



## Security for smart Electricity GRIDs

# Intrusion Tolerant SCADA

*André Nogueira, Alysson Bessani, Nuno Neves*  
*Faculty of Sciences of the Univ. of Lisboa (FFCUL)*

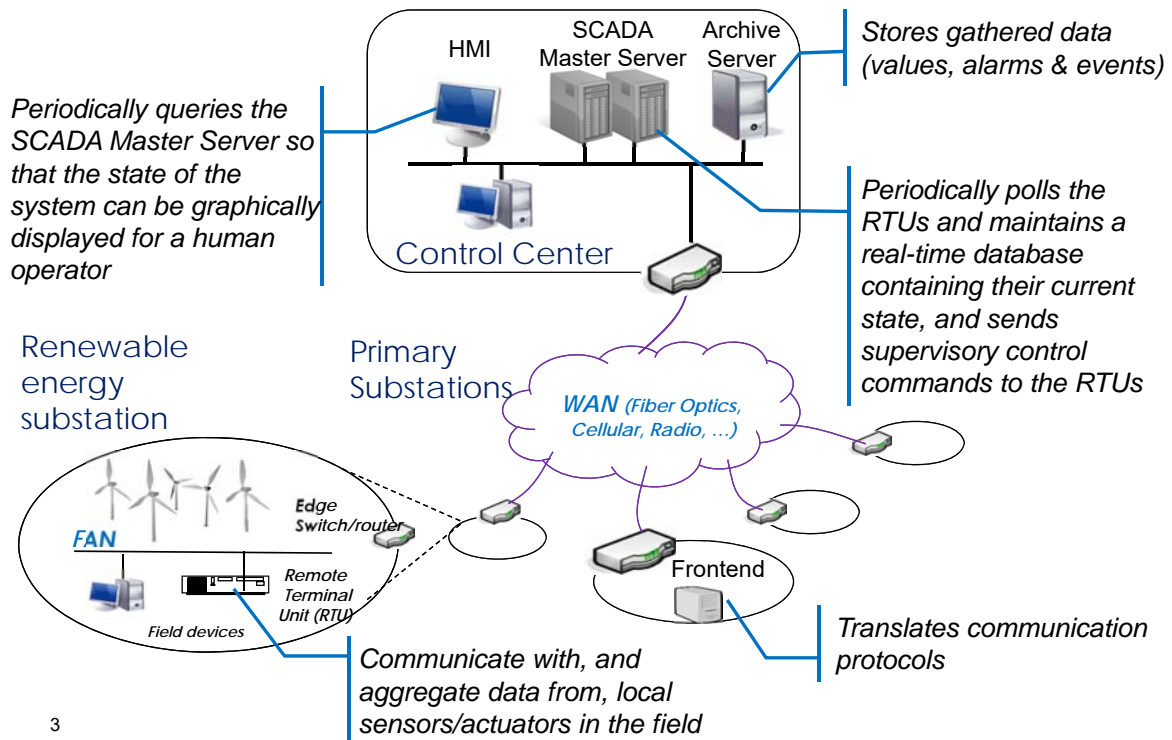
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 607109



## **Goal: Demonstrate a SCADA system capable of tolerating intrusions**

- › Show how an attacker can corrupt the execution of a critical infrastructure by compromising the SCADA Master server
- › Show a more resilient SCADA solution, where the SCADA Master maintains system correctness in the presence of intrusions

