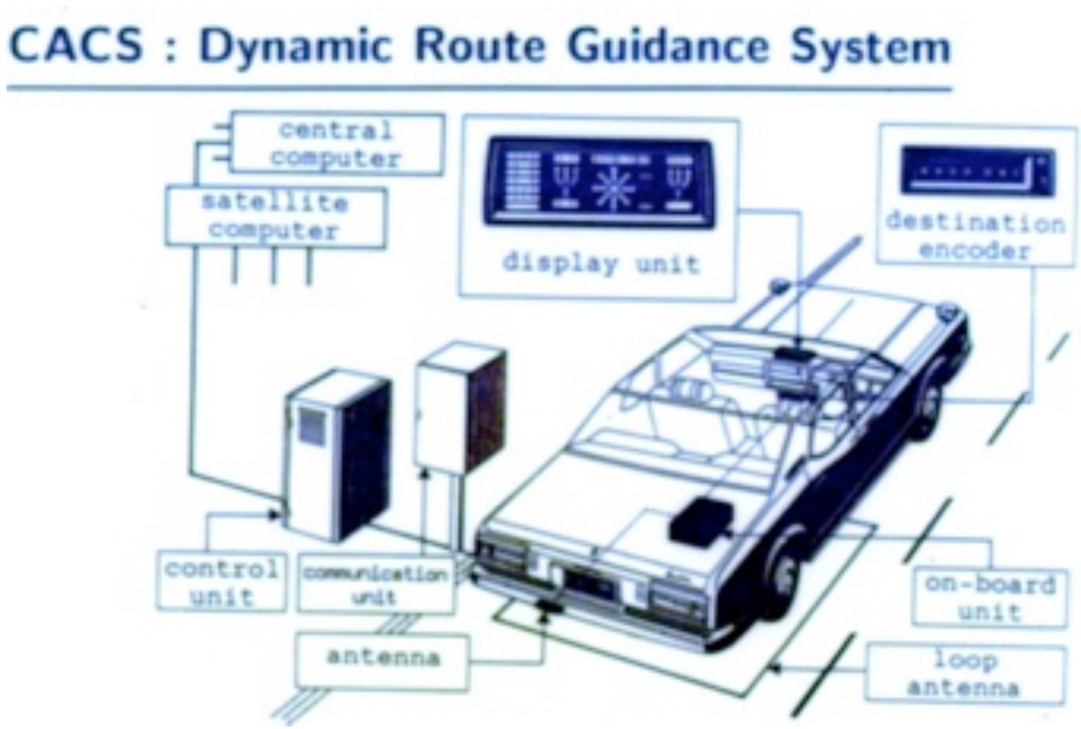
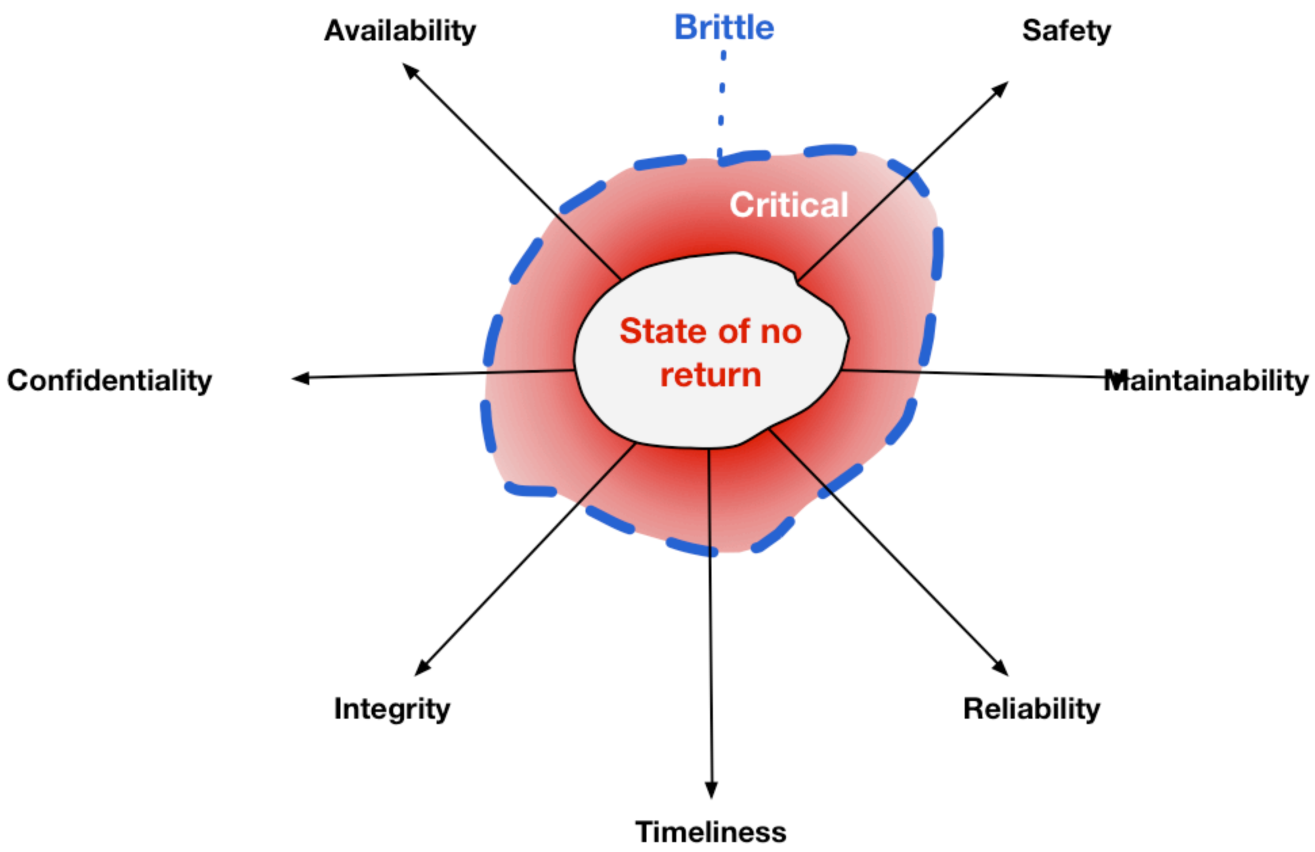
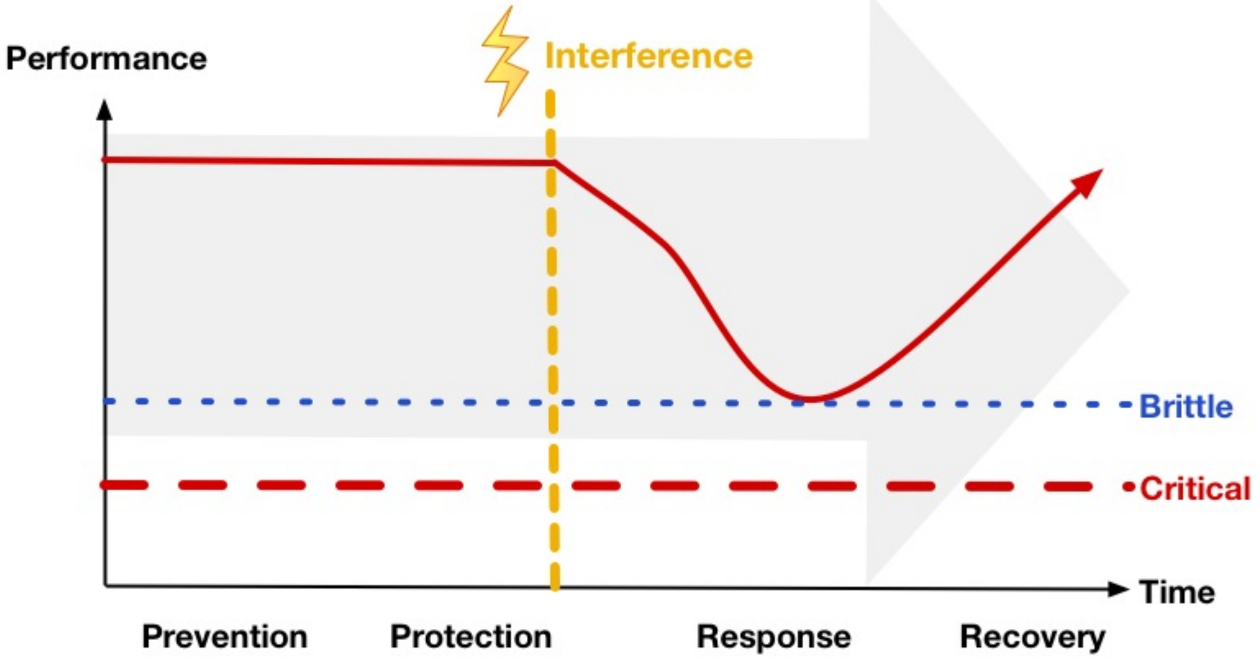
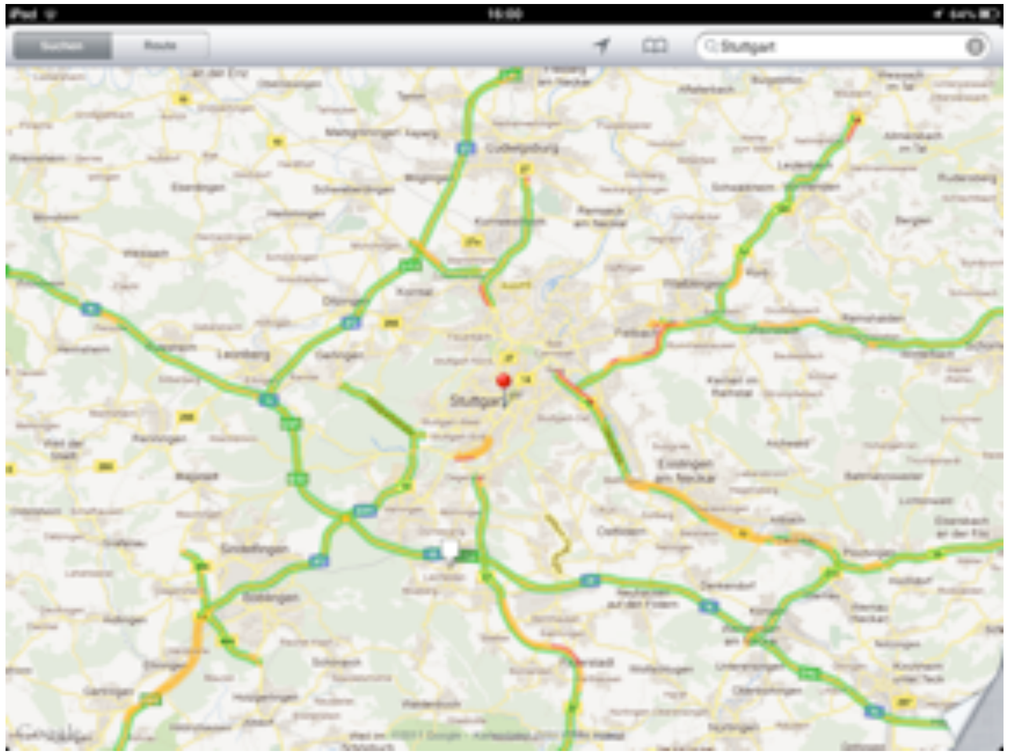








