Information Infrastructure Interdependencies: systemic risk issues

IFIP WG 10.4 - Dependable Computing and Fault Tolerance

42nd meeting, 28 June - 1 July 2002

Marc Wilikens, Marcelo Masera

Joint Research Centre of the EC

http://cybersecurity.jrc.it

Marc.Wilikens@jrc.it

JRC

Contents

- Background
- CIP and interdependencies
- Information infrastructures issues
- Dependability and Risk perspectives
- Conclusions and Future initiatives

Background

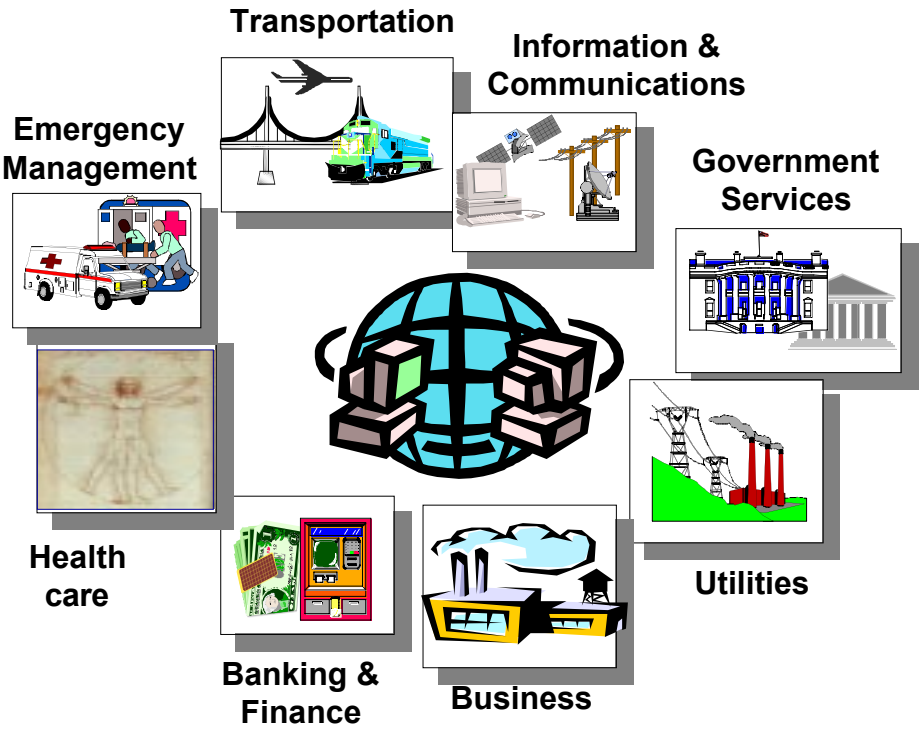
- European Dependability Initiative
  - Preparatory studies during 1997-1998: Large-scale systems
  - IST programme, FWP5, DePAUDE, DSOS, MAFTIA
- USA, CIP PDD-63 (1998), Survivability programs, *Trust* (FS) EPRI/DoD: complex interactive networks/systems initiative
- National CIP (NL, UK, S, N..), EU cybersecurity (policy, JRC)
- Information Infrastructure Interdependencies and Vulnerabilities (http://deppy.jrc.it)
  - Workshop, Brussels, 27-28 March, 2001
  - Workshop, Milan, 19-20 November, 2001
- *Interdependency* problem is intuitive but not well mastered
- ICT as enabler of interdependencies

Contents

- Background
- CIP and interdependencies
- Information infrastructures issues
- Dependability and Risk perspectives
- Conclusions and Future initiatives