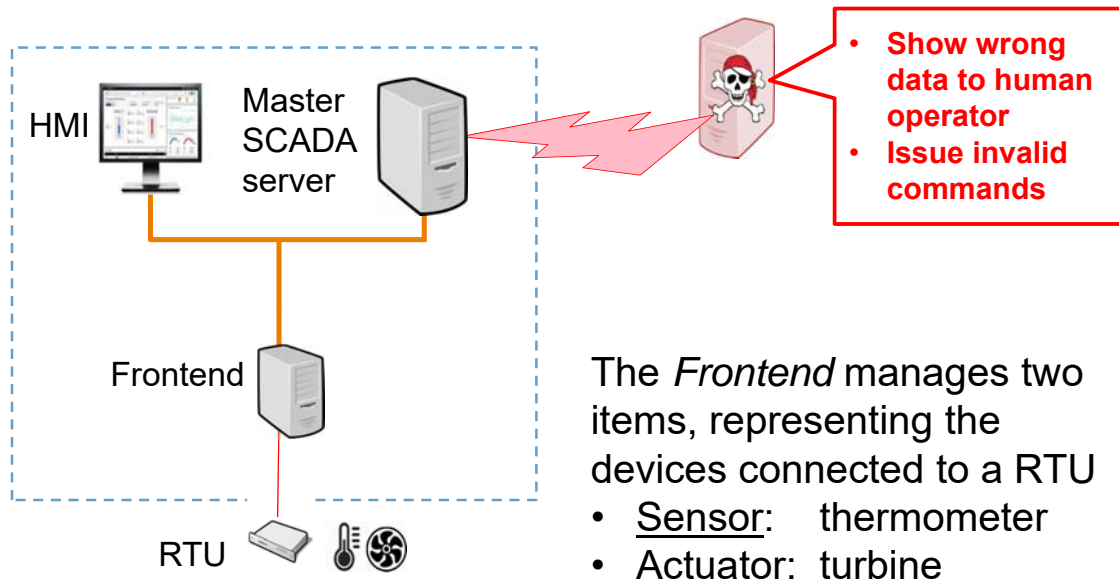
# Simplified SCADA system



3



## Demo scenario



4

## The prototype and experimental environment

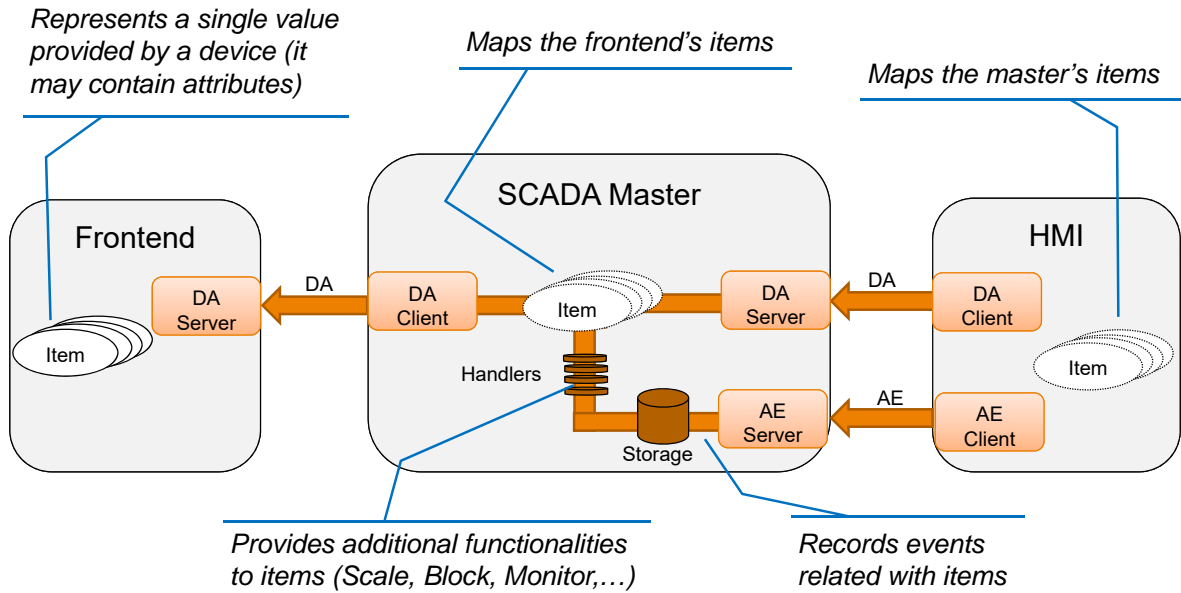
5

### Prototype

- › System based on the **Eclipse SCADA** open source project
- › Eclipse SCADA provides a modular “construction kit” to create a custom SCADA
- › IBH SYSTEMS GmbH is the leading contributor
- › In production for instance at:
  - E.ON solar plants
  - OMV business processes

6

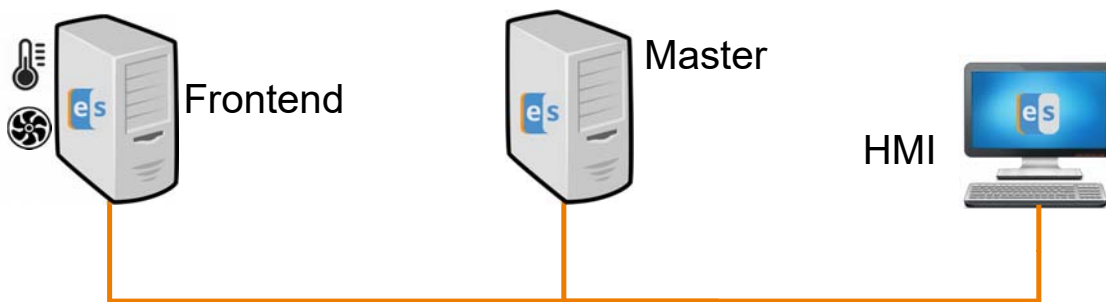
# EclipseSCADA: Components



7

# Experimental Environment

## › Eclipse SCADA & Emulated RTU Items



8

## Demonstration

9

## Demonstration: 4 Steps

1. Interact with RTU items using Eclipse SCADA
2. Impact of an intrusion in the SCADA Master
3. Interact with RTU items using intrusion-tolerant Eclipse SCADA
4. Impact of an intrusion in a SCADA Master replica



