CRUTIAL:
The Blueprint of a Reference Critical Information Infrastructure Architecture

Paulo Veríssimo, Nuno Neves, and Miguel Correia

51st Meeting of the IFIP 10.4 WG on Dependable Comp. and F/T
Gosier, Guadeloupe, France, January 10-14, 2007

Extended, first presented at CRITIS @ ISC'06, Samos – Greece, August 2006

Contact information

Paulo Esteves Veríssimo
http://www.di.fc.ul.pt/~pjv

Phone: ***+351-21 7500 103***

Fax: ***+351-21 7500 087***

e-mail: ***pjv@di.fc.ul.pt***

Navigators Group, LaSIGe
Lab. for Large-Scale Informatics Systems
Univ. of Lisboa, Portugal

CRUTIAL
Critical Utility InfrastructurAL Resilience
STREP Project FP6-2004-IST-4-027513
Coordinator: CESI RICERCA SpA
January 2006 - December 2008

Vision

Resilient distributed power control in spite of threats to the information and control infrastructures

Objectives

Provide modelling approaches for understanding and mastering the various interdependencies among power, control, communication and information infrastructures

Investigate distributed architectures enabling dependable control and management of the power grid

Problems

- problem of resilience of critical utility infrastructures is not completely understood, mainly to the hybrid composition of these infrastructures:
  - SCADA, PCS systems that yield the operational ability to supervise, acquire data and control physical processes
  - interconnections to the standard corporate intranet, where services and engineering reside
  - The Internet, to which, and often unwittingly, the SCADA network is sometimes connected to
- also because it became inter-disciplinary:
  - SCADA systems are real-time systems with some reliability or fault-tolerance concern, classically not designed to be widely distributed or remotely accessed, let alone open, and designed without security in mind

Our position

- the computer-related operation of a critical utility infrastructure became thus a *distributed systems problem*, including:
  - interconnected SCADA/embedded networks, corporate intranets, and Internet/PSTN access subsystems
- that distributed systems problem is hard:
  - includes facets of real-time, fault-tolerance, and security

Our objective

- We focus on the computer systems behind electrical utility infrastructures as an example, and propose:
  - a distributed systems architecture that we believe may come to be useful as a reference for modern critical information infrastructures
  - a set of classes of techniques and algorithms based on paradigms providing resilience to faults and attacks in an automatic way
- This work is ongoing and is done in the context of the recently started European project

CRUTIAL, CRitical UTility InfrastructurAL resilience

Further insight on the CII problem

- *Problem of CII insecurity is mostly created by:*
  - **the informatics nature of many current infrastructures**
    - **read "computerised", "controlled by computers"**
  - **the generic network interconnection of CIIs**
    - **which bring several facets of exposure**
- *also*
- Critical information infrastructures (CII) feature a lot of legacy subsystems and non-computer-standard components (controllers, sensors, actuators, etc.)
- Conventional security and protection techniques, when directly applied to CI controlling devices, sometimes stand in the way of effective operation
- *Above two will hardly change*
  - **make them research challenges**

Further insight on the CII problem

- *What can be done at architectural level to address this problem and achieve resilient operation?*

An R&D roadmap to solutions

- **PROPOSITION 1**: Classical security and/or safety techniques alone will not solve the problem:
  - largely based on prevention and ultimately disconnection
  - we must bet on the tolerance paradigm

