CRUTIAL

Critical UTility InfrastructurAL Resilience

(EU IST project)

G. Dondossola, G. Deconinck, F. Di Giandomenico, S. Donatelli, M. Kaâniche, P. Verissimo

CESI RIC. (It), KUL (Be), CNR-ISTI (It), CNIT (It), LAAS-CNRS (Fr), FCUL (Pt)

***Presented by*: Paulo Esteves Veríssimo**

Univ. of Lisboa, Portugal

pjv@di.fc.ul.pt

http://www.di.fc.ul.pt/~pjv

Models

Power control infrastructures

Evaluations

Architectures

LAAS
ISTI
ISTITUTO DI SCIENZA E TECNOLOGIE DELL'INFORMAZIONE "A. FAEDO"
CESI
cnit
consorzio nazionale interuniversitario per le telecomunicazioni
KU LEUVEN
FACULDADE DE CIÊNCIAS
UNIVERSIDADE DE LISBOA

Problems

- 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

Status quo

- This hap hazardous evolution led to the inevitable:
  - access to operational networks e.g. for remote SCADA/DCS maneuvering, ended up intertwined with access to corporate intranets and thus with public Internet
  - existing computational and resilience models do not understand (*represent*) the entanglement of the information flows of the three above-mentioned realms and the resulting interference
  - Unlike what exists in classical settings (e.g. web-based server infrastructures on Internet) it is currently in most circumstances infeasible to devise a dependability/security case for these interconnected critical utility infrastructures
- Risk is not well mastered
  - current configurations probably risk far more damaging **failure scenarios** than anticipated
  - The **damage perspectives** that may result from this exposure are overwhelming

Solutions?

- This problem is complex and must be tackled with the right weapons:
- Simultaneously under a security and a dependability viewpoint, what might be termed a ***trustworthiness*** perspective
- Achieving predictability in uncertain conditions, what might be termed a ***dependable adaptability*** perspective
- Encompassing correctness and continuity of service under a holistic viewpoint in what might be termed a ***resilience*** perspective

Ideas for an R&D roadmap to solutions (I)

- We lack a reference architecture of “modern critical infrastructures”
  - Three interconnection realms: operational SCADA/embedded networks; corporate intranets; Internet/PSTN access.
- We lack models for behaviour of modern critical infrastructures in critical scenarios
  - Derive common denominators: exposure, vulnerability, accidental malicious threat, unsafety.
  - Model *types of failures* specific to critical infrastructures: cascading, escalating, common cause failures
- We should be talking about “distributed, R/T and F/T, security critical systems”
  - Minimal first step: merge the concepts of CII and CI
  - The most modern concepts of DisSys will be needed
  - “Beyond SCADA” means union of SCADA, DCS, PCS, C3

Ideas for an R&D roadmap to solutions (II)

- Investigate architectural configurations that induce *aprioristic* prevention
  - of the more severe interaction faults, and attack and vulnerability combinations.
- Investigate middleware devices that achieve *automatic* tolerance
  - of remaining faults and intrusions
- Investigate trustworthiness monitoring mechanisms allowing unforeseen *adaptation*
  - to situations not predicted or that go beyond assumptions