Designing Modular and Redundant Cyber Architectures for Process Control:

Lessons learned in the CRUTIAL project

Paulo Verissimo, Alysson N. Bessani,
Miguel Correia, Nuno F. Neves, Paulo Sousa

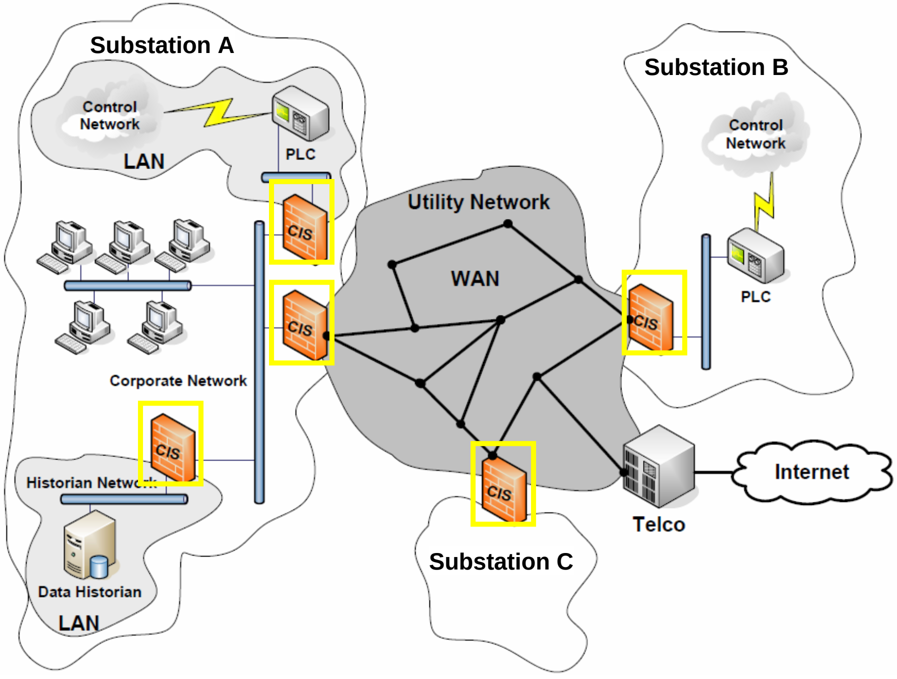
Problem to be solved

- classical firewall-based security not sufficient
  - primarily based on perimeter principle
  - also plagued by bugs and vulnerabilities
- component-based security not sufficient
  - cannot replace all components by new secure versions
  - cannot harden most of legacy components
  - misses security of the overarching architecture
- current system support not secure
  - many CII control systems applications rely on insecure infrastructure
- need *architectural solutions* that yield a global security case but preserve legacy
  - without large modifications to the original SCADA/PCS systems

Outline

- Motivation
- **An architecture for power grid protection**
- CIS Versions
- Evaluation
- Conclusions

Architecture – CIS



CIS - CRUTIAL Information Switch

- Purpose: to ensure that incoming / outgoing LAN traffic satisfies the *security policy* defined to protect the infrastructure (PolyORBAC)
- It is a *kind of firewall* but it has to fulfil a set of unusual challenges:

  dependability and security against cyber-attacks
  - in an *automatic* and *unattended* way
  - *perpetual* operation (or very low unavailability)
  - *resilience* against unexpected or overstress situations

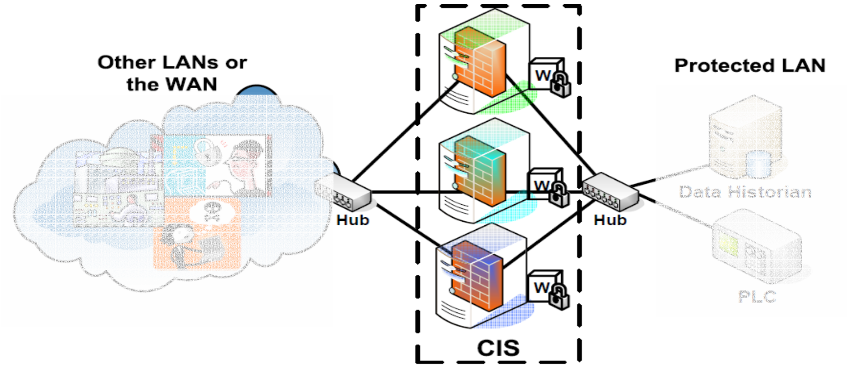
Outline

- Motivation
- An architecture for power grid protection
- **CIS Versions**
- Evaluation
- Conclusions

What has been achieved (cont.)