Security considered insufficient

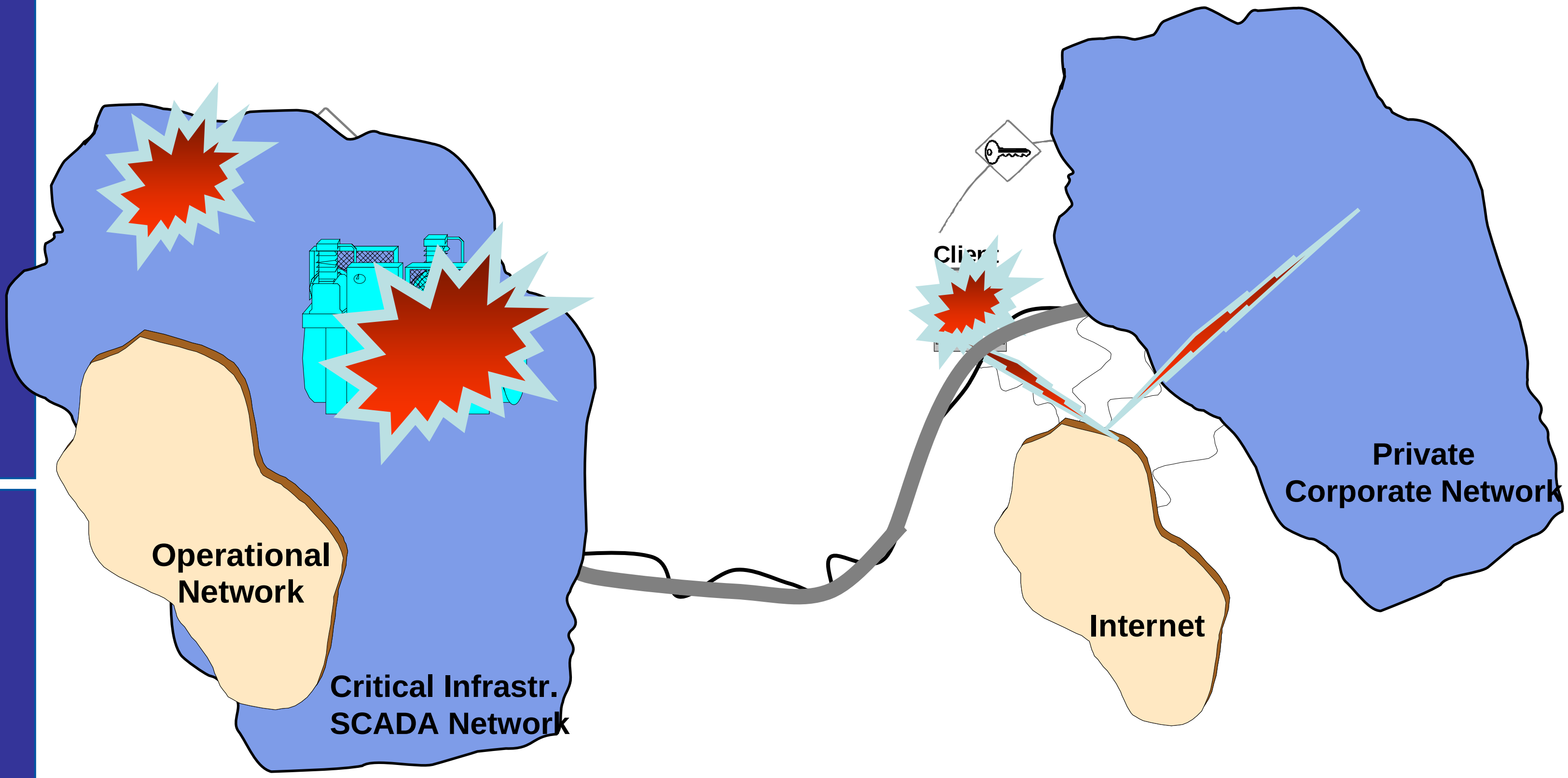
- Basic engineering remedies place RTE (real-time and embedded) systems at most at the current level of commercial systems' Sec&Dep !!
- But current level of IT Sec&Dep not sufficient:
  - IT systems constantly suffer attacks, intrusions, some massive (worms)
  - most defences dedicated to generic, non-targeted attacks
  - they degrade business, but do virtual damage, unlike RTE systems' risks of physical damage
- Some current IT Sec techniques can negatively affect RTE system operation w.r.t. availability, timeliness, etc.
  - contrary to F/T techniques, which fly planes, cars, etc.

An R&D roadmap to solutions

- **PROPOSITION 1**: Classical security techniques alone will not solve the problem:
  - largely based on prevention and ultimately disconnection
- **PROPOSITION 2**: Any solution passes by automatic control of macroscopic command/information flows
  - essentially between local/virtual LANs composing the CII

Complexity and Interdependence

- Uncertainty, Interference, Error propagation
- Almost impossible to manage in a manual and/or device-specific way



An R&D roadmap to solutions

- **PROPOSITION 1**: Classical security and/or safety techniques alone will not solve the problem:
  - largely based on prevention and ultimately disconnection
- **PROPOSITION 2**: Any solution passes by automatic control of macroscopic information flows
  - essentially between the virtual LANs composing the C.I.
- **PROPOSITION 3**: Need a reference architecture of "modern critical information infrastructure":
  - different interconnected realms: SCADA; intranets; Internet
  - different kinds of risk throughout the physical and the information subsystems
  - adequate granularity: LANs as first-order citizens, with varying trust levels

An R&D roadmap to solutions

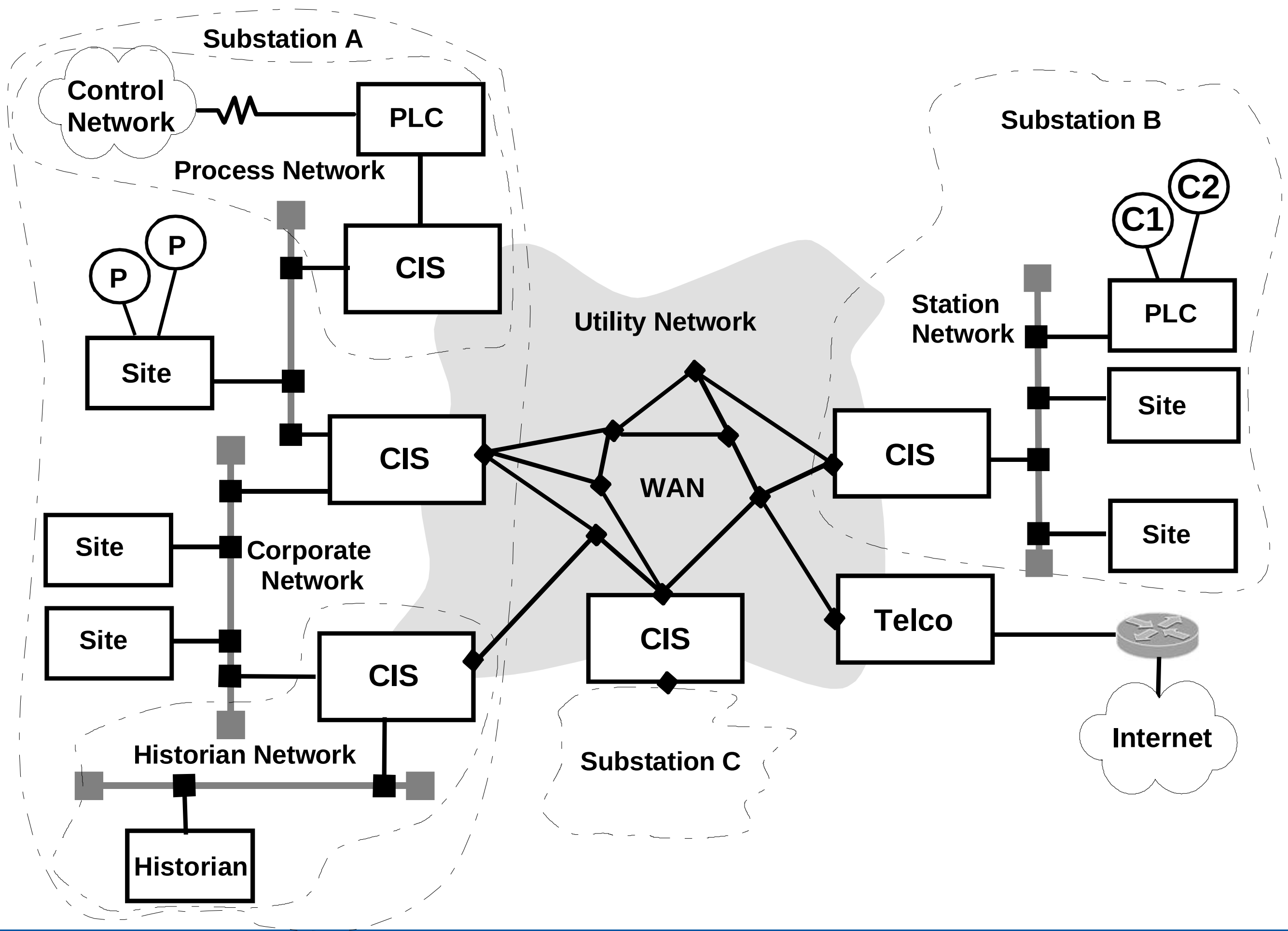
- **PROPOSITION 1**: Classical security and/or safety techniques alone will not solve the problem:
  - largely based on prevention and ultimately disconnection
- **PROPOSITION 2**: Any solution passes by automatic control of macroscopic information flows
  - essentially between the virtual LANs composing the C.I.
- **PROPOSITION 3**: Lack a reference architecture of “modern critical information infrastructure”:
  - different interconnected realms: SCADA; intranets; Internet
  - different kinds of risk throughout the physical and the information subsystems
  - LANs as first-order citizens, with varying trust levels

