Designing Modular and Redundant Cyber Architectures for Process Control: Lessons learned

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

HICCS @ Hawaii
Jan 2009

Designing Modular and Redundant Cyber Architectures for Process Control: Lessons learned

i.e., critical infrastructures,
mainly the power grid

main goal: protection from cyber-attacks

Designing Modular and Redundant Cyber Architectures for Process Control: Lessons learned

Motivation (I)

- The value of the power grid to society is incommensurably larger than that of common ICT systems (commercial, finance, etc.)

- Past:
  - Power grid used to be highly isolated, mostly proprietary
  - Hence secure against most threats

Motivation (II)

- Present:
  - Power grid undergone significant computerisation and interconnection (even with the Internet)
  - Great progress in terms of management
  - More complexity, higher level of vulnerability
- Future:
  - Distributed generation, smart metering
  - More complexity

Motivation (III)

In a nutshell

- We are witnessing the accelerated mutation of the power grid to computer-electrical or cyber-physical systems
- Systems are becoming connected to the Internet and often use common operating systems
- The risks they incur may drastically increase, if the problem is not tackled with the adequate weapons

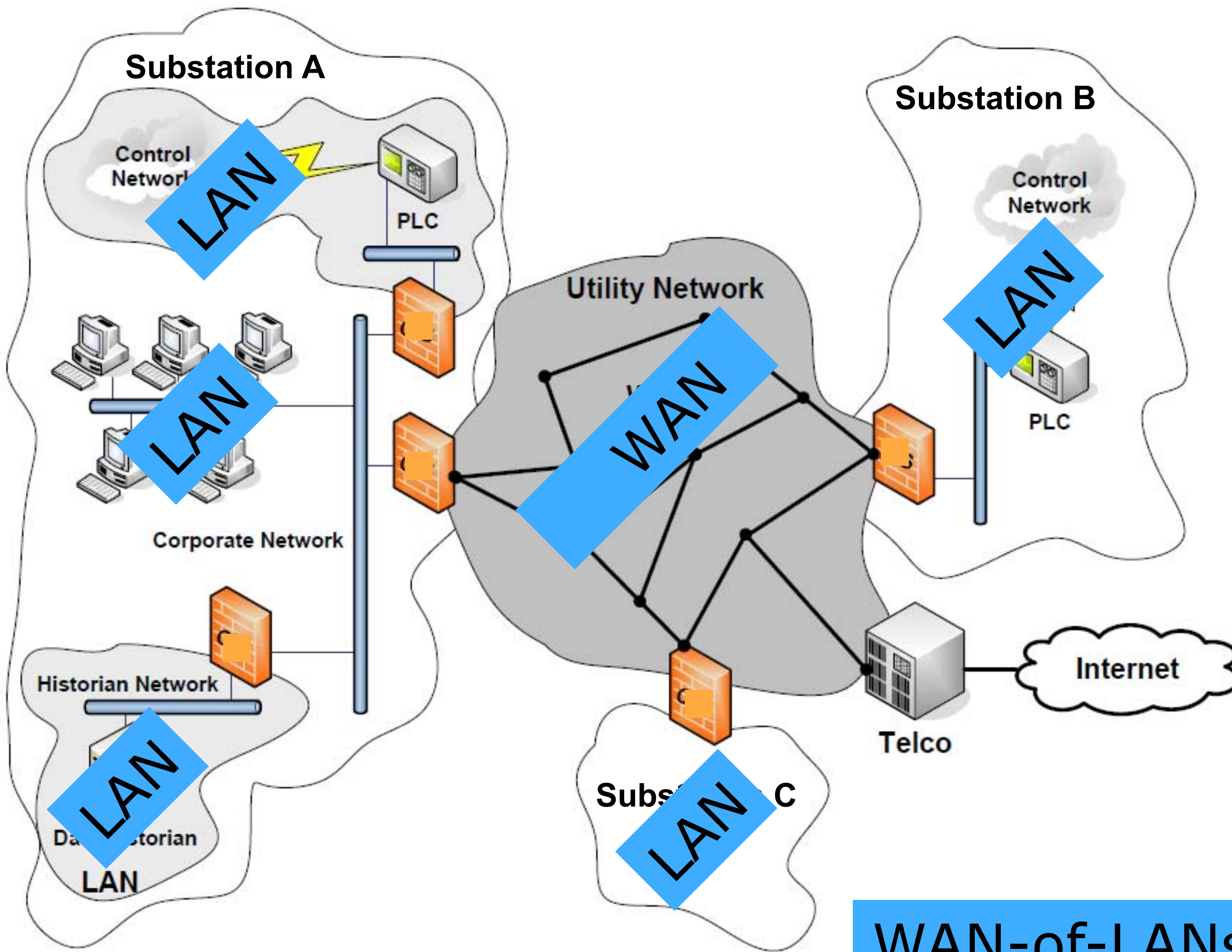
Outline

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

Outline

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

Architecture

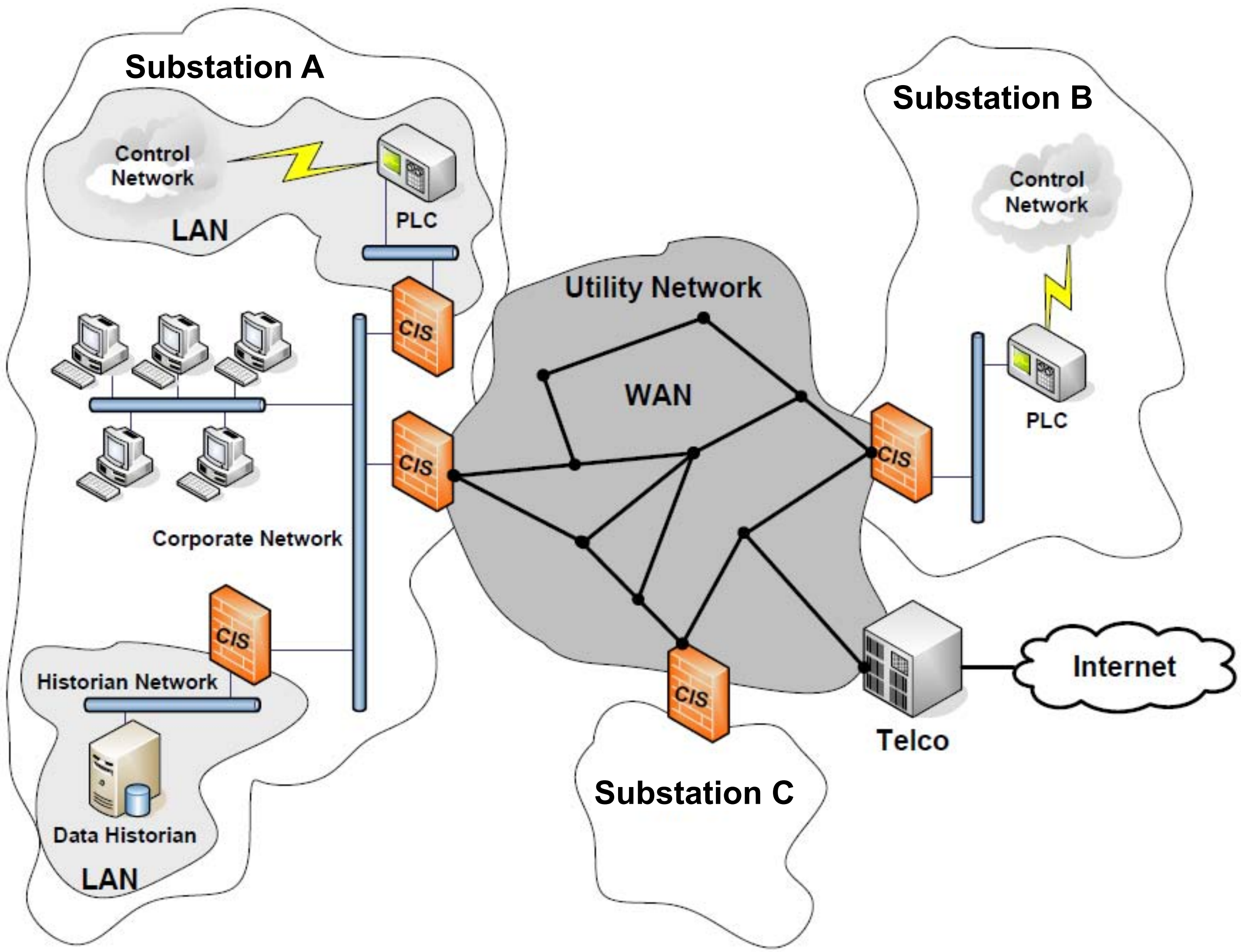


WAN-of-LANs model

Important observations

- Perimeter security is not sufficient
  - since modern threat scenarios include insider intruders
  - This architecture offers the right modularity by defining the LAN as the unit of trust
- Securing individual components (e.g. controllers, PCs) is important, but does not solve the problem
  - because one cannot assert the security of the overarching system architecture
  - This architecture puts the first order security assertions at the level of information flow between LANs

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

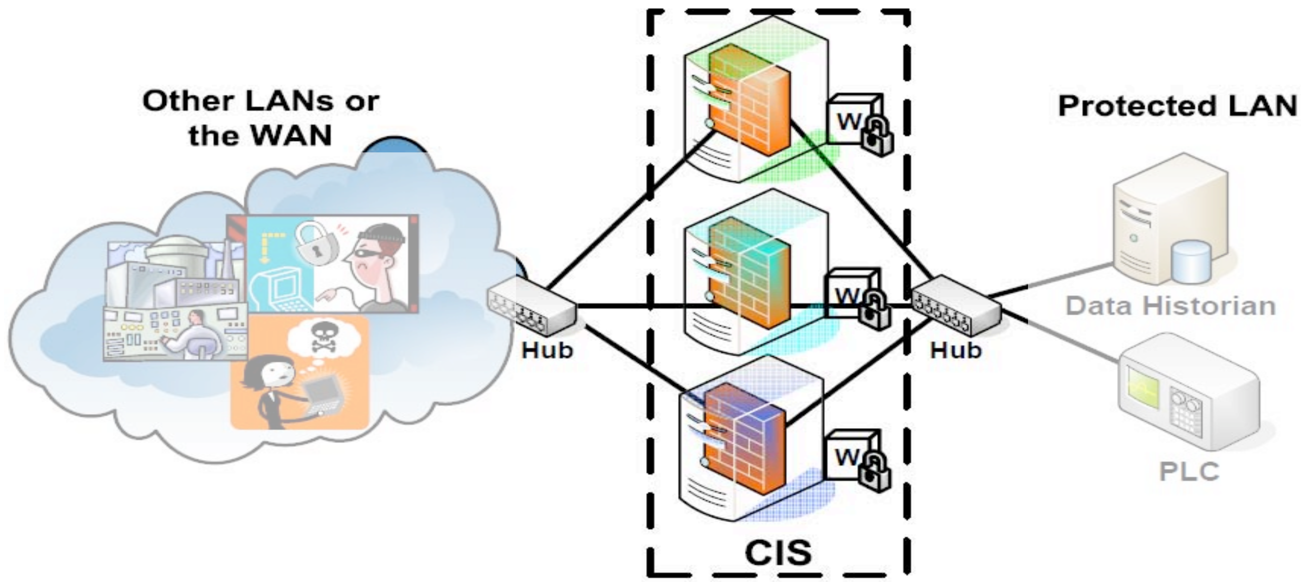
CIS characteristics

- It works at application layer and is a distributed firewall
  - offering richer semantics than e.g. TCP/IP packet filters
  - it can enforce the security policy everywhere
- It is intrusion tolerant thanks to replication
  - it does intrusion prevention even if some of its replicas suffer cyber-attacks and intrusions
  - uses architectural hybridization to improve its intrusion tolerance
- It is self-healing thanks to replica rejuvenation
  - replicas are rejuvenated (recovered) to remove the effects of malicious attacks that may have compromised them
  - proactively, i.e., periodically to remove undetected intrusions
  - reactively, i.e., when a replica misbehaves

Outline

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

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*

CIS Versions

- Each CIS has **N** replicas
  - **F** = maximum number of replicas that can be successfully attacked in a window of time (F < N/2)
  - **K** = max num. of replicas that may be rejuvenated at same time

We consider 3 CIS versions:

- Intrusion-tolerant CIS without hybridization
  - 3F+1 replicas (no tamperproof component)
- Intrusion-tolerant CIS with hybridization
  - 2F+1 replicas with tamperproof component (W)
- Self-healing CIS (with hybridization)
  - 2F+K+1 replicas with tamperproof component

Outline

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

Evaluation

- Objective: to justify design choices made, showing the reliability tradeoffs involved

- We consider a single CIS and evaluate it as doing a firewall service
  - comparing the several CIS versions

Evaluation methodology

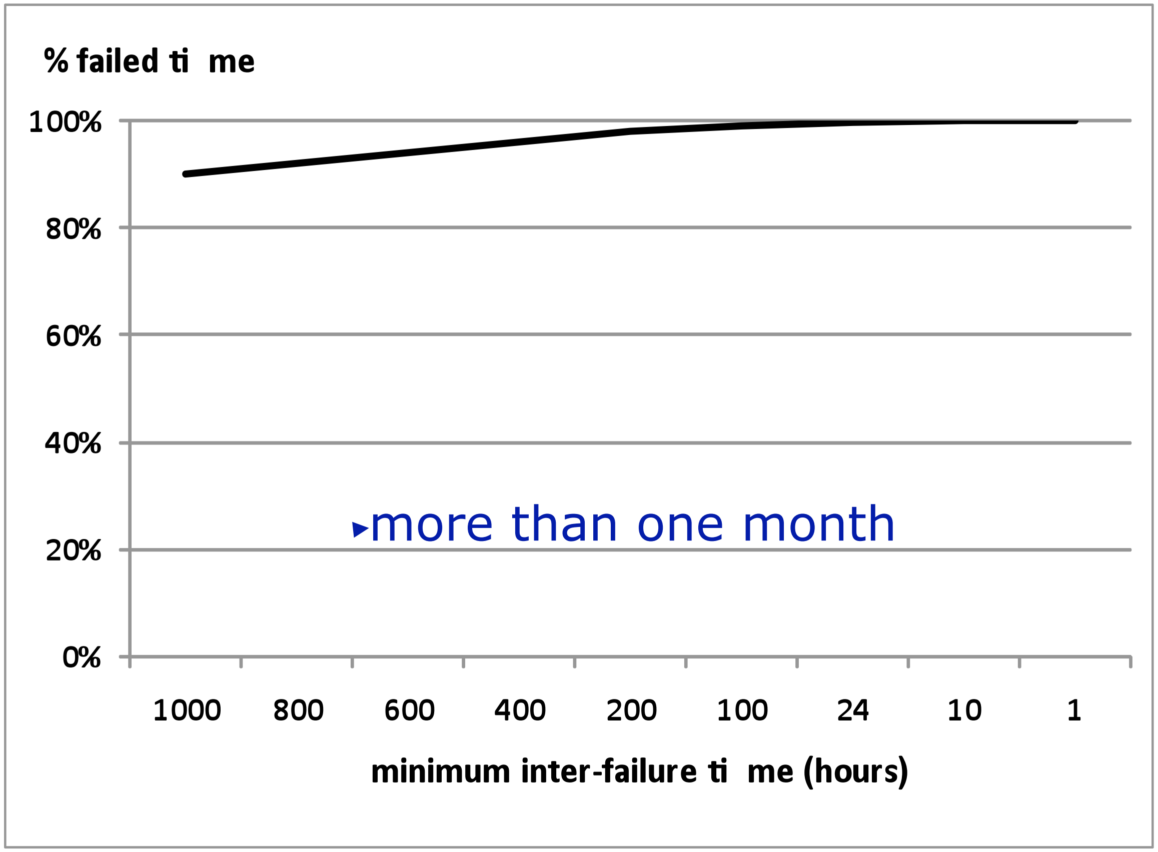
- The evaluation was done using the Möbius tool
  - Each CIS and a *simplex firewall* was modeled in Möbius
- The reliability metric used was the percentage of failed time
  - amount of time the firewall/CIS is failed, during a period of unattended mission
  - a CIS is said to be failed if more than F replicas are failed