- Hierarchy of protection devices with incremental resilience, for practicality:
- 1. non-replicated
  - cheap, functional, not highly-resilient
- 2. intrusion-tolerant, replicated
  - resists up to f failures with 2f+1 replicas
- 3. self-healing intrusion-tolerant
  - tolerates an unbounded number of faults & intrusions
- 4. alternative PHY or VM replication of 2 & 3
  - VM-rep an excellent cost/value tradeoff
    (may preserve legacy HW investment)

Basic architecture of a CIS



- CIS has **N** diverse replicas (3 in the figure)
- Each replica may optionally contain a tamperproof component (**W**)
  - That’s what we mean by *architectural hybridization*

Outline

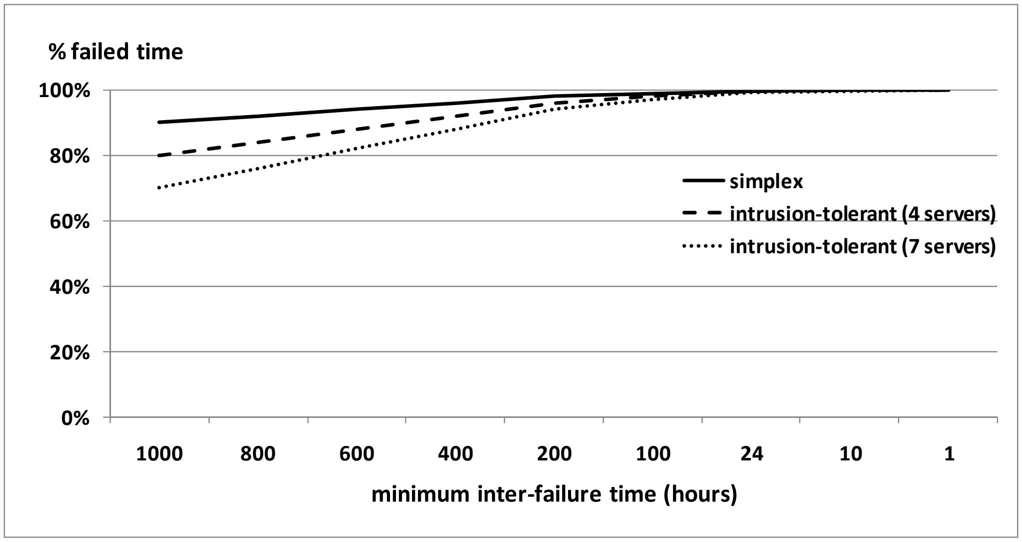
- Motivation
- An architecture for power grid protection
- CIS Versions
- Evaluation
- Conclusions

What has been achieved (cont.)

- wide set of simulation runs on working model of the CIS
- wide set of lab experiments on a real implementation of the CIS
- both show very promising performance vs. trustworthiness

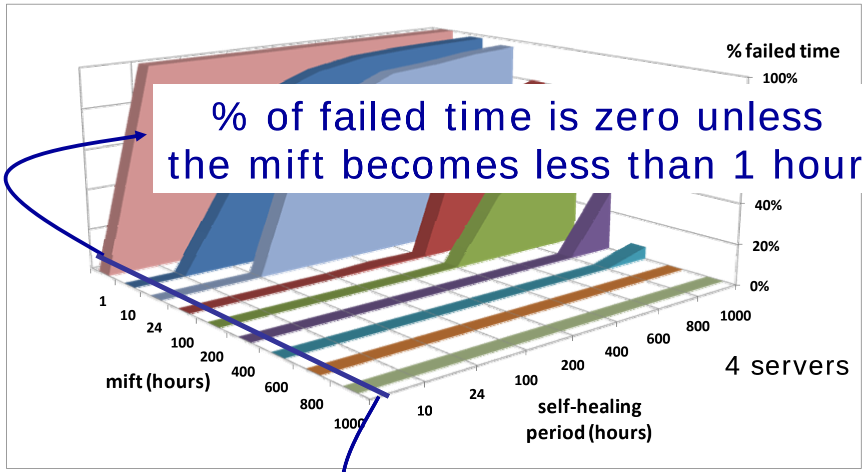
Intrusion-tolerant CIS without hybridization

– % failed time improves because attacker must control F+1 replicas for failure (no longer 1)



Self-healing CIS

– Replicas are rejuvenated, so % failed time is much reduced



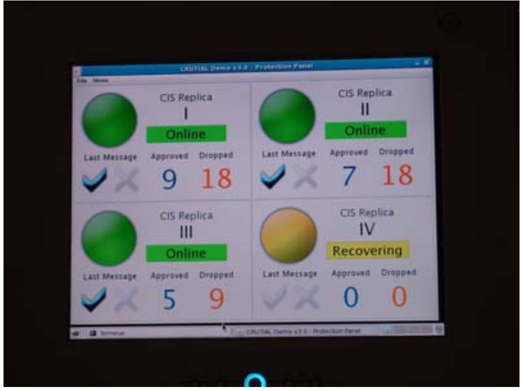
% of failed time is zero unless the mift becomes less than 1 hour!

our current prototype can rejuvenate all replicas in 10 minutes!