Interactions among Critical Infrastructures are increasing

Critical Infrastructures



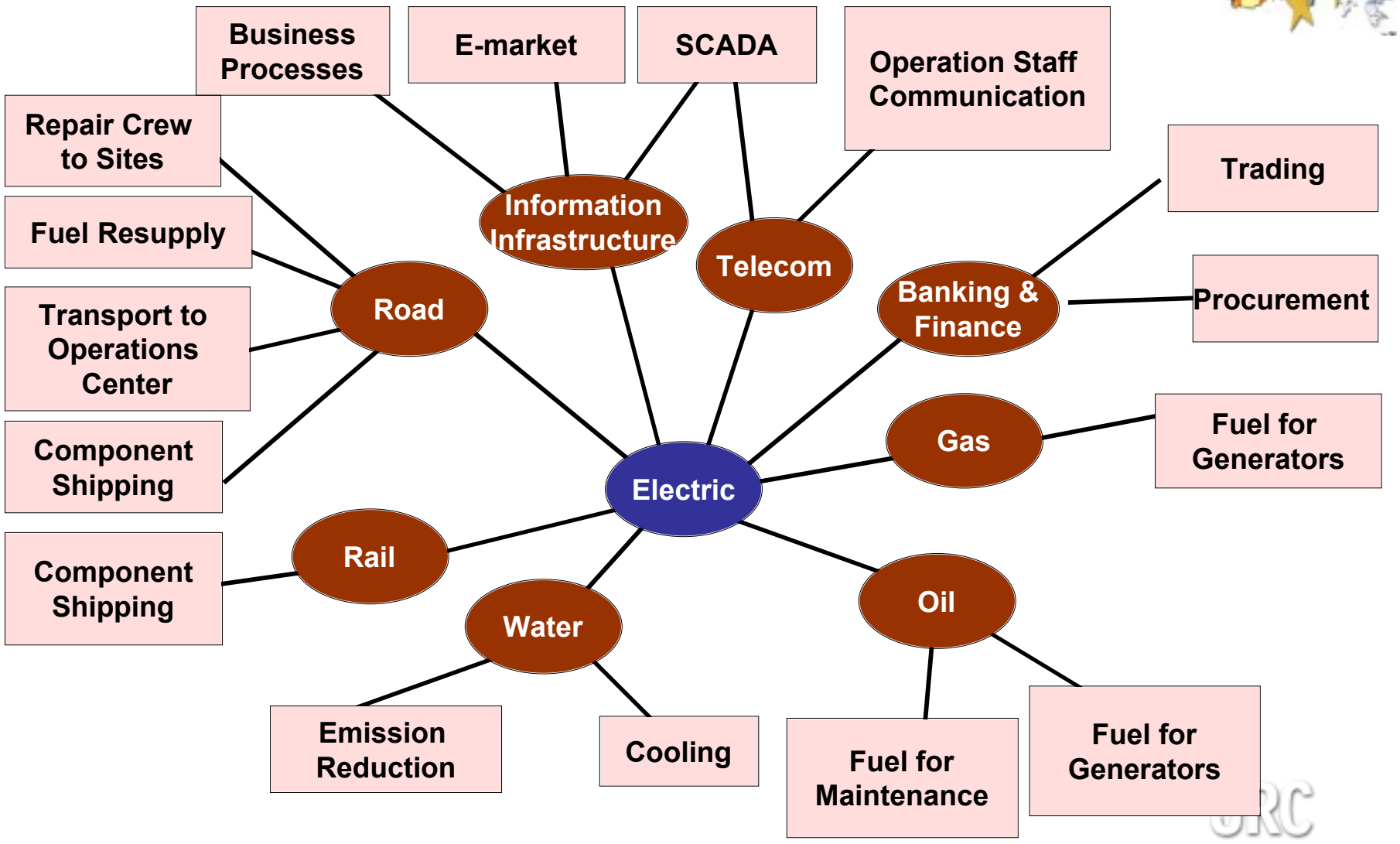
Types of Interactions

- **Physical** (e.g., material output of one infrastructure used by another)
- **Informational** (e.g., electronic, informational linkages, digital assets)
- **Organisational** (e.g., dependency through policies/regulation, financial markets, human)

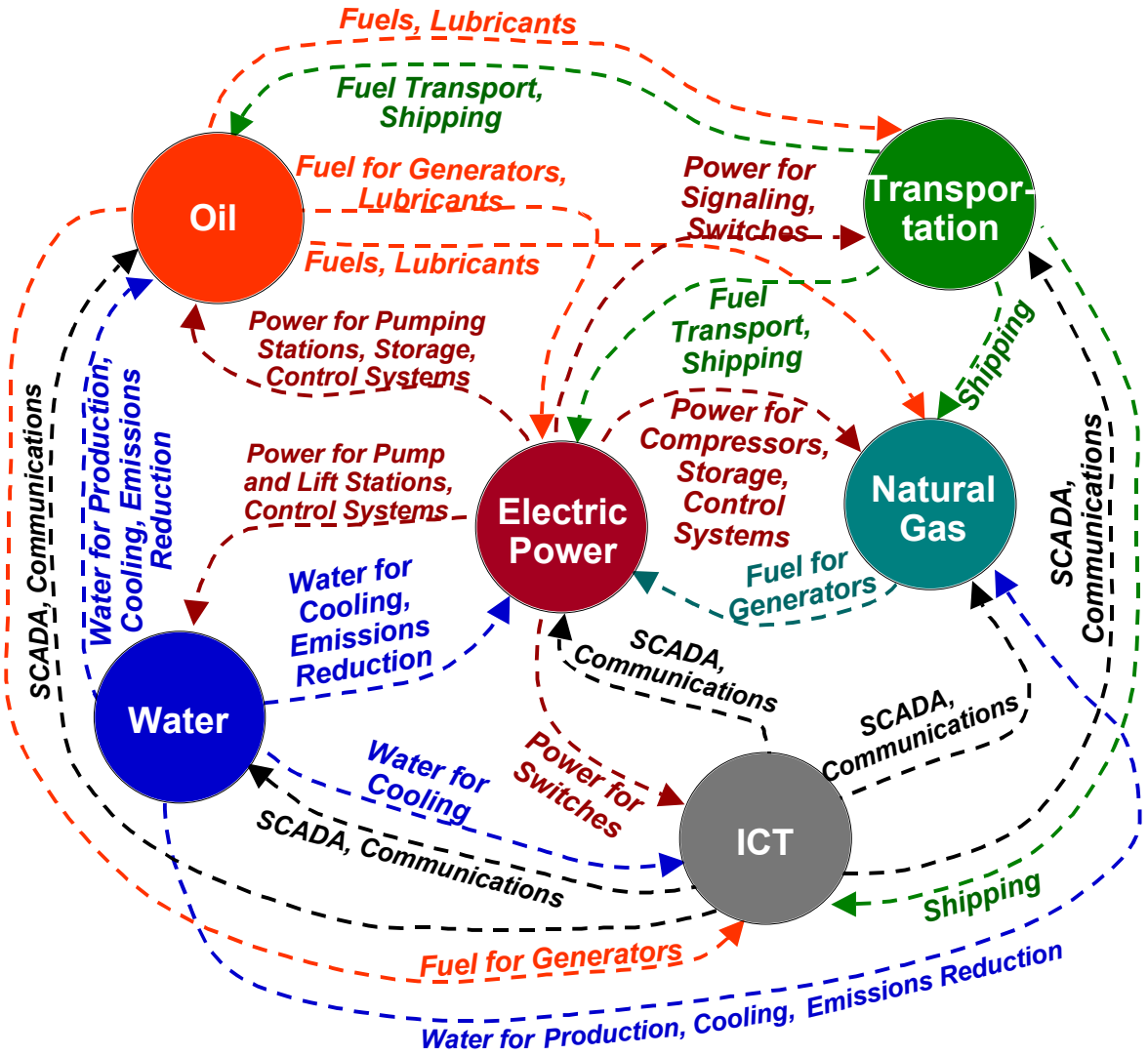
Infrastructure?

- "Complex set of interconnected, interdependent systems on which Nations, business and individuals depend for goods and services".
- Infrastructure Connection
  - A linkage between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other.
- Interconnection
  - A bi-directional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other.

Illustrative example of Infrastructures Connections *(adapted from Rinaldi et al.)*



Illustrative example of **Inter**connections
(derived from Rinaldi et al.)



