Security for smart Electricity GRIDs

Intrusion Tolerant SCADA

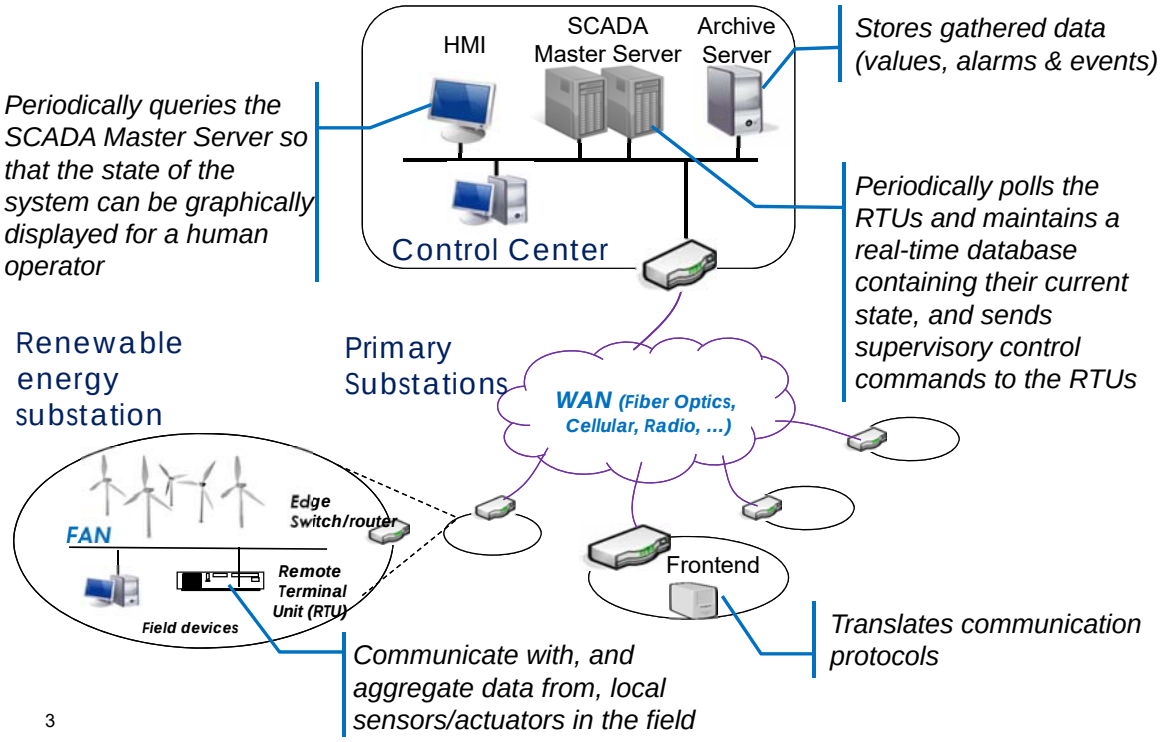
André Nogueira, *Alysson Bessani*, ***Nuno Neves***
Faculty of Sciences of the Univ. of Lisboa (FFCUL)

