 69]

The general admission of the existence of the software failure
in this group of responsible people is the most
refreshing experience I have had in a number of years,
because the admission of shortcomings is
the primary condition for improvement.

Dependability Context/Motivation/ Historical evolution



1968
Software crisis
(umastered complexity)
[Naur et al 69]

1980
Dependability-WG
[IFIP-WG-10.4]

1992
Dependability concepts
[Laprie 92]

2004
Dependability concepts
-evolution-
[Avizienis et al 04]

2008
Dependability concepts
-evolution
(Resilience)-
[Laprie 08]

2014
I ReSA4CI
Workshop

Dependability -Preliminary concepts-

[Avizienis et al 04]

- System - entity that interacts with other entities, i.e, *other systems*, including hardware, software, humans, and the physical world
  - Remark- From a structural point of view, a system is composed of a set of components bound together in order to interact where each component is another system, etc. The recursion stops when a component is considered to be atomic (limit of resolution)
  - Remark-These *other systems* are the environment of the given system

Dependability -Preliminary concepts-

[Avizienis et al 04]

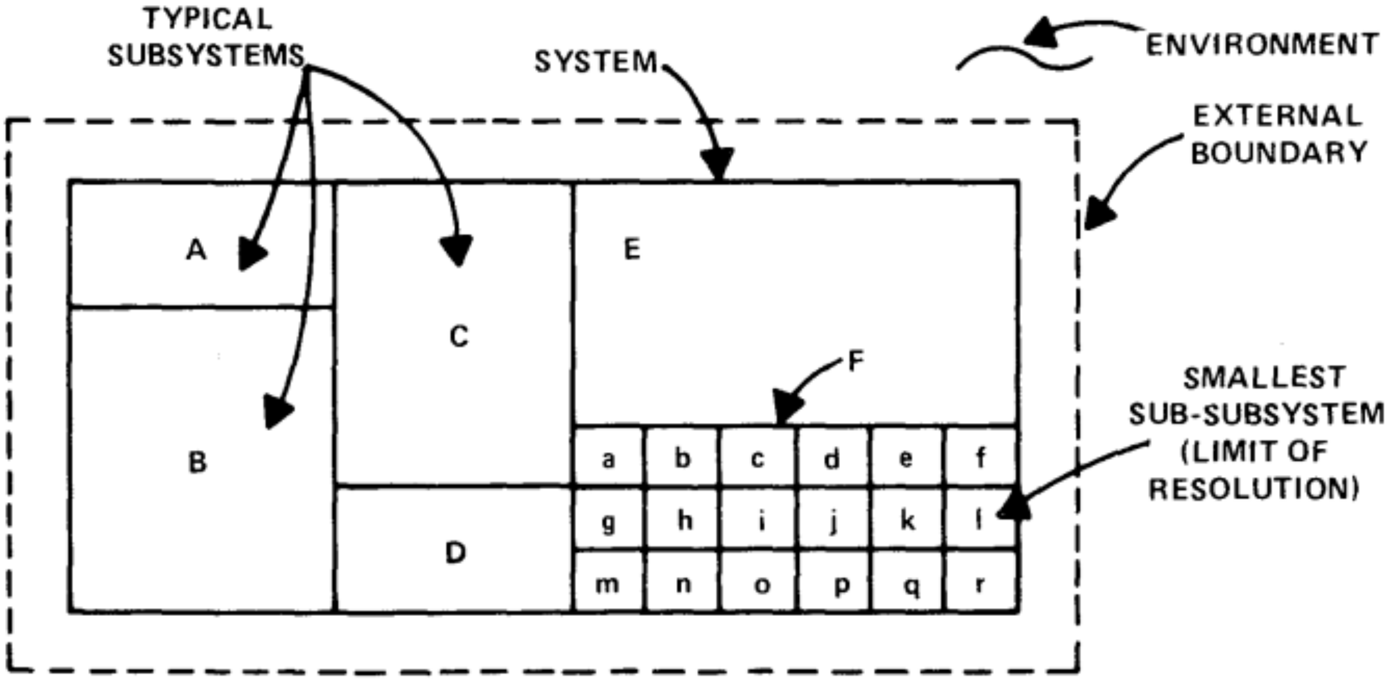
- System boundary - common frontier between the system and its environment

Remark: The problem to be addressed helps in restricting the system to be examined

– e.g. phone call (Human interface for dialing a number, setting up the communication between caller and callee, etc)

Dependability -Preliminary concepts-

- System definition: internal and external boundaries



[FTA Handbook]

Dependability -Preliminary concepts-

[Avizienis et al 04]

- State – condition of a system (w.r.t. computation, communication, stored information, interconnection, and physical condition)
  - Remark: State (w.r.t. stored information) - mapping from storage unit names to values storable in those units.

