A FAULT- AND INTRUSION-TOLERANT ARCHITECTURE FOR THE PORTUGUESE POWER DISTRIBUTION SCADA

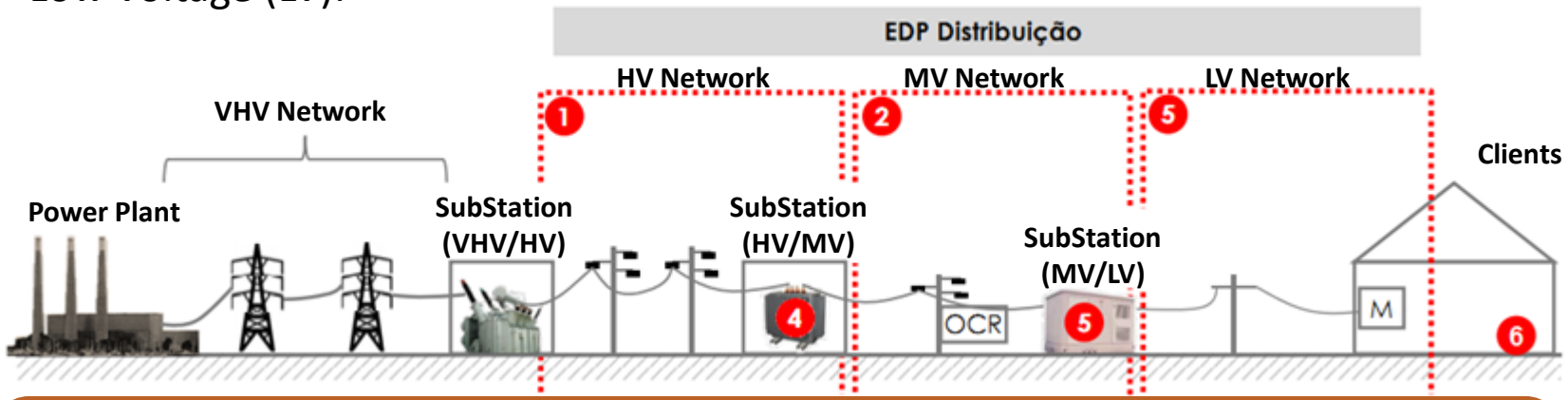
Nuno Medeiros Alysson Bessani

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DE LISBOA

Context: EDP Distribuição

EDP Distribuição is the utility responsible for the distribution of electricity in Portugal.

- Medium Voltage (MV) and High Voltage (HV)
- Low Voltage (LV).



Numbers:

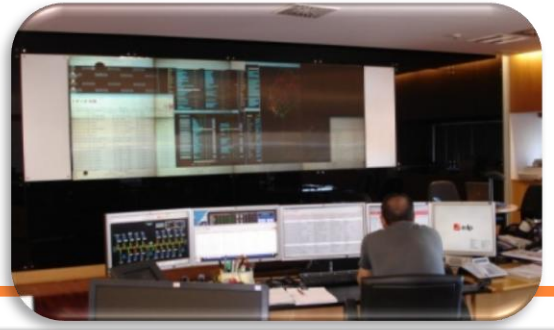
1. 9.000 Km
2. 73.500 Km
3. 136.000 Km
4. 402 SSs HV/MV
5. 62k SSs MV/LV
6. 6,1 M Clients

The main concern: Ensuring quality of technical service

Context: SCADA

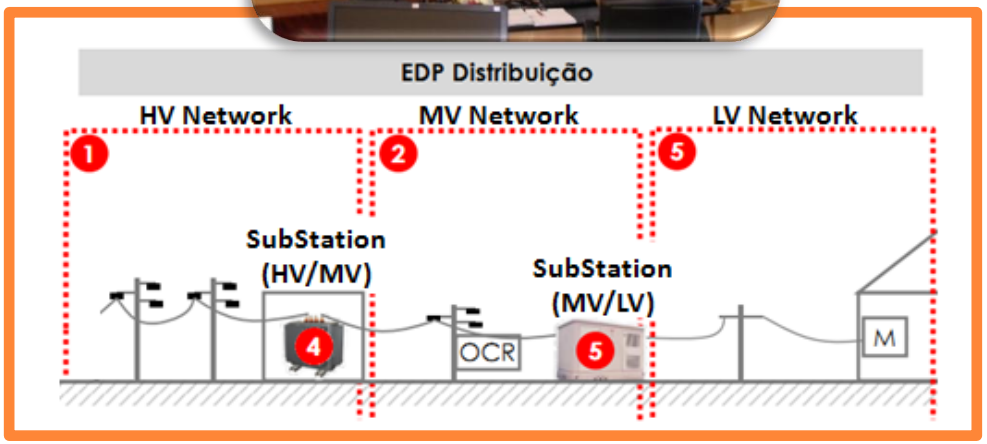
SCADA Systems

- Supervision and Remote Control
- Near Real-Time information



Principles

- Global network supervision
- Optimizes flow of energy
- Restoration-time reduction



Requirements

- Dependability - Provide correct service at all times
- Security - Potentially catastrophic cyber attacks

Change of Paradigm

The power grid is a critical infrastructure with high societary value.

Hackers destroy water pump in SCADA attack

Posted on November 18, 2011 - 12:54 by **Trent Nouveau**

An unknown team of hackers recently destroyed a pump owned by a US water utility after accessing the industrial control system used to operate its machinery.

According to security researcher Joe Weiss, the IP address of the digital infiltrators was traced back to a Russian network.

"It is believed the supervisory control and data acquisition (SCADA) software vendor was hacked and customer usernames and passwords stolen. [However], it is unknown if other water system SCADA users have been

CIA Confirms Cyber Attack Caused Multi-City Power Outage

Previous: Tax Season Presents Opportunities for Scammers Next: A New Year and a TCP Vulnerability

Jan 22, 2008 by Beau Woods

Filed under Research category.

In the movie "Live Free or Die Hard," street-wise cop John McClain battles it out with the bad guys using computers to carry out their crimes. In this movie, we are introduced to a term called a "Fire Sale" where hackers take out critical systems to cause chaos. It is literally a movie plot terror threat, and seems pretty unlikely to happen outside of the theaters.