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

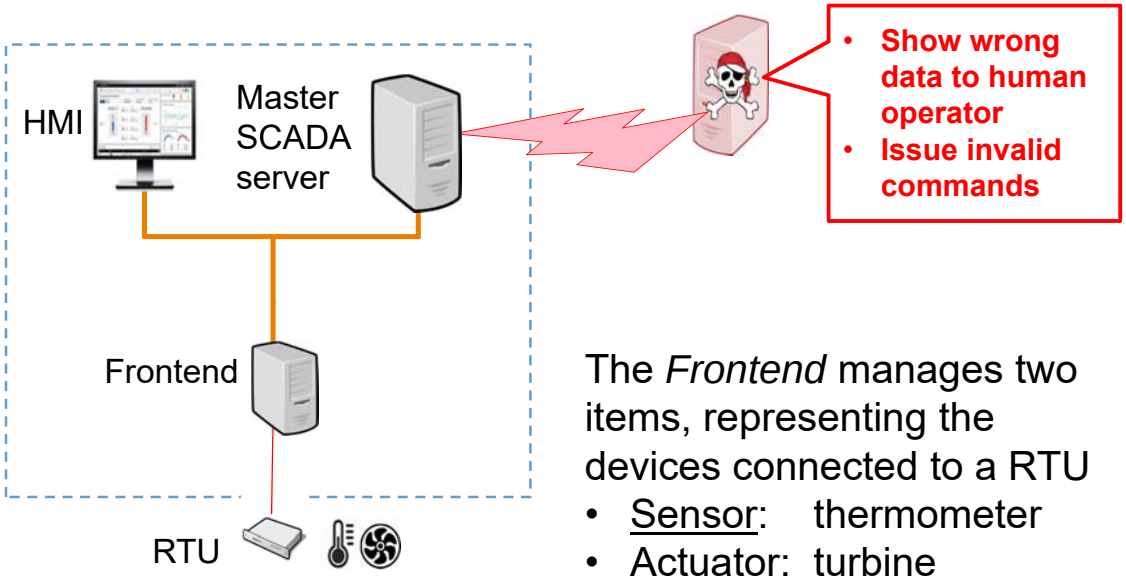
Goal: Demonstrate a SCADA system capable of tolerating intrusions

- 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



Demo scenario



The *Frontend* manages two items, representing the devices connected to a RTU

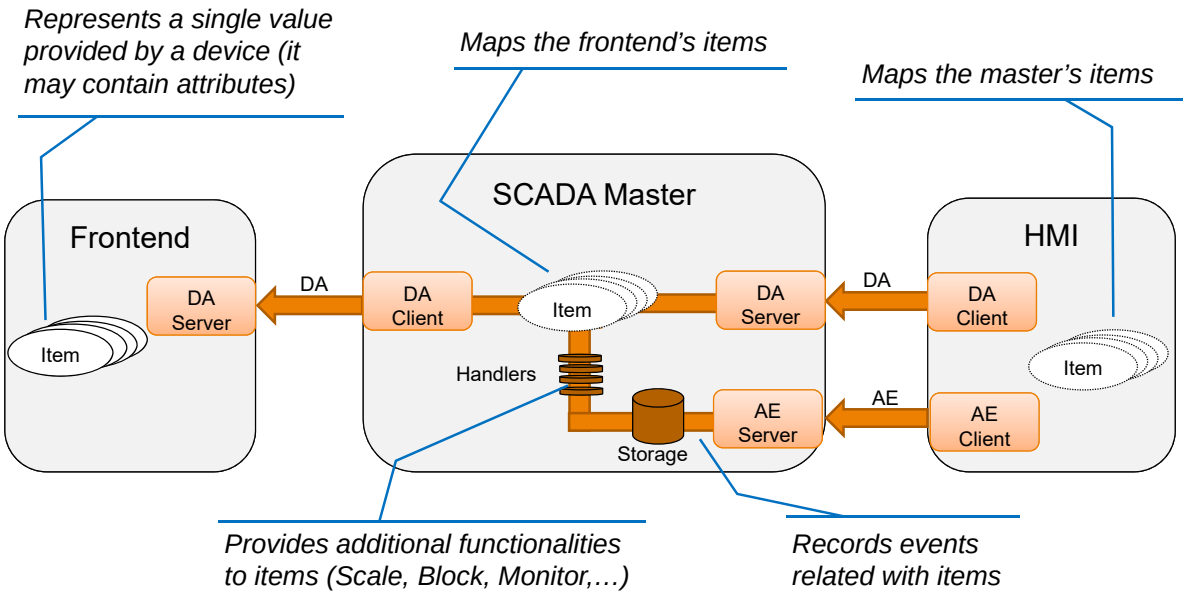
- Sensor: thermometer
- Actuator: turbine