On Resilient Computing

ISSI 2011, Tokyo, Japan
February 16, 2012

Sven Wohlgemuth
Transdisciplinary Research Integration Center
National Institute of Informatics, Japan
Research Organization for Information and Systems, Japan

Agenda

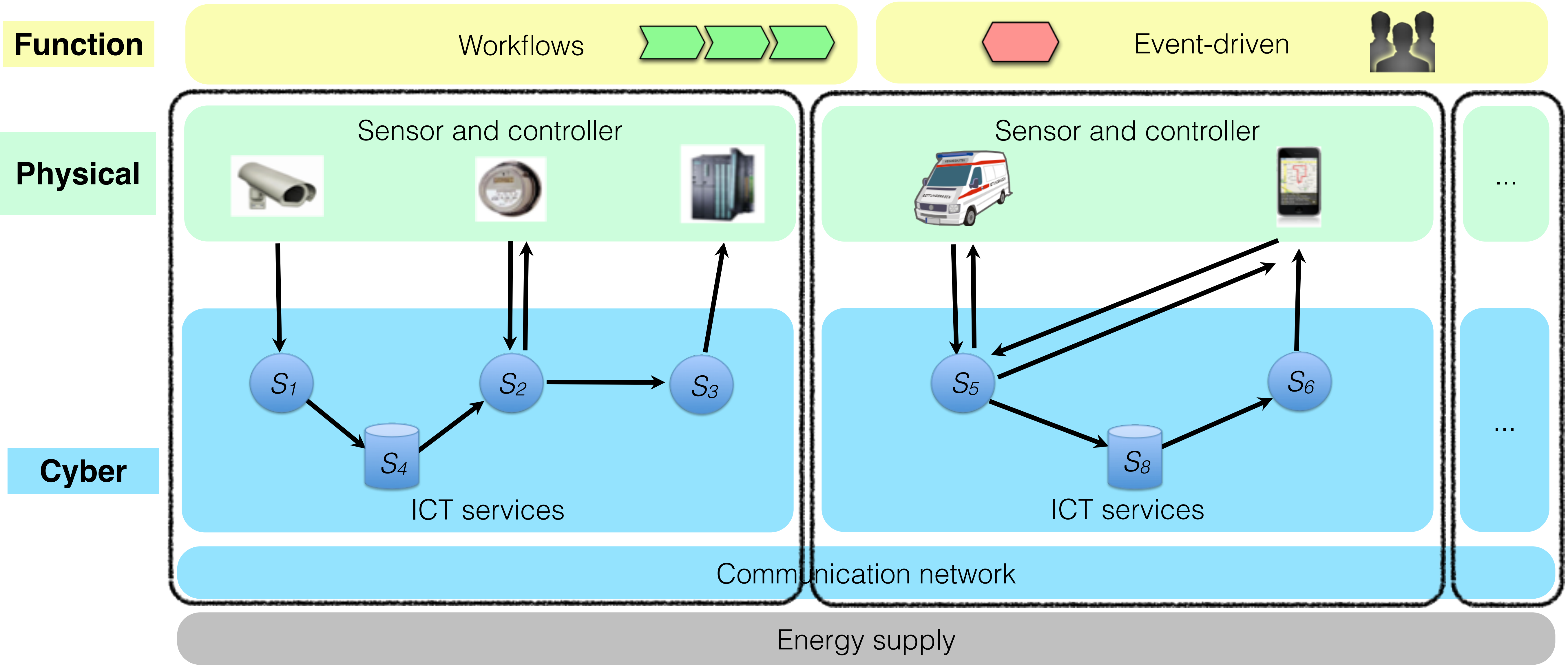
I. Social Infrastructures and ICT

II. Adaptation and Interdependencies

III. Isolation Mechanisms

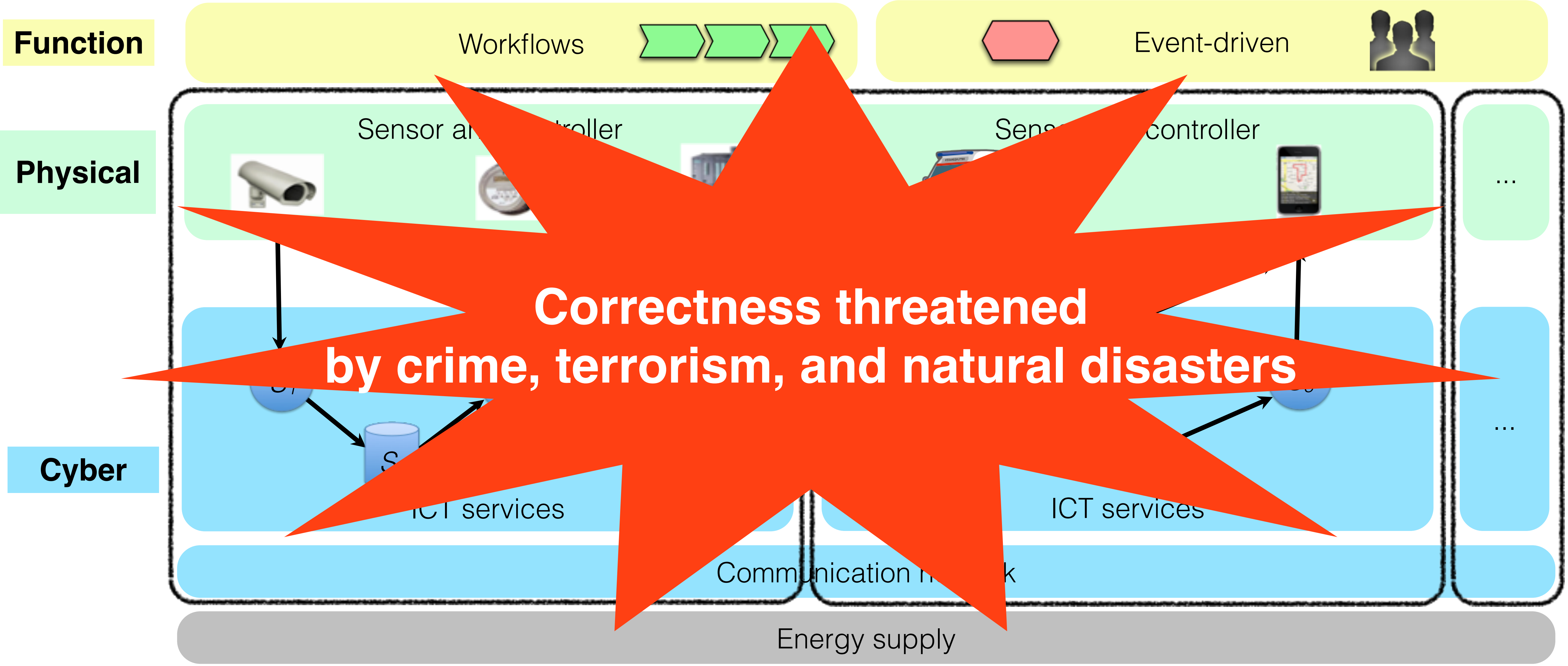
IV. Resilient Computing

I. Social Infrastructures and ICT



- ICT control systems implement functions of social infrastructures
- Real-time processing of context data and controlling location
- Centralized control
- Operated by public or private organizations