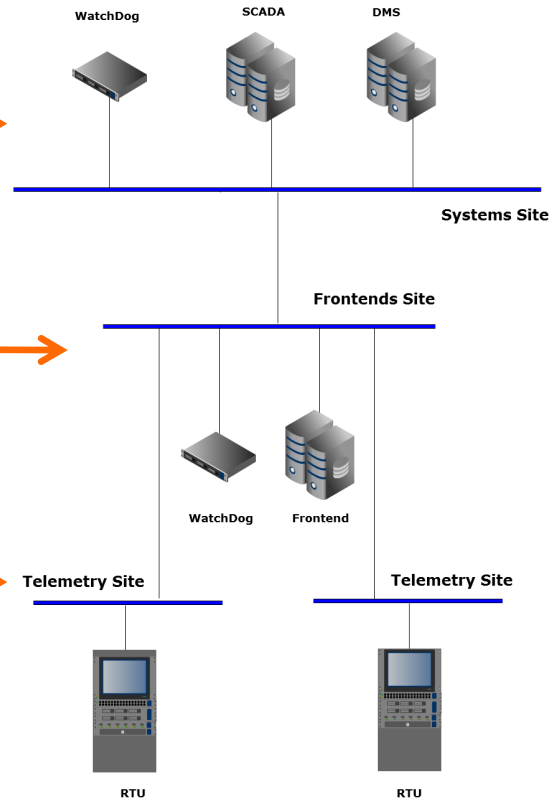
But late last week we got news of a similar scenario being carried out in foreign countries. Cyber criminals extorting public utilities with threats of taking down the facility. It seems that in at least one case, the attackers made good on their threats, affecting multiple cities. The Daily Mail of London indicates that these attacks have been carried out as near as "Central and South American countries including Mexico."

New challenges:

- Address the current implementation gaps and weaknesses
- Create dependable and secure information infrastructure
- Apply modern technologies

This Work

- We analyzed the most critical components of the EDP Distribuição SCADA system, GENESys:
  - **Core Systems**
  - **Frontends**
  - **Remote Terminal Units**



- We identified some weaknesses
- We present a fault- and intrusion-tolerant architecture for GENESys
- We perform a cost-benefit analysis of the proposal

Outline

~~Context~~

~~Contribution~~

GENESys System

Fault- and Intrusion-Tolerant GENESys

Analysis

Conclusion

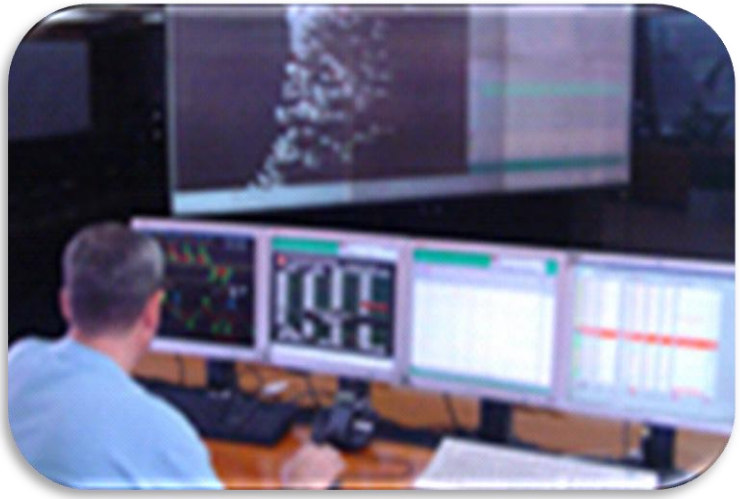
GENESys System

GENESys System

In EDP Distribuição, the platform to manage, monitor and remote control the power grid is called Generation Network Information System (GENESYS).

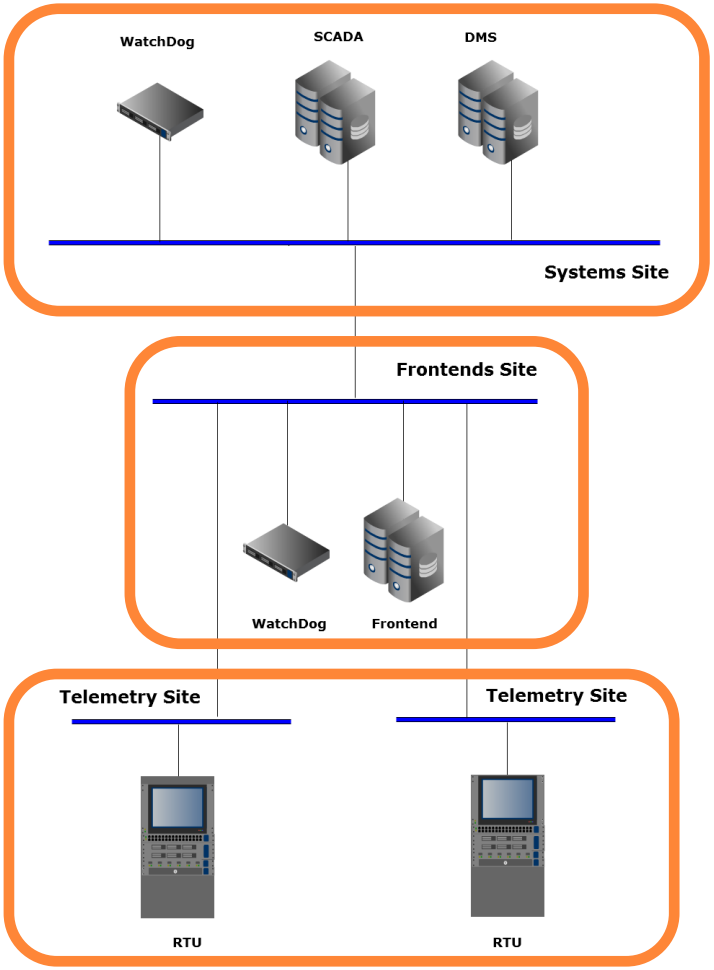
SCADA – A computational system that allows the supervision and remote control of the infrastructure.

DMS – Provides features to manage the distribution of energy, reflecting in a more efficient power grid operation.



GENESys Architecture

The GENESys system is composed by several components spread over three different layers.



