

# Interdependencies and vulnerabilities in information infrastructures: implications for embedded systems

Marcelo Masera

Real-time & Embedded Systems Forum  
The Open Group  
25<sup>th</sup> April, 2001



Joint Research Centre  
European Commission



Institute for Systems,  
Informatics and Safety





# Contents

- **Institutional context:**
  - Joint Research Centre - EC
  - The Dependability Initiative (EC R&D Framework Programme)
  - The eEurope Initiative
- **Interdependencies and vulnerabilities**
- **Trust, security and Information Infrastructures**
- **The challenge of information assets**
- **R&D concerns for embedded systems**



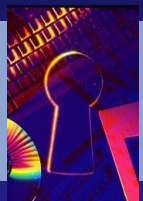
# JRC's Mission

The **Joint Research Centre** is a Directorate General of the European Commission.

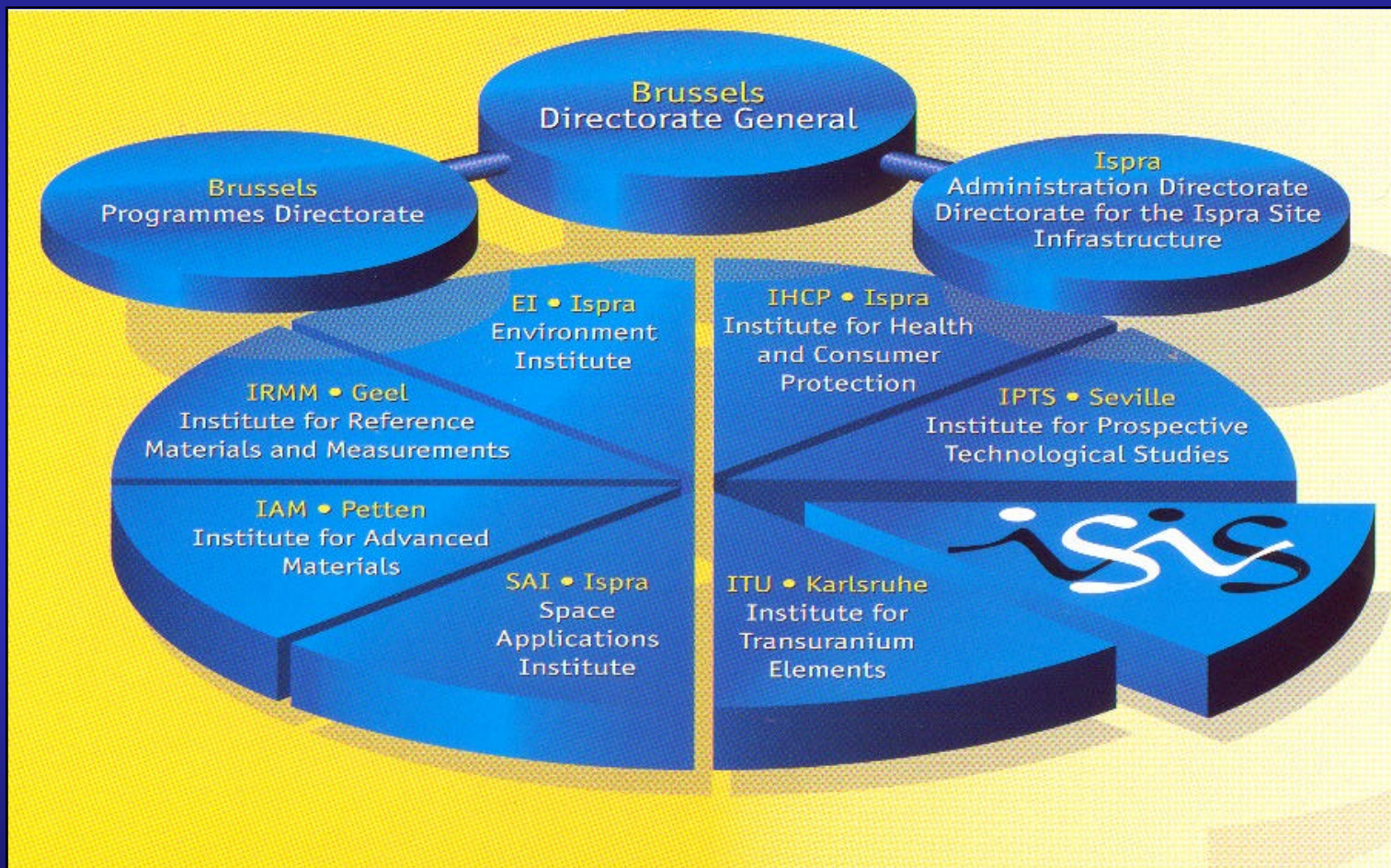
The JRC mission is:

*".. to provide **customer-driven scientific and technical support** for the conception, development, implementation and monitoring of **EU policies**...*

*...Close to the policy-making process, it serves the **common interest** of the Member States, while being **independent** of special interests, whether private or national."*



# JRC's institutes





- Guiding principle:
  - Citizen concerns and the public interest
- Support **EU policies** - focus areas:
  - Raise profile of technology issues and challenges
  - Promote technology validation and common evaluation criteria
  - Complement the implementation of EU R&D (IST programme)
- Foster **European R&D**
  - networks of research, industry, customers
  - knowledge integration
  - technology trials & demonstrators
  - knowledge dissemination



# JRC & Information Society

- **Focus on assuring trust and confidence in the Information Society**
  - Provide S&T support to the conception & implementation of EU policy
- **Current activities:**
  - Dependability of critical information infrastructures
  - Online privacy and filtering
  - Online out-of-court dispute settlement systems
  - Combating cyber abuse
  - Trial infrastructure: TRINIDAD



# JRC's role

- **JRC's role:**
  - ⇒ act as technical liaison between practitioners and EU policy, in the understanding of new **risks**, **vulnerabilities**, technical **challenges** and **criteria**
- **Focal point:**
  - Better integrate technical skills at the intersection ***Access-Trust***: new vulnerabilities, knowledge access and user empowerment tools for safeguarding citizen rights in a digital world.

# Focus areas

**Technical context (ICT)**

- Multimedia communications
- Mobile and configurable systems
- Embedded & RT systems
- New business processes/ intermediaries
- Standards, CC

**Complexity & dependability**

**Policy context**

- eEurope
- eCommerce
- eLearning
- Data protection
- Consumer protection
- Cybercrime communication
- EU top level domain

**Social context**

- Commerce
- Education and Training
- Health care
- Energy & information
- On-line financial services
- Government and public services

**Trust & Confidence**

The eCitizen

Challenges addressed by JRC

Safeguarding citizen rights

User empowerment and access to reliable knowledge resources

Well-founded trust in the information infrastructure

Redress mechanisms  
Online privacy

enabler

Content evaluation and filtering

Web access tools

enabler

Trust intermediaries  
Vulnerabilities, threats



# 5<sup>th</sup> Framework Programme

- **Trust and dependability: horizontal concerns**
- **Dependability Initiative:**
  - *IST 2000/1 CPA4: Towards dependable and survivable systems and infrastructures*
    - *dependability and survivability of the global information infrastructure*
  - *IST 1999 CPA2: Dependability in services and technologies*
- **On-line Forum: <http://deppy.jrc.it>**



# Future FwP..

- **IST High-level advisory group (ISTAG):**  
*“Start creating the **ambient intelligence** landscape for seamless delivery of services and applications in Europe ...”*
- **New R&D paradigm:**
  - ubiquitous computing +
  - ubiquitous communication +
  - intelligent interfaces



- **Policy framework**
- **“An Information Society for all”**
  - one of the objectives:
    - **secure electronic access** (Secure networks and smart cards)
- **Stockholm European Council (23-24 March 2001)**
  - “...the Council together with the Commission will develop a comprehensive strategy on security of electronic networks including practical implementing action. This should be presented in time for the Göteborg European Council.” (June 2001)