Main CRUTIAL architecture principles

- *architectural configurations* with trusted components that *a priori* induce *prevention*
  - of some faults, and certain attack and vulnerability combinations
- *middleware devices* achieving runtime *automatic tolerance*
  - of remaining faults and intrusions, supplying trusted services out of non-trustworthy components
- *recovery and diversity* mechanisms for *exhaustion-safety*
  - for unattended and perpetual operation in face of continuous production of faults and intrusions
- *trustworthiness monitoring* mechanisms allowing *adaptation*
  - to situations not predicted, or beyond assumptions made
- *security policies* yielding *organisation-level access control* models
  - for information flows w/ different criticality within/in/out CIIs

A more detailed look at architecture and algorithms

Example Architectural devices: WAN-of-LANs



Main characteristics - WAN and CIS

- System is a WAN-of-LANs:
  - packets are switched through a global interconnection network, through facility gateways, representative of each LAN
  - WAN is a logical entity operated by the CII operator, which may use parts of public network

- CRUTIAL facility gateways are called **CRUTIAL Information Switches (CIS)**, and in a CII they act as a set of servers providing distributed services:
  - achieving *control of the command and information flow*, and securing a set of necessary *system-level properties*
  - like sophisticated firewalls combined with intrusion detectors, connected by distributed protocols

Main Characteristics - LAN

- A LAN is a logical unit that may or not have physical reality
- More than one LAN can be connected by one facility gateway
- All traffic originates from and goes to a LAN

- Example LANs:
  - administrative clients and servers LANs; operational (SCADA) clients and servers LANs; engineering clients and servers LANs; PSTN modem access LANs; Internet and extranet access LANs

System Model

- Distributed system with N nodes, asynch/arbitrary model, strengthened by using wormholes
- Faults (accidental, attacks, intrusions) continuously occur during the life-time of the system
- A maximum number of f malicious (or arbitrary, or Byzantine) faults can occur within a given interval