10

## Demonstration: 4 Steps

1. Interact with RTU items using Eclipse SCADA
2. Impact of an intrusion in the SCADA Master
3. Interact with RTU items using intrusion-tolerant Eclipse SCADA
4. Impact of an intrusion in one SCADA Master replica

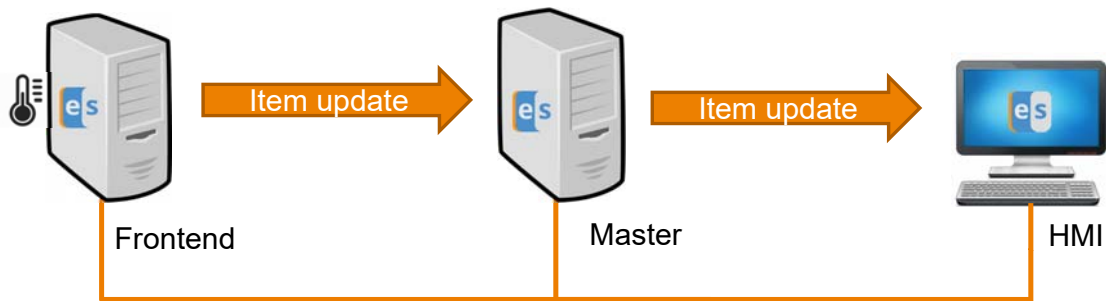
11

## Use cases

- › Simulate temperature updates in thermometer item 
- › Simulate switch on/off commands in turbine item 
- › Setup an alarm that goes off if the temperature reaches a threshold value

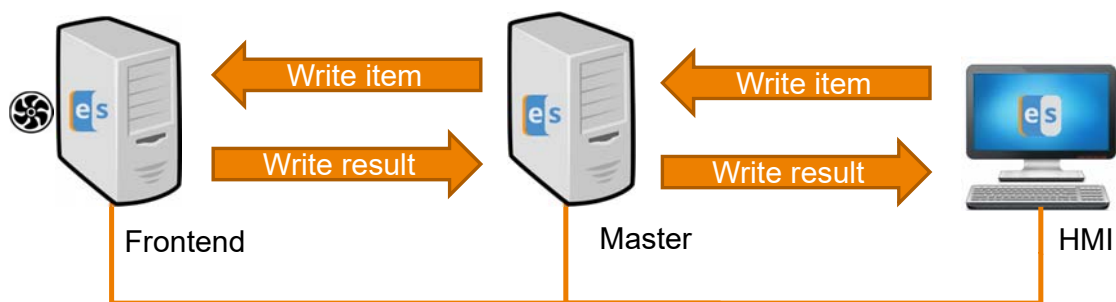
12

## Thermometer Item use case



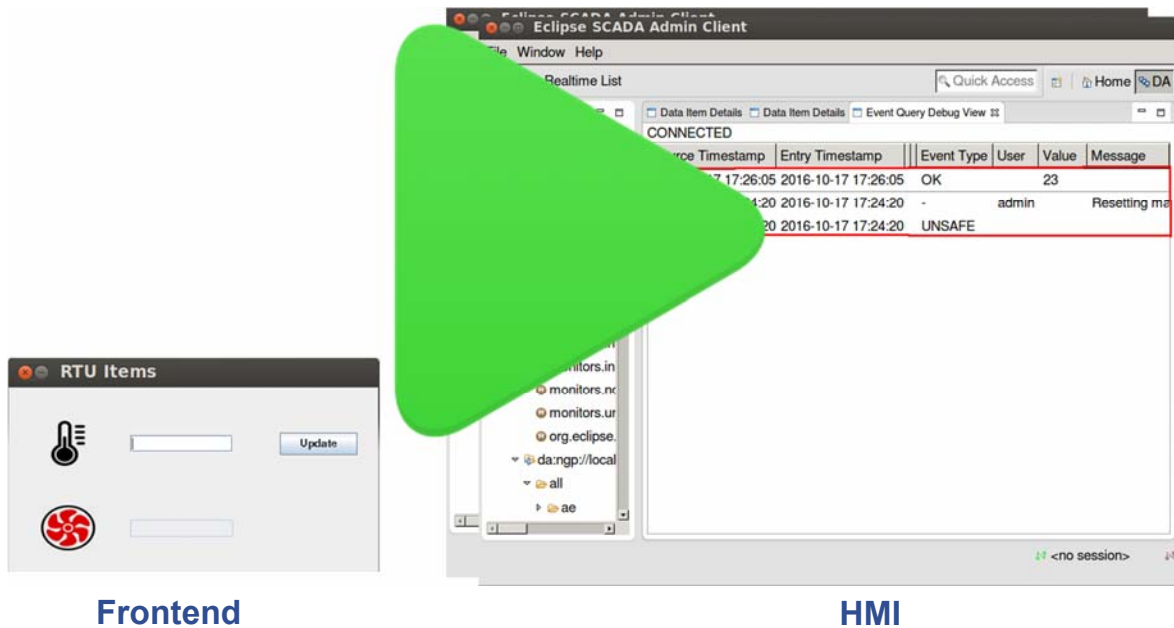
13

## Turbine Item use case



14

## Demo



15

## Demonstration: 4 Steps

1. Interact with RTU items using Eclipse SCADA
2. Impact of an intrusion in the SCADA Master
3. Interact with RTU items using intrusion-tolerant Eclipse SCADA
4. Impact of an intrusion in one SCADA Master replica