# Strategic issues

- **Trust & Dependability in the Information Society:**
  - Ensure that specific policy support activities reach all the interested EC DG's and broaden policy support to other EU policy making institutions.
  - **Trust** is a encompassing concept considering the viewpoint of the final user
  - **Dependability:** “trustworthiness of a system such that reliance can justifiably be placed on the service it delivers”, subsuming the traditional attributes: reliability, availability, safety and security



## Strategic issues /2

- **Investigation of new *working mechanisms*:**
  - **Community building with critical stakeholders:**
    - better exploit *electronic forum* concept within specific areas of JRC competence (econfidence, deppy, privacy, cyber-abuse)
  - **Involving networks of research organisations in supporting EU policies**
  - **Pilot actions: position papers, scenario exercises**
  - **Collaboration agreement with NIST-USA**



# Trust and Dependability

- Objective:
  - Exploring ideas for rethinking the concept of **dependability** in the frame of complex information infrastructures, and for supporting the **trust** on information services
  - New issues for **networked systems**
    - Information infrastructure
    - Interdependencies
    - Vulnerabilities
    - Information assets assurance
    - Enforcement of dependability attributes



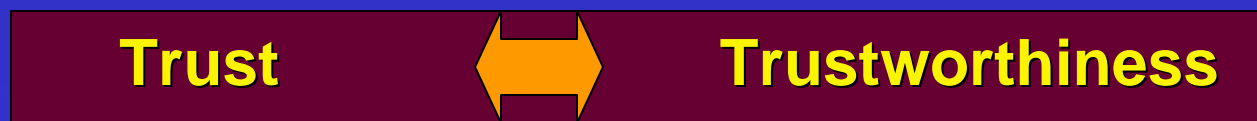
# Trust and Dependability /2

- **Dependability** is a major focus in the scenarios envisaged for the construction of the Information Society. It pursues the convergence of different communities:
  - correctness & safety
  - fault tolerance
  - reliability
  - information and network security
  - survivability
  - ...
- **Trust** is about interactions/transactions among actors/nodes that need to assure their trustworthiness



# Trust vs. trustworthiness

- **The users' viewpoint:**
  - Assurance from criteria and testing programs?
  - Who is listening to users' IT security requirements?



**Which are the trade-off factors?**

**users need vs. industrial offer**

**affordability vs. feasibility**

**cost-effectiveness vs. functionality vs. risks**



# Workshop

- **“Interdependencies and Vulnerabilities in Information Infrastructures”**
  - 27-28 March, Brussels
  - Sessions:
    - Telecommunications
    - Information assets
    - Health care
    - Energy and utilities
    - Finance
  - Result:
    - Report (available at [deppy.jrc.it](http://deppy.jrc.it))
    - Working Group to be set (information exchange)
    - Scenario exercises to be launched



# Background

## **Society is changing....**

- Economically.... *e-Business, e-Services, e-Markets*
- Culturally.... *e-Learning, Knowledge access*
- Organisationally ..... *e-Government, Healthcare*

## **But relying upon:**

- public networks deployed over multiple jurisdictions
- largely-deployed homogeneous technologies,
- technologies not always designed for open environments
  - f.i. IP applications assume trust among nodes



# Motivation

## General concerns arising from:

- complexity and interrelationships of infrastructures (systems-of-systems)
  - dependence on ICT and especially on open communications networks
  - widening of threat base (malicious, accidental)
- 
- **New, unknown vulnerabilities**
    - Asymmetric exposure
    - Single points of failure
  - **Not fully understood interdependencies**
    - Possibility of great disruptions
  - **Too many actors and dispersed responsibility**
    - Definition and allocation of **requirements**



# Drivers

- From **monolithic proprietary systems to open systems-of- systems** with greater **interconnectivity** and **complexity**
- The pressure to produce **cost effective systems** places increasing reliance on COTS, reuse and the evolution of legacy systems, tap open source components
- Convergence is increasing the **refinement** (e.g. multiple technologies, stringiest attributes) and the **complexity** of systems
- Rapid **evolution of standards** (mainly de facto)
- Implicit urgent **need to establish an interoperable infrastructure of trustworthy services**