The prototype and experimental environment

Prototype

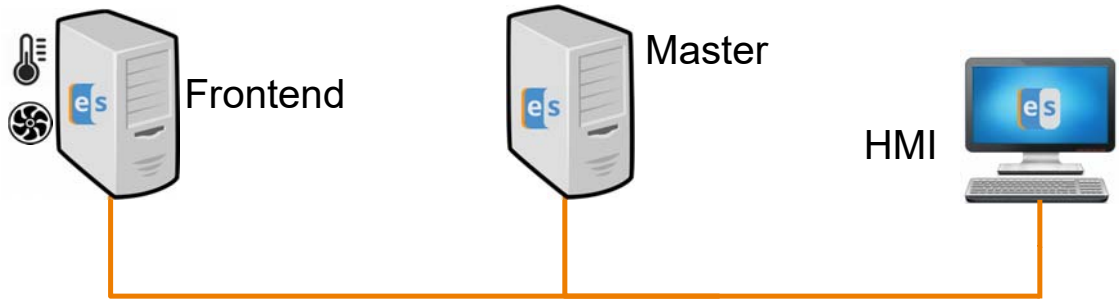
- System based on the **Eclipse SCADA** open source project
- Eclipse SCADA provides a modular “construction kit” to create a custom SCADA
- IBH SYSTEMS GmbH is the leading contributor
- In production for instance at:
  - E.ON solar plants
  - OMV business processes