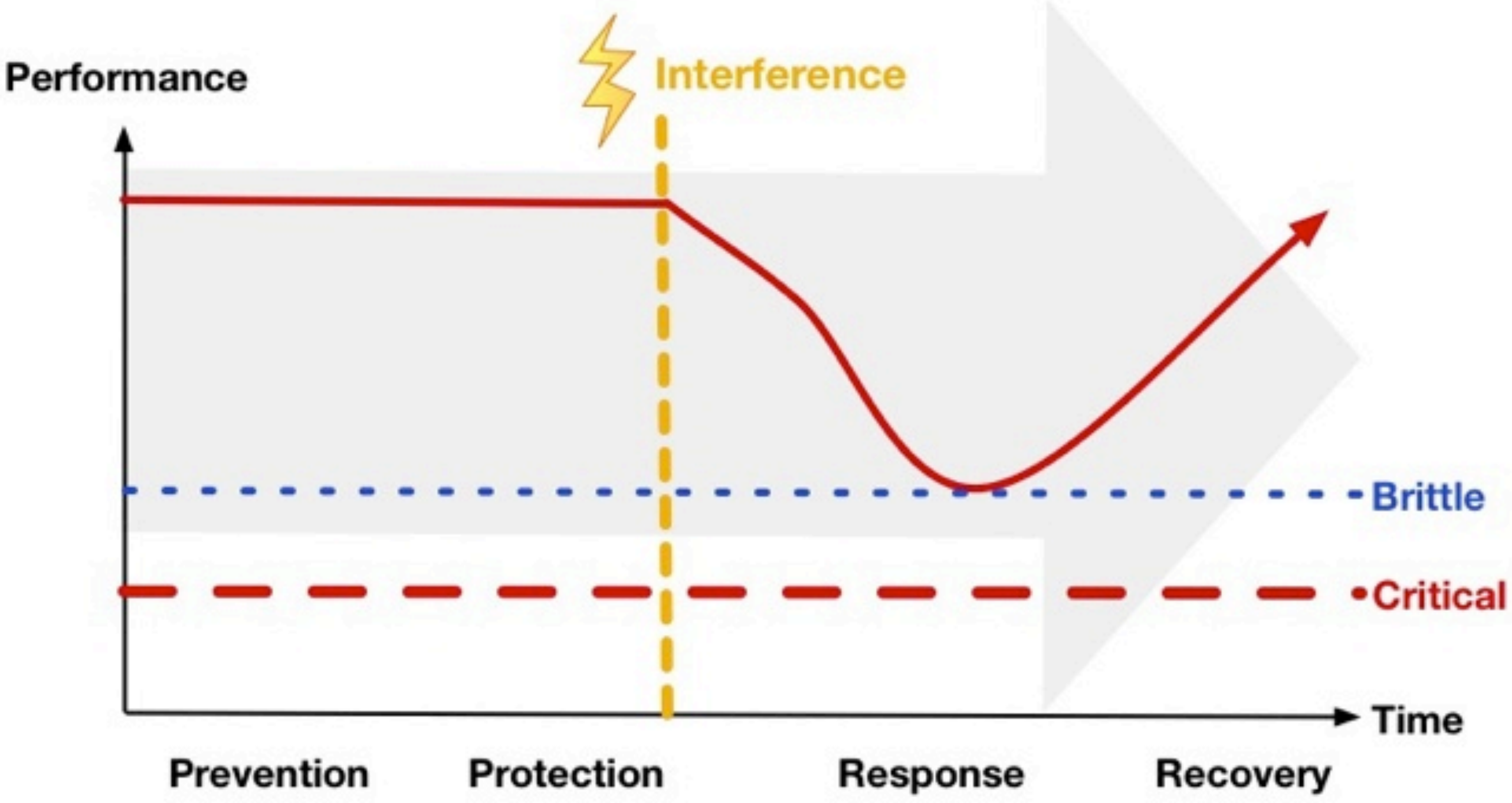
I. Social Infrastructures and ICT



- ICT control systems implement functions of social infrastructures
- Real-time processing of context data and controlling location
- Centralized control
- Operated by public or private organizations

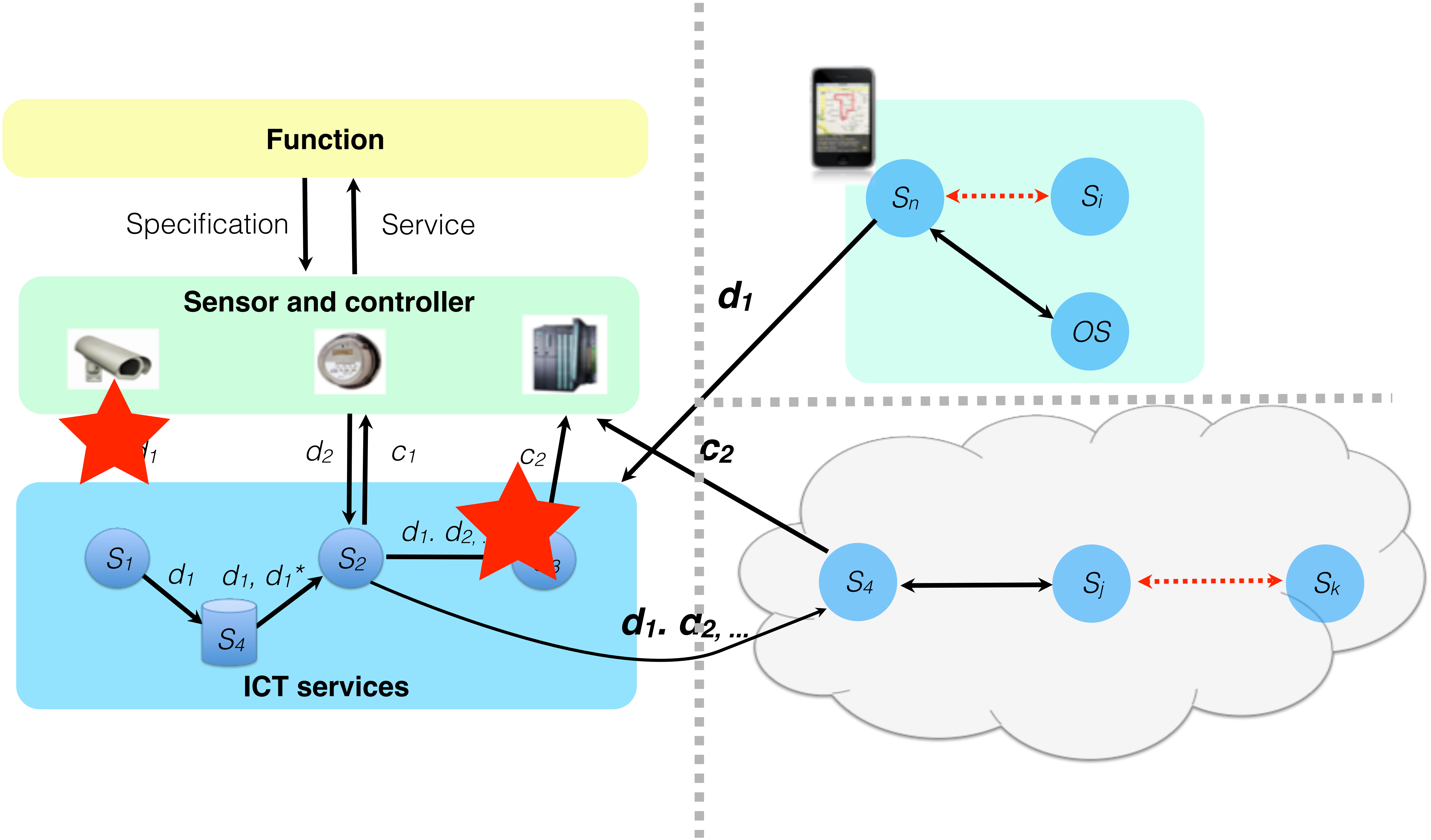
Resilience and ICT

- Persistence of dependability when facing changes (Laprie, 2008)
- Ability of an ICT system to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation (Sterbenz et al., 2010)
- An affected resilient ICT system delivers at least correct critical services in a hostile environment (brittle) (Hollnagel et al., 2006)