# Trends

- **The Always-on, ubiquitous Net:**
  - Billions of fixed/mobile devices proliferate that are always on and always connected
  - Every single object having an ID and being able to communicate, at least in very short ranges.
- **Smart appliances:**
  - Highly configurable and adaptable devices, ready-to-easy-use
- **Cellular sensors/actuators:**
  - “Ambient intelligence” – remotely measuring, controlling, interacting with the social/working environment
- **Info-mobility:**
  - Send-access information on-the-move, where you need it, where you want



# Bottleneck

- **Information Assurance**

- Assurance about the partner that will have access to the data
- Assurance about the end-point smart appliance / communications device
- Assurance about the interaction/transaction intermediaries and third parties
- Assurance about the complex infrastructure that supports all of them

Failures can be in the organisation, in the software, in the user's own lack of awareness or errors



# Issues

***Assets → value → potential damage***

**Thus, the main issue is Risk:**

...for society at large (e.g. national security)

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

- **It should dominate the Trust & Confidence debate,**
  - policy, standards
  - evolution of the applications and technologies

***But the perception of benefits and risks  
is not clearly delineated  
for developers and users***



# The value of information

- **Information:**

- ...is estimated to constitute 50% of the value of corporations, and this percentage is growing rapidly with the growth of the Internet and of e-commerce.
- The on-line citizen will put its more valued information at risk (identify, health, finance, home security...)

- **Threats:**

- Growing (more manifest)
- For counteractions: imperative information assurance and security.

***Information is an asset***



# Information assets

- **Not just raw data**
    - Not a commodity
  - **But assured information**
    - Contents
    - Digital envelope:
      - Univocal identification
      - Life-cycle events
      - Trust properties
- Ref: ISTPA framework

From  
commodity



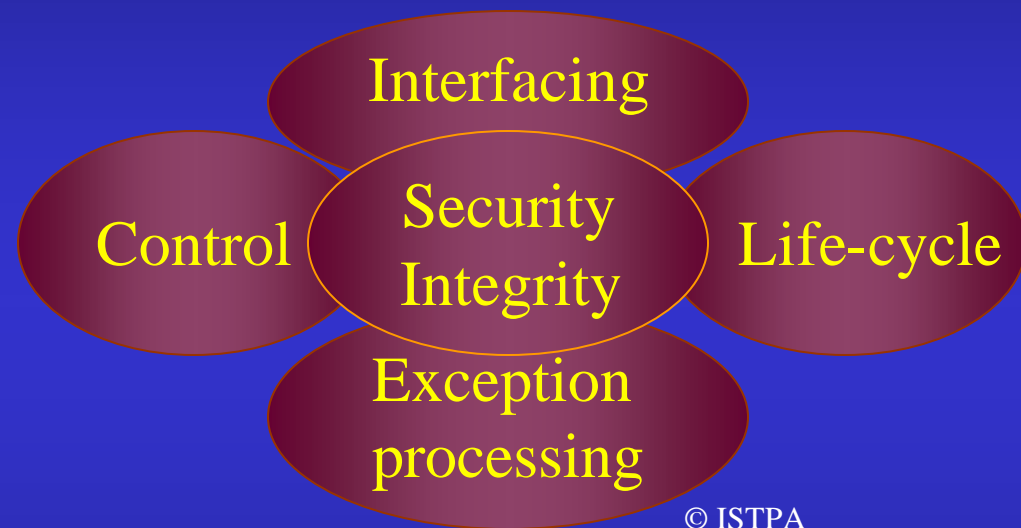
To assured  
product



# IA attributes

- **IA Attributes:**

- Access control
- Authorisation
- Availability
- Identification
- Authentication
- Confidentiality
- Integrity
- Non-repudiation
- Timeliness
- Privacy (!)