EclipseSCADA: Components



Experimental Environment

- Eclipse SCADA & Emulated RTU Items



Demonstration

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

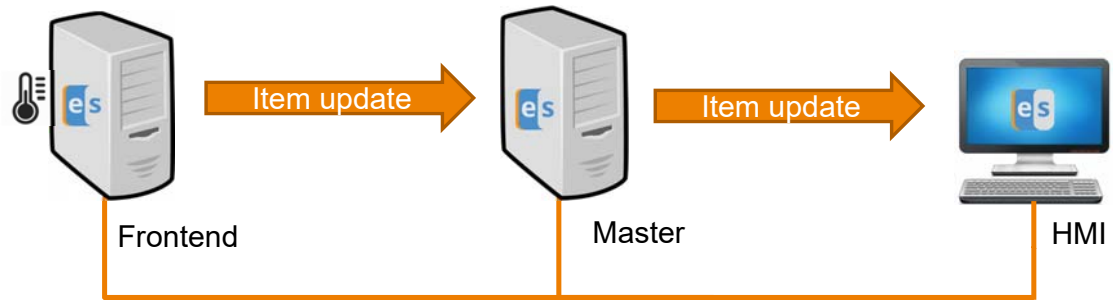
Demonstration: 4 Steps

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

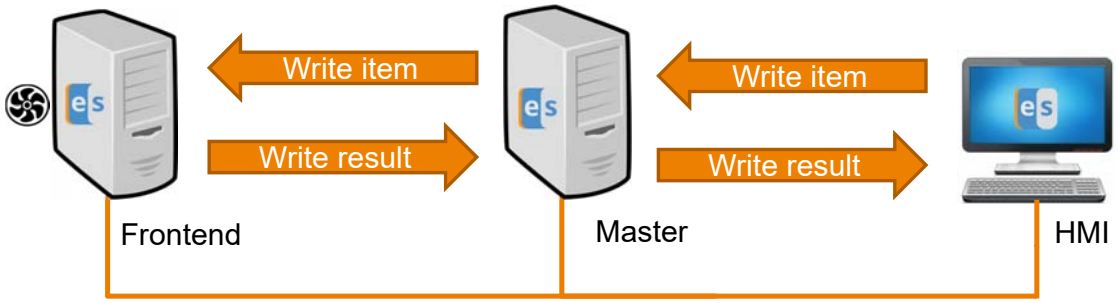
Use cases

- 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

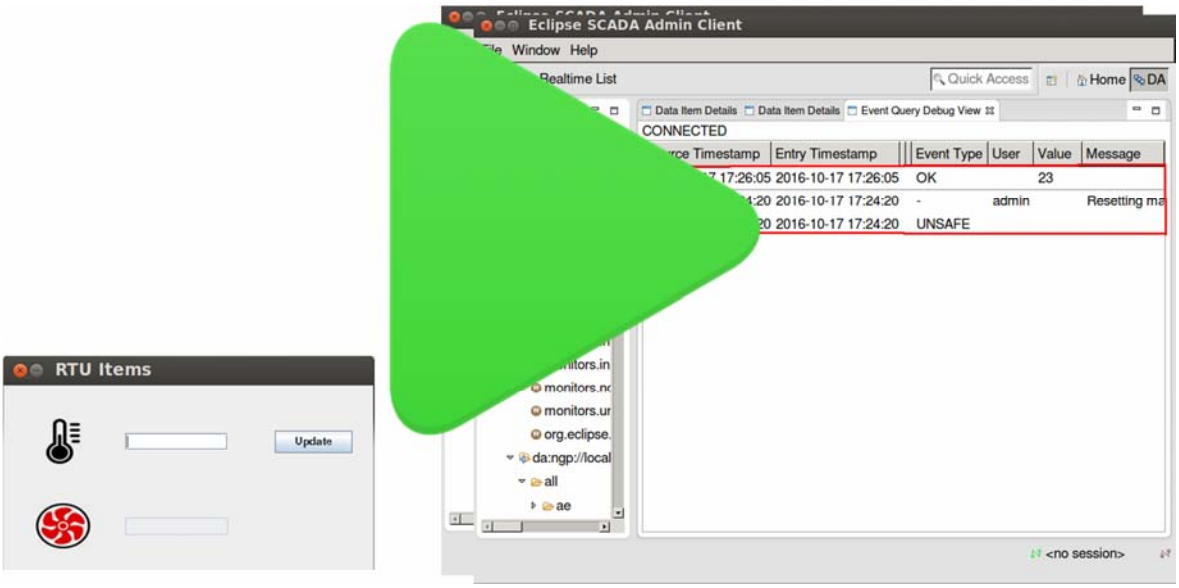
Thermometer Item use case



Turbine Item use case



Demo



Frontend **HMI**