- System specification – prescription of the desired relationship existing between the input state and the output state

Dependability -Preliminary concepts-

[Avizienis et al 04]

- Functional specification – description of what the system is expected to do (its function)
- Service delivered by a system (provider) – system’s behaviour as it is perceived by its user(s)
- User - another system, which receives service from the provider
- Correct service - the system implements its specification (what the system is intended to do)

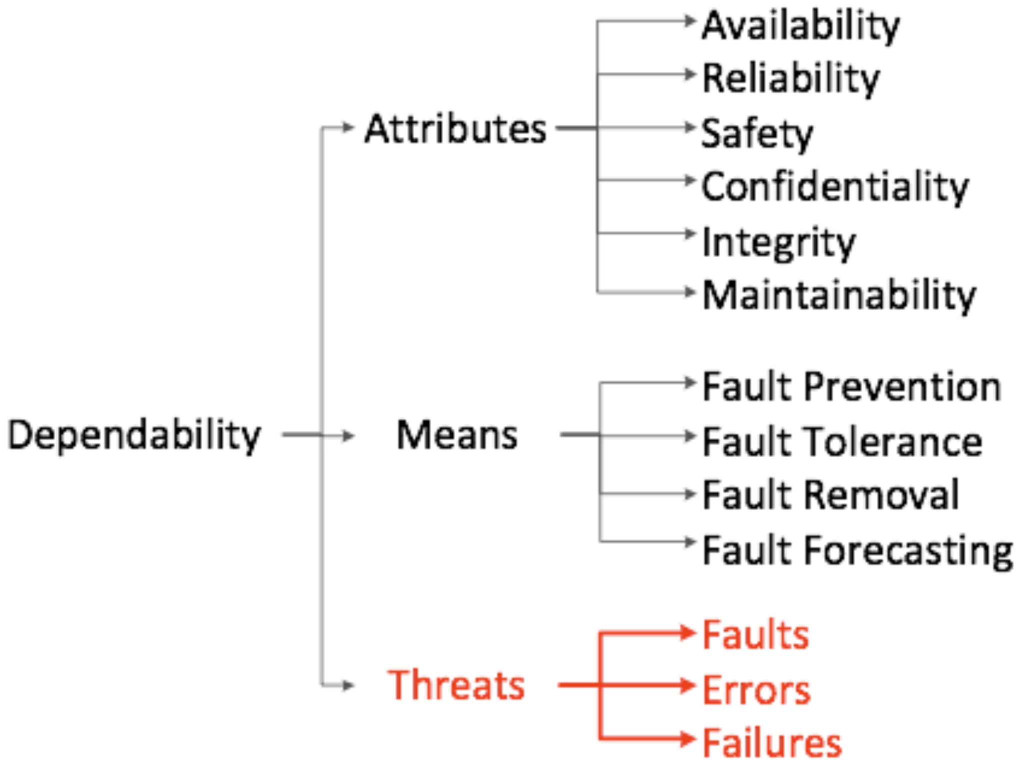
Dependability-Definitions-

- Qualitative def- the ability to deliver services that can be justifiably trusted [Avizienis et al 04]
- Quantitative def- the ability to avoid service failures that are more frequent and more severe than is acceptable to the user(s) [Avizienis et al 04]
- Trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers [IFIP-WG-10.4]

→Subjective evaluation

Dependability -Overview-

adapted from [Avizienis et al 04]



Dependability–Attributes -Safety-

- Safety - absence of catastrophic consequences on the user(s) and the environment [Avizienis et al 04]
  - Focus on those threats that lead to catastrophic consequences

Dependability–Attributes
-Reliability-

- Reliability - continuity of correct service [Avizienis et al 04]
  - probability that an item fulfils the required functions for the required duration