19

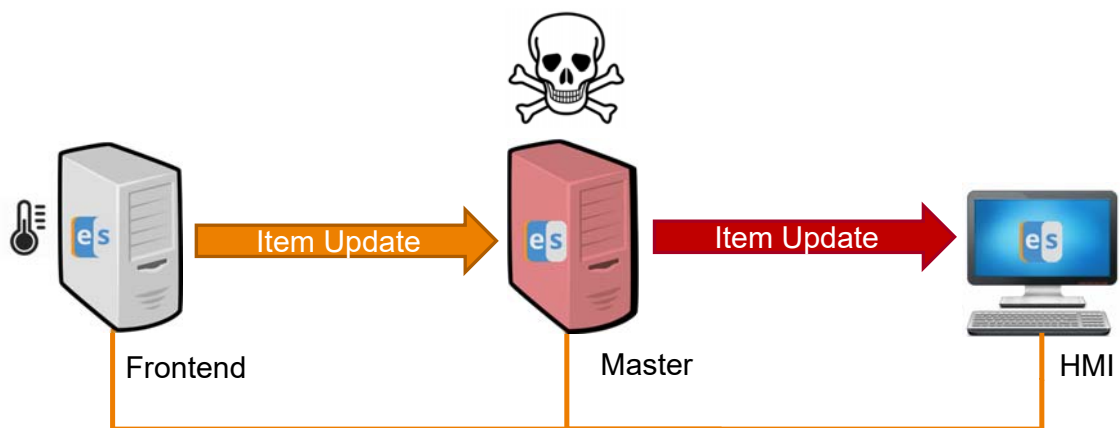


## Attack scenario

- › An attacker gains access to the Master
- › Modify data exchanged between the Frontend and the HMI

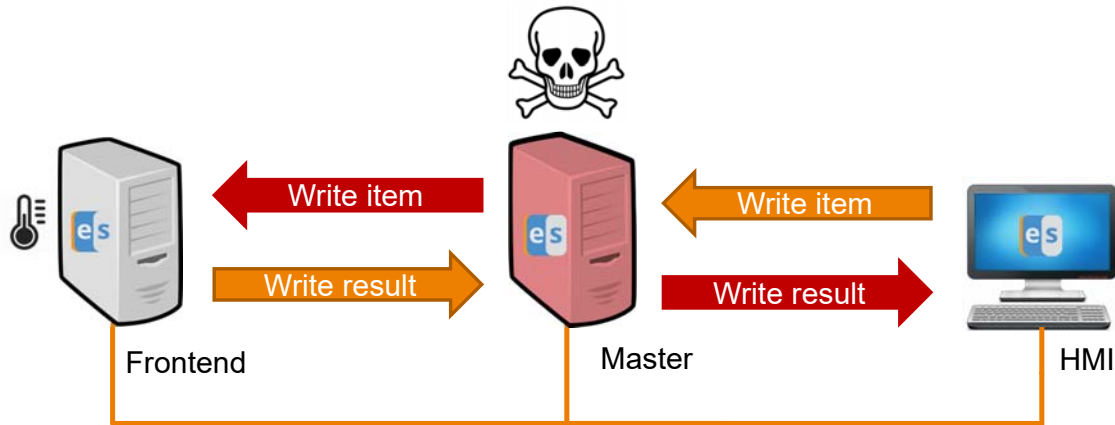
20

## Thermometer Item use case



21

## Turbine Item use case



22

## Demo

The demo shows three windows:

- Attacker:** A window titled "God's view" showing a red circle labeled "Server".
- Frontend:** A window titled "RTU Items" with two input fields and an "Update" button.
- HMI:** A screenshot of the "Eclipse SCADA Admin Client" showing a "Realtime List" table with the following data:

Source Timestamp	Entry Timestamp	Event Type	User	Value	Message
17:26:05	2016-10-17 17:26:05	OK		23	
17:24:20	2016-10-17 17:24:20	-	admin		Resetting ma
17:24:20	2016-10-17 17:24:20	UNSAFE			

23

---

## Demonstration: 4 Steps

1. Interact with RTU items using Eclipse SCADA
2. Impact of an intrusion in the SCADA Master
3. Interact with RTU items using intrusion-tolerant Eclipse SCADA
4. Impact of an intrusion in one SCADA Master replica