Examples of Infrastructure disruptions

- California power outages, 2001
  - Disrupted US power grid, oil, gas, water supply
  - Affected other industries (e.g. air transport, agriculture)
- Galaxy 4 communications satellite control failure, 1998
  - Outage of 90% of pagers
  - Disrupted financial, banking and emergency services
- Glass fibres cuts, Telecom (NL), 1999
  - emergency microwave links were not activated!
- Electric power e-market computer intrusion, 2000
  - Anonymous ftp exploit used for interactive games; 95% bandwidth
- Tunnel fires destroying fibre optic cables, Sweden (2001-2)
- → Due to interdependencies: high severity losses; unforeseen low frequency causes

Emerging R&D analysis frameworks

- Meta-infrastructure systems approaches
  - Modelling interactions and reactions to disruptions
  - Complex Adaptive Systems (CAS): emergent systemic behaviour, capabilities of components change in response to interactions
  - Characterisation framework (Rinaldi et al.)
- Agent Based Simulation (North)
  - Agent Based Simulation (ABS) to predict and control infrastructure systems (e.g. decision rules).
  - Agent: entity with location, capabilities and memory
- Self-healing systems (Amin)
  - Infrastructure system agents reconfigure a system
- Risk Management with economic models (Haimes et al.)
  - Evaluate risk of inoperability, resource constraints to manage the risks

Issues

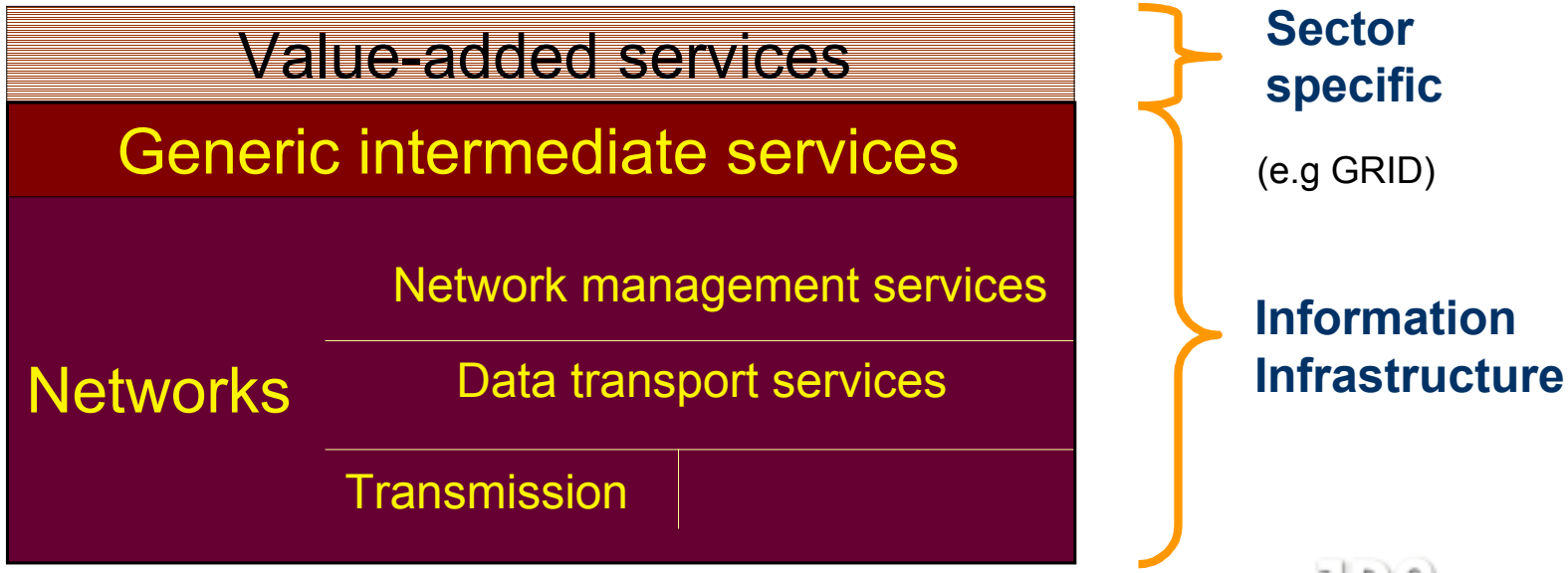
- Suitable Dependability framework
  - Focus on Modelling & Simulation and control paradigms
  - Failure concepts: disruptions, outages, …
  - Criticality detached from risk concepts
  - No coverage of interdependencies from resource sharing (CCF)
- Challenges of simulation-based approaches
  - Amount of data needed for analytical models
  - Data & model owners? (Industry, associations, Government)
  - Predictability from great number of connected models
  - Cope with evolutionary aspects of infrastructures - correctness of models?

Contents

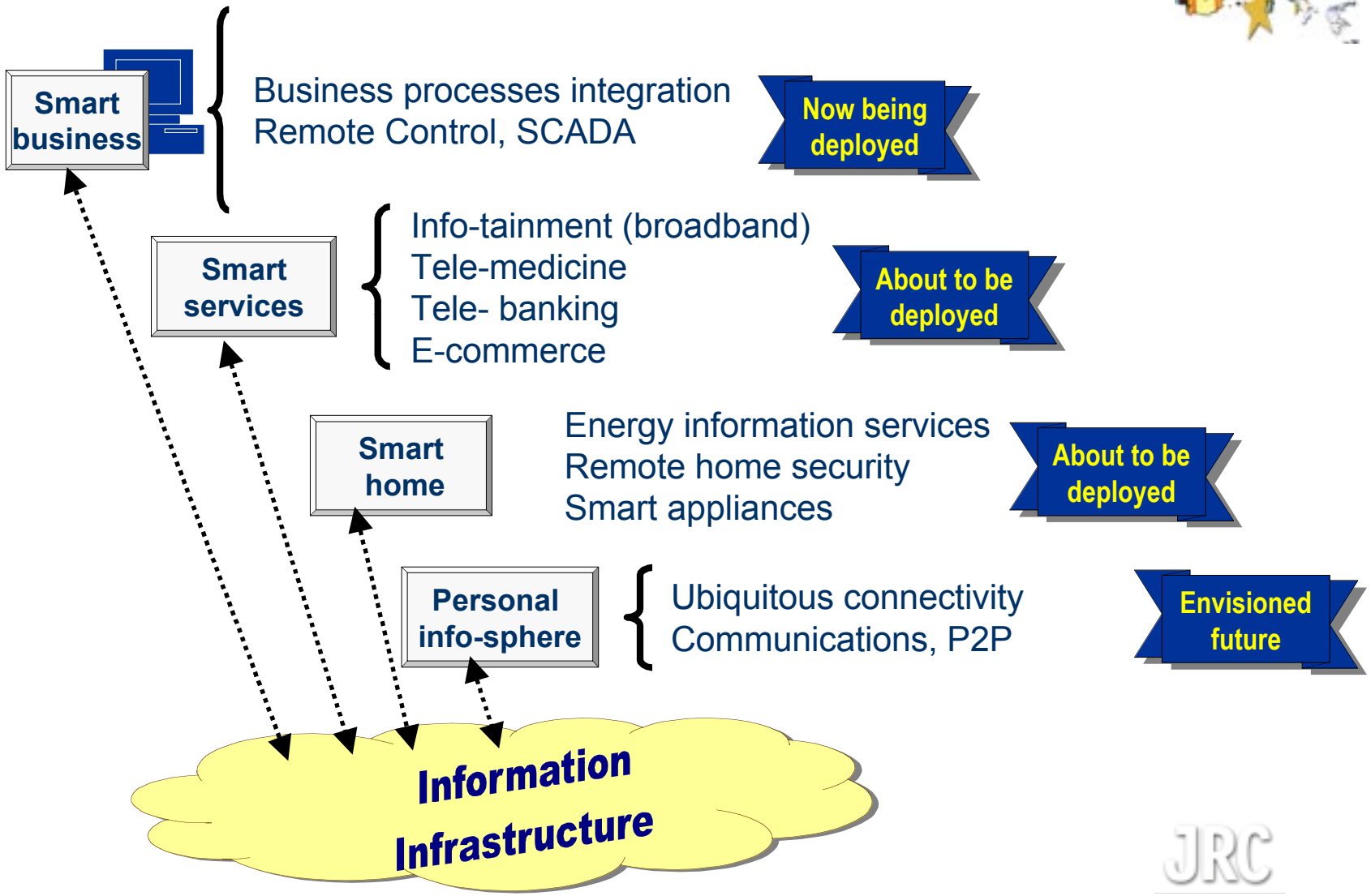
- Background
- CIP and interdependencies
- Information infrastructures issues
- Dependability and Risk perspectives
- Conclusions and Future initiatives