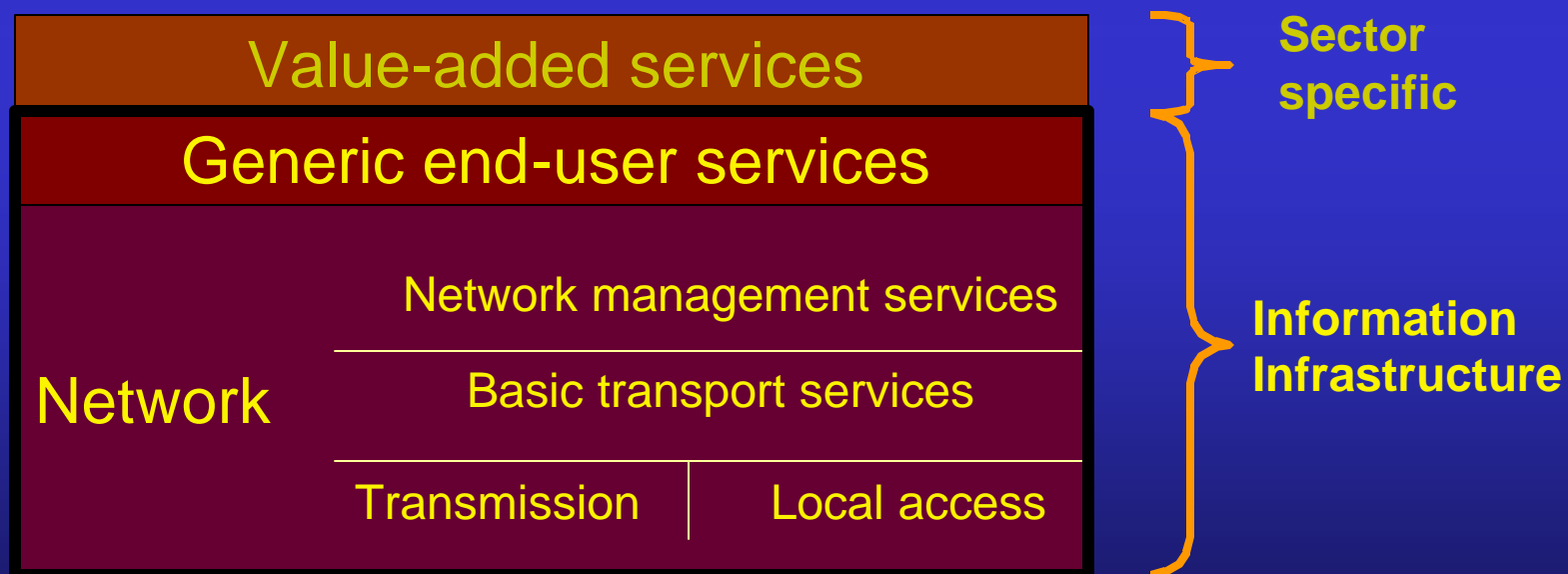


© ISTPA



# Information infrastructure

- **No universally accepted definition...**
- **Agreement:**
  - Comprising all data/voice communications means
  - Comprising all intermediate services





# Interdependencies

- **Interdependencies:**
  - Growing dependencies intra- and inter-infrastructures
  - Increasing use of the II for remote data access, operations and transactions
- **Concerns:**
  - Complex systems with interdependency loops and non-linearity
  - Emergent adverse behaviour
  - Fault propagation and cascading
  - Interactions security-reliability-availability
  - Unexpected and/or undesirable side effects on adjacent systems
  - Effects on other unrelated applications sharing the same resources



# Interdependencies /2

- **New Risks for:**
  - Energy
    - power grid, electricity on-line markets, services over power lines, remote control...
  - Healthcare
    - tele-medicine, remote access to records, pharmaceutical value-chain, automatic trolleys...
  - Finance
    - on-line services, payments, transactions...
  - Transport
    - ...