Experimental evaluation

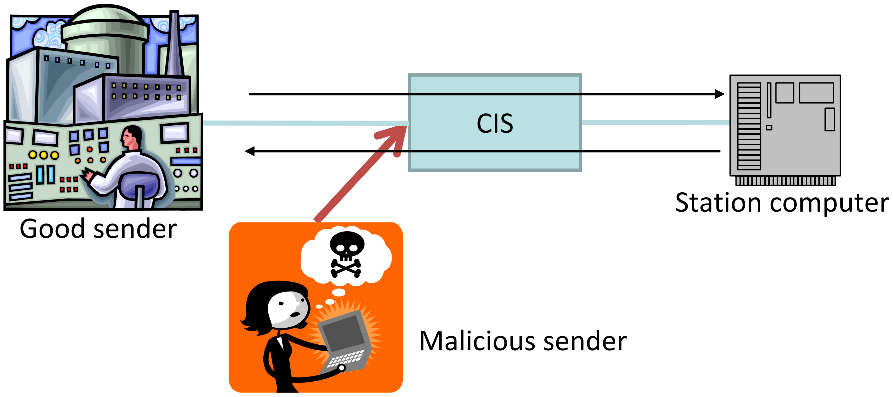
- We implemented 2 CIS prototypes:
  - With physical replicas
    - each replica runs in 1 computer
  - With virtual replicas in a single PC
    - each replica runs in 1 virtual machine

- Using these devices we measured:
  - latency introduced by the CIS (~1 ms)
  - loss rate under DoS attack (< 5% with up to 100 Mbps DoS traffic)



Experimental Evaluation (2)

- Testbed (cont.)
  - WAN side
    - 1 PC emulating a good sender, 1 PC emulating a malicious sender
  - LAN side
    - 1 PC emulating a station computer