Own illustration following (Sheffi, 2005; Günther et al., 2007; McNanus, 2009)

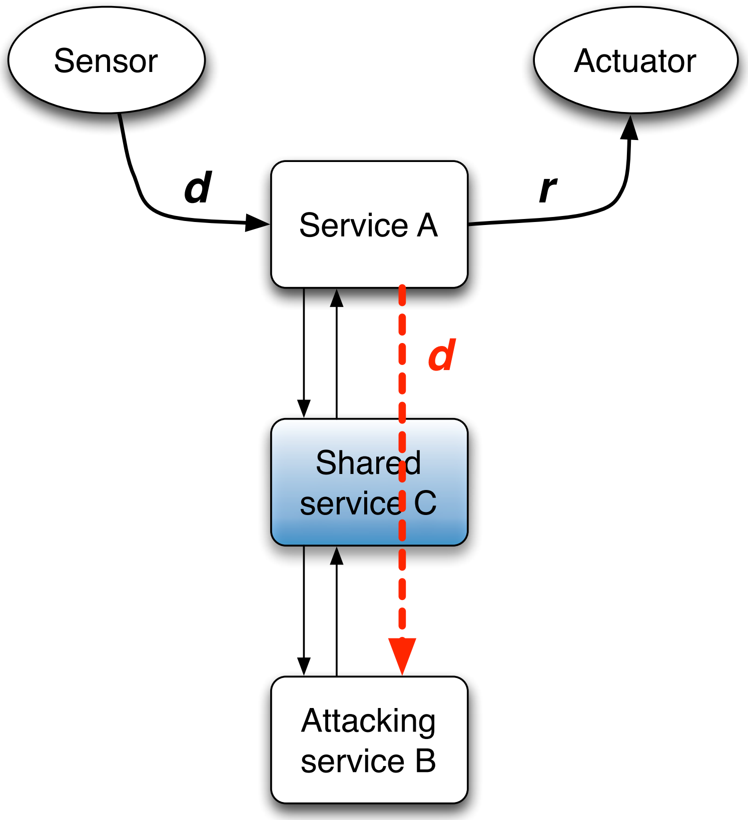
II. Adaptation and Interdependencies



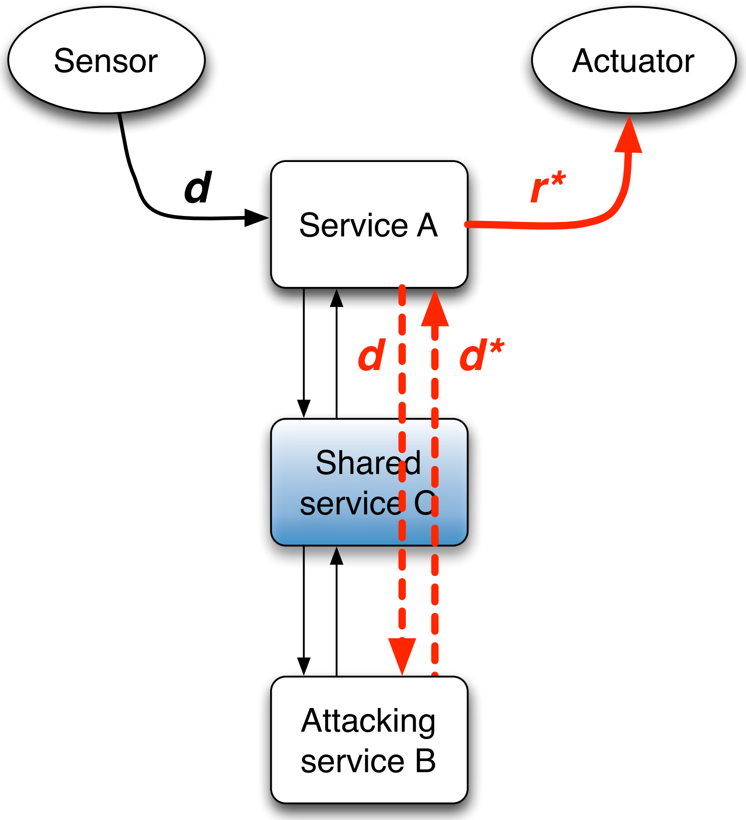
Adaptation of an ICT system → Data flows describe interdependencies