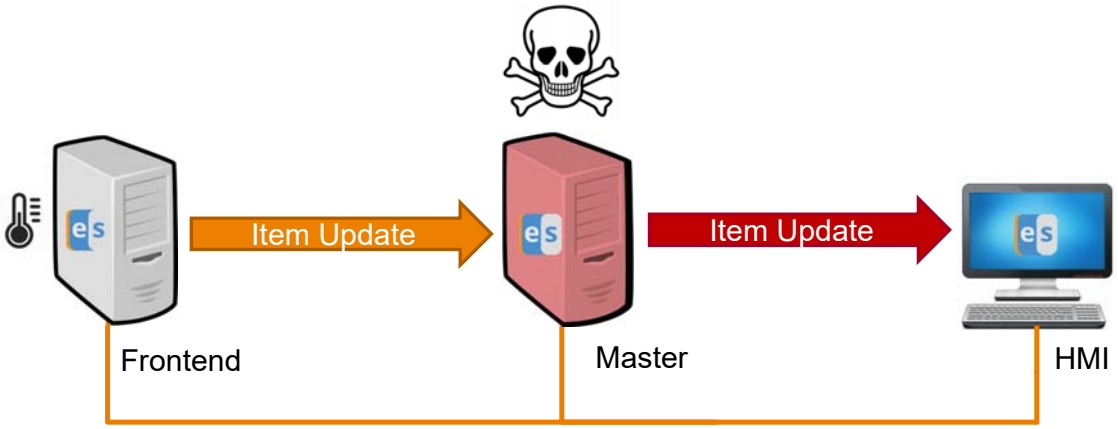
Demonstration: 4 Steps

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

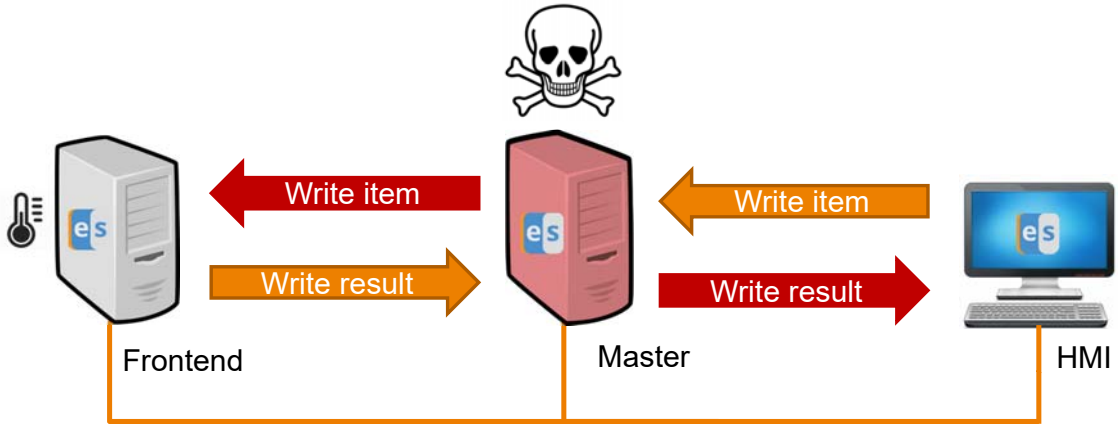
Attack scenario

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

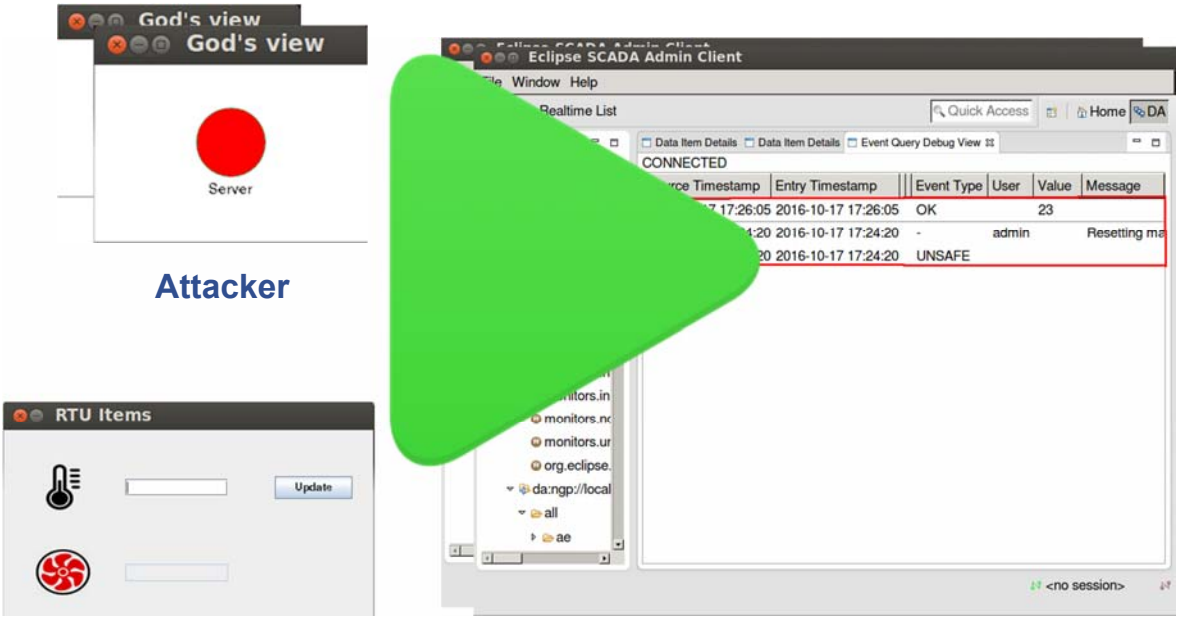
Thermometer Item use case



Turbine Item use case



Demo



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

Prototype

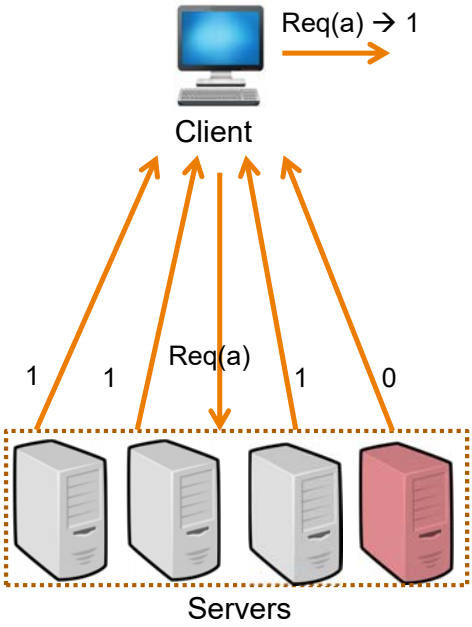
- Intrusion-tolerant Eclipse SCADA
  - Modified Eclipse SCADA to support the **replication** of the SCADA Master