CIS

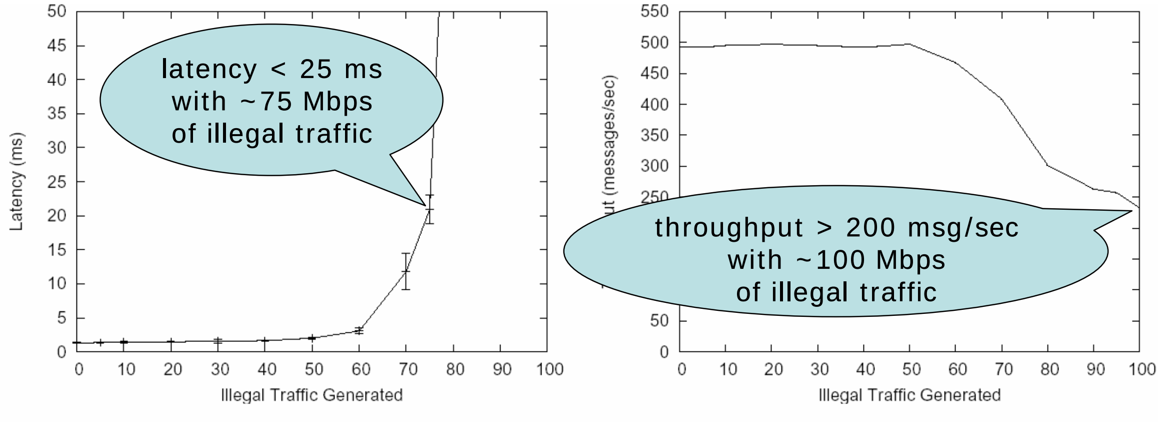
Good sender

Station computer

Malicious sender

SH PRRW CIS – Throughput and Latency

- Latency and throughput under a DoS attack from the WAN



latency < 25 ms with ~75 Mbps of illegal traffic

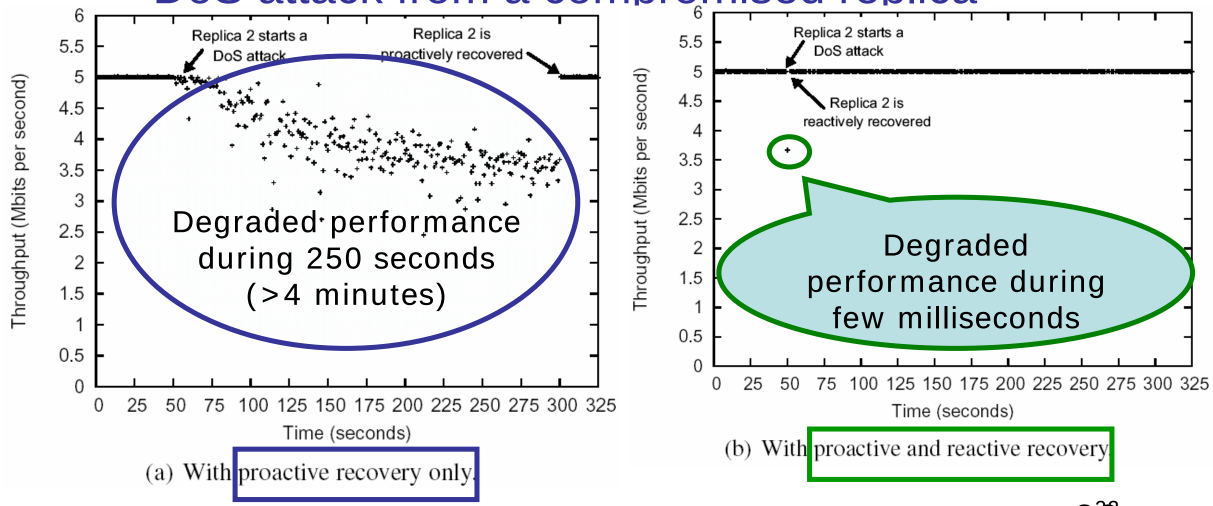
throughput > 200 msg/sec with ~100 Mbps of illegal traffic

(a) Average latency.

(b) Maximum throughput.

SH PRRW CIS – DoS resilence

- Throughput under a
  DoS attack from a compromised replica



(a) With proactive recovery only.

(b) With proactive and reactive recovery

Conclusions (1)

Configuration	cost €	# replicas	Resilience to Replica Faults		Resilience to (External) DoS attacks			
			# tolerated intrusions	tolerates HW faults?	DoS rate	Latency	Throughput	Loss Rate
IT CIS - Physical Replicas	2.250 €	3	1	YES	70 Mbps	3 ms	250 pack/sec	5%
IT CIS - VM Replicas	2.000 €	3	1	NO	100 Mbps	2 ms	450 pack/sec	10%
SH CIS - Physical Replicas	3.000 €	4	6 per hour	YES	60 Mbps	3.5 ms	250 pack/sec	10%
SH CIS - VM Replicas	2.000 €	4	6 per hour	NO	100 Mbps	2 ms	450 pack/sec	10%

The most expensive solution has the worst performance under DoS attack, but is the most resilient to replica faults

The least expensive (VM) solutions have the best performance under DoS attack, but do not tolerate hardware faults

Physical replicas have the same performance under DoS attack, tolerate HW faults, but SH CIS is more resilient to intrusions

Conclusions (2)

Configuration	cost €	# replicas	Resilience to Replica Faults		Resilience to (External) DoS attacks			
			# tolerated intrusions	tolerates HW faults?	DoS rate	Latency	Throughput	Loss Rate
Non-Rep CIS - 32 bits	750 €	1	0	NO	90 Mbps	2 ms	500 pack/sec	10%
Non-Rep CIS - 64 bits	2.000 €	1	0	NO	100 Mbps	1 ms	500 pack/sec	10%
IT CIS - Physical Replicas	2.250 €	3	1	YES	70 Mbps	3 ms	250 pack/sec	5%
IT CIS - VM Replicas	2.000 €	3	1	NO	100 Mbps	2 ms	450 pack/sec	10%
SH CIS - Physical Replicas	3.000 €	4	6 per hour	YES	60 Mbps	3,5 ms	250 pack/sec	10%
SH CIS - VM Replicas	2.000 €	4	6 per hour	NO	100 Mbps	2 ms	450 pack/sec	10%

64-bit machines are more resilient to DoS attacks
Why? Java is much faster on 64-bit machines!

More information:

- CRUTIAL web site: http://crutial.erse-web.it/
- A recent paper:
- IEEE Security & Privacy magazine, Nov/Dec 2008
The Crutial Way of Critical Infrastructure Protection
Alysson N. Bessani, Paulo Sousa, Miguel Correia, Nuno F. Neves, Paulo Veríssimo