Dependability–Attributes -Availability-

- Availability - readiness for correct service [Avizienis et al 04]
  - describes the extent to which an item is operational and able to perform any required function or set of functions if a demand is placed on it

Dependability–Attributes -Maintainability-

- Maintainability - ability to undergo modifications and repairs [Avizienis et al 04]
  - the probability that a maintenance activity can be carried out within a stated time interval

Dependability–Attributes -Confidentiality-

- Confidentiality - absence of unauthorized disclosure of information

Dependability–Attributes -Integrity-

- Integrity - absence of improper system alterations

Dependability attributes

[Laprie 08]

Primary Attributes

- Availability
- Reliability
- Safety
- Confidentiality
- Integrity
- Maintainability

Secondary Attributes:

- **Robustness**
- **Survivability**
- **Resilience**

Remark: Dependability is an ‘umbrella’ term

Dependability–Threats
-Fault-

[Avizienis et al 04]

- Fault - adjudged or hypothesized cause of an error.
  - When active, it can be seen as an event (an erroneous transition) that causes a state change, which brings the system from a valid state to an erroneous state
- Faults classification: Malicious/Non malicious, Internal/external,Accidental/Incompetence, Deiliberate/Non deliberate, etc.

Dependability–Threats
-Error-

[Avizienis et al 04]

- Error - part of the total state of the system that may (in case the error succeeds, by propagating itself, in reaching the external system state) lead to its subsequent service failure

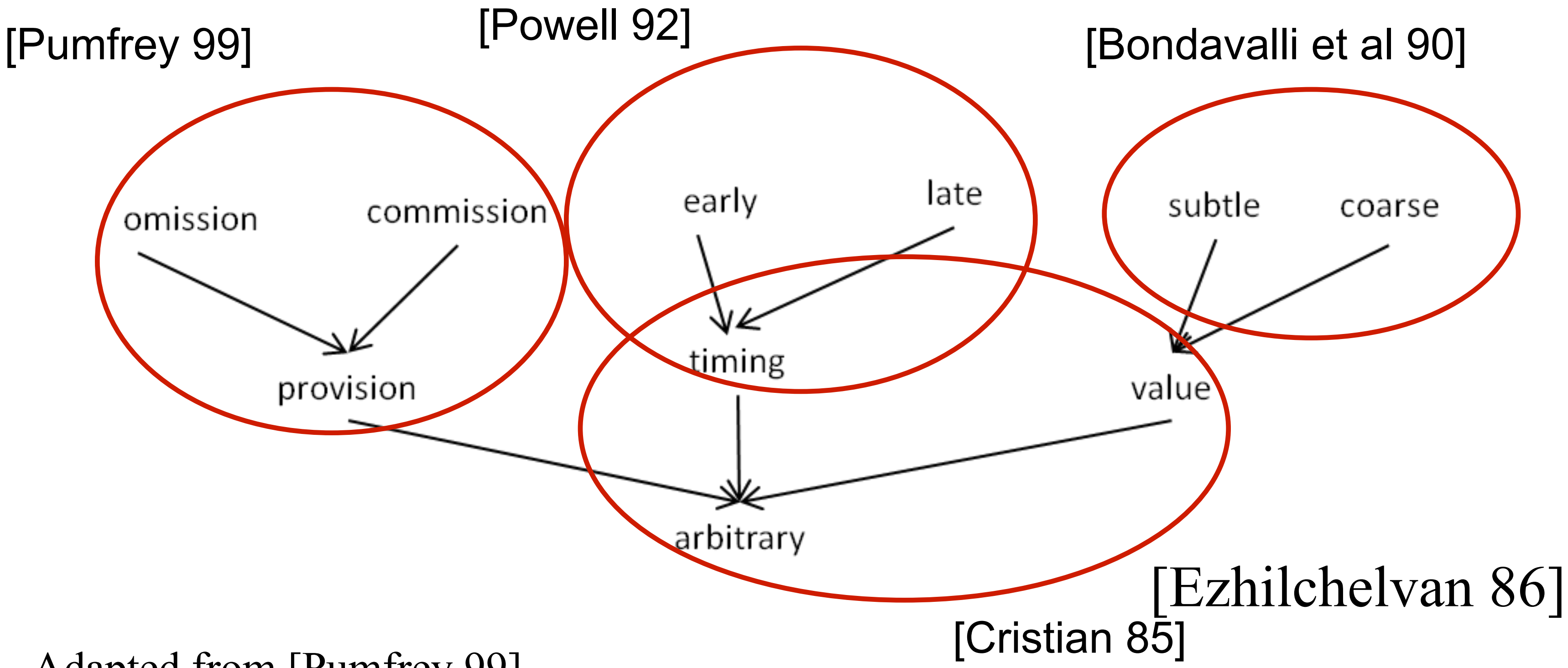
Dependability–Threats
-Failure and failure mode-

