Architecting Critical Information Infrastructures:
when computers meet the real world

Presented at the Architecting Dependable Systems Workshop, WADS@DSN 2007, Edinburgh

Paulo Esteves Veríssimo

Navigators Group,
LaSIGe, Laboratory for Large-Scale Informatic Systems
Univ. of Lisboa, Portugal
pjv@di.fc.ul.pt
http://www.di.fc.ul.pt/~pjv

The critical infrastructures resilience problem

Problem statement

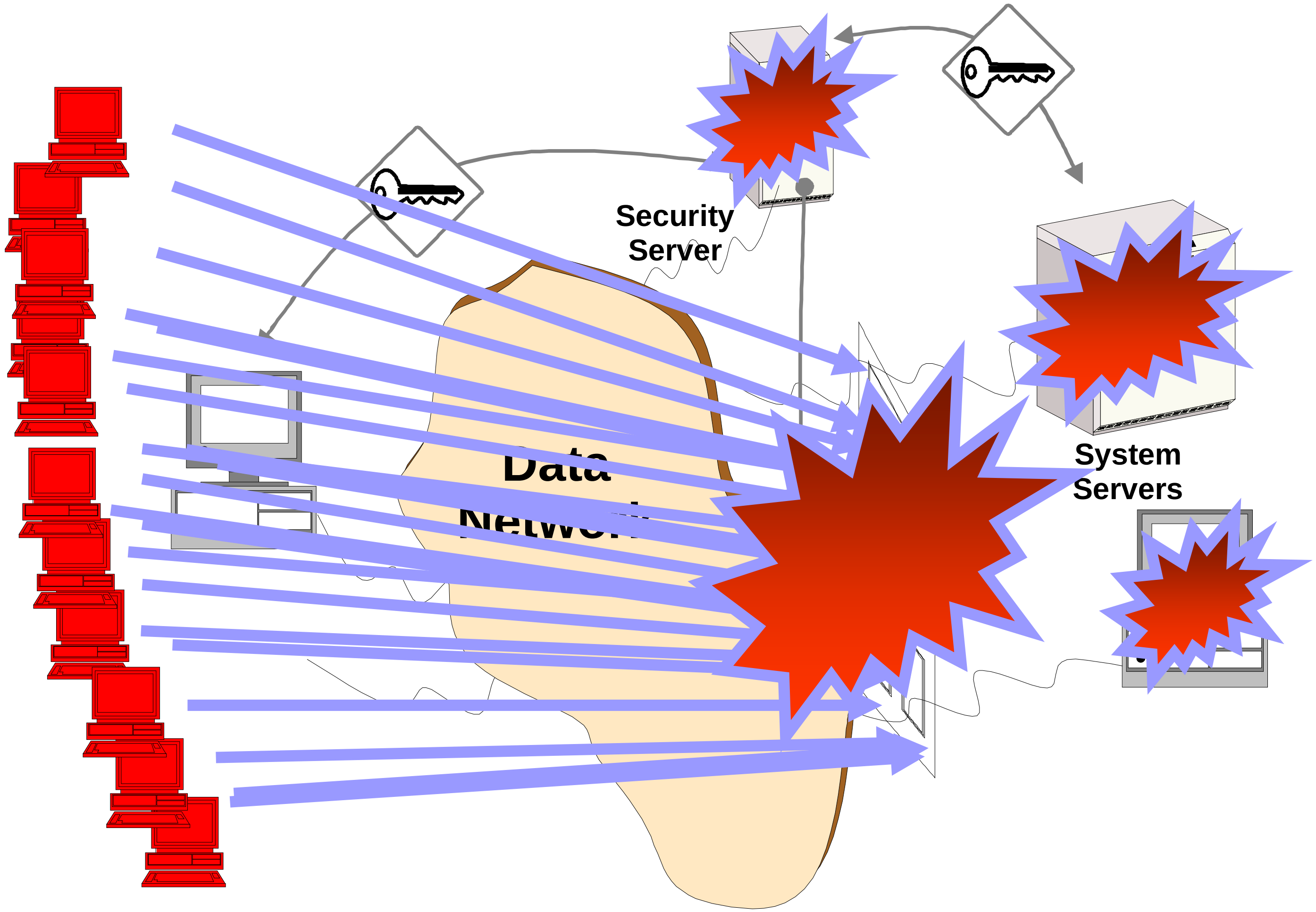
- problem of resilience of *critical utility infrastructures* is not completely understood
- mainly to the hybrid composition of these infrastructures:
  - **SCADA** systems which yield the operational ability to supervise, acquire data and control
  - interconnections to the standard **corporate intranets** and often unwittingly to the **Internet**
  - advent of **distributed generation**
- also because it became inter-disciplinary:
  - SCADA systems are **real-time** sys with some **fault-tolerance** concern classically **not** designed to be widely **distributed** or remotely accessed or **open**, and designed w/o **security** in mind