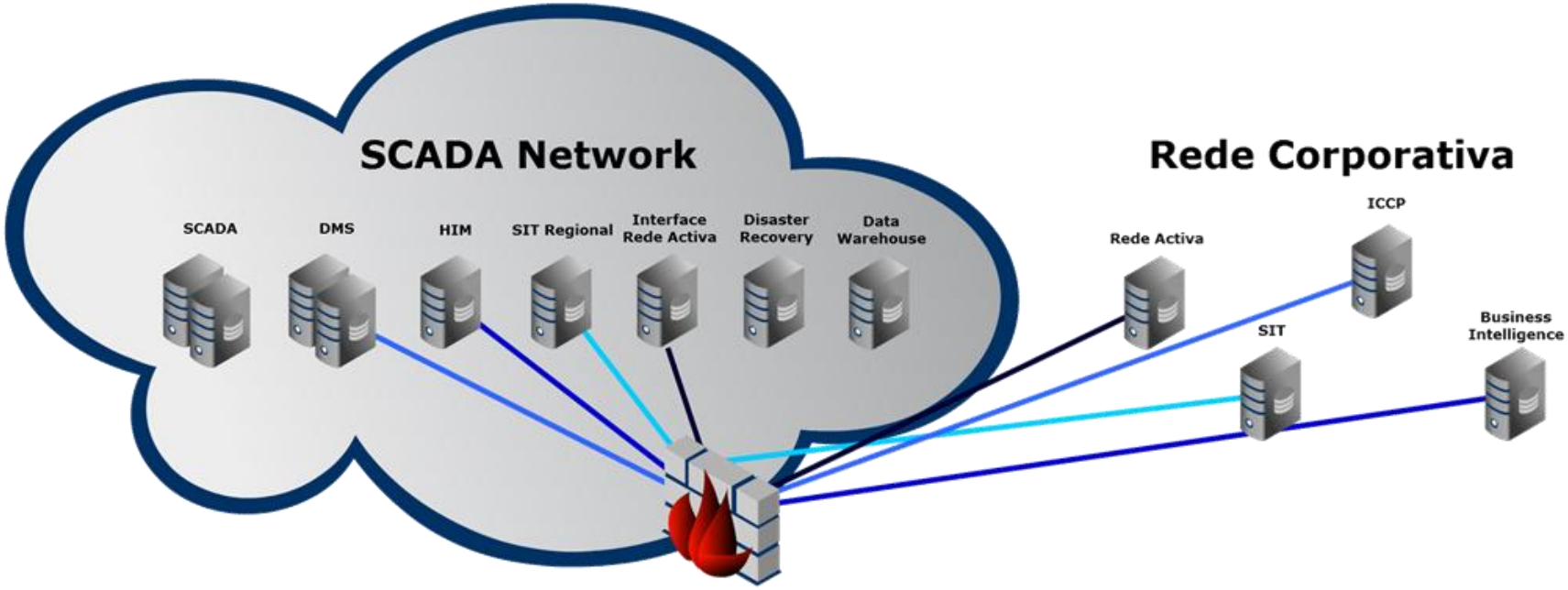
Systems Site – Higher layer of the architecture where the SCADA servers, the DMS and workstations are deployed.

Frontend Site – Middle layer where Frontend servers are deployed, responsible for data collection and protocol translation.

Telemetry Site – Corresponds to the electrical facilities where RTUs are installed for interface between the digital and analog domain.

Interconnection with other systems

GENESys also exchanges information with other corporate systems….



Current Dependability Solutions

Creating a dependable and secure power grid IT infrastructure is one of the main goals for EDP Distribuição.

- **Disaster Recovery System**
- **Network security mechanisms**
- **“Applicational” Access Control**
- **Security Audits**
- **Security Projects underway**

Fault- and Intrusion-Tolerant GENESys

Fault- and Intrusion-Tolerant GENESys

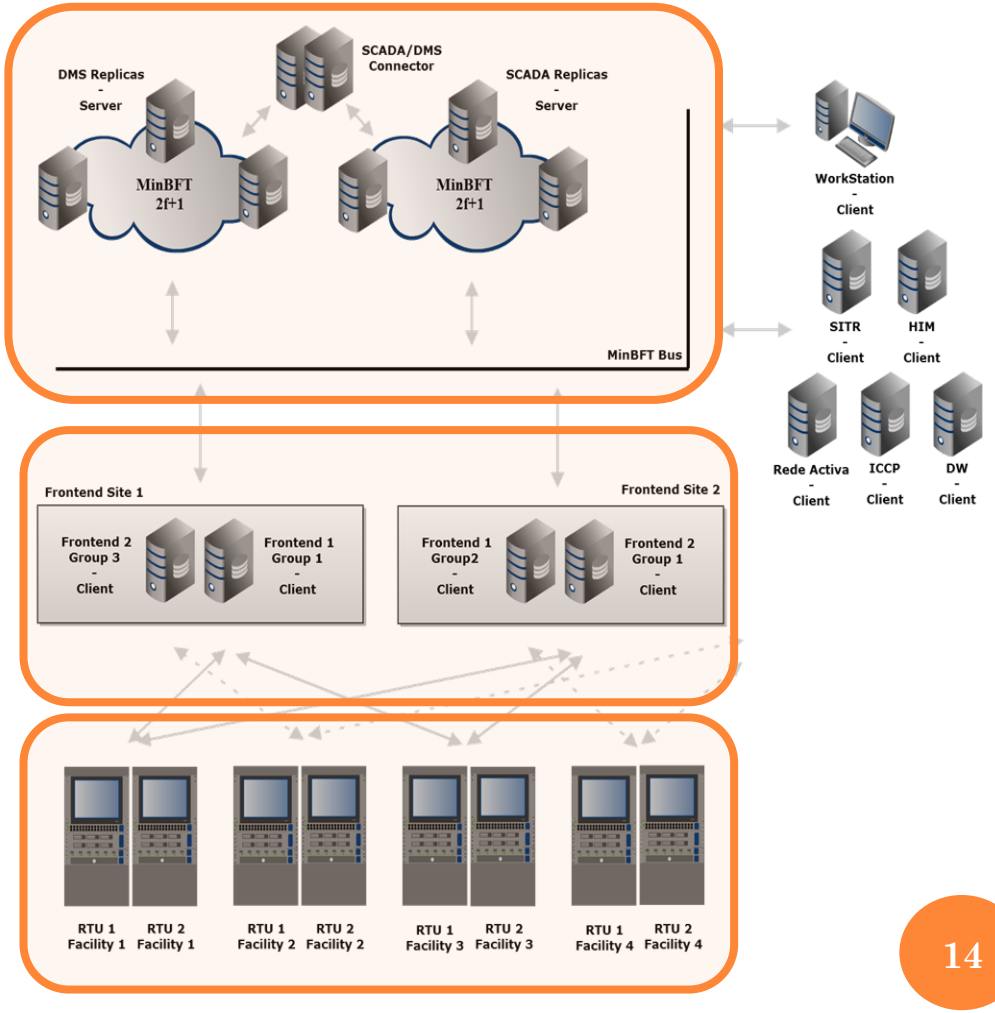
The new architecture is composed by three different solutions aiming the different layers of the system.