Information infrastructure?

- No universally accepted definition…
  - Comprising data/voice/mobile communications systems + intermediate services
  - *Unbounded, global socio-technical system, that acts as a public utility for digital data transmission/computation*



Information infrastructure as service enabler



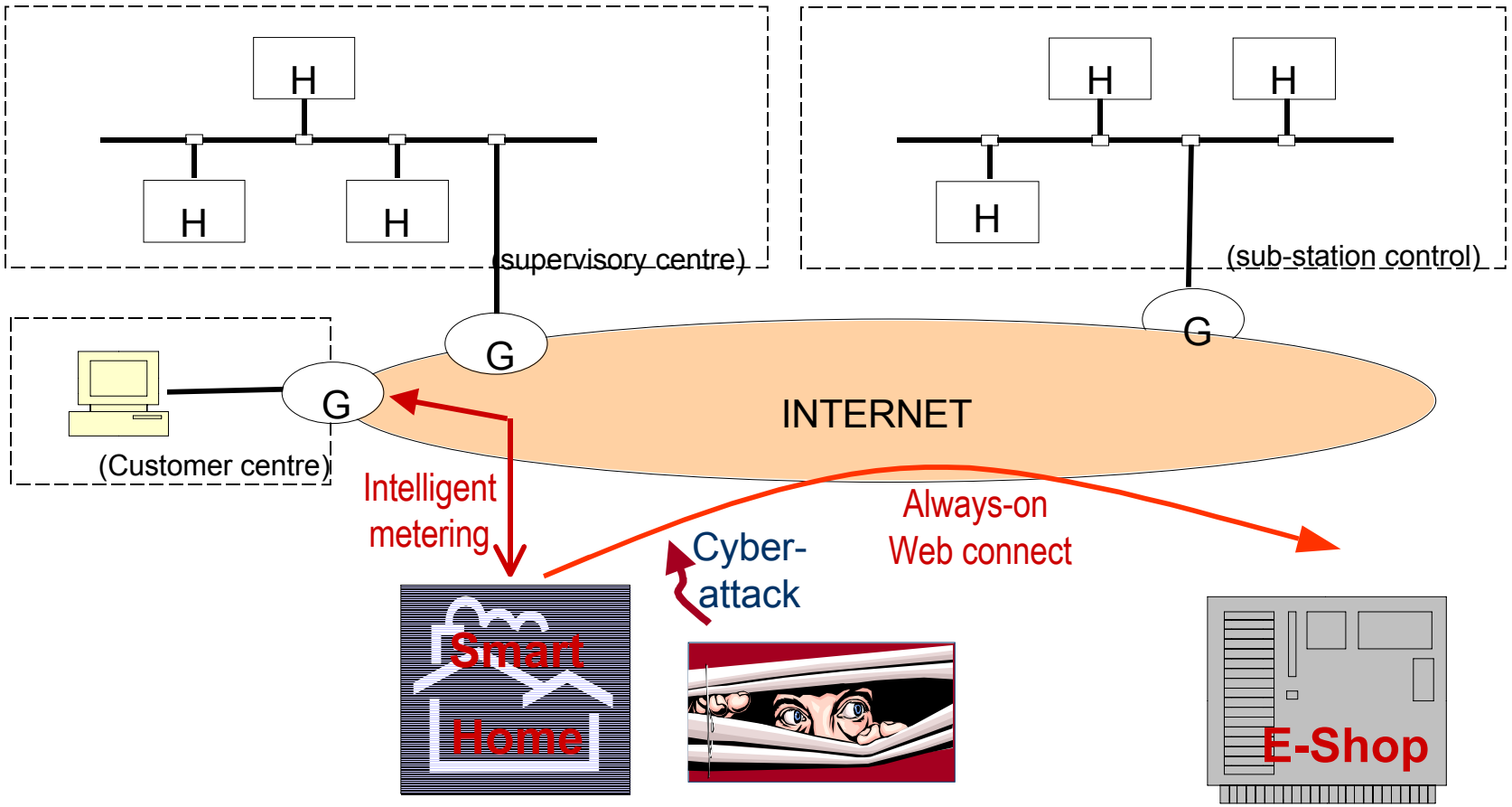
JRC

Information Infrastructure – vulnerability concerns

- Extensive ICT interdependencies, relatively new, not fully understood
  - Many actors and responsibilities without central control
  - Physical ICT security and "cyber" dependability aspects
  - Openess of infrastructure,widening threat base (malicious, accidental)
  - In 2001, 100% increase of Internet incidents and vulnerabilities reported to CERTs
  - Tight intercations: e.g. Limited slack in capacity; just-in-time business processes
  - Complex and tightly coupled interactions are more likely to produce unpredictable or unforeseen faulty situations (cf. Perrow – Normal Accidents)

➢Uncertainty in threats and vulnerabilities

Example scenario: Utilities



Contents

- Background
- CIP and interdependencies
- Information infrastructures issues
- Dependability and Risk perspectives
- Conclusions and Future initiatives

Why critical?