Threats

Exposure

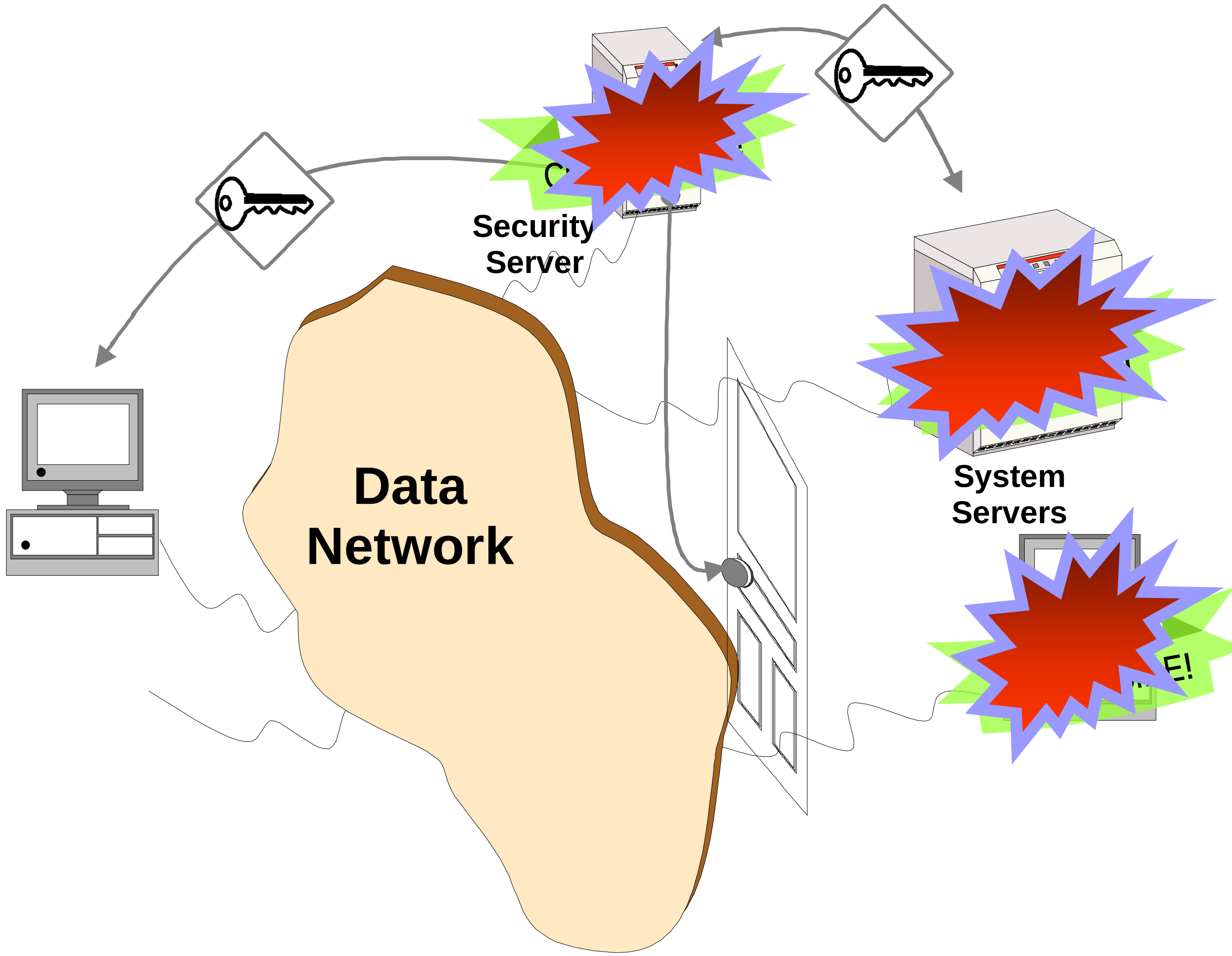
Faults/Attacks/Errors/Intrusions

external attacks



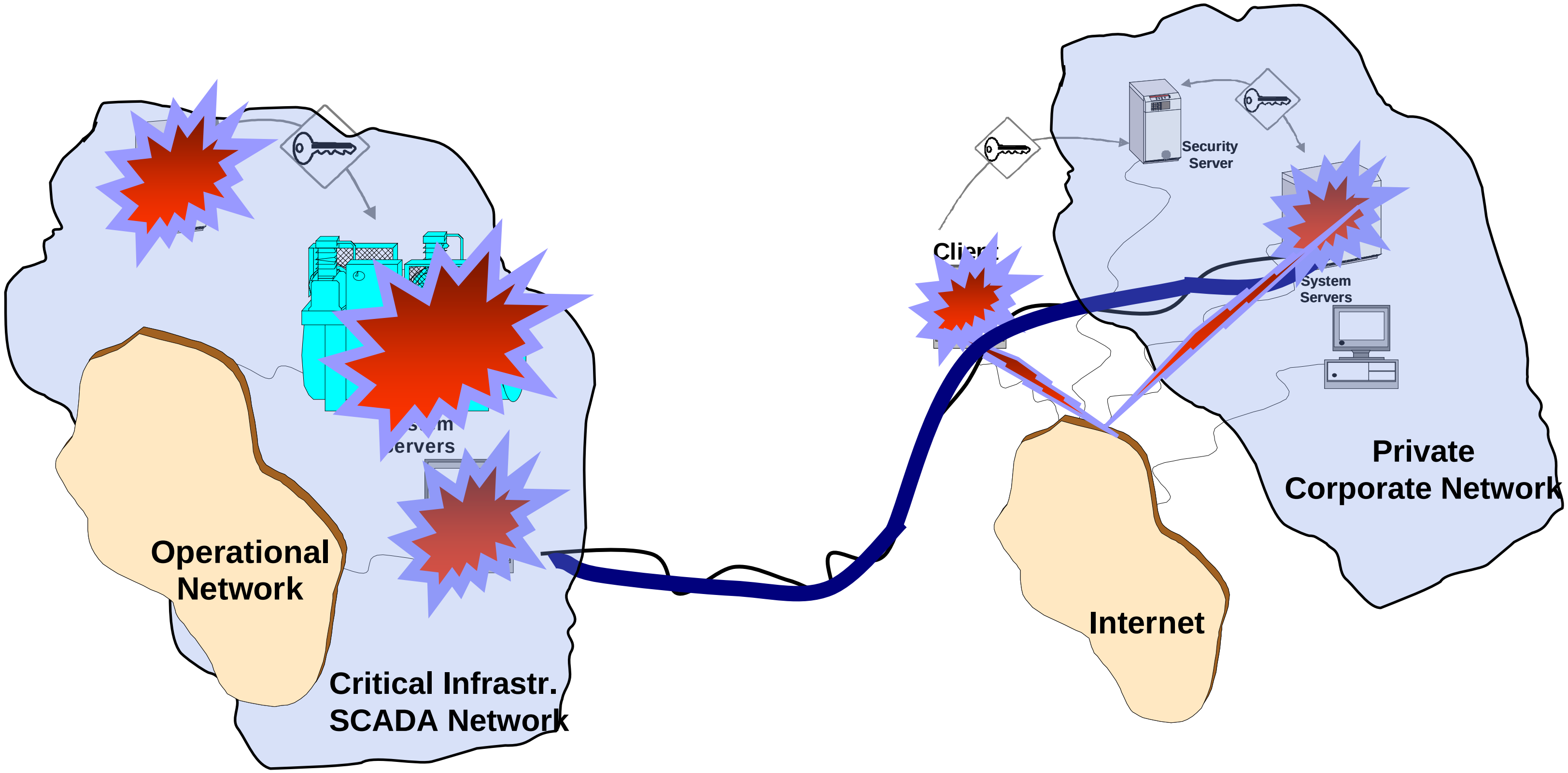
Exposure

Faults/Attacks/Errors/Intrusions
internal design faults



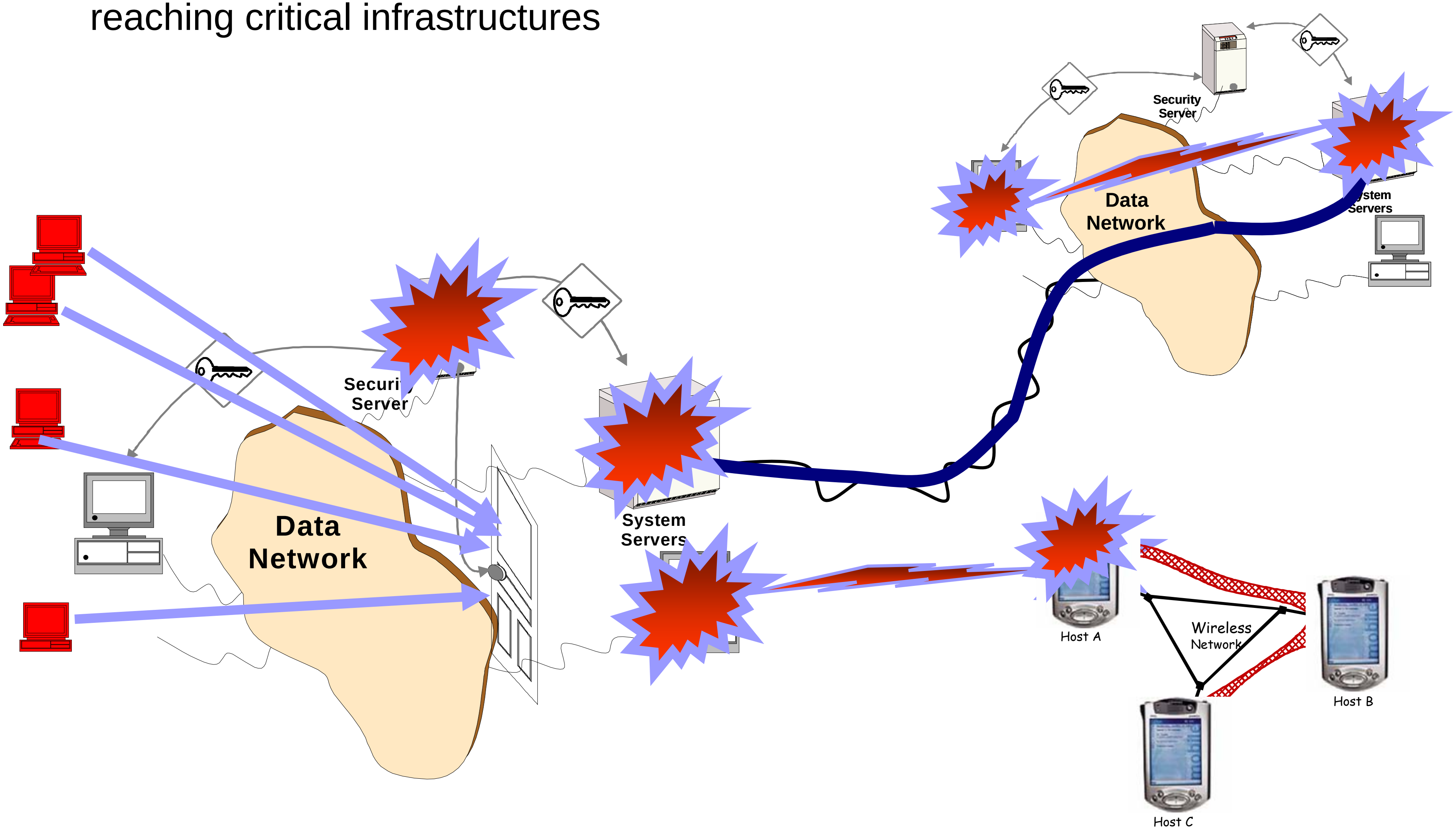