- **Intrusion-Tolerant SCADA and DMS**
- **Fault-Tolerant Frontend**
- **Redundant Remote Terminal Unit**

Different fault assumptions:

- **Criticality of failures**
- **Cost of the solutions**

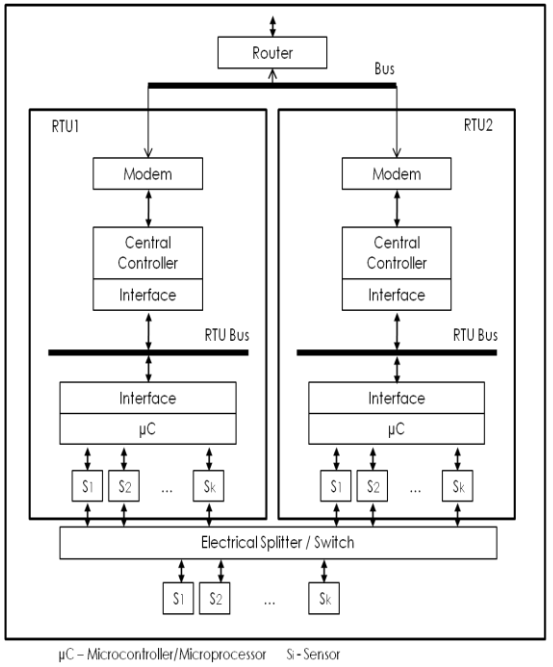
Can be individually implemented

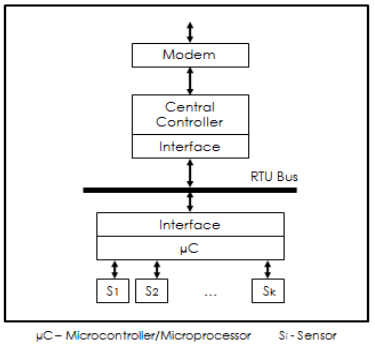


Redundant Remote Terminal Unit

Deployment of two redundant RTU components at the telemetry sites working together with an online/standby switchover mode, ensuring, fail-over operation.

- Two physical components making one logical RTU
- An electrical splitter/switch for sensing propagation to both RTUs
- Software development at all layers of the GENESys architecture
- Different network addresses
- A monitoring SCADA process





VS

Redundant Remote Terminal Unit: Benefits?

RTU Downtime Causes	Probability
RTU Motherboard	4%
RTU Communication Board	2%
Other RTU components	1%
Network	92%
Other	1%

Table 10 – Probability of the several RTU downtime causes.

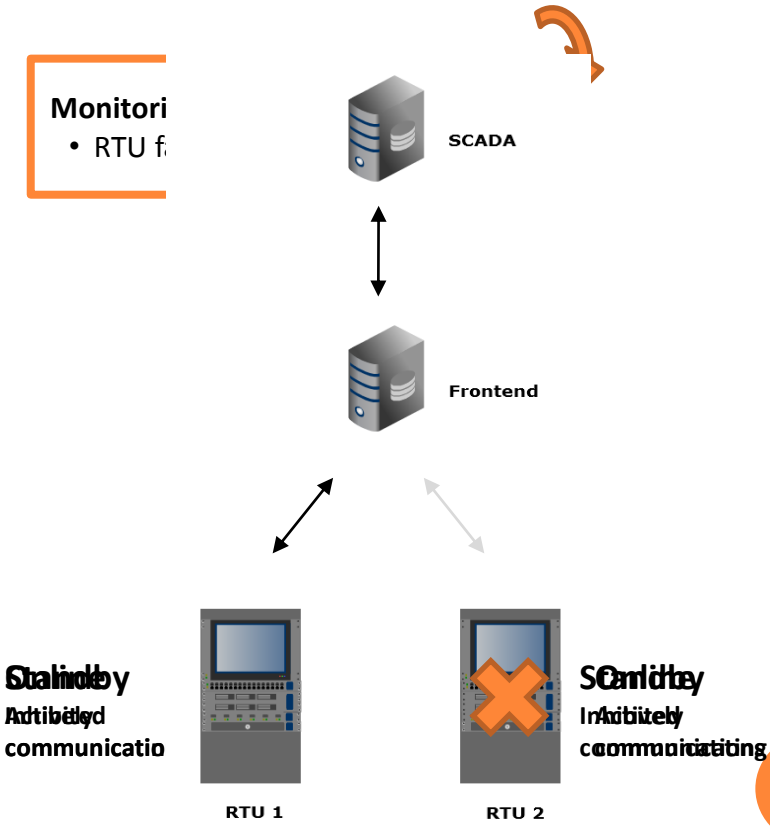
Telemetry Site Solution	Downtime (hours)	Uptime (%)
Single RTU	16:50:00	99,7338
Redundant RTU	15:20:00	99,7525

Table 11 – RTU Site communication details for the conventional and the proposed RRTU architectures. We provide the communication downtime and uptime percentage.

Redundant Remote Terminal Unit - Operation

The correct operation of the SCADA monitoring process is critical to ensure that the whole system remains synchronized relatively to the online/standby RTU states.