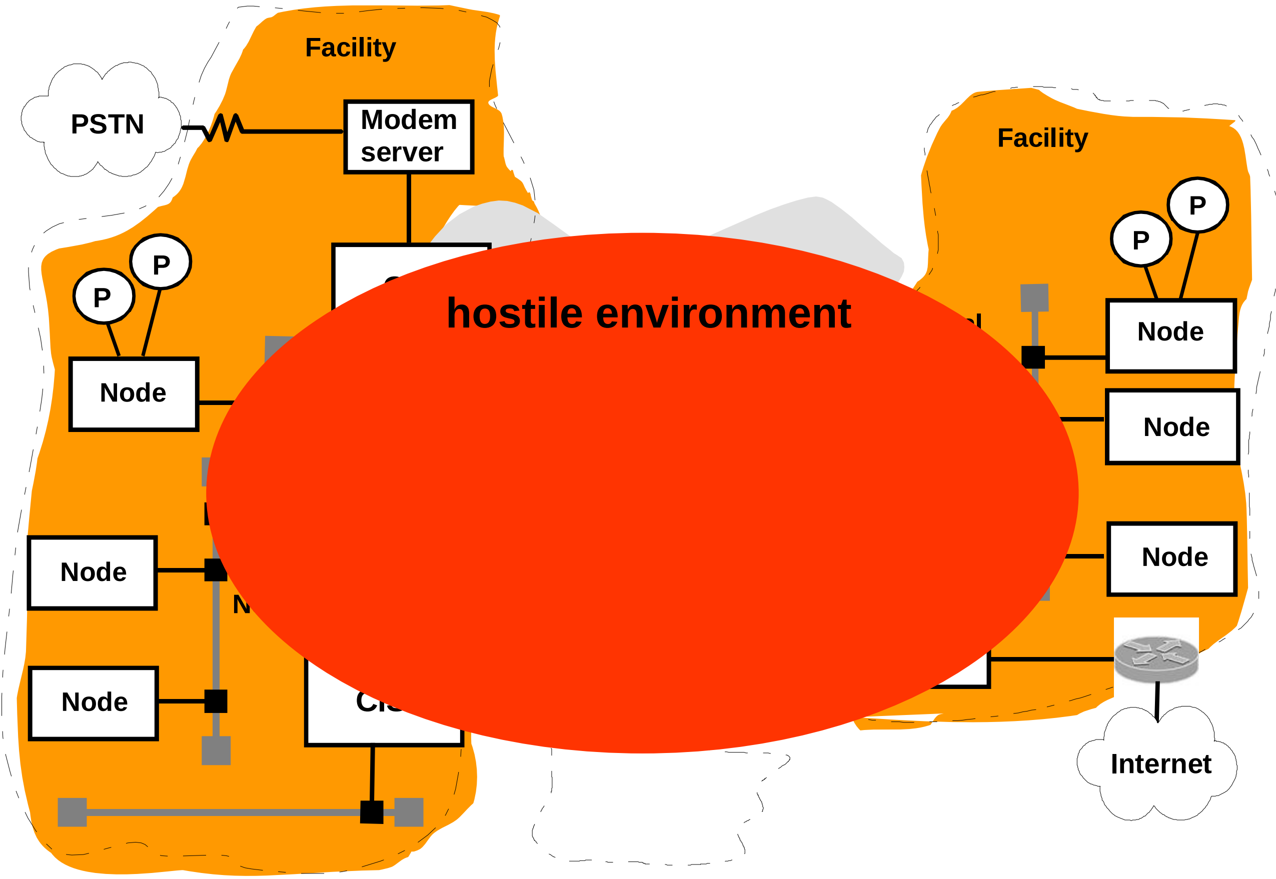
- HARD PROBLEMS:
  - Some of the services running in CIS may require some degree of timeliness, given that SCADA implies synchrony
  - Systems should operate non-stop, despite the continued production of faults during the life-time of a perpetual execution system

System Model

- An assumed number of CIS can be corrupted, under conditions:
  - CIS must be *intrusion-tolerant*, prevent resource exhaustion providing *perpetual operation*, and endure assumption coverage uncertainty providing *resilience*
- The distributed services implemented on CIS must be intrusion-tolerant:
  - a logical CIS may actually be a set of replicated physical units (CIS replicas) according to fault and intrusion tolerance needs
  - likewise, CIS are interconnected with intrusion-tolerant protocols, in order to cooperate to implement the desired services

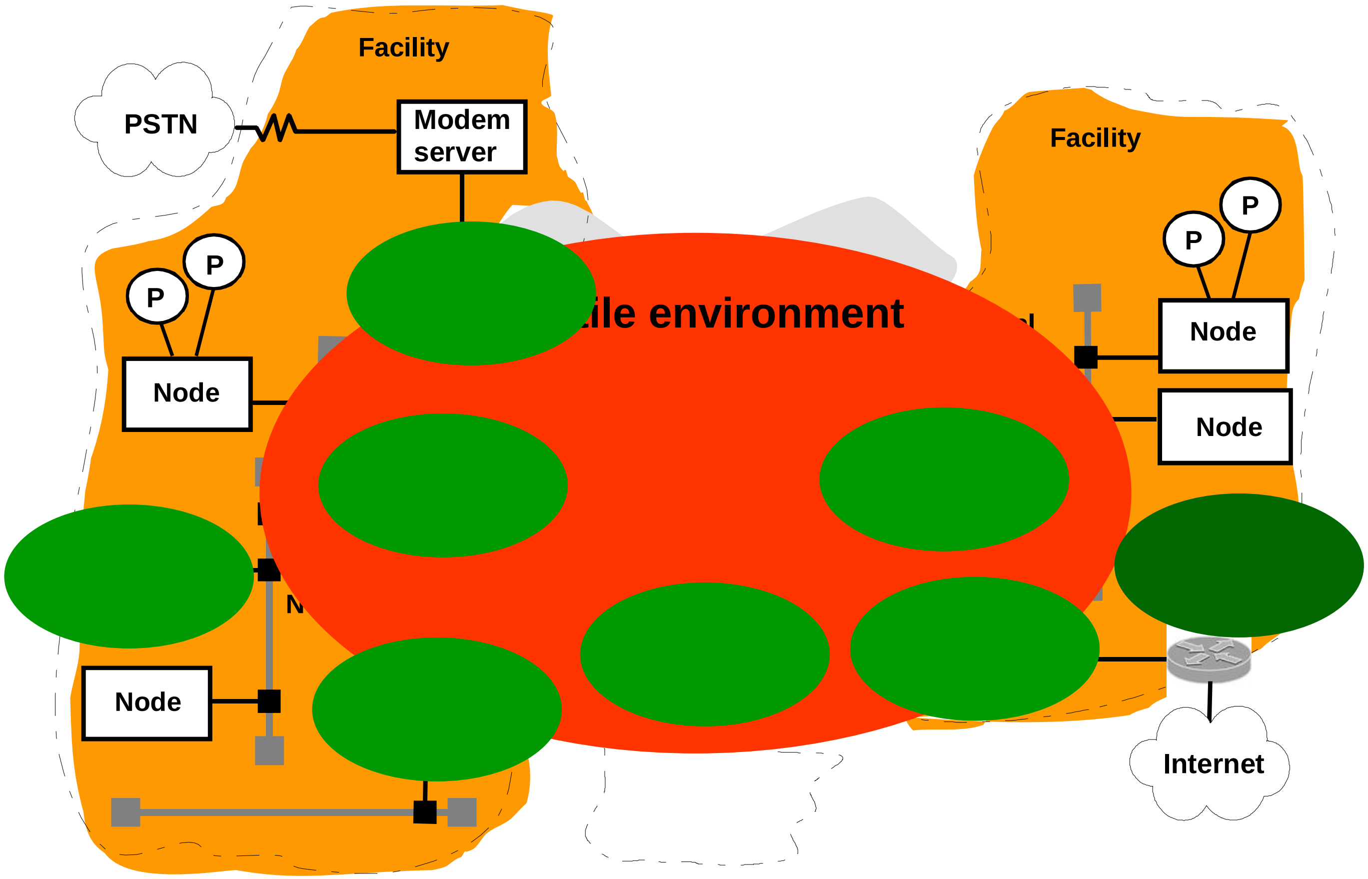
Example Architectural devices: WAN-of-LANs