Complexity and Interdependence

Uncertainty, Interference, Error propagation



Interdependence

Interference, Error propagation reaching critical infrastructures



Consequences

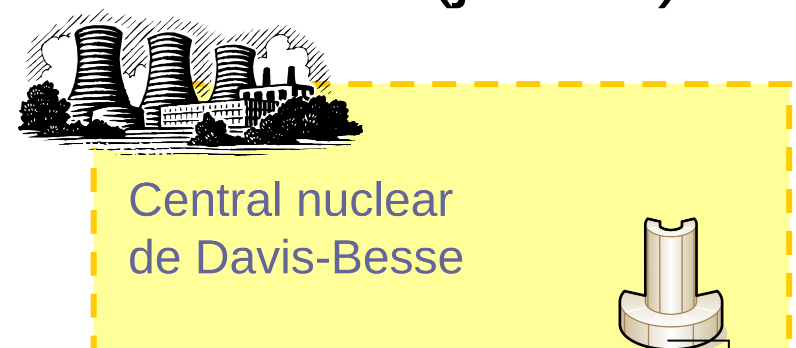
- The damage perspectives that may result from these threats are overwhelming:
  - wrong maneuvering by inept users inside the own company's corporate networks
  - malicious (or disastrously curious) actions from users somewhere in the Internet
  - targeting computer control units, embedded components and systems, that is, devices connected to