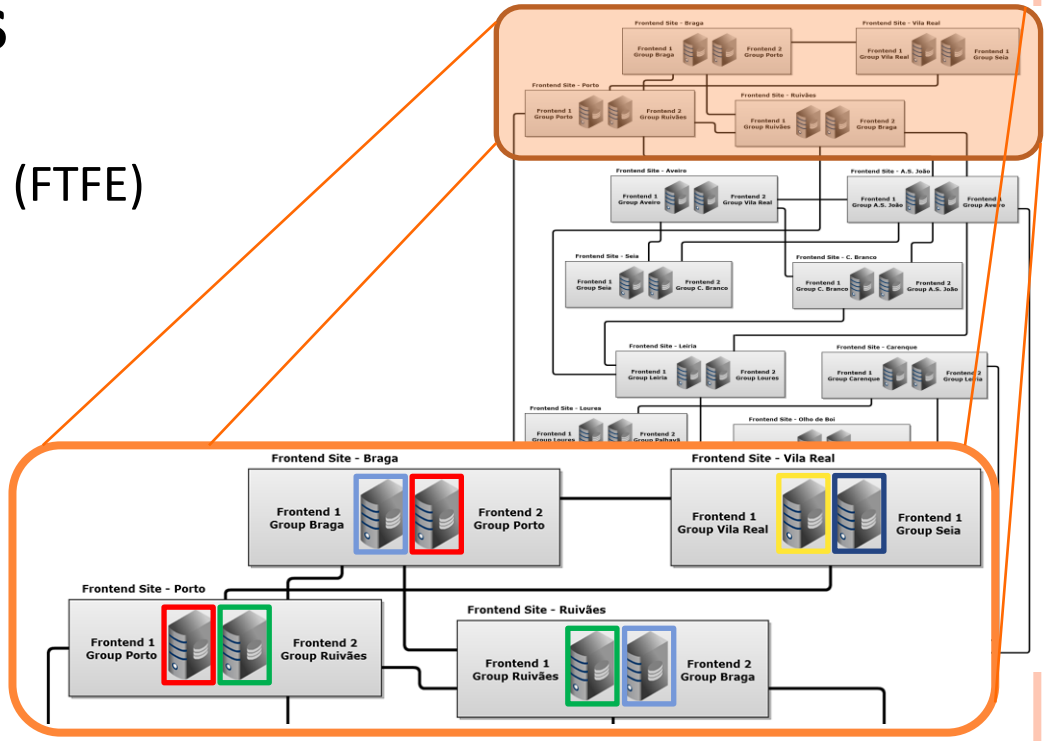
- Frontend detects RTU failure
- Delivers failure info to the SCADA
- Monitoring process triggers commutation procedure:
  1. **Changes Physical RTU for the logical connection**
  2. **Sends inhibit/activate control to online/stanby RTU**



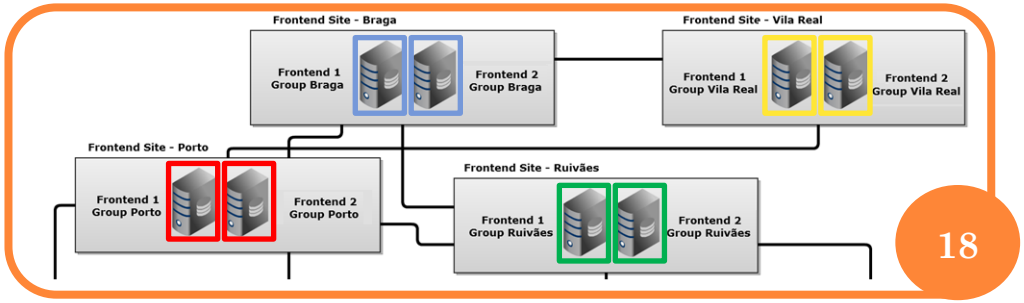
Fault-Tolerant Frontends

We propose an Fault-Tolerant Frontend (FTFE) based on redundant components.

- Different geographical locations
  - **Redundant end-to-end connections**
  - **Resistant to Site disasters**
- Operating in Online/Online mode
- Communication port-based commutation
- Require updates at all layers of the GENESys architecture
- A monitoring SCADA process



VS



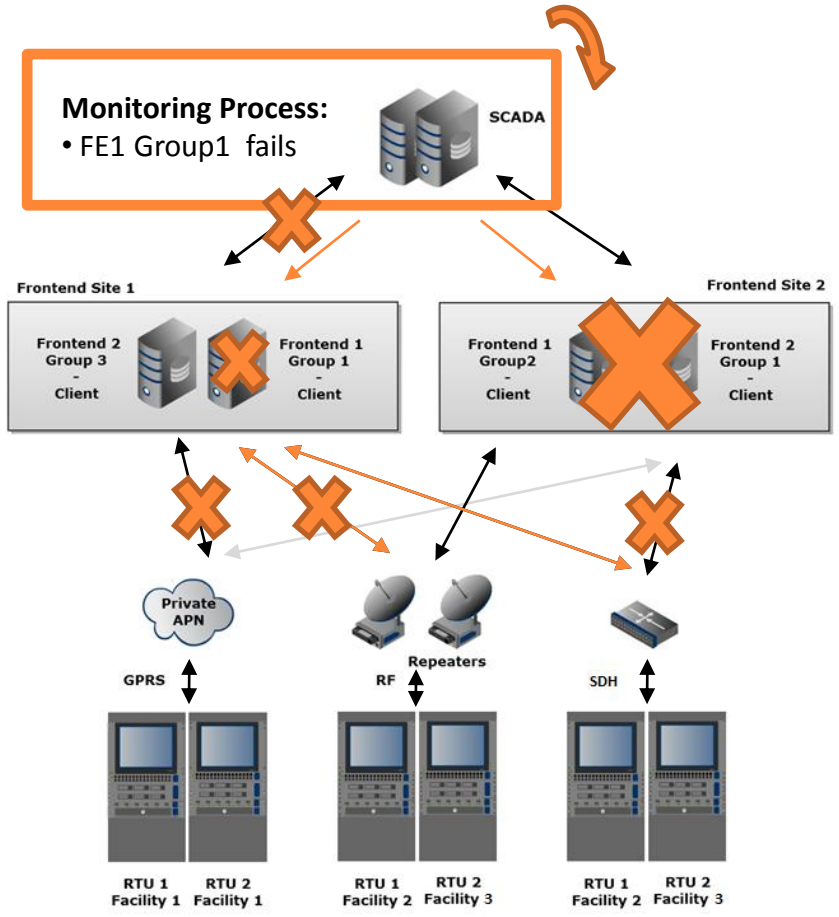
Fault-Tolerant Frontends: Benefits?