  - Integrated a **Byzantine fault-tolerant state machine replication library** developed in Java, called BFT-SCADA
  - Explores results from other European projects involved in the development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

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)

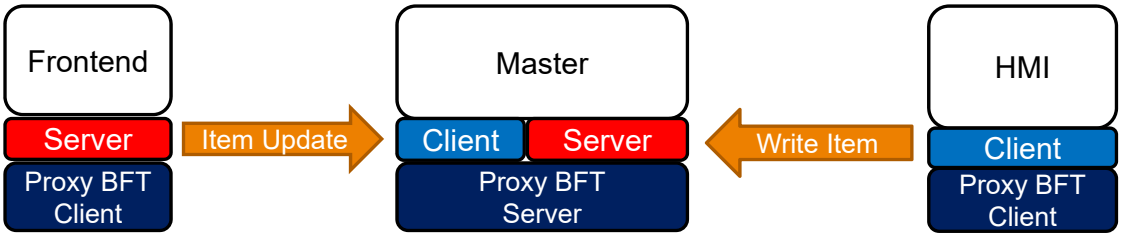


Eclipse SCADA integration challenges

- 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

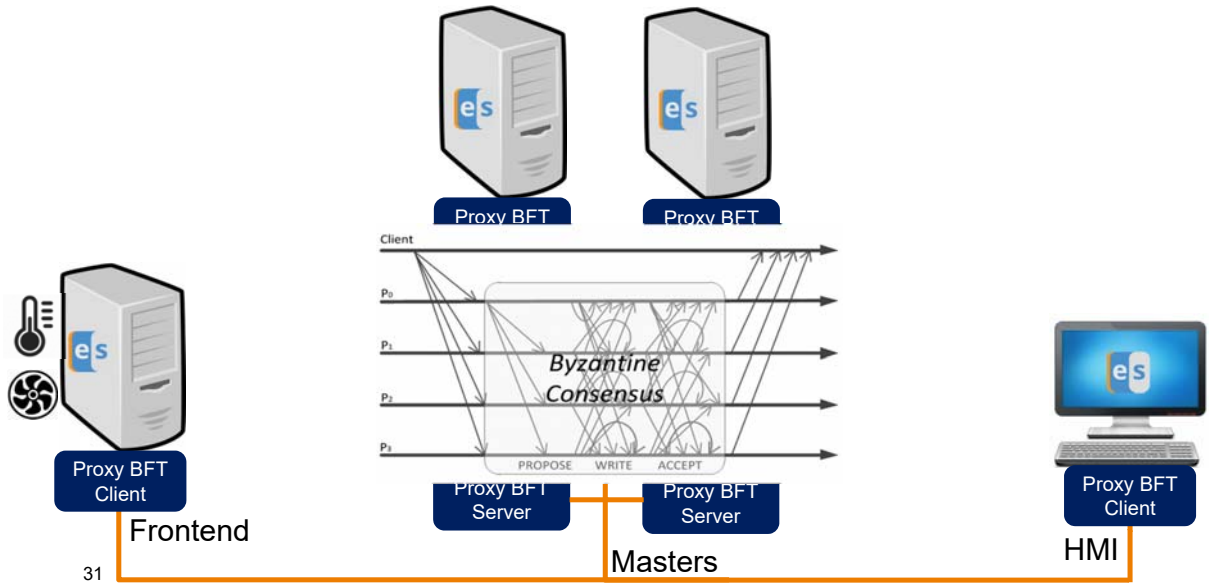
Eclipse SCADA integration challenges (cont)

