Architecting Critical Infrastructures

Andrea Bondavalli

Università di Firenze

Critical Infrastructures

We are witnessing the construction of large-scale Critical Infrastructures which is moving at an always faster and faster rhythm.

They are growing (and becoming more and more critical) because of integration of previously disjoint systems.

They need to survive failures of components or subsystems, as well as attacks and intrusions and under no circumstances a complete denial of service is acceptable.

Instead, some level of (reduced) functionality must be provided - ALWAYS.

The composing elements

Unfortunately the Infrastructures that we have to operate and need to make resilient and survivable are not new brand systems that we can take the challenge to design anew!!

Massive deployment of low-cost, relatively unstable COTS hardware and software, as well as the integration of old legacy subsystems, seriously undermines the possibility of meeting stringent requirements.

Still we need proper efficient architectural solutions for the melting of these composing elements!!

Without them large resilient and survivable infrastructures are virtually impossible to obtain.

Challenges

- **Monitoring, Diagnosis and Recovery**
- **Self Awareness and Uncertainty**
- **Integration of Safety and Security**

Monitoring, Diagnosis and Recovery

For obtaining properties such as resiliency and making infrastructures able to survive failures, attacks and dynamic environments

- **the capability to monitor what happens, to detect errors or component failures, intrusions, attacks, deviations from expected behaviour,**
- **the ability to correctly diagnose the status or health of components (including entire legacy subsystems), and**
- **the availability of quick and intelligent reconfiguration and fault treatment strategies**

are key features.

A few relevant questions …

- **What to monitor? At what level should a system be instrumented? What should be the elements being monitored – What are the failure detectors?**
- **Where to monitor and who monitors? As a static structure is non adequate, where to place the monitors?**
- **How to derive consequences from observations? Are sophisticated diagnosis structures and solutions required? Who collects and interprets data?**
- **How to react? How to use this information and for what? For how long are the decisions taken after processing observed data valid given the dynamicity of the environment? Who enforces the decision?**

Self Awareness and Uncertainty

Runtime adaptation requires to monitor the environment and the timing of events. In distributed settings also time synchronization is required. To this end assumptions are made. However

- **the (hostile) environment does not allow to evaluate a worst-case scenario or this is too pessimistic and far from the normal case**
- **the quality of clock synchronization is a variable factor, very hard to predict.**

We need the ability of stating whether a single measurement result is reliable or not, through the awareness of the quality of synchronization.

Being able to distinguish measurement data has positive effects: e.g. we can filter them before using. This is an important step to be able

i) to *estimate* the *uncertainty* and

ii) to *increase* the *quality* and *reliability*

of monitored Data (and of decision taken based on that)

Safety & Security

The integration of legacy and the opening of SAFETY Critical Infrastructures has brought security into the forefront alongside safety. There are two problems when security is introduced into the safety-critical design process:

- **Although security related *techniques* exist, the safety-critical design process as yet has no "security critical design process" counterpart. – e.g. no "security integrity level" exists – essential to a defined, manageable, and verifiable design process.**
- **Little is known about the interaction between safety and security properties and between mechanisms and policies for supporting them in critical Infrastructures. To what extent the one might affect the other?? What trade-offs do exist?? How to define a combined measure of safety and security?/ (and use it)**

Safety and security are *emergent* properties of a system. A holistic development methodology appears to be necessary.

Is a component-based development processes viable??

Conclusions

Trying to provide some answers such as

R&SAClock: Reliable and *Self-Aware Clock*

Abstraction of the local clock

It hides to applications the existence of the synchronization mechanism(s) that it is monitoring: it shows the current time value (Local Clock Time) and the current accuracy of such information

in a few (EU funded) projects we are involved in.

Critical UTility InfrastructurAL Resilience

(IST 027513, http://crutial.cesiricerca.it)

HIghly DEpendable ip-based NETworks and Services

(IST 26979, http http://www.hidenets.aau.dk)