Some Observations re the Workshop on Critical Infrastructure Protection

John F. Meyer
jfm@umich.edu

IFIP WG 10.4
Le Gosier,
Guadeloupe
January 12, 2007

Critical Infrastructures

- Both Bill and Jean-Claude presented lists of infrastructure domains that are (generally?) regarded as being critical
- Infrastructures considered explicitly in the workshop presentations were
  - information (Internet, telecom)
  - distribution and control of electrical power
  - process control (including BIG processes such as oil refinement)
- However, it appears that many of the protection, control, and evaluation techniques discussed will apply to other infrastructures as well

Legacy Systems

- As noted several times during the past two days, legacy systems are a deterrent to progress in the protection and control of certain critical infrastructures (those that have been around for awhile)
- But what about infrastructures that are relatively young or, better yet, in the process of being born (e.g., intelligent vehicle-highway systems)?
- In the latter case, it would seem that sophisticated “high-tech” solutions can be realized much more easily

Domain Specificity

- Some of the presentations were quite domain (application) specific while others were not.
- An important question in this regard is the following:
- What can be gained by taking maximum advantage of knowledge of the infrastructure being protected and controlled (its structure and its use environment)?
- In order to answer this, one should begin with a specification of what the infrastructure is (structurally) and does (behaviorally).

Repeat This for Several Domains

- Consider a second, third, etc. domain and do the same thing.
- Then compare these descriptions and determine the amount of overlap in both structural and behavioral requirements.
- Conjecture: Differences will outweigh similarities

Modeling and Evaluation

- Why are critical infrastructures difficult to evaluate?
- As compared with most other computer-based systems, there are typically additional difficulties due to
  - a wide variety of supported services
  - complicated service specifications
  - geographically distributed implementations involving diverse hardware and software components
  - interdependencies
  - extreme penalties (large losses of money, perhaps lives) in the case of severe failures due to either accidental faults or security breaches.

Measures

- Of principal importance in system (and likewise infrastructure) evaluation are the measures used to quantify what it
  - is, e.g., the integrity of its resources, and
  - does, e.g., how well it serves its users
- Generally, what a system does can be represented by
  - random variables
    - system-oriented (e.g., resource utilization, fault-recovery time)
    - user-oriented (e.g., throughput, end-to-end delay)
- A probabilistic measure of an RV provides its quantification
  - mean, higher order moments, PDF
- Note: Although this jargon appears to be model-oriented, it applies as well to direct measurements of an actual system.

Measure Specification/Formulation

- Specification
  - Natural language
  - Formal (logical, analytical)
  - Not too difficult
- Formulation
  - Model-based evaluation - HARD
  - Based on actual system – EASIER
    - Sometimes obtained directly
    - In the case of more complex performability and QoS measures, formulation is a function of lower-level RVs that can be monitored directly

Model-Based Evaluation

- Measures need to be formulated in terms of model behavior
- Current practice
  - Based on the measure’s specification, construct a high-level model of the system that appears to support its evaluation
  - Elaborate model accordingly
  - Iterate
    - Attempt to formulate measure
    - Revise model

    until formulation appears to be correct
  - Verify formulation
- Steps 3) and 4) are currently (human) labor intensive, requiring a great deal of knowledge regarding the system and expertise regarding use of the modeling tool (not practical to do this without a tool).

How This Should be Done in the Future

- Construct a detailed model of the infrastructure.
- Given a specified measure, its formulation and verification are fully automated via tools that require minimum human interaction.
- What will this permit?
  - Widespread application of model-based evaluation, and in turn, model-based validation w.r.t quantitative requirements.
    - Rapid prototyping
    - Models in the loop of autonomic systems
    - Service qualities guaranteed
    - And on and on

More on Legacy Systems

- As noted earlier, in the case of
  - entrenched (a.k.a. old)
  - extensive
  - expensive

  infrastructures, legacy systems are a deterrent to realizing effective means of protecting and controlling critical infrastructure systems
- Can the same be said for legacy WG 10.4 members?
- No! However, they have certain properties in common such as long lives in spite of known vulnerabilities

This is Illustrated in the Following Image (Recycled from the Annapolis Meeting)