- Multiple I/O channels

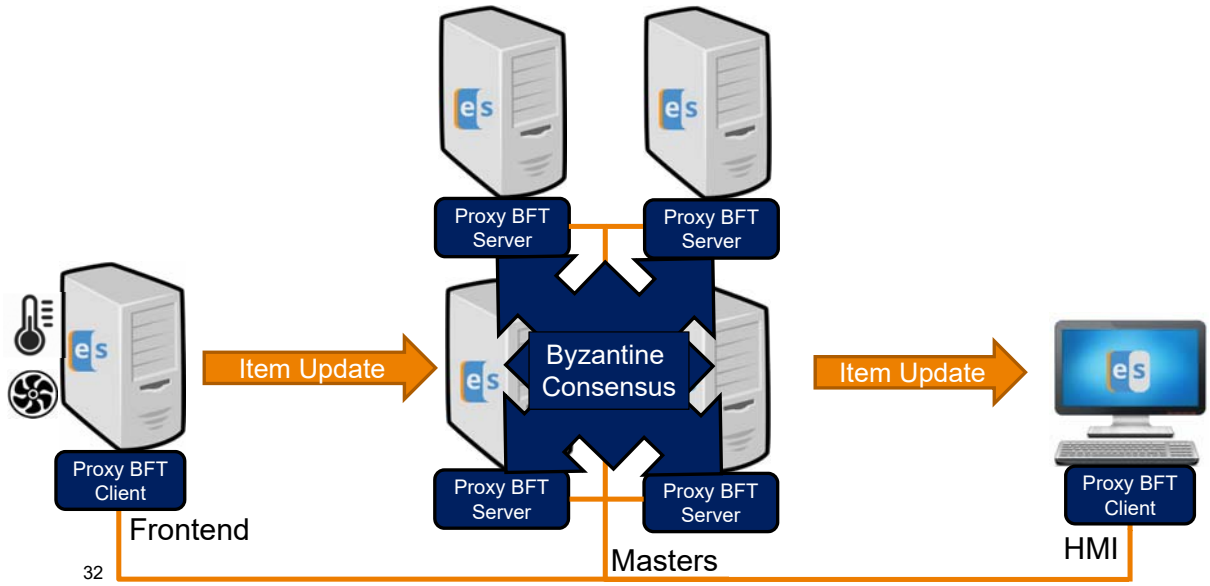


- Concurrency through multiple threads
- Asynchronous messages
- Non-deterministic actions (e.g., get timestamps)
- Performance