operational hardware (e.g., water pumps and filters, electrical power generators and power protections, dam gates, etc.)
- Such mishandling may cause severe damage
  - to people, economy, and environment

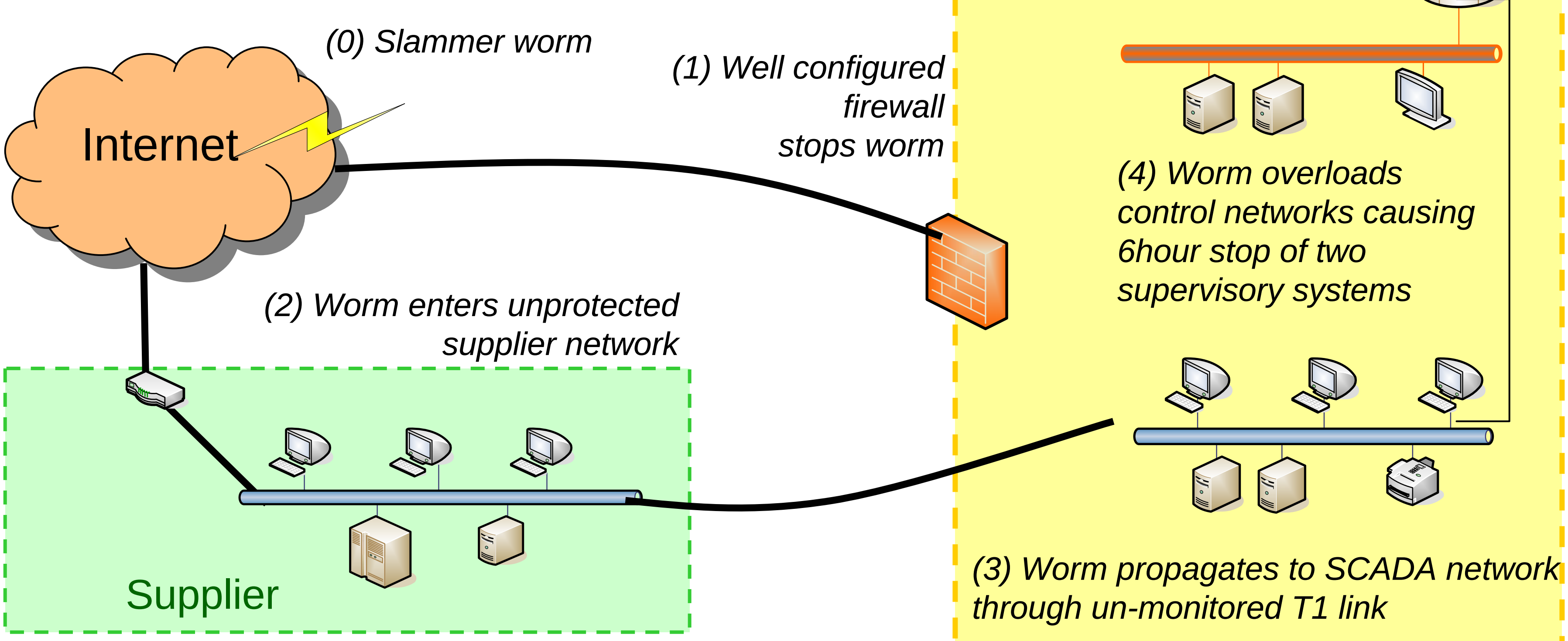
How probable are intrusions?