Parameters of the simulations

- Maximum execution time (*met*):
  - mission time of the firewall/CIS
  - was set to 10,000 hours (about 1 year) in all simulations
- Minimum inter-failure time (*mift*):
  - minimum time interval between successful attacks
  - in each successful attack, the adversary randomly compromises one replica
  - *mift* varied in order to simulate different adversarial power

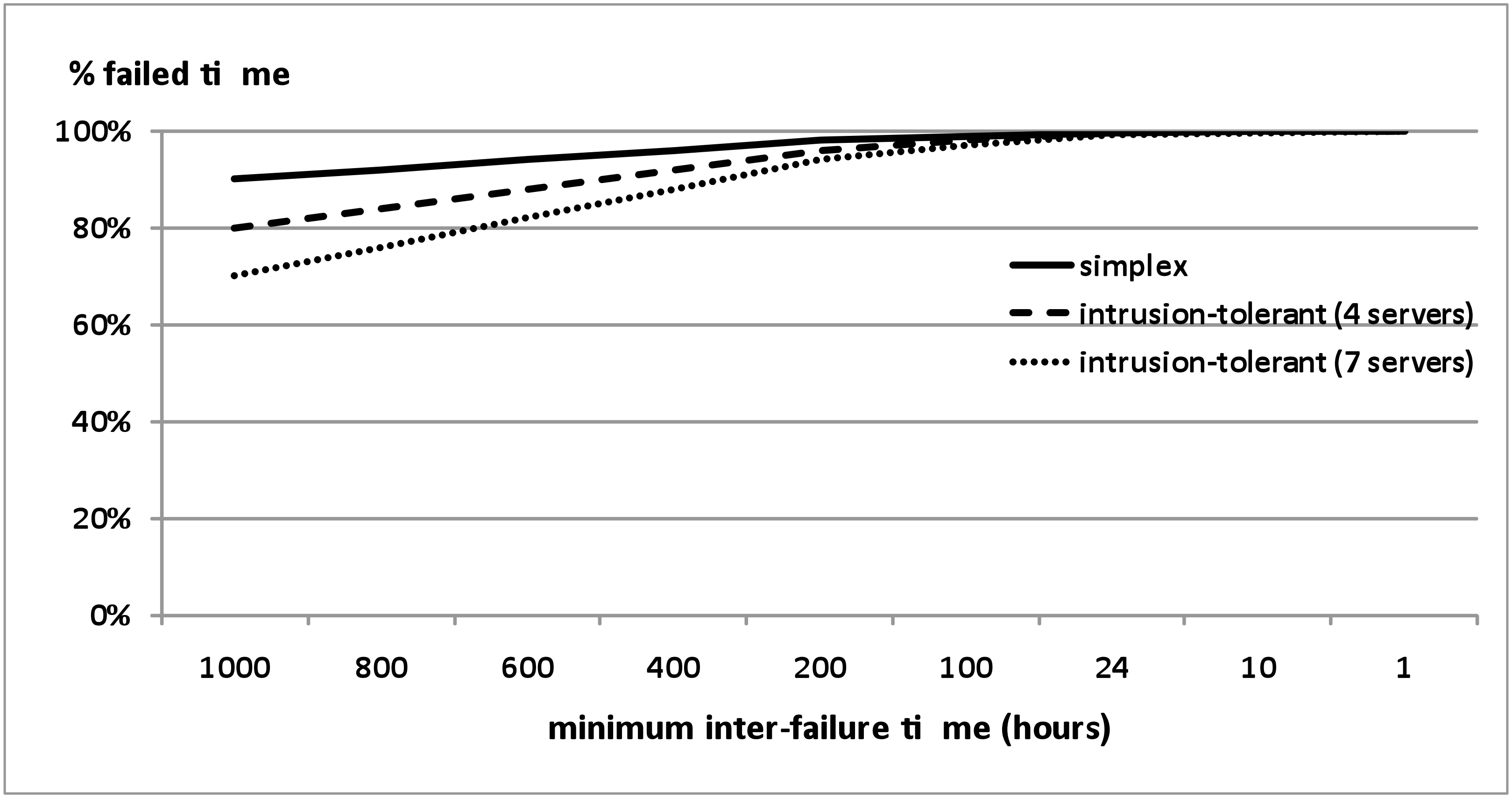
Simplex firewall evaluation

- % failed time very high even when inter-failure time is moderate



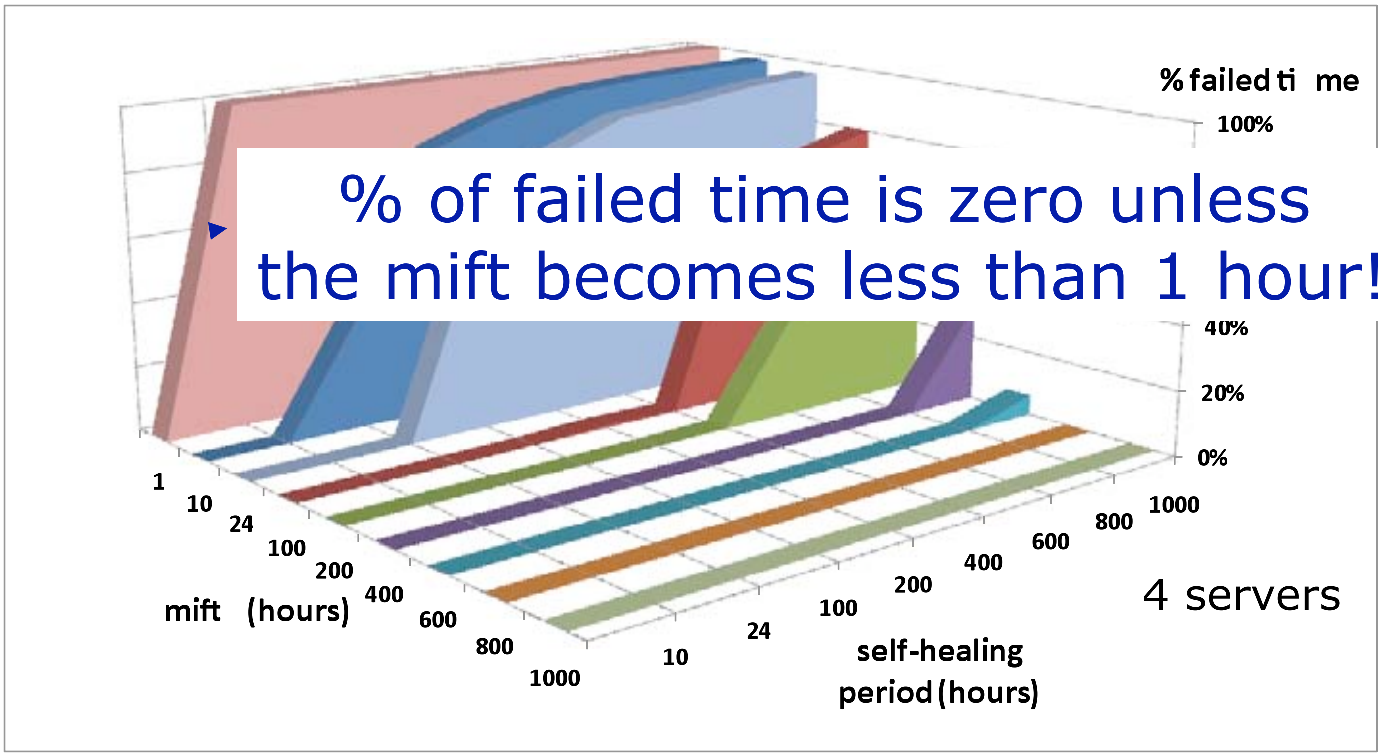
Intrusion-tolerant CIS
without hybridization

- % 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!

Other evaluations (not in this paper)

- 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)

Outline

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

Conclusions

- We presented a novel architecture for the protection of cyber-physical infrastructures
  - mainly the power grid
- We reported some of the lessons learned in the development, analysis and evaluation of the proposed architecture
  - The results look very promising in terms of usability of the concepts in real-life systems
- We have shown the incremental power of the several mechanisms used to enhance the operation of the CIS
  - which is the core component of the architecture

Future work

- Protection inside the control network
  - no longer generic computers but control devices
- Reliability and timeliness of the communication in the WAN
  - Utility networks prone to disconnections, possibly DoS attacks, and other problems

More information:

- Our HICCS 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
- www.navigators.di.fc.ul.pt