Covert Channels

Malicious interferences

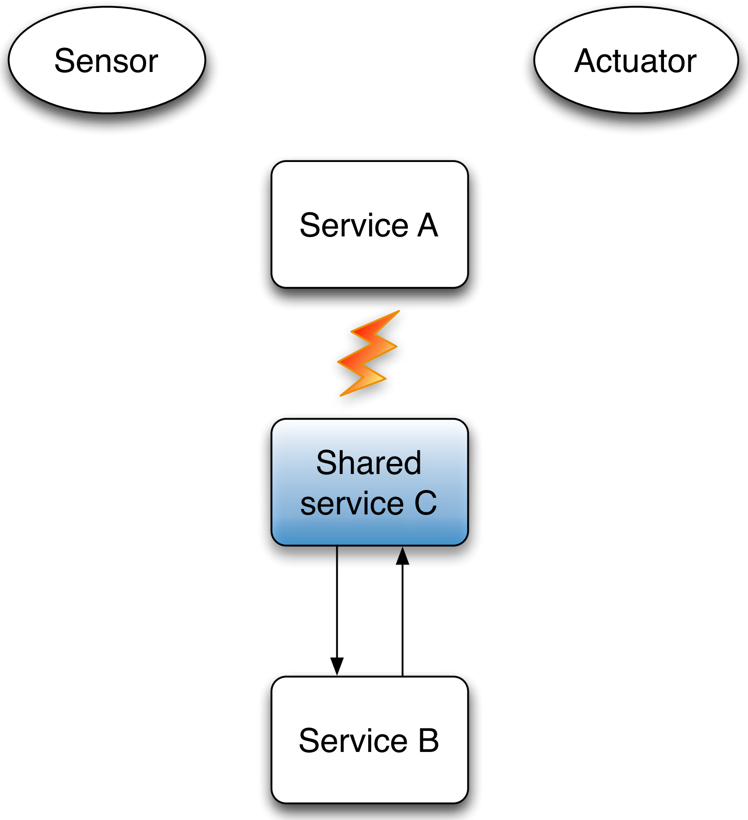


Case (a) - Passive attack



Case (b) - Active attack

Non-malicious interference



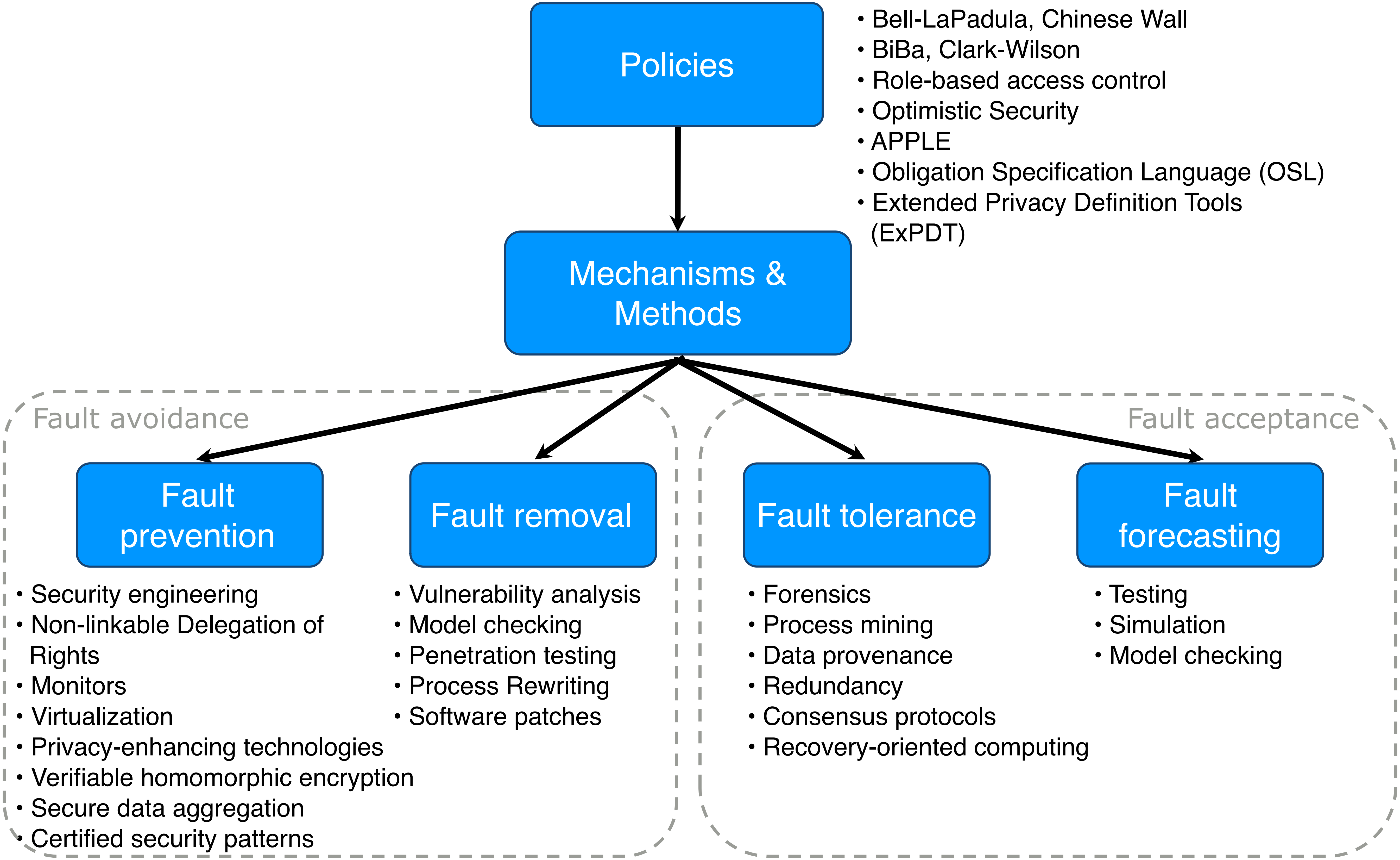
Case (c) - Non-availability

*d, d** : Input data for a data processing
*r, r** : Result of a data processing
▯ : Shared used service

Automatic detection of all cover channels is impossible (Wang and Ju, 2006)

Covert channels may be unknown and lead to a failure → Fault isolation

III. Isolation Mechanisms



Policies

- Bell-LaPadula, Chinese Wall
- BiBa, Clark-Wilson
- Role-based access control
- Optimistic Security
- APPLE
- Obligation Specification Language (OSL)
- Extended Privacy Definition Tools (ExPDT)

Mechanisms & Methods

Fault avoidance

Fault prevention

- Security engineering
- Non-linkable Delegation of Rights
- Monitors
- Virtualization
- Privacy-enhancing technologies
- Verifiable homomorphic encryption
- Secure data aggregation
- Certified security patterns

Fault removal

- Vulnerability analysis
- Model checking
- Penetration testing
- Process Rewriting
- Software patches

Fault acceptance

Fault tolerance

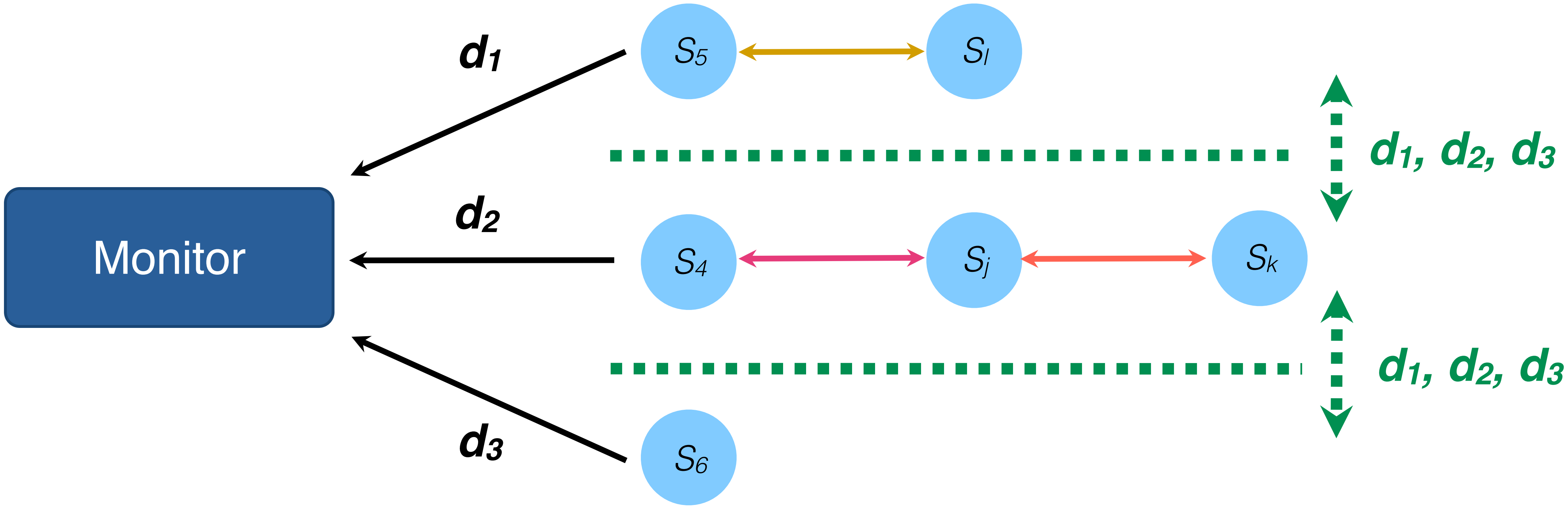
- Forensics
- Process mining
- Data provenance
- Redundancy
- Consensus protocols
- Recovery-oriented computing

Fault forecasting

- Testing
- Simulation
- Model checking

Consensus and Adaptation

Objective: Majority on correct data (sensor data, computation result)



$d_{correct} \overset{?}{=} (d_1=d_2=d_3), (d_1=d_2), (d_1=d_3)$ OR $(d_2=d_3)$

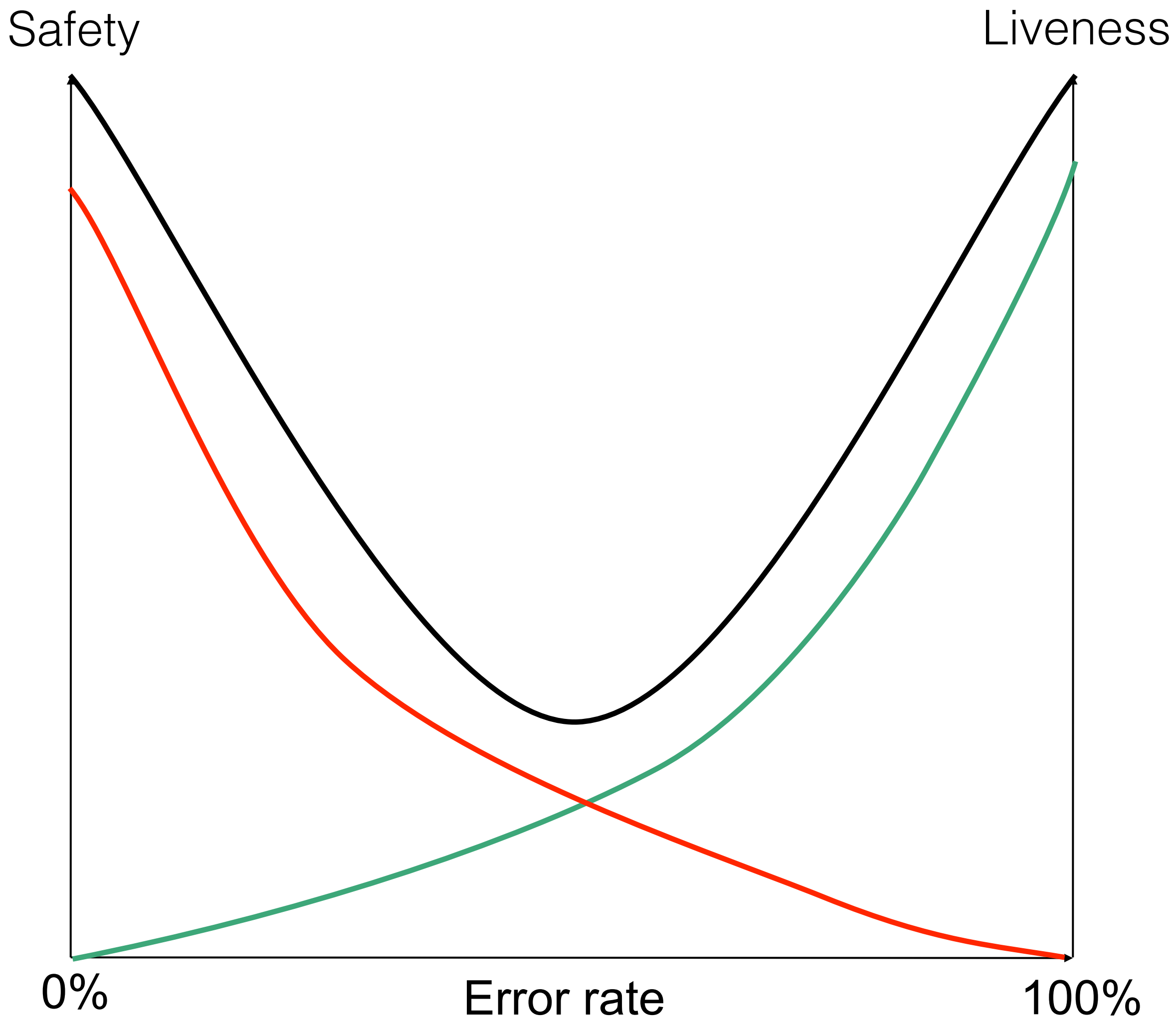
Consensus protocols and malicious faults:

- **Asynchronous communication:** Consensus not possible if one process fails
- **Synchronous communication:**
  - Tolerates t < n/3 faulty processes, with authenticated messages: t < n
  - **But: Bears risk of failure due to non-availability of data**

Cachin et al. 2011

IV. Resilient Computing

Challenge: Correct data processing in spite of covert channels

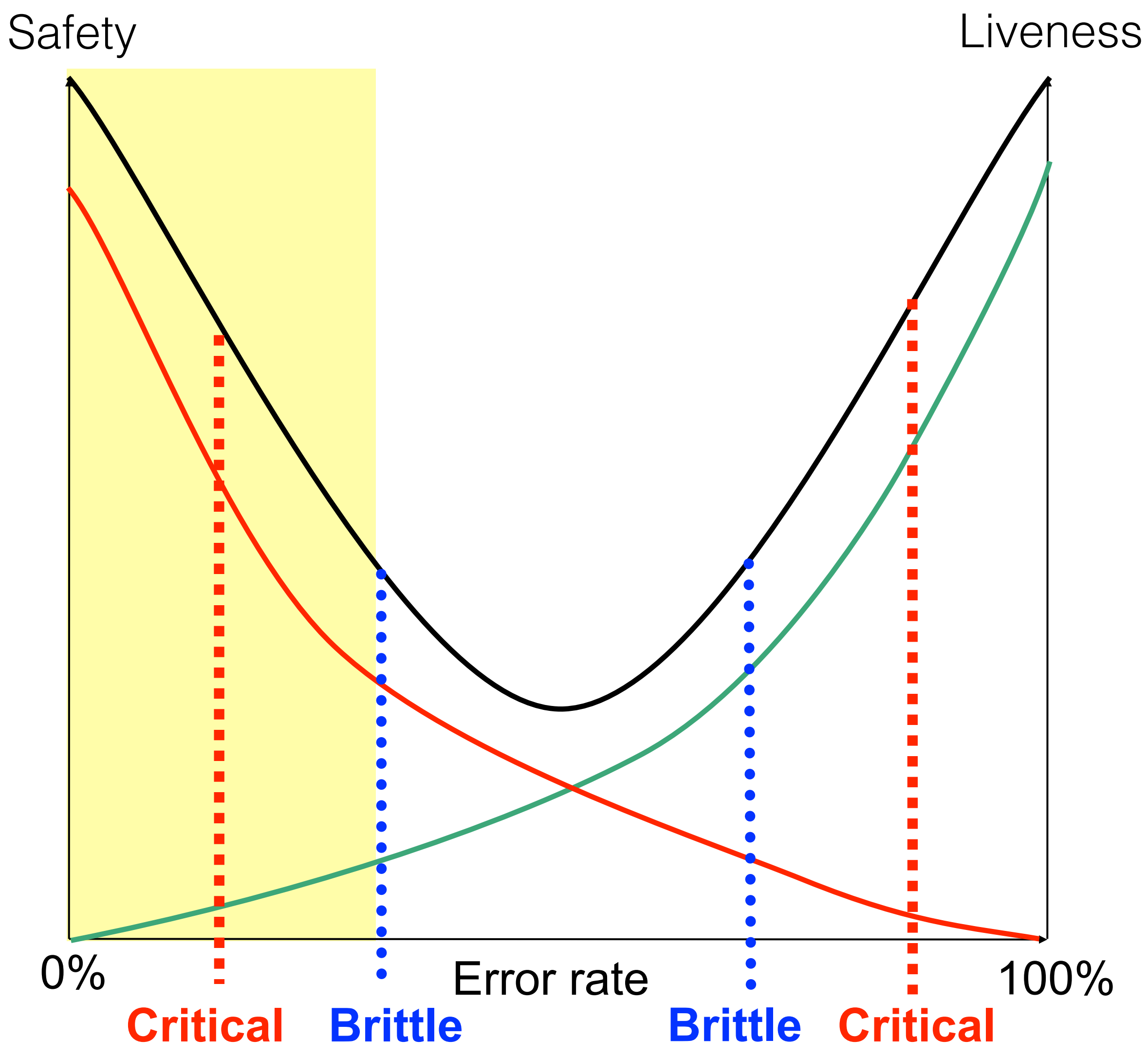


- 🟥 Fulfilled **safety** (correct) properties
- 🟩 Fulfilled **liveness** (adaptation) properties
- ⬛ Expected risk of failure

The ***Error rate*** represents the probability of faulty services of a system according to its specification