North				South			
Frontend Site	Downtime (min.)	Uptime (%)	Mapped RTUs	Frontend Site	Downtime (min.)	Uptime (%)	Mapped RTUs
AVEIRO	00:55:00	99,9893	202	BEJA	04:10:00	99,9512	181
BRAGA	02:17:00	99,9733	212	CARENQUE	01:50:00	99,9785	160
CASTELO BRANCO	00:00:00	100,0000	34	LEIRIA	11:50:00	99,8615	293
COIMBRA	00:31:00	99,9940	303	LOULE	02:09:00	99,9748	263
PORTO	00:11:00	99,9979	278	LOURES	04:26:00	99,9481	157
SEIA	00:55:00	99,9893	287	OLHO BOI	08:17:00	99,9031	156
VILA REAL	01:09:00	99,9865	186	PALHAVA	00:10:00	99,9980	58
RUIVAES	01:02:00	99,9879	154	SETUBAL	01:55:00	99,9698	384

Table 12 - Frontend Sites communication details in 2010. The analysis is divided in the two regions in which the system is separated. For each Frontend Site we provide the communication downtime, the uptime percentage and the number of mapped RTUs.

Fault-Tolerant Frontends - Operation

Both Frontends are actively communicating with RTUs. Each RTU has redundant paths to the redundant Frontend servers and can communicate by both paths.



Frontend Failure

- The monitoring process detects failure
- It triggers commutation procedure:
  - **Changes physical path to all RTUs mapped to the Frontend**
  - **Delivers the change to both redundant Frontends**
- RTUs automatically route through active paths.

Other Fault Scenarios

Intrusion-Tolerant SCADA and DMS

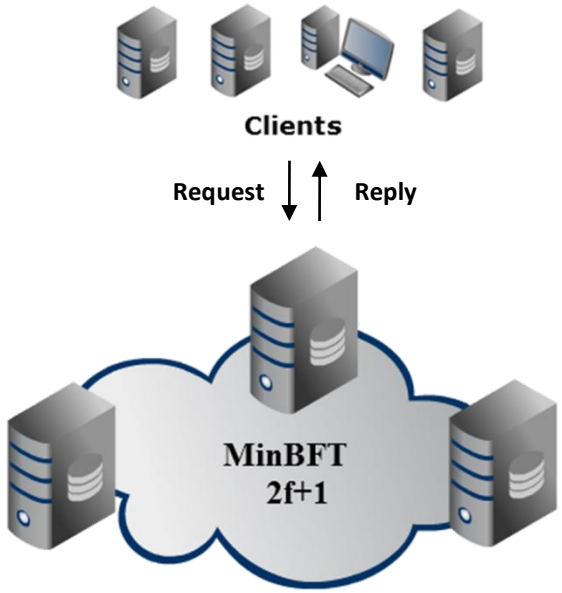
SCADA and DMS represent the Core systems of GENESys

The most critical components of the architecture

- **If they fail there is no power grid management**
- **If they are attacked the power grid can be compromised**

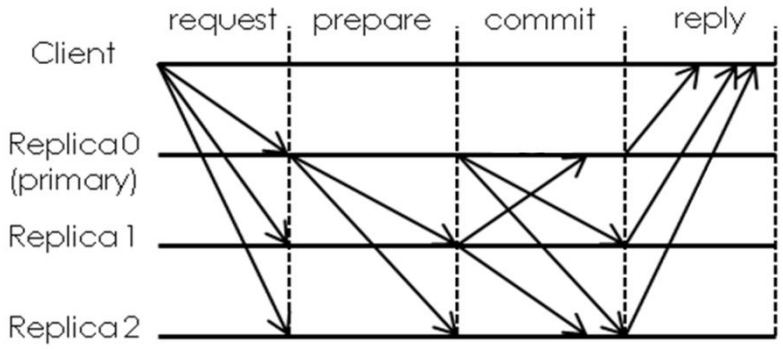
Intrusion Tolerance is considered affordable

- **Critical servers are replicated**
- **Byzantine fault tolerance state machine replication protocols can be used**
- **Diversity should be employed**



MinBFT Protocol [Veronese et al, IEEE TC 2013]

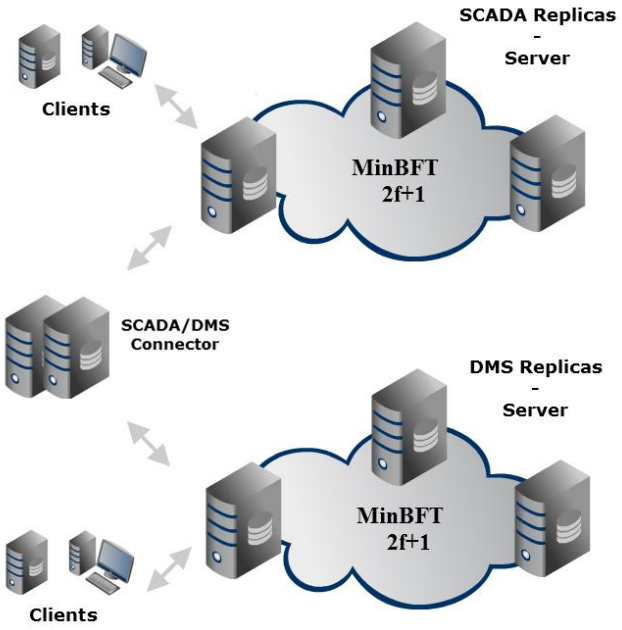
- **Tolerates *f* out-of *2f+1***
- **Uses Trusted Platform Module (TPM)**
- **One less communication step**



Intrusion-Tolerant SCADA and DMS

The MinBFT protocol is used for replicating both the SCADA and DMS servers.

- **SCADA/DMS replicas will be the server components of the protocol**
- **All other GENESys components are clients**



Clients – They request replicas for state information, to modify or delete its states. They wait for *f+1* matching replies to complete their operations.

Server – They represent the SCADA/DMS services provided by MinBFT. The protocol requires a client request to trigger any interaction.

SCADA/DMS Connector – A stateless component included in the architecture to safeguard the required exchange of information between the SCADA and DMS.

Intrusion-Tolerant SCADA and DMS

Three replicas per service to tolerate one compromised replica.