- Weak assumptions: hostile interconnection environment



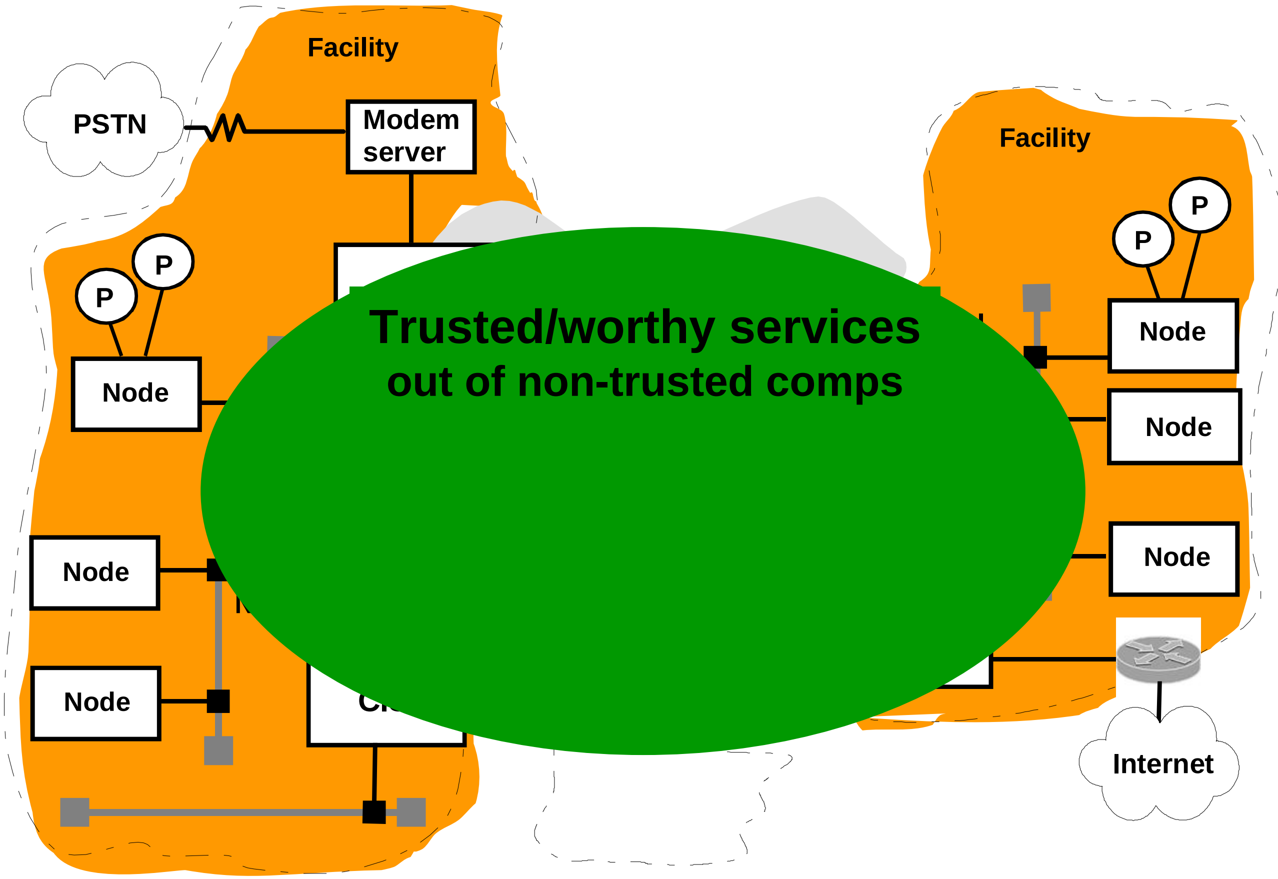
Example Architectural devices: WAN-of-LANs