Assets ➔ value ➔ potential loss

No full protection

Thus, the main issue is Risk:

…for government (e.g. national security)

…for companies (e.g. continuity, data confidentiality)

…for the individual citizen (e.g. privacy)

→ Stakeholder viewpoints on risks

Risk R&D issues

Risk Assessment → **Risk Management** → **Risk Communication**

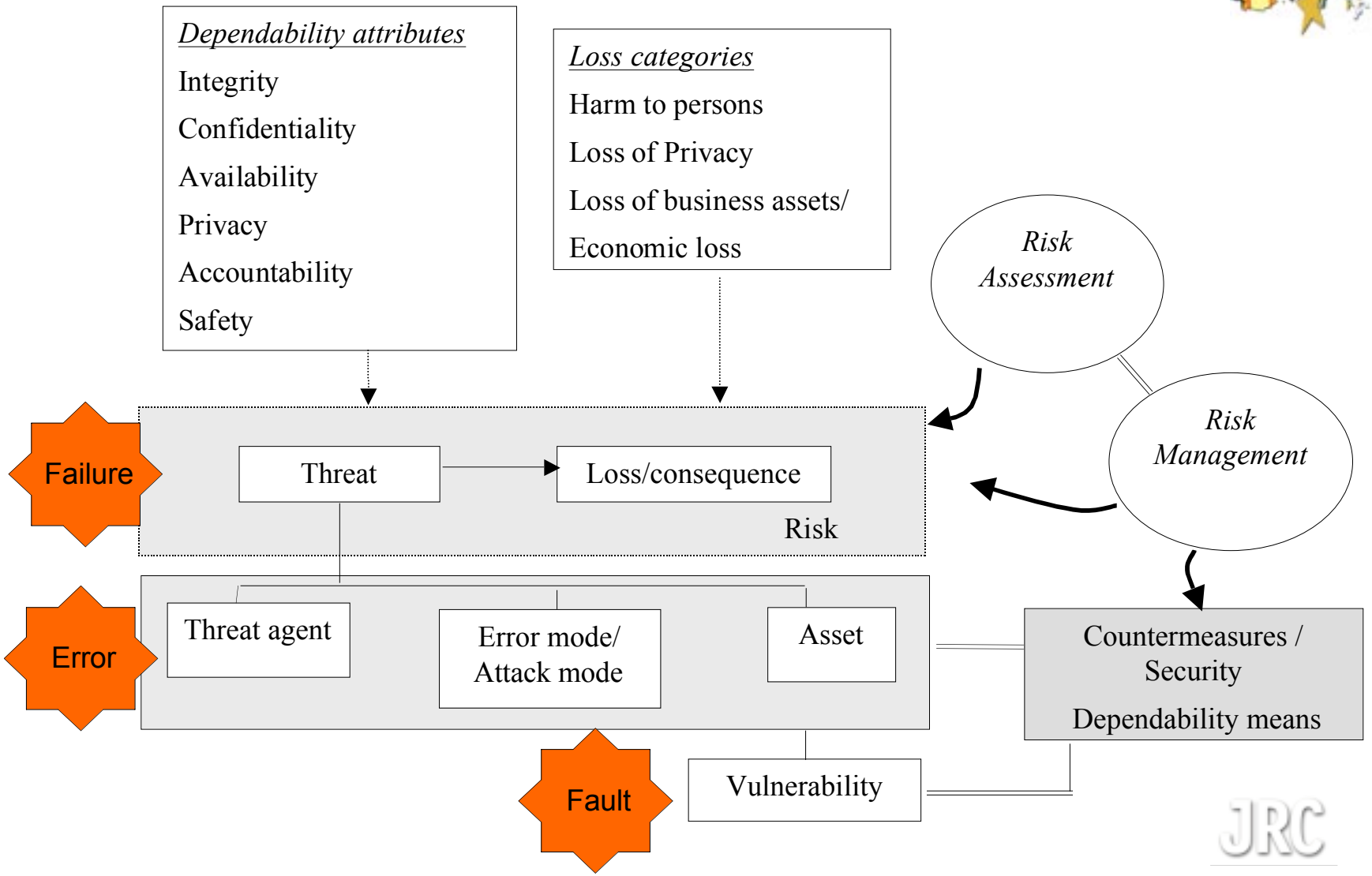
- **Likelihood estimation, uncertainty**
- **Threat, vulnerability, consequence analysis**
- **Dependability means**
- **Business Continuity**
- **Threat evolution**
- **Regulatory, ethical**
- **Policy Makers**
- **Public**

CC - ISO 15408

ISO 17799

JRC

Threat/vulnerability assessment



Categories

- **Vulnerabilities** ***(from R. H. Anderson et al., RAND, 1999)***
  - Inherent Design/Architecture
  - Complexity
  - Operation
  - Indirect/Non-physical exposure
  - Direct physical exposure
  - Dependencies on support
  - Organisational
- **Attacks** ***(SW – examples)***
  - DoS, DDoS
  - Password cracking
  - Sniffing
  - Spoofing
  - Computer intrusion
  - Session hijacking….
- **Threats (*example – selection*)**
  - Confidentiality
    - Unauthorised disclosure to TP
    - Unauthorised rights usage
    - Communications interception
  - Privacy
    - Disclosure of personal data
    - Profiling
    - Location tracking
    - Identity theft
  - Availability
    - Comm QoS deterioration
    - Data processing disruption
  - Integrity ….

Understanding Interdependencies- linear causal relationships

- Threat
  - Internal
  - External
    - Independent
    - Dependent on faults within other infrastructures
- Threats caused by faults within other infrastructures

  Probability that an error will be present in infrastructure k given that a fault appears in infrastructure i=1, 2, …
- Interdependence

  Measure of the effect of an error in infrastructure k, caused by a fault in infrastructure i=1,2, …, on the dependability attributes of a specified service in k.

Understanding Interdependencies- is the fault pathology different?