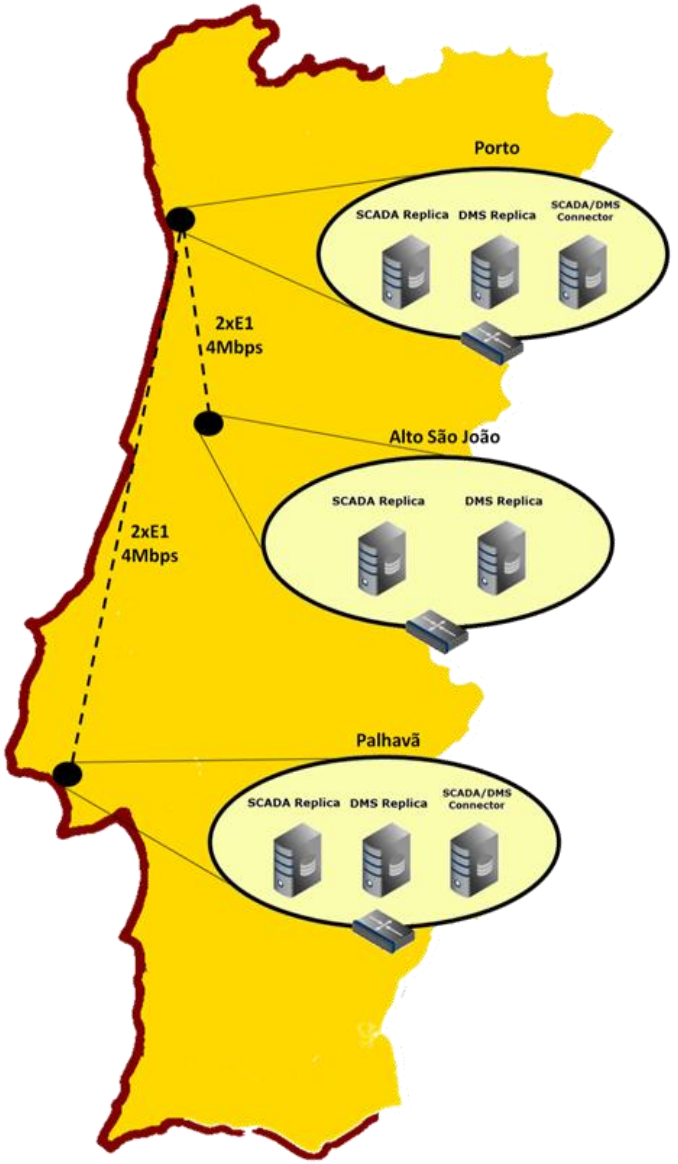
1. **Reducing the costs**
2. **Reducing the network load**

Replicas are deployed with diversity:

1. **Location diversity**
   - **Tolerate Site disasters**
   - **Large-scale DoS attacks**
2. **Software diversity**
   - **Common mode failures**

Sites were chosen based on:

1. **Network throughput**
2. **Lowest latency values**



Intrusion-Tolerant SCADA and DMS: Benefits?

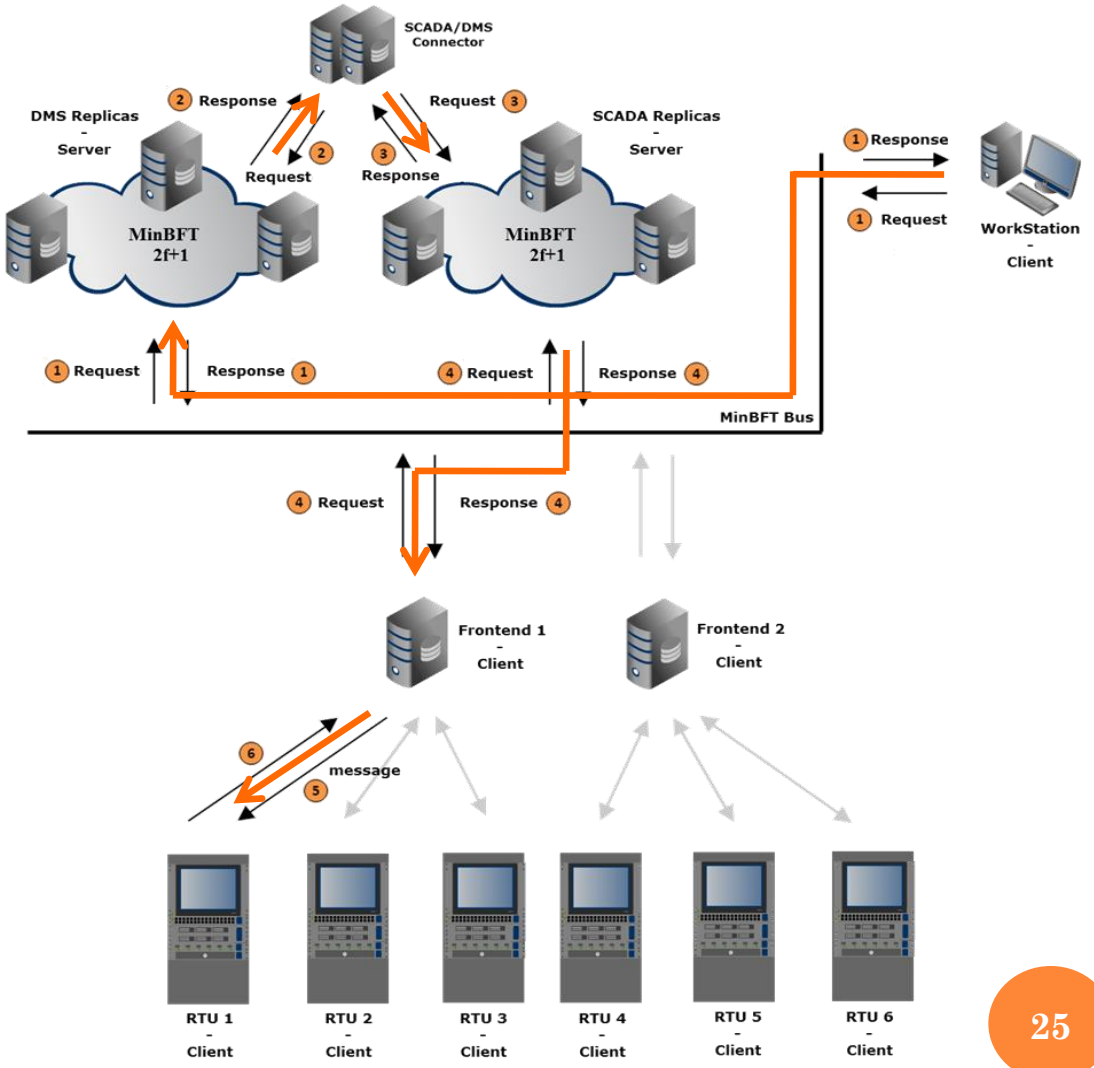
Site	Downtime (min.)													Uptime (%)
	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	2010	
North	207	0	107	89	163	52	116	99	40	110	0	6	989	99.81
South	5	70	100	0	21	23	73	60	0	72	45	290	759	99.85
Total	212	70	207	89	184	75	189	159	40	182	45	296	1748	99.66