- Intrusion tolerance for trust

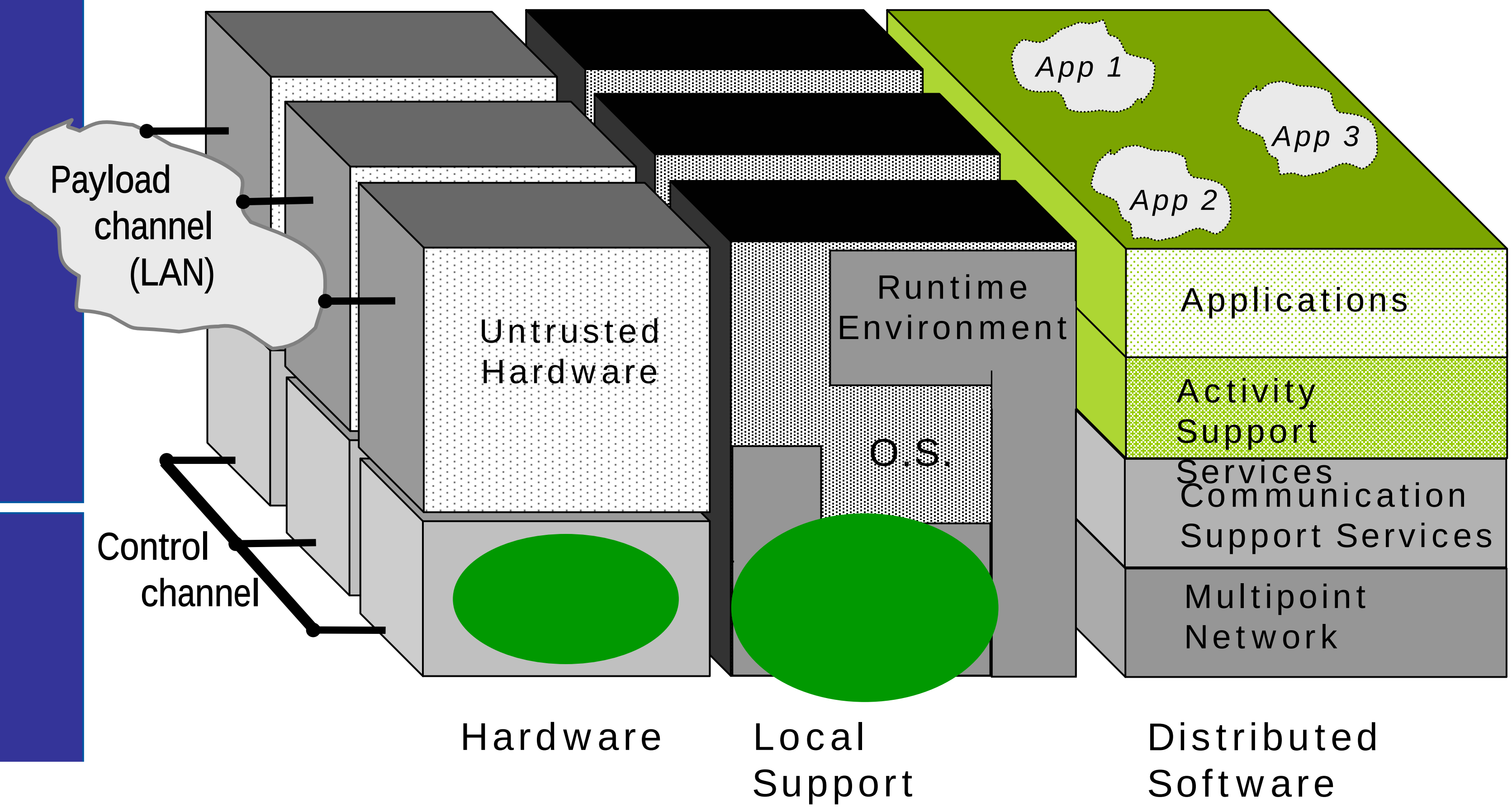


Example Architectural devices: WAN-of-LANs

- Trusted/trustworthy services out of non-trusted comps



Example Architectural devices: Node Architecture and Interconnection



CRUTIAL Middleware

- The environment formed by the WAN and all the CIS is hostile
- LANs trust the services provided by the CIS, but are not necessarily trusted by the latter
- CIS securely switch information flows as a service to edge LANs