26

---

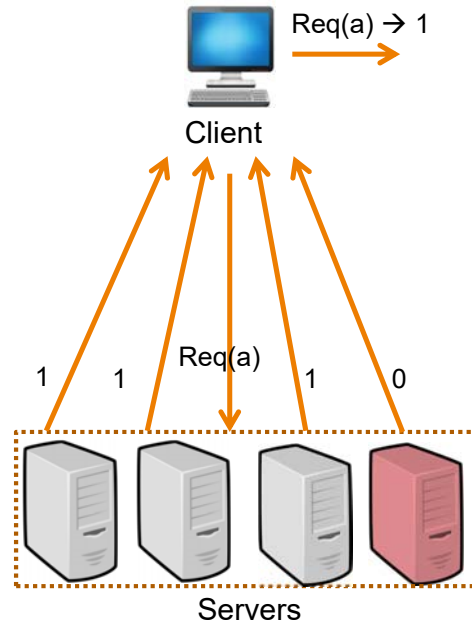
## Prototype

- › Intrusion-tolerant Eclipse SCADA
  - › Modified Eclipse SCADA to support the **replication** of the SCADA Master
  - › Integrated a **Byzantine fault-tolerant state machine replication library** developed in Java, called BFT-SCADA
  - › Explores results from other European projects involved in the development of the BFT-SMART library: Massif, Tclouds, Supercloud

27

## How does BFT-SMART work?

1. Every client request is processed by a group of servers
  2. Servers must execute the same sequence of requests
  3. The client infer the correct result of a request from the majority of the answers
- › Servers coordinate to decide the order of request processing
  - › Servers should run diverse softw/hardw
  - › Weakest possible failure assumption  
 $n = 3f + 1$     ( $f=1, n=4$ )



28

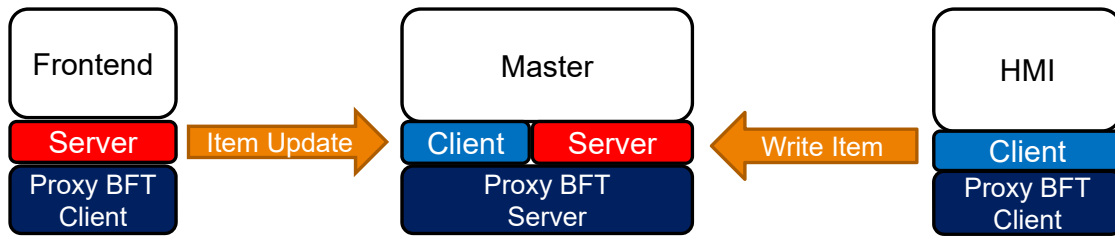
## Eclipse SCADA integration challenges

- › Eclipse SCADA is a framework and not a ready-to-use solution
- › Reasonably large project size
  - more than 500 sub-projects → 6100 Java files (900.000 LOC)
- › Poor software documentation
  - source code
  - use cases examples

29

## Eclipse SCADA integration challenges (cont)

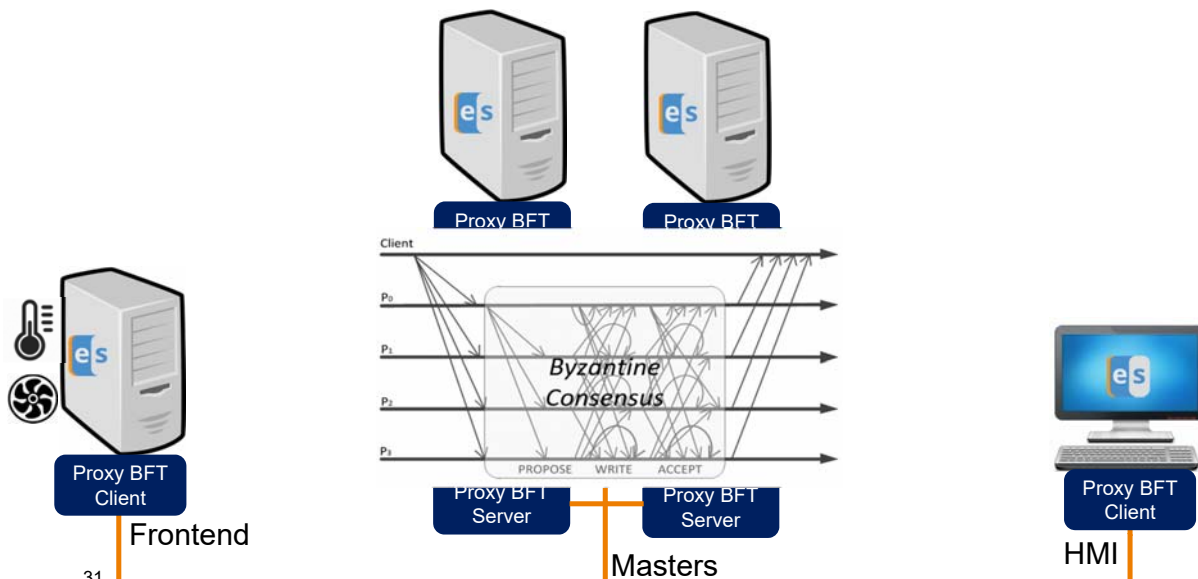
### › Multiple I/O channels



- › Concurrency through multiple threads
- › Asynchronous messages
- › Non-deterministic actions (e.g., get timestamps)
- › Performance