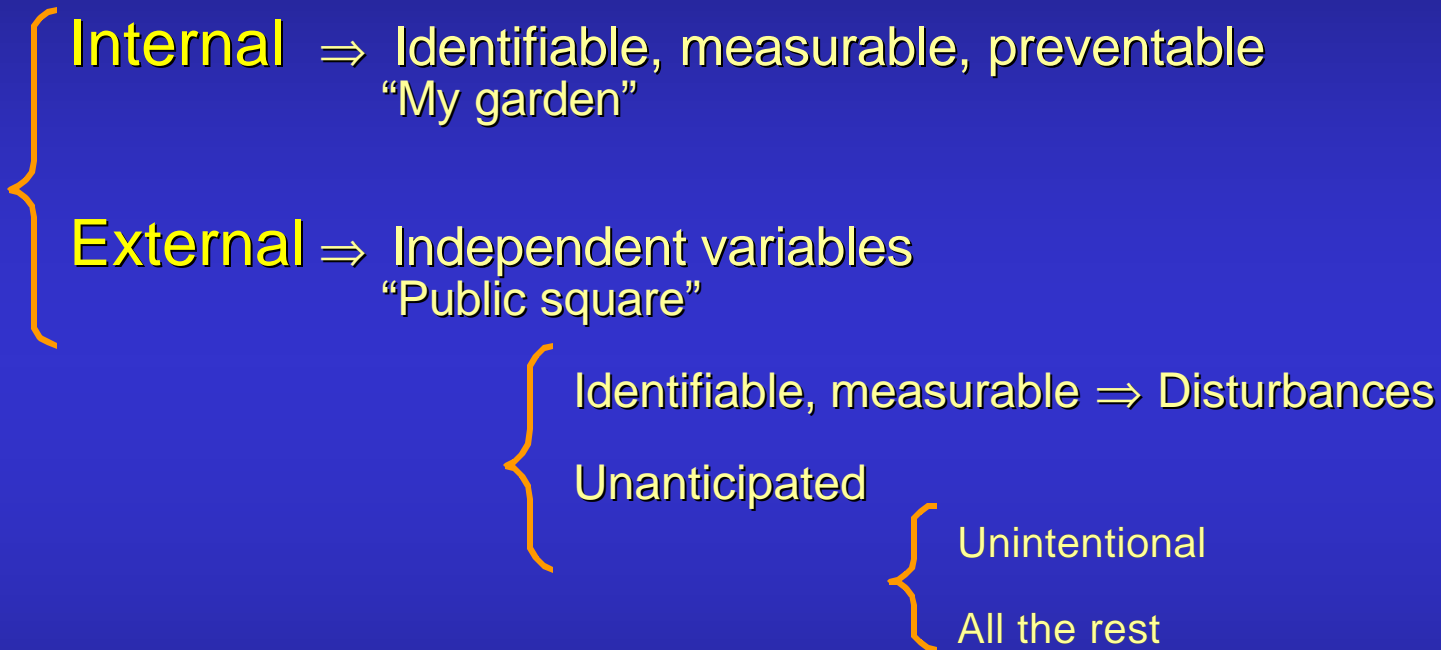


# Vulnerabilities, threats

- **Threats:**
  - Too many definitions
    - Agent, means, circumstances, event...
  - Scarce understanding
    - Taxonomy, motivation, capabilities
- **Vulnerabilities:**
  - any fact about a computer system that is a legitimate security concern
  - Maturing at the technical component level:
    - Dictionary: Common Vulnerabilities and Exposures (Mitre)
    - DBs: CERTs, companies, universities...
    - Life-cycle: discover, analyse, collect, protect, detect, handle



# Threats to information



**Threat concerns should influence system design**



# Security, survivability

## Security

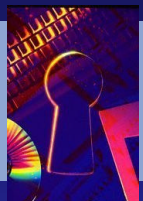
- Barrier to isolate application from intentional (& accidental) threats that could harm information assets
- Tolerance of application to the presence of intentional (& accidental) threats
  - Threats to the application through the communications system
  - Threats to the communications system

## Survivability

- Ability to provide essential services in the presence of attacks and failures, and recover full services in a timely manner