CRUTIAL Middleware

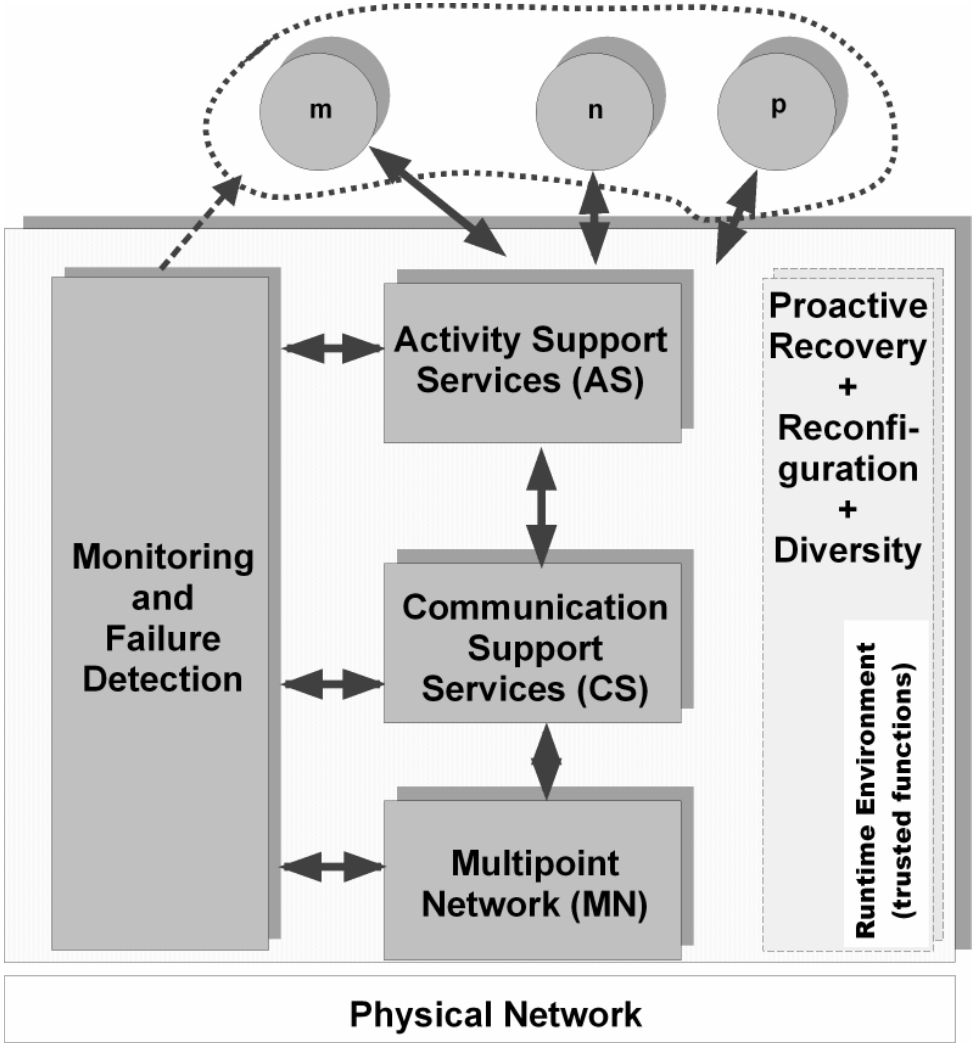
- LAN-level services:
  - A LAN is the top-level unit of the granularity of access control
  - A LAN is also a unit of trust or mistrust thereof, LANs may deserve different levels of trust
  - Traffic (packets) originating from a LAN receive a label that reflects this level of trust, and contains access control information
  - We assume that a label is an authenticated proof of a capacity

Example WAN-level services

- Byzantine-resilient information and command dissemination
  - between CIS units, with authentication and cryptographic protection (broadcast, multicast, unicast)
- Pattern-sensitive information and command traffic analysis
  - (behaviour and/or knowledge based intrusion detection) with Byzantine-resilient synchronisation and coordination between local IDS units
- Protection: egress/ingress access control
  - based on LAN packet labels and/or additional info/mechanisms, with Byzantine-resilient synchronisation and coordination between local FW units

CIS architecture

middleware and runtime



CIS architecture

middleware and runtime

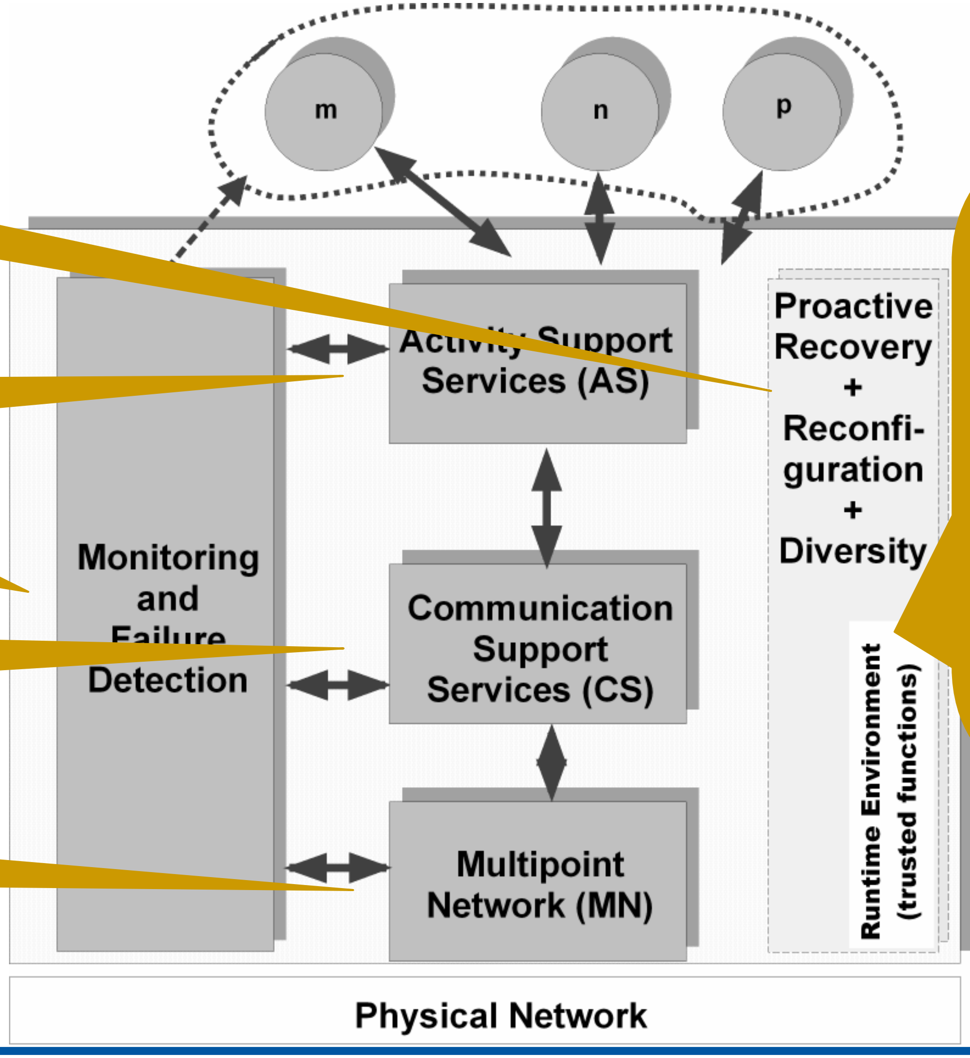
Key and/or Code/State Recovery

OrBac access ctl; StateM ServElem; IDS ServElem

Trustworthiness monitoring and adaptation

Byzantine-resilient x-cast, consensus, etc.