- Fault -> Error -> Failure model
- Fault = vulnerability? Yes for, design process, component, operation, human, …
  - Maturing at the technical component level:
    - Dictionaries: CVE.Mitre.org; DBs: CERTs, …,
- Vulnerabilities generated from complex interactions?
  - Facilitator for triggering dormant faults
  - Reinforce effects of existing faults
    - Cascading, escalating failures
  - Other types of failures (slow moving, a-symmetric)
  - Fault as an exploitation of a normal capability (exposure)
- Need to address faults at higher abstraction levels
  - At infrastructure level and business process level

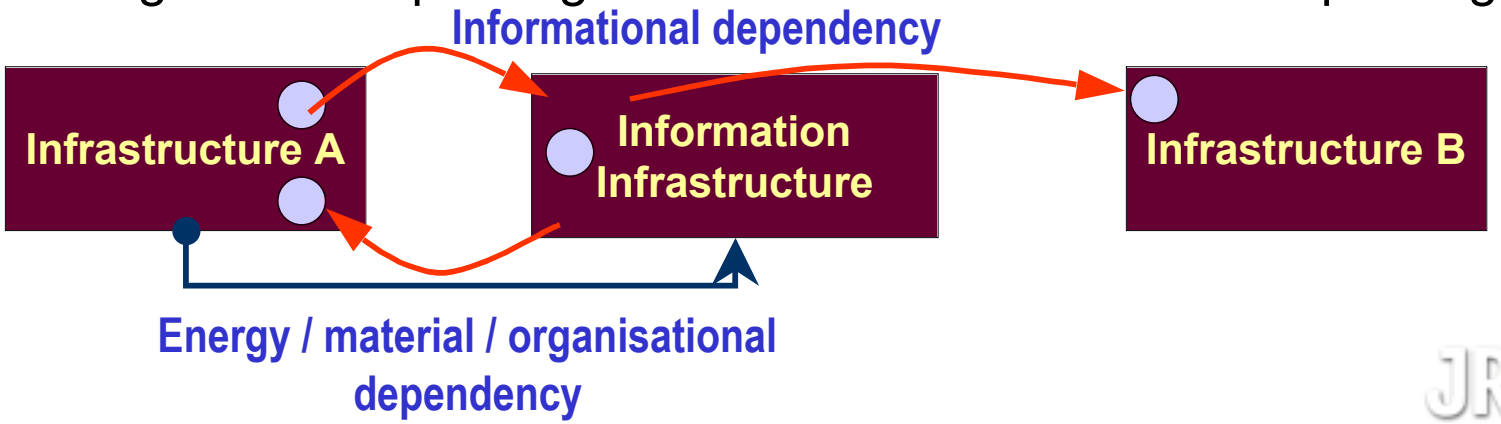
The increasing role of informational dependency

Nature of the vulnerability problem:

- Information Infrastructure acts as container and transport medium for critical information assets - an asset of one system crosses boundaries of jurisdiction
- Assets exposed to vulnerabilities of the information infrastructure (protocols)
- Enables tight coupling: small modifications (f.i. integrity) might provoke crucial disruptions in applications

Assure business continuity in case of compromise of information assets (e.g. emergency/ crisis management situations)

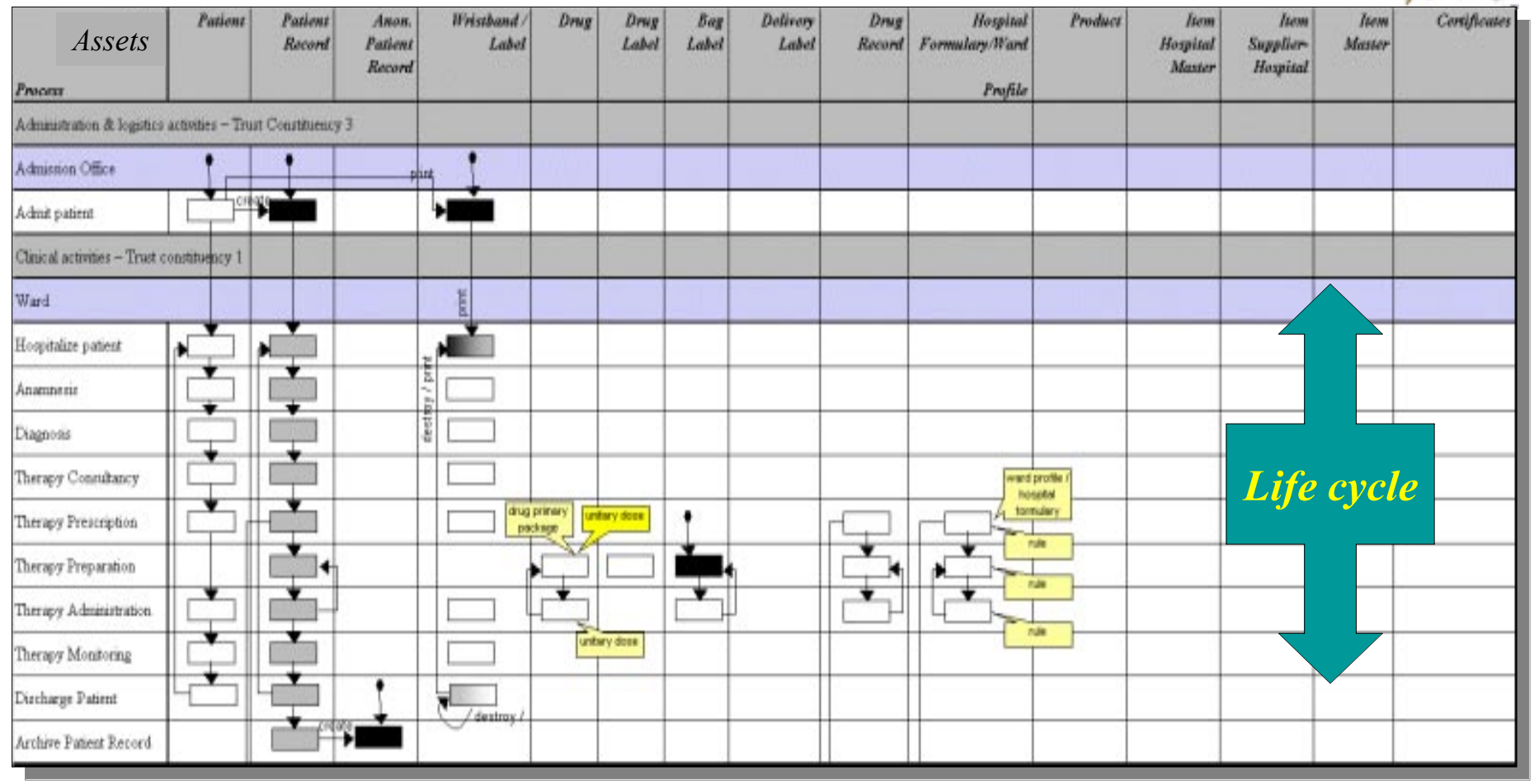
Needs 'Usage Control' paradigm in addition to access control paradigm