- Intrusions may hit where least expected
- Because one of the current problems in CI’s is that people often worry about the tree, and forget the forest

Real cases: nuclear central under attack! (jan 03)

Slammer worm penetrated control systems of nuclear power central in Ohio. Caused two critical monitoring systems to stop.





State of play

- Basic engineering remedies place RTE systems at most at the current level of commercial systems' Sec&Dep !!
- But current level of IT Sec&Dep not sufficient:
  - IT sys constantly suffer attacks, intrusions, some massive (worms)
  - they degrade business, but do virtual damage
- Some current IT Sec techniques can negatively affect RTE system operation (availability, timeliness,...)
  - contrary to FT techniques, which fly planes, cars, etc.

State of play

- Not to mention the dimension of physical damage in the scenario of RTE systems
  - many R/T and embedded systems are attached to physical and environmental devices
  - their mis-operation or failure can lead to high losses, of property and/or lives, and to large effect on society (even if just massive unavailability)
  - script-kids can blow a power station, instead of blowing a server
- Where do we go from here?

Cyber Security for SCADA and embedded control systems: how much time have we?

- It is common knowledge among Sec&Dep people that :
  - Assumptions are vulnerabilities that are attacked by hackers in ways much more severe than accidental faults would
  - The less coverage an assumption has, the more fragile to attack it is
- It is a matter of time until hackers understand how to attack control systems underlying critical infrastructures, cars or trains
- Maybe all it takes is a **www.scada_rootkit.com**

The road to CII security (1)

- Securing individual components (e.g. chips, PLCs, industrial PCs) is important, but does not solve the problem:
  - Cannot assert the security of the overarching system
  - There are many legacy devices
  - Classical security techniques hamper R/T operation
- So:
  - We will not deploy really secure RTE components in a near future
  - Maybe we will never be able to deploy completely secure RTE components (e.g. vulnerability-free)

The road to CII security (2)

- We should be talking about "distributed, R/T and Fault/Intrusion tolerant systems" when talking about CII's
- We need a reference architecture of "modern critical information infrastructures"
  - Three interconnection realms: operational SCADA/embedded networks; corporate intranets; Internet/PSTN access.
- We need models for behaviour of modern critical infrastructures in critical scenarios
  - Derive common denominators: exposure, threat, vulnerability, unsafety.

A research grand-challenge for architecting Critical Information Infrastructures

- Withstand combinations of faults and intrusions in an automated way:
  - architectural configurations that induce prevention of the more severe interaction faults, attacks and vulnerabilities;
  - middleware devices that achieve tolerance of the remaining faults/intrusions (architectural blocks, protocols);
  - sophisticated system trustworthiness monitoring mechanisms;
  - High-level access control models discriminating different criticality information flows within and in/out a CII.

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

Models

ISTITUTO DI SCIENZA E TECNOLOGIE DELL'INFORMAZIONE "A. FAEDO"

CESI

Power control infrastructures

consorzio nazionale interuniversitario per le telecomunicazioni

FACULDADE DE CIÊNCIAS UNIVERSIDADE DE LISBOA

LEUVEN

Evaluations

Architectures

Thank you!