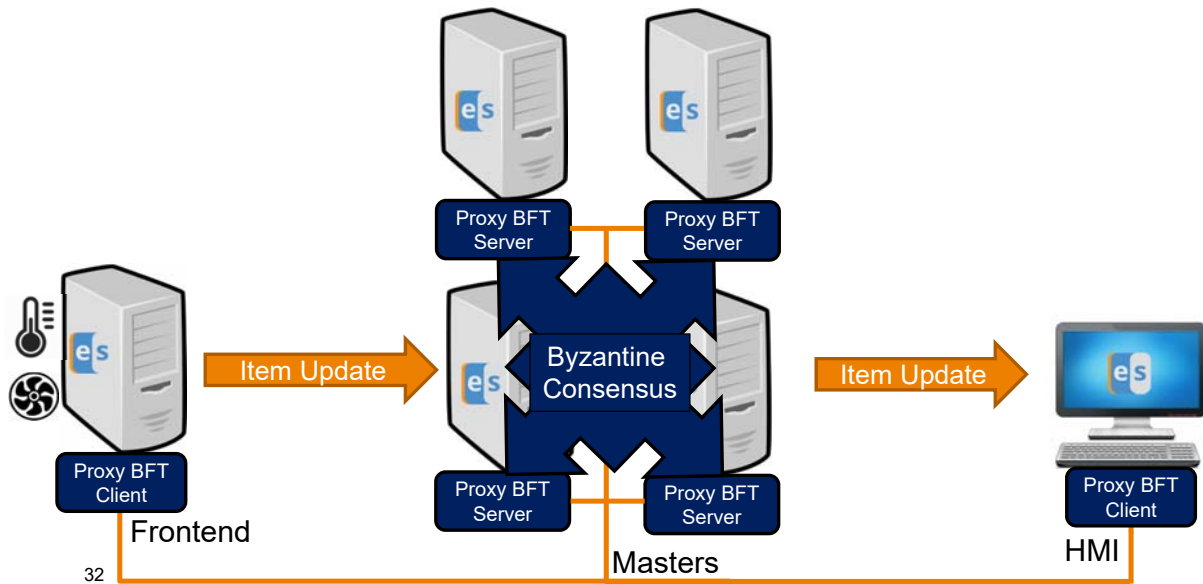
30

## Intrusion tolerant operation

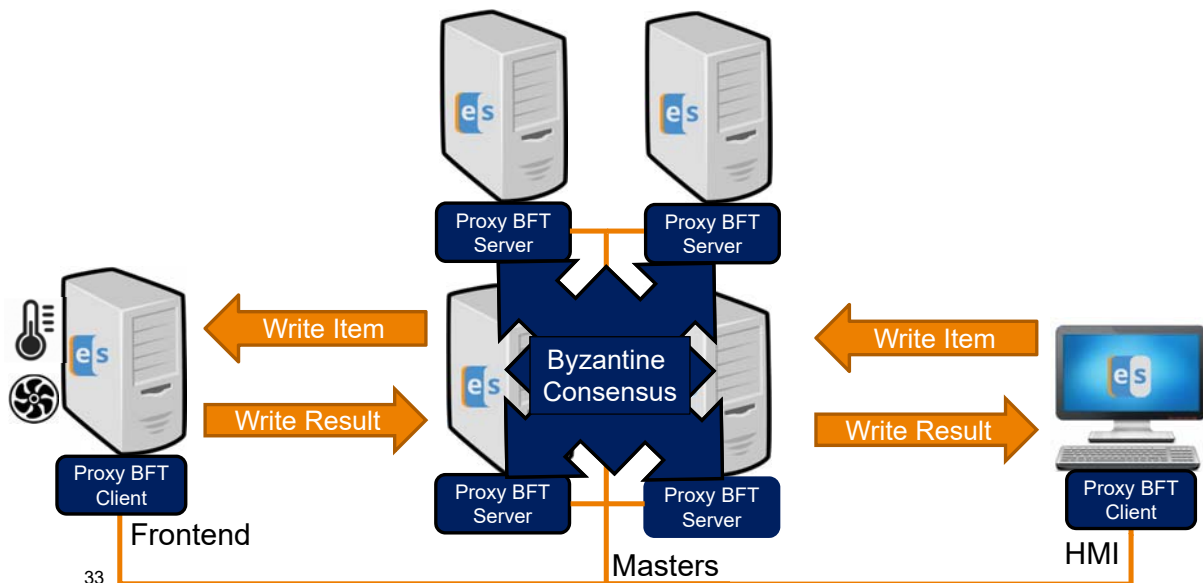


31

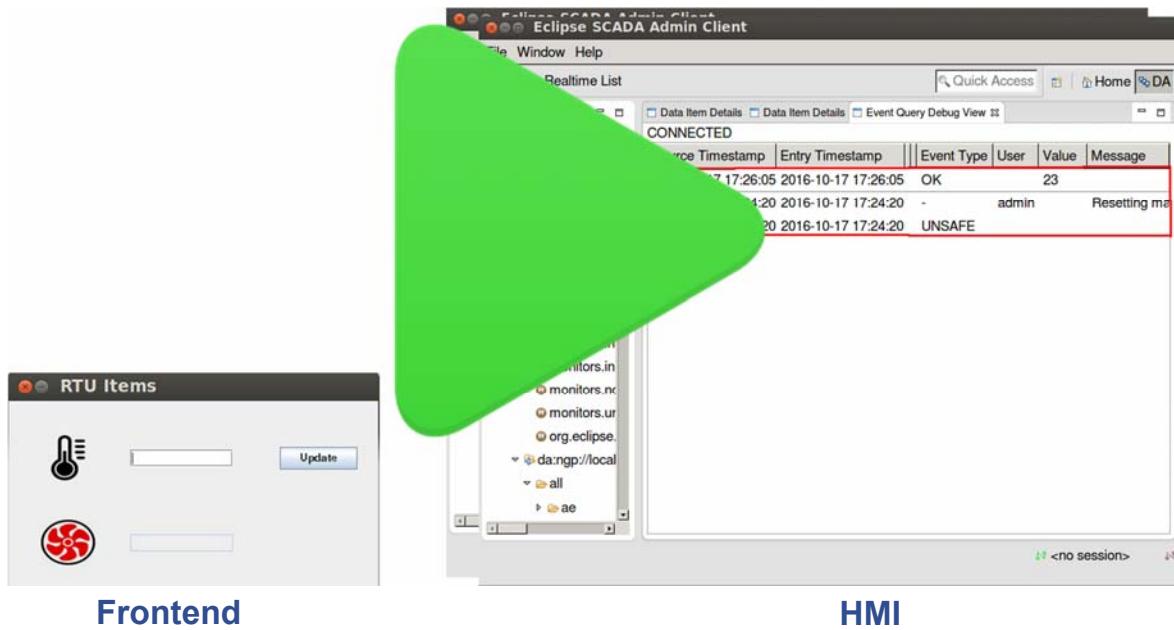
## Thermometer Item use case



## Turbine Item use case



## Demo



34

## The Demonstration: 4 Steps

1. Interact with RTU items using Eclipse SCADA