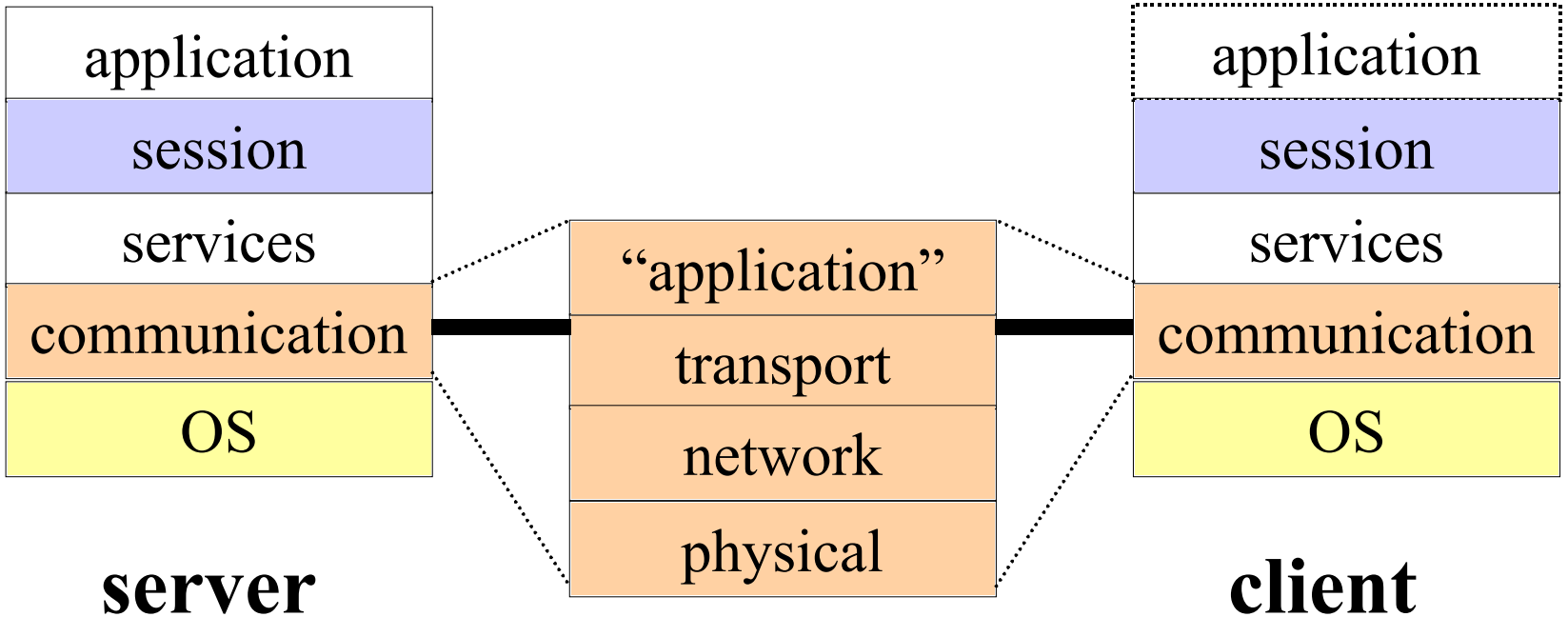
Digital Assets

- **SCADA applications (example)**
  - **Control commands**
  - **Configuration parameters**
  - **Information requests/provision**
  - **Events**
  - **Alarms**
  - **Periodic status values**
  - **Maintenance**: software updates
- **Business processes**
  - **Life-cycle models of assets**
- **Personal data**