IV. Resilient Computing

Challenge: Correct data processing in spite of covert channels

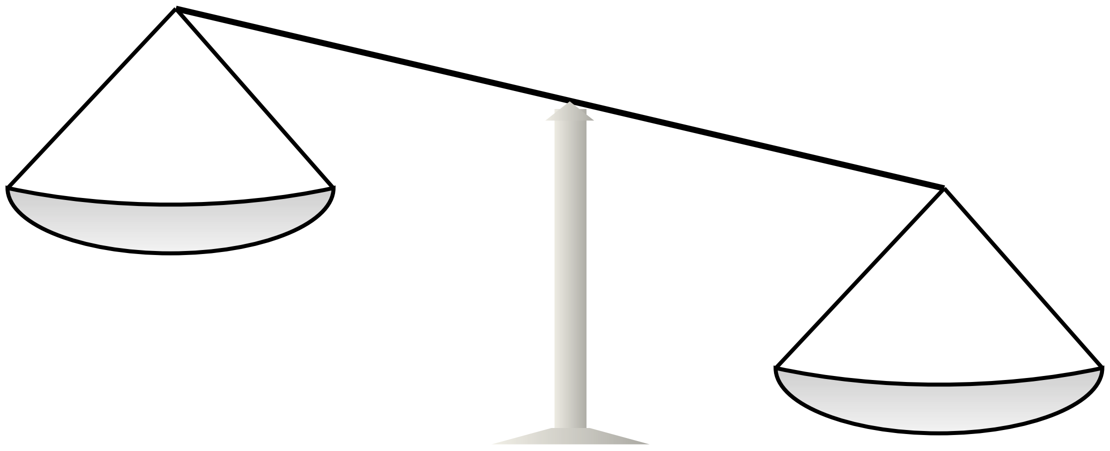


🟥 Fulfilled **safety** (correct) properties

🟩 Fulfilled **liveness** (adaptation) properties

⬛ Expected risk of failure

Failure due to safety

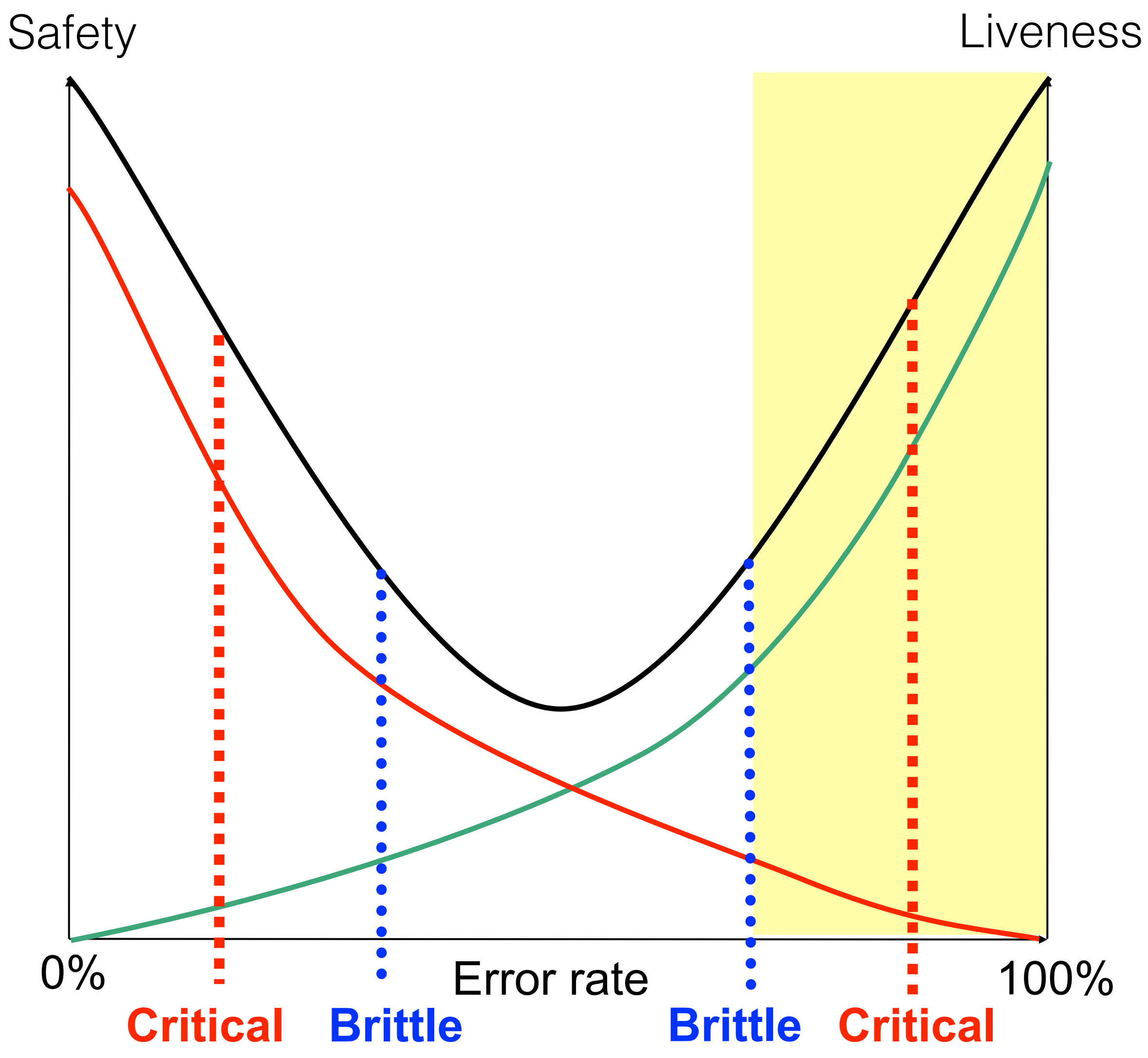


High capability of correct data processing

Few on demand data processing

IV. Resilient Computing

Challenge: Correct data processing in spite of covert channels

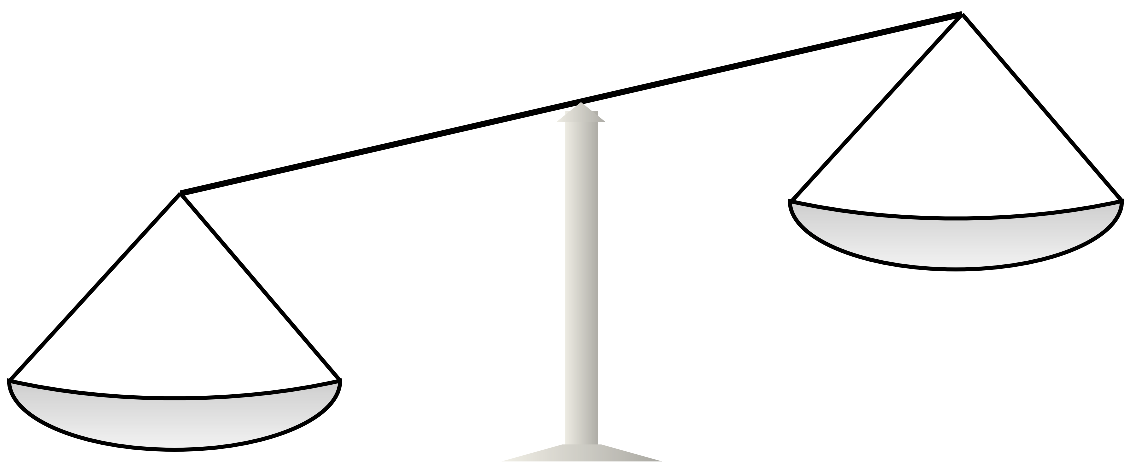


🟥 Fulfilled **safety** (correct) properties

🟩 Fulfilled **liveness** (adaptation) properties

■ Expected risk of failure

Failure due to liveness

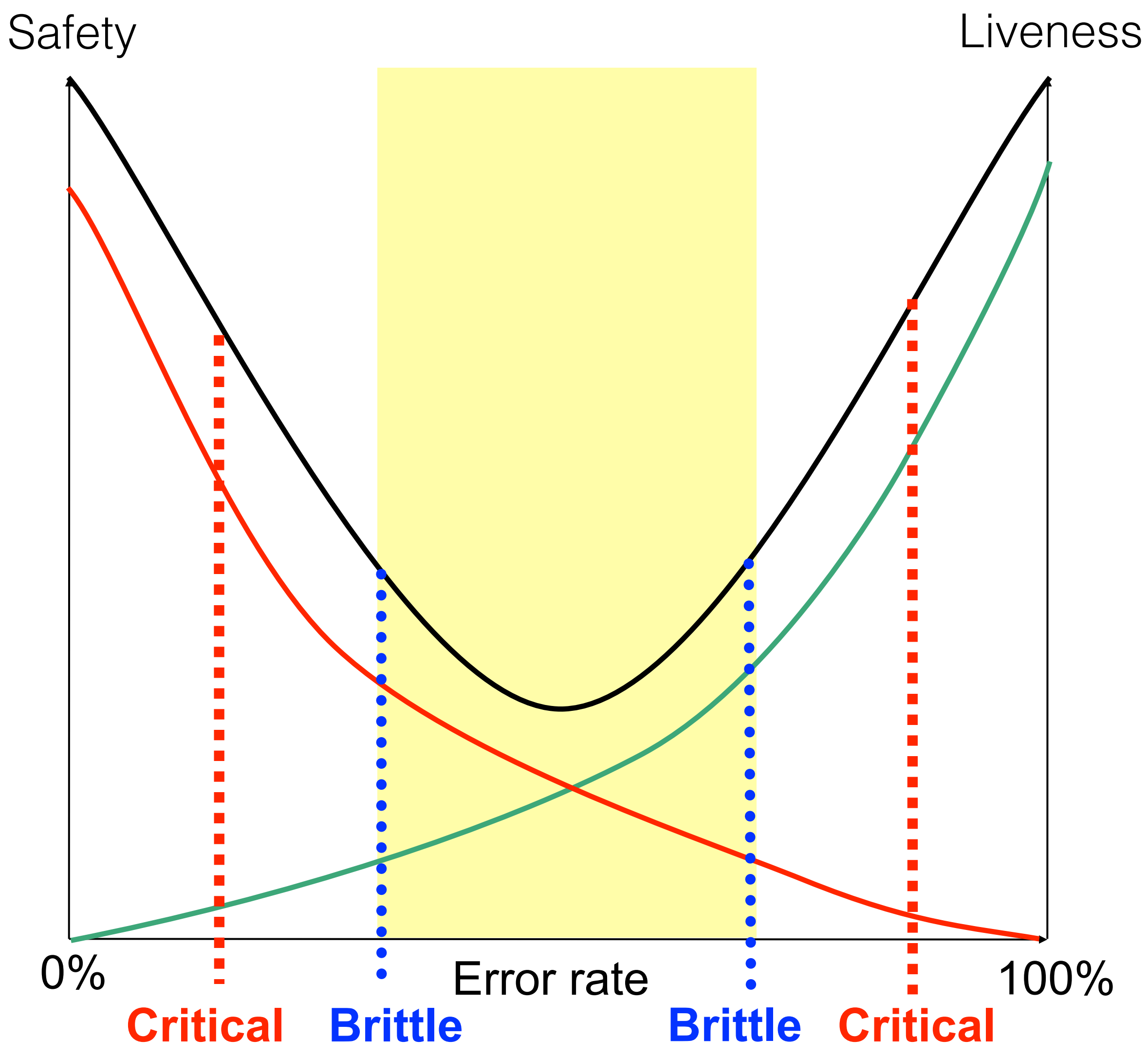


Low capability
on correct data processing

High on demand data
processing

IV. Resilient Computing