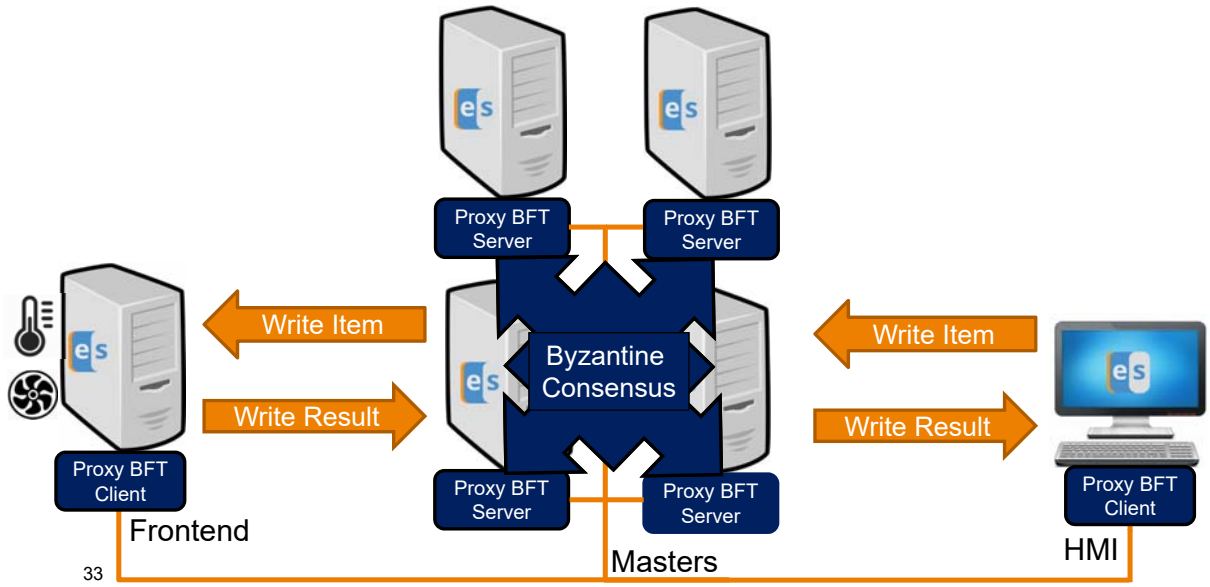
Intrusion tolerant operation



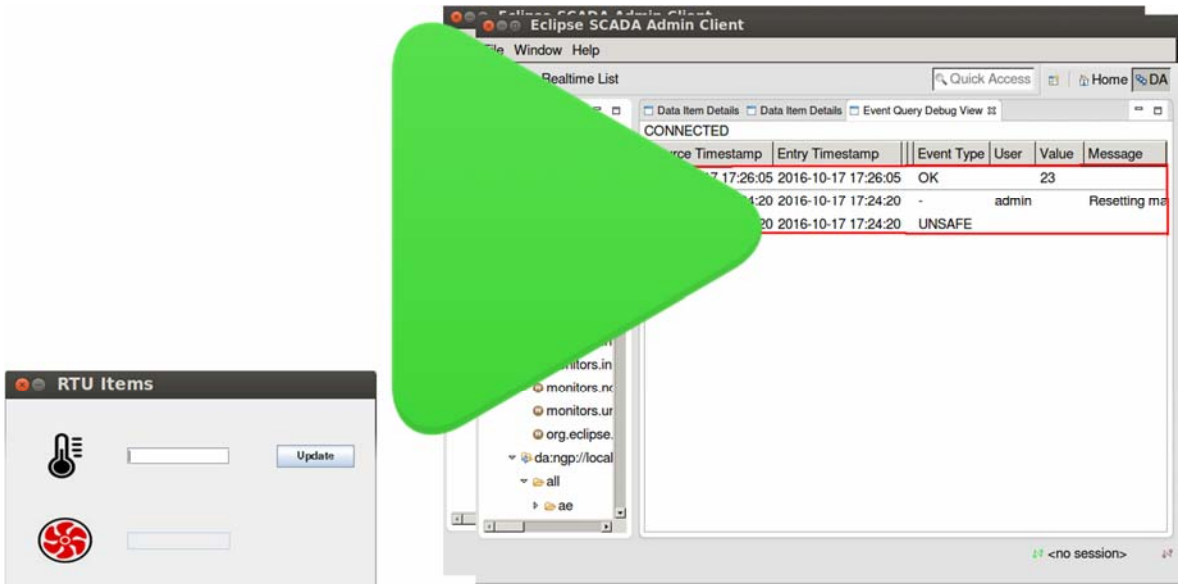
Thermometer Item use case



Turbine Item use case



Demo



Frontend **HMI**