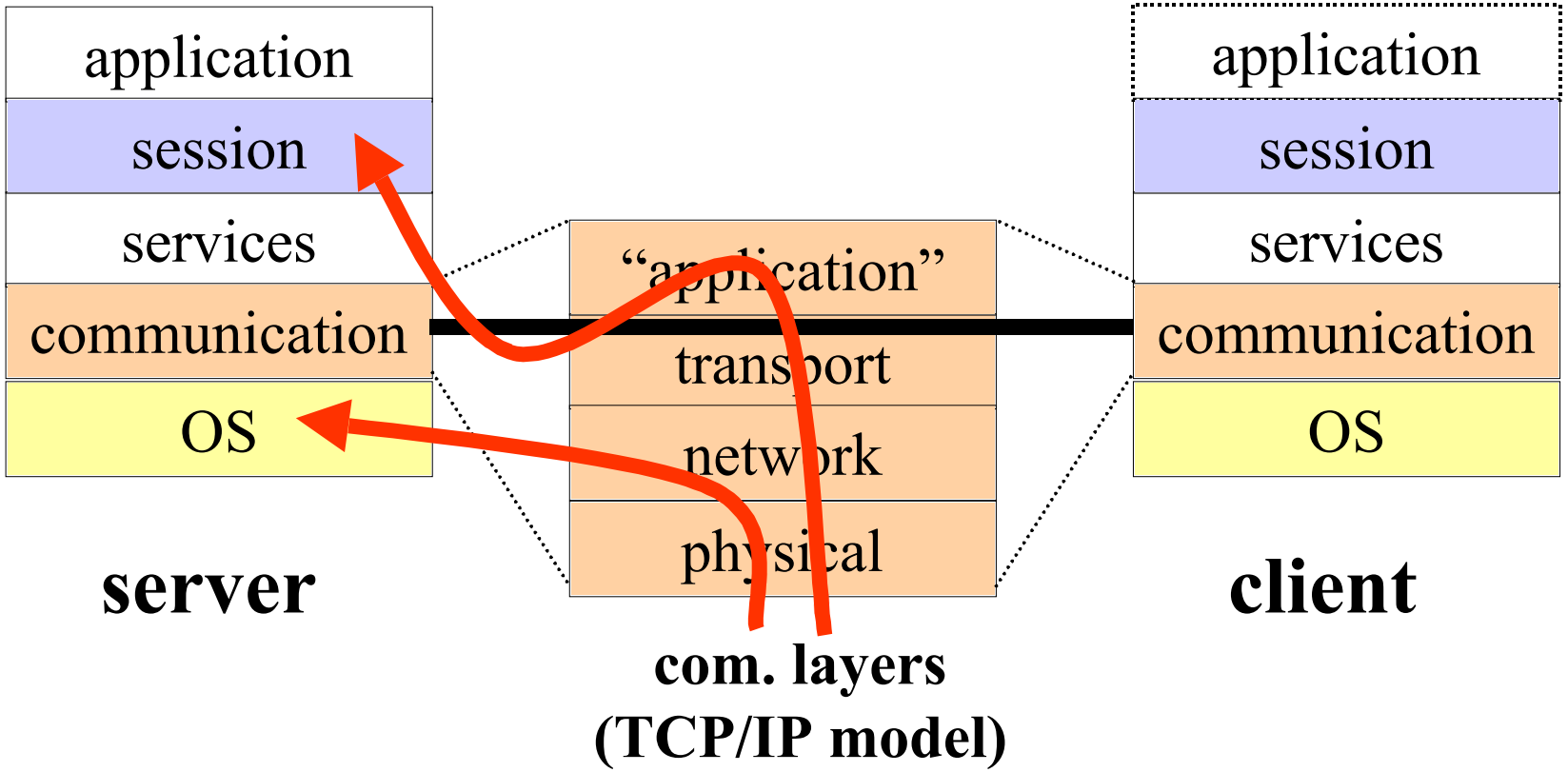
Asset life-cycle models: Health process



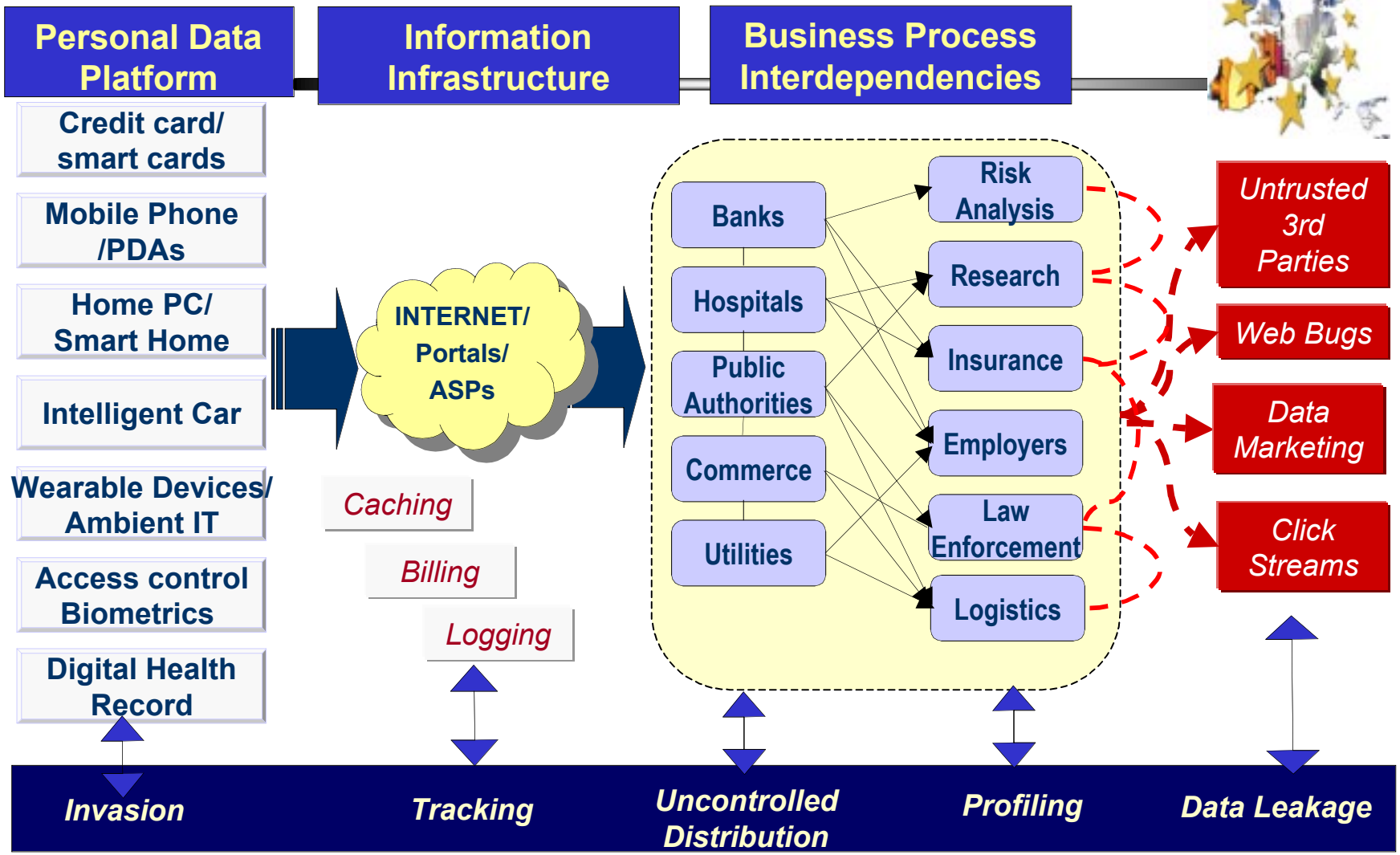
Need for vulnerability models at the different layers of the II



Need for vulnerability models at the different layers of the II



I3V and Privacy/Identity perspective



Contents

- Background
- CIP and interdependencies
- Information infrastructures issues
- Dependability and Risk perspectives
- Conclusions and Future initiatives

Concluding remarks

- Some challenges:
  - Modelling interdependencies from dependability perspective
  - Concepts, attributes
  - Risk Management methods across interdependent infrastructures
    - Systemic risk, evidence of events, liabilities in interconnected systems
- Cross-industry sectors + government problem
- Requires comprehensive and interdisciplinary R&D
  - dependability, risk, modelling/simulation
  - legal, socio-economic and policy research
- FWP6-R&D roadmapping: AMSD, DDSI, ACIP
  - workshop 19-20 September 2002

A Declaration of Interdependence

JRC