Table 14 – SCADA/DMS downtimes (in minutes) per month in 2010.

GENESys Data Flow - Example

Remote Control

- A remote control is executed
- The control is sent to the DMS service
- The Connector is used to deliver the control to the SCADA service
- The SCADA service places it in the pending controls stack
- The Frontends request for pending commands for its mapped RTUs
- The Frontend delivers commands to the RTU
- The RTU executes the commands
- The command is validated



GENESys Analysis

Fault- and Intrusion-Tolerant GENESys Analysis

Fault Tolerance Capabilities Analysis

Acknowledging the fault tolerance capabilities of the several system components

- **Remote Terminal Units**
- **Frontends**
- **SCADA/DMS services**

Cost-Benefit Analysis

Acknowledging the main operational and technical advantages of the several proposals, trying to highlight the costs and benefits of its implementation.

Fault Tolerance Capabilities Analysis

	Conventional	Proposal
RTU Layer	• No fault tolerance mechanisms • Not able to tolerate faults on the components or the network	• Masking mechanism • Due to RTU redundancy it tolerates **omission** faults on one component
Frontend Layer	• Masking mechanism • Tolerates **omission** faults on one Frontend • Several single points of failure	• Masking mechanism • Tolerates **omission** faults on one Frontend • Due to spacial redundancy it eliminates single points of failure between the RTUs and FEs
SCADA/DMS Layer	• Masking mechanism • It tolerates **omission** faults on one server • Several single points of failure	• It eliminates single points of failure on redundant servers • Tolerates one faulty replica with **Arbitrary** behavior in a total of three replicas

Cost-Benefit Analysis

	Cost	Benefit
Redundant RTU	• Only for HV/MV substations • R&D costs not considered • RTU and its deployment costs • Increases **21.750€** on total cost • Represents an increase of **9,75%**	• An expected reduction of **7%** downtime on average per RTU • Represents an average of **1h30min** of increased uptime
Fault-Tolerant Frontend	• R&D costs not considered • Logistic costs for re-distributing the current Frontend servers • Estimated costs of **95.000€**	• Expected elimination of frontend groups downtime • Represents a total of **17h47min** • Reduces RTU downtime due to duplicated redundant links
Intrusion-Tolerant SCADA/DMS	• R&D costs not considered • Replicas costs: 5.000€ X6 • Connectors costs: 2.500€ X2 • Deployment costs: 2.500€ X8 • Estimated total cost of **55.000€**	• Expected elimination of SCADA/DMS services downtime • Estimated reduction of **26h** • Not measurable benefit of tolerating at-most one intrusion, that could be **catastrophic**

Conclusion

GENESys is an indispensable tool for the power grid management.

Much to be done regarding its fault tolerance capabilities.

The weaknesses are addresses with our proposed fault- and intrusion-tolerant GENESys, scoping with the three system layers.

- **Specified for GENESys but adaptable to other SCADA infrastructure**
- **Advantages of creating a practical scenario**
- **Designed with realism, regarding costs and technical details**

We described the benefits of our GENESys architecture and consequently how they would affect the power grid operation.

Conclusion

GENESys is an fundamental tool for the power grid management.

There are still a lot of opportunities for improving its dependability.

The weaknesses are addresses with our proposed fault- and intrusion-tolerant GENESys, scoping with the three system layers.

- **Specified for GENESys but adaptable to other SCADA infrastructure**
- **Advantages of creating a practical scenario**
- **Designed with realism, regarding costs and technical details**

We described the benefits of our GENESys architecture and consequently how they would affect the power grid operation.

Thanks for your attention

Cost/Benefit Details: RRTU

Pos.	Designation	Quantity	Price
1	**Equipment**		190.000 €
1.1	RTU	1	18.000 €
1.2	Other	1	172.000 €
2	**Development**		8.000 €
3	**Testing**		10.000 €
3.1	Factory Acceptance Test	1	5.000 €
3.2	Sight Acceptance Test	1	5.000 €
4	**Comissioning**		15.000 €
	Total		223.000 €

a) Cost analysis of a standard RTU architecture.

Pos.	Designation	Quantity	Price
1	**Equipment**		208.000 €
1.1	RTU	2	36.000 €
1.2	Other	1	172.000 €
2	**Development**		8.000 €
3	**Testing**		10.000 €
3.1	Factory Acceptance Test	1	5.000 €
3.2	Sight Acceptance Test	2	5.000 €
4	**Comissioning**		18.750 €
	Total		244.750 €

b) Cost analysis of a RRTU architecture.

Table 9 - Cost comparison between a standard and a Redundant RTU architecture.

Cost/Benefit Details: InTol SCADA/DMS

Pos.	Designation	Porto		Alto de S. João		Palhavã	
		Quantity	Cost	Quantity	Cost	Quantity	Cost
1	**Equipment**		12.500 €		10.000 €		12.500 €
1.1	SCADA replica	1	5.000 €	1	5.000 €	1	5.000 €
1.2	DMS replica	1	5.000 €	1	5.000 €	1	5.000 €
1.3	SCADA/DMS connector	1	2.500 €			1	2.500 €
2	**Deployment**		2.500 €		2.500 €		2.500 €
	Total		15.000 €		12.500 €		15.000 €

Table 13 – Cost of the proposed backend systems architecture (per site).