2. Impact of an intrusion in the SCADA Master
3. Interact with RTU items using intrusion-tolerant Eclipse SCADA
4. Impact of an intrusion in a SCADA Master replica

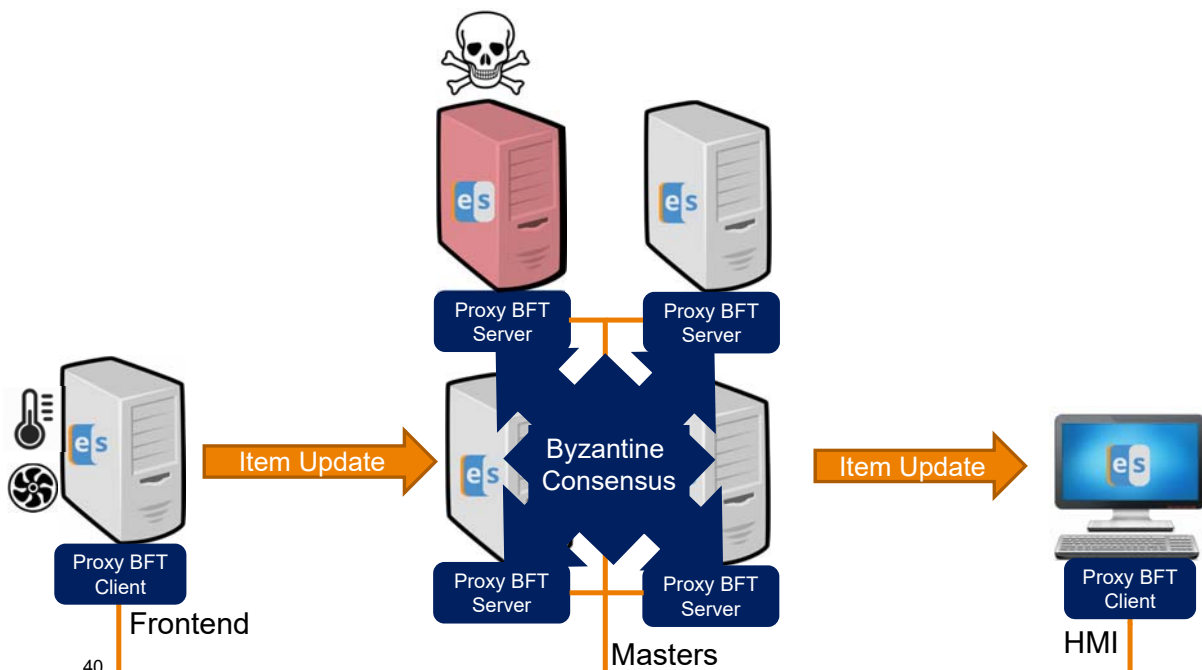
38

## Attack scenario

- › An attacker gains access to one of the Master replicas
- › Modifies data exchanged between the Frontend and the HMI