Challenge: Correct data processing in spite of covert channels

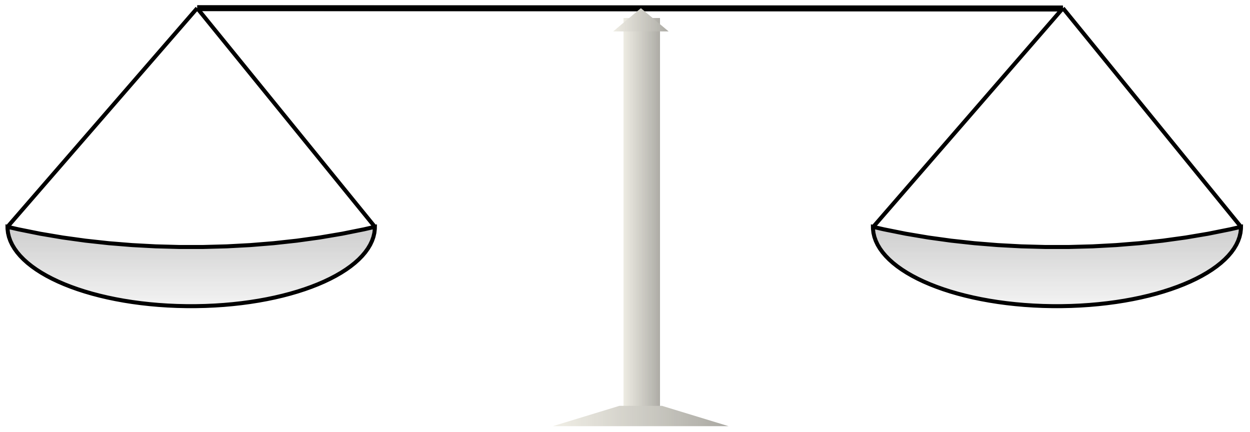


🟥 Fulfilled **safety** (correct) properties

🟩 Fulfilled **liveness** (adaptation) properties

■ Expected risk of failure

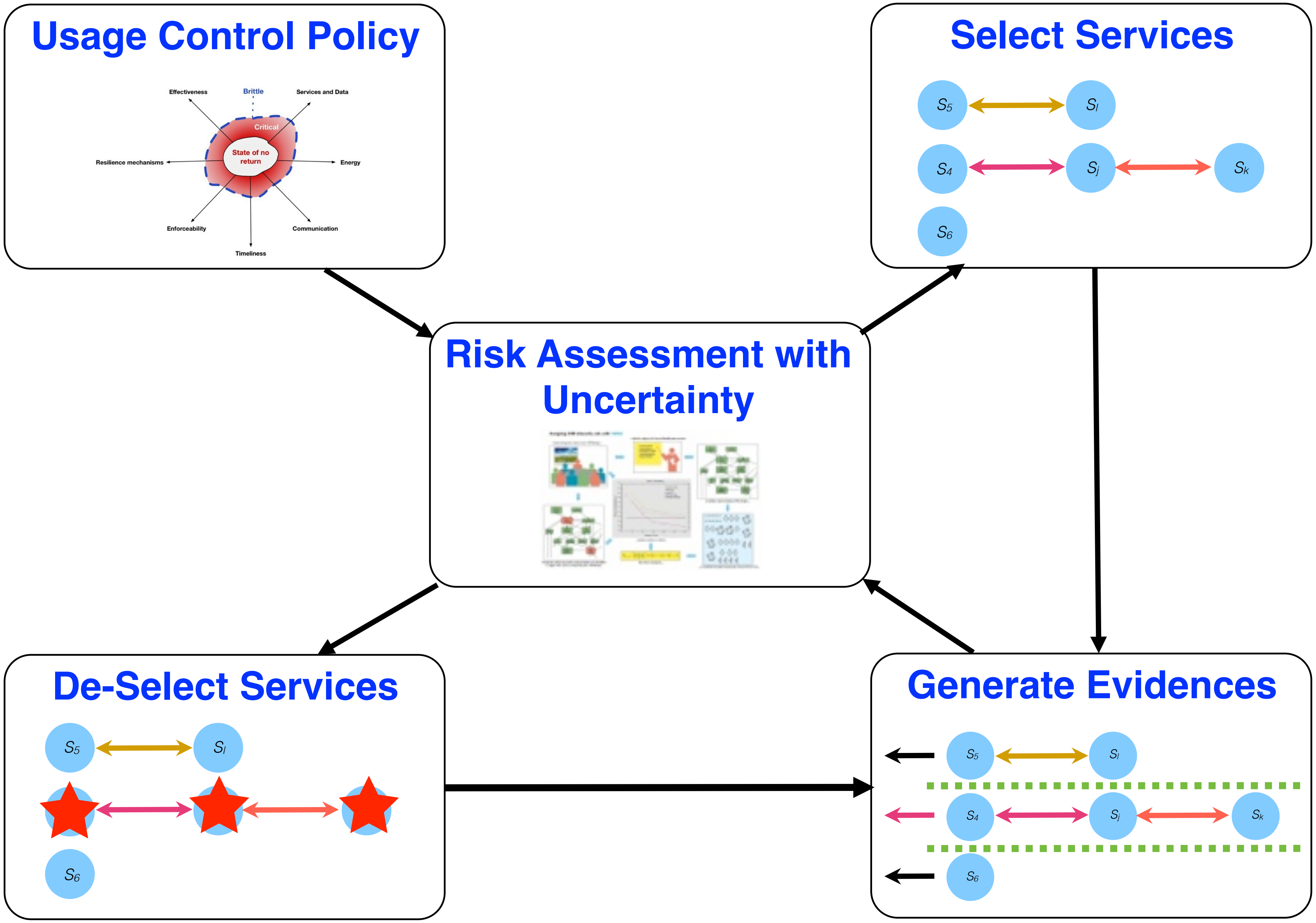
Acceptable states



Acceptable correctness of
data processing

Acceptable on demand
data processing

Security Architecture for Resilient Computing



Usage Control Policy

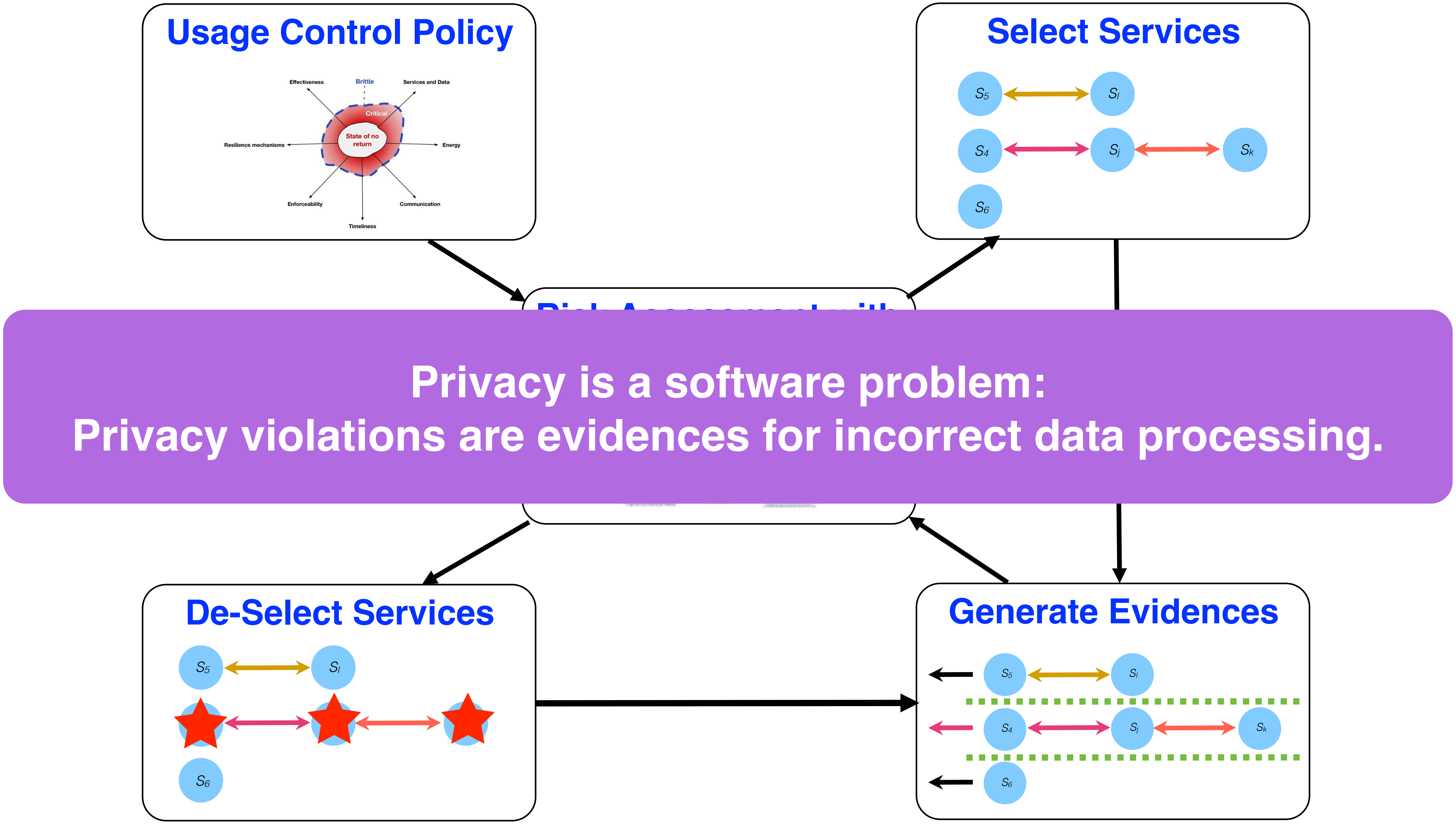
Select Services

Risk Assessment with Uncertainty

De-Select Services

Generate Evidences

Security Architecture for Resilient Computing



Privacy is a software problem:
Privacy violations are evidences for incorrect data processing.

Preliminary work: DREISAM (Delegation of Rights) & DETECTIVE (Data Provenance)