TCP/UDP/IP, IPSEC, SSL, etc.

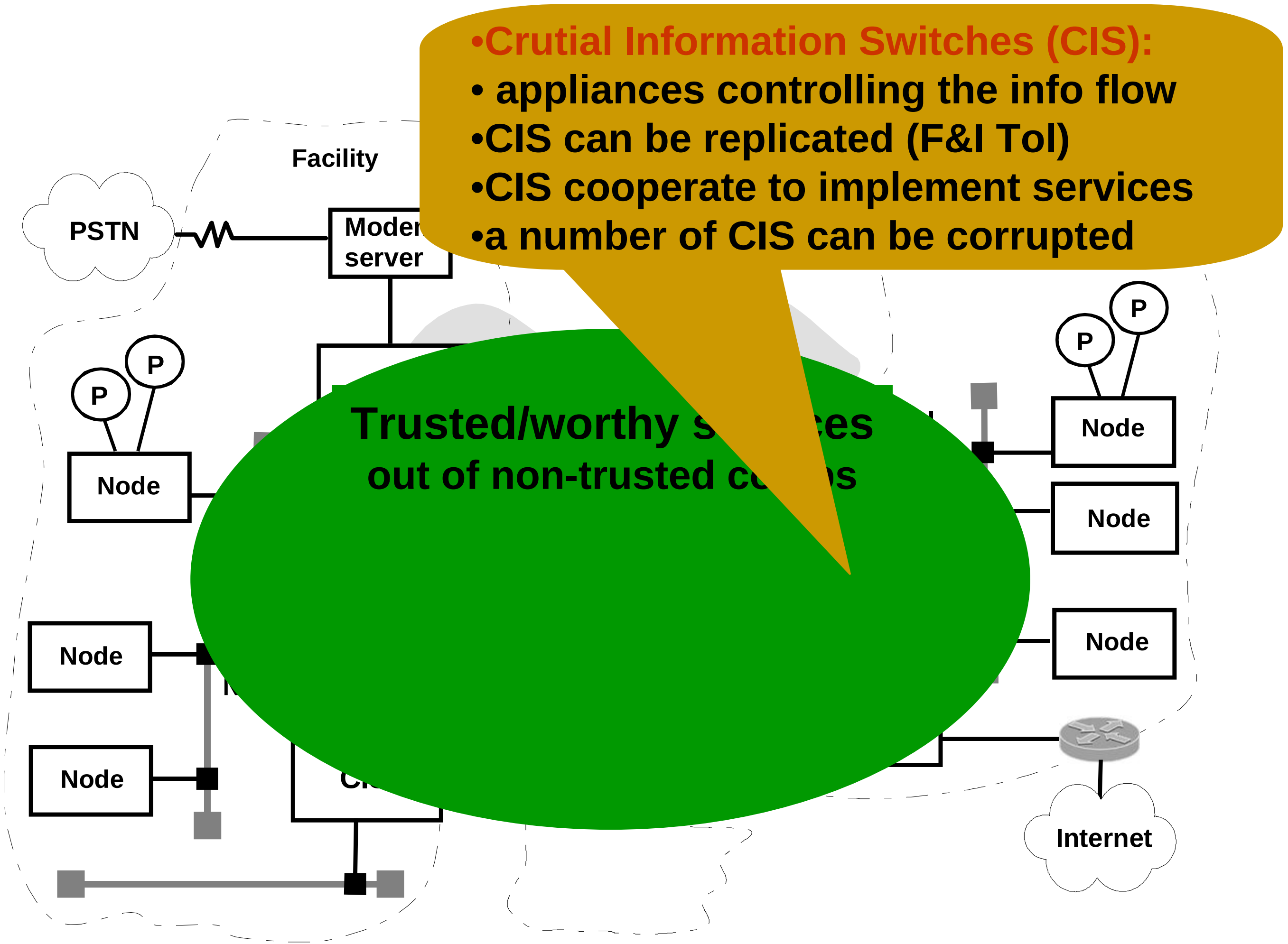


Runtime: Java VM, OS

Trusted HW: JavaCard, SIM, Appliances, Ctrl Networks

wrapped in: Security kernels

CRUTIAL Reference Architectural



Conclusions

- Presented a blueprint of a *distributed systems architecture for resilient critical information infrastructures*
- Based on three fundamental propositions:
  - classical security and/or safety techniques alone not enough
  - need automatic control of macroscopic command/info flows
  - need a reference architecture performing CII realms integration
- Range of basic mechanisms of incremental effectiveness:
  - trusted components in key places induce prevention
  - middleware software attains automatic tolerance
  - recovery/diversity achieve perpetual operation
  - trustworthiness enforcing and monitoring mechanisms allow adaptation to extremely critical situations, beyond assumptions
- Rich variety of CIIP services to be implemented on top
  - Robust CII-specific applications
- Expect to show this model and architecture capable of automatically securing information flows with different criticality in a CII