39

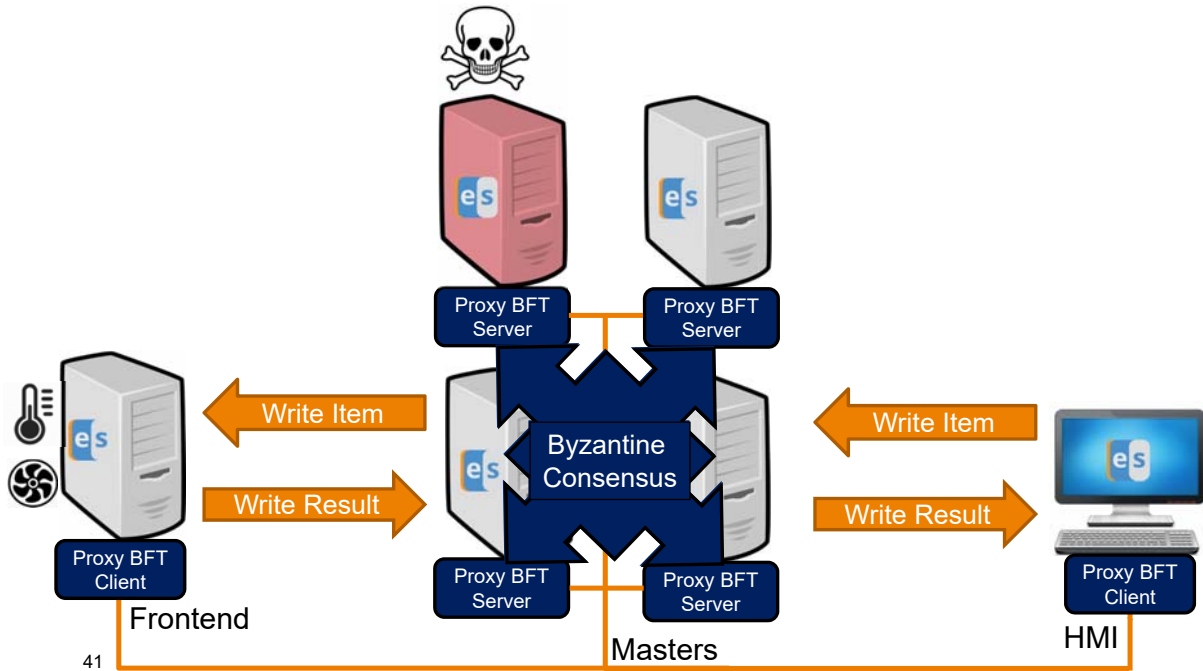
## Thermometer Item use case



40



# Turbine Item use case



41

# Demo

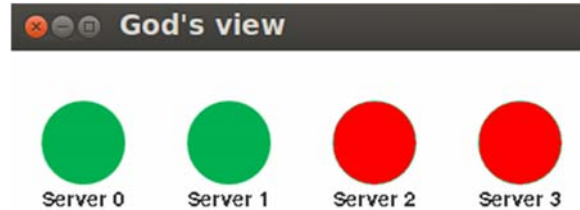
The screenshot shows the Eclipse SCADA Admin Client interface. A large green play button is overlaid on the interface, indicating a demo. The interface includes a 'God's view' window with four server status indicators (Server 0, Server 1, Server 2, Server 3). A table titled 'Realtime List' displays event data. Below the table, there are 'RTU Items' and 'Attacker' labels. The 'Attacker' label is positioned above the 'RTU Items' window.

Event Timestamp	Entry Timestamp	Event Type	User	Value	Message
2016-10-17 17:26:05	2016-10-17 17:26:05	OK		23	
2016-10-17 17:24:20	2016-10-17 17:24:20		admin		Resetting ma
2016-10-17 17:24:20	2016-10-17 17:24:20	UNSAFE			

42

## Byzantine fault-tolerant limitations

› What happens when more than  $f$  replicas are compromised?



- If 2 replicas are compromised, the system stops making progress, but does not do mistakes
- If 3 replicas are compromised, then a clever attacker can make the system take incorrect actions

45

SEGRID

**Thank you!** Any questions?

This was:  
**Intrusion-Tolerant SCADA**

Web: <http://segrid.eu>

<http://www.navigators.di.fc.ul.pt>