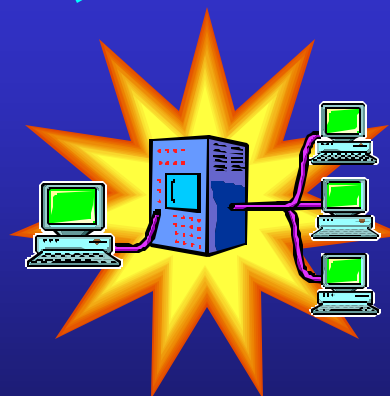
*Security: information assets*

*Survivability: mission*



# Dependable ES

- What to rely on?
- What to protect?
  - Content (information asset)
  - Container (critical hw/sw)





# Workshop conclusions

## 1. Short-term actions (2001-2002)

- European Working Group on Interdependencies and Vulnerabilities
  - Information collection and exchange
  - Scenario exercises
  - Elicitation of R&D challenges

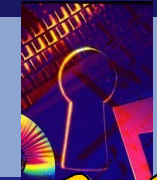
## 2. Medium-term actions (2003-2007)

- R&D challenges (Dependability Initiative in 6<sup>th</sup> Framework Programme)
  - Interdisciplinary & complexity
  - Dependency loops & non-linearity
  - Modelling and simulation, risk models
  - Migration to new technologies
  - Benchmarking
  - Prevention, tolerance, removal, prediction



# IVII workshop: ES concerns

- **Embedded systems**
  - Access points for users
  - Remote data access
- **Concerns:**
  - Several missions with different criticality
  - Several levels of required dependability attributes
  - New requirements: privacy, accountability, non-repudiation
  - Connectivity: propagation of faults
  - Handling of information assets



**ES concerns**

# Mission & criticality

- **Concept of mission**
  - Many even for simple systems
- **Concept of criticality:**
  - Varying levels of dependability
  - Influenced by external factors
    - Fault propagation
    - Containment/tolerance mechanisms
- **Many standpoints:**
  - Developer
  - End-service provider
  - Intermediate services
  - Infrastructure



**ES concerns**

# Dependability requirements

- **ES as key part of a dependable, pervasive information infrastructure**
  - dependability requirements for contents and container
  - Quality/dependability attributes are imposed on ES from any sources
- **Important questions**
  - What specific security requirements are needed to address highly reliable, real-time systems?
  - Which assurance for making users trust IT products?
  - How can the results from component product testing and evaluation be used to increase the level of confidence of users?



# Information assurance

- **New type of requirements for ES:**
  - **Privacy:**
    - proper handling of personal information, consistent with preferences of user
  - **Accountability:**
    - Ability to address information improper handling
    - Life-cycle traceability for responsibility & liability
  - **Non-repudiation:**
    - Undeniable proof of participation
  
- **Assurance for trustworthiness demonstration**



# Fault propagation

- **Emergent effects**
  - From systems complexity: unforeseen situations and conditions, incapable of identifying the causing factors.
- **Interdependencies**
  - Failures are not independent
  - Interactions: functionality, behaviour
- **Vulnerabilities:**
  - Mainly exploitable characteristics from the information standpoint

# Connectivity



- **Distribution of identically weak software (!)**
  - Proprietary vs. open source
- **Standard security architectures**
  - Security services like authorization, certificate management, encryption, intrusion detection
- **Trust frameworks and domains**
  - Liability issues
- **ES as part of “end-to-end” solutions**
  - Manage dependability in largely distributed environments
- **Dynamic, temporary applications/networks**
  - Manage dependability in re-configurable environments

**The “big picture”**



# Information handling

- How to provide unique **identification** to all devices?
- How to bind devices to an **authorized** individual or entity?
- How to manage authorization **decisions** that limit the scope of activities allowed?
- Issues of **identity** and **authority** when these devices conduct activities for people without human intervention, when no one is around to notice
  - People will delegate their autonomy to these devices which will make decisions on their behalf.
  - Several devices can now represent an individual, creating identity conflict.

**Technology + users behaviour + security policy**



# Conclusions

- Need to rapidly converge on a common understanding of requirements, security, dependability, interdependencies, survivability
- Need to develop the concept of information assets in open networked environments
- Need for assessment methods for threats, vulnerabilities, complexity issues
- Need to adopt a risk management approach