[Avizienis et al 04]

- Failure – event (transition) that occurs when the delivered service deviates from correct service (the system specification)
- Failure mode - the way in which a system can fail

Dependability–Threats

-Failure modes classification evolution-



Adapted from [Pumfrey 99]

Dependability–Threats
-Failure modes classification evolution-

- I^4

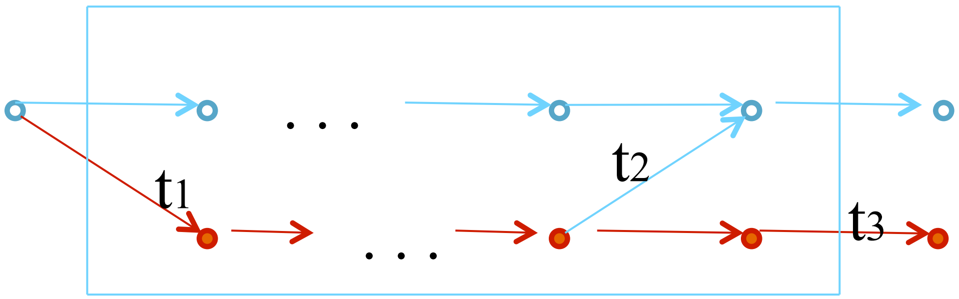
  Incompletion

  Inconsistency

  Interference

  Impermanence

Dependability–Threats -Graphical summary-



Legend

□ System boundary

○ Valid states

● Erroneous states

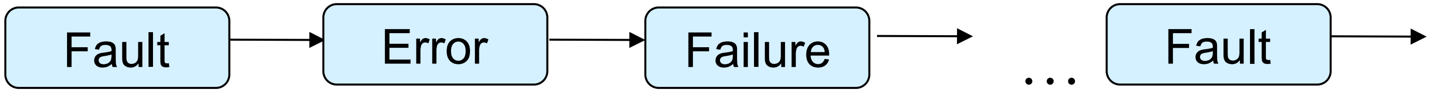
t_i → Transition (where $1 \le i \le 3$)

Dependability–Fault Models
-Causality chain-

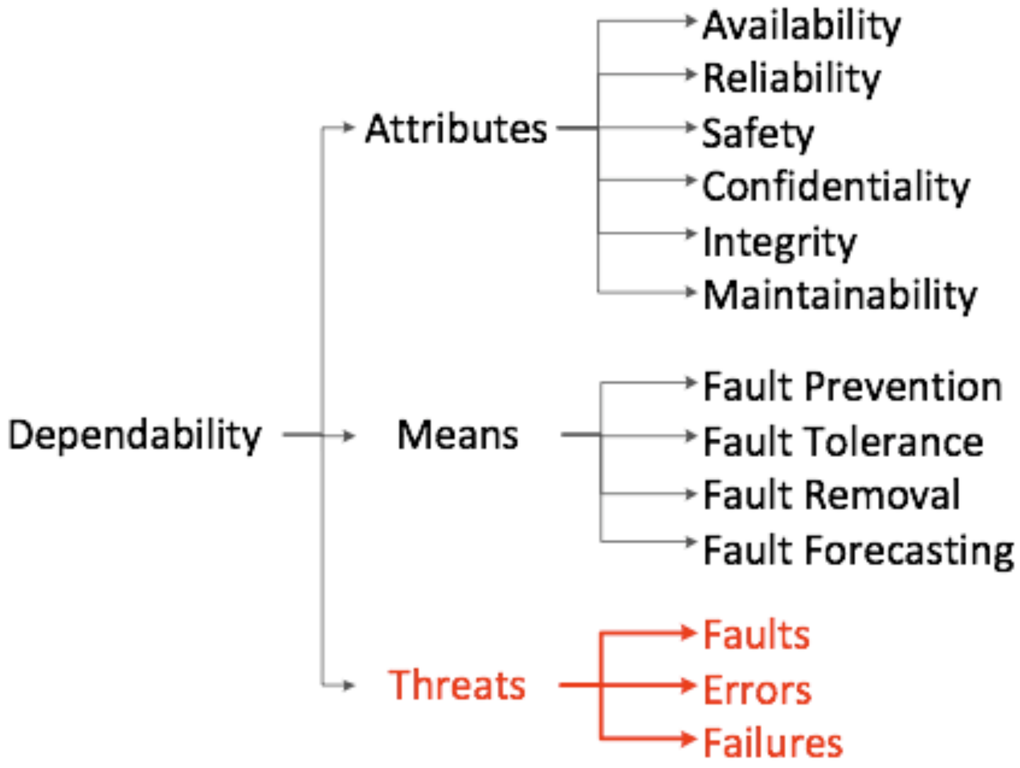
[Randell 00]

Focus on technical aspects

- What if we have a structured system?
  - Failure propagation



Dependability Recreation to embrace CIs



Secondary Attributes:

- **Robustness**
- **Survivability**
- **Resilience**

Protection

Cyber attacks
Vulnerabilities
Disruptions

Dependability–Means
-Fault Prevention-

- Goal: to prevent the occurrence or introduction of faults [Aviezienis et al 04]
  - Remark: a fault which is never introduced costs nothing to fix!

- Approaches in team management
  - Security training (to prevent (non)malicious faults)
  - Training (to prevent i.e. non-deliberate faults due to incompetence)
- Approaches during software development
  - Selection of programming languages
  - Selection of development processes

Dependability–Means -Fault Removal-

- Goal: to reduce the number and severity of faults [Aviezienis et al 04]
- Approaches:
  - During development:
    - Verification
      - Static analysis (e.g.theorem proving, model checking, etc)
      - Dynamic analysis (e.g.testing, symbolic execution, etc)
    - Diagnosis
  - During operational life:
    - Corrective or preventive maintenance

Dependability–Means
-Fault Tolerance-

- Goal: to avoid service failures in the presence of faults [Aviezienis et al 04]
  - Software/hardware redundancy introduction
- Phases:

  1- Error detection

  2- Damage confinement & assessment

  3- State restoration

  4- Fault treatment & continued service

Dependability–Means
-Fault Forecasting-

- Goal: to estimate the present number, the future incidence, and the likely consequences of faults [Aviezienis et al 04].
- Approaches can be classified as:
  - Qualitative - consist of the identification, the classification, and the ranking of the failures modes at component level and their consequences at system level
    - FMEA, FMECA, FTA, HAZOP, etc.
  - Quantitative - consist in measuring quantitatively the extent to which the relevant attributes of dependability are satisfied.
    - FTA, etc.

Lessons learned

- Decade after decade dependability renews itself
  - The renewal must be made explicit
- We should not limit ourselves in rewriting the history, by rewriting the syntax. We should instead focus on the semantic differences to distinguish new from old challenges and corresponding implications

Lessons learned

- CIs call for cross-domain, cross-country (→ spatial, legal, political, economical implications), federated, and cooperative solutions
  - Risk-driven processes
  - Common goals/different but coherent requirements
  - Holistic models for accident investigation
  - Hierarchical fault-tolerant units for structuring the system
    - Cooperative exception handling
  - Compositional fault removal
  - Cross fertilization of dependability means
    - i.e., security means should benefit from reliability means

Main references

- [Avizienis et al 04] Avizienis, A., Laprie, J., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. In: IEEE Trans. Dependable Sec. Comput. 1(1): 11-33, 2004
- [Laprie 08] Laprie, J.-C. 2008. From Dependability to Resilience. LAAS Report no. 08001. LAAS-CNRS, Toulouse, France.
- [Rinaldi et al 01] Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE* , vol.21, no.6, pp.11,25, Dec 2001

Thank you for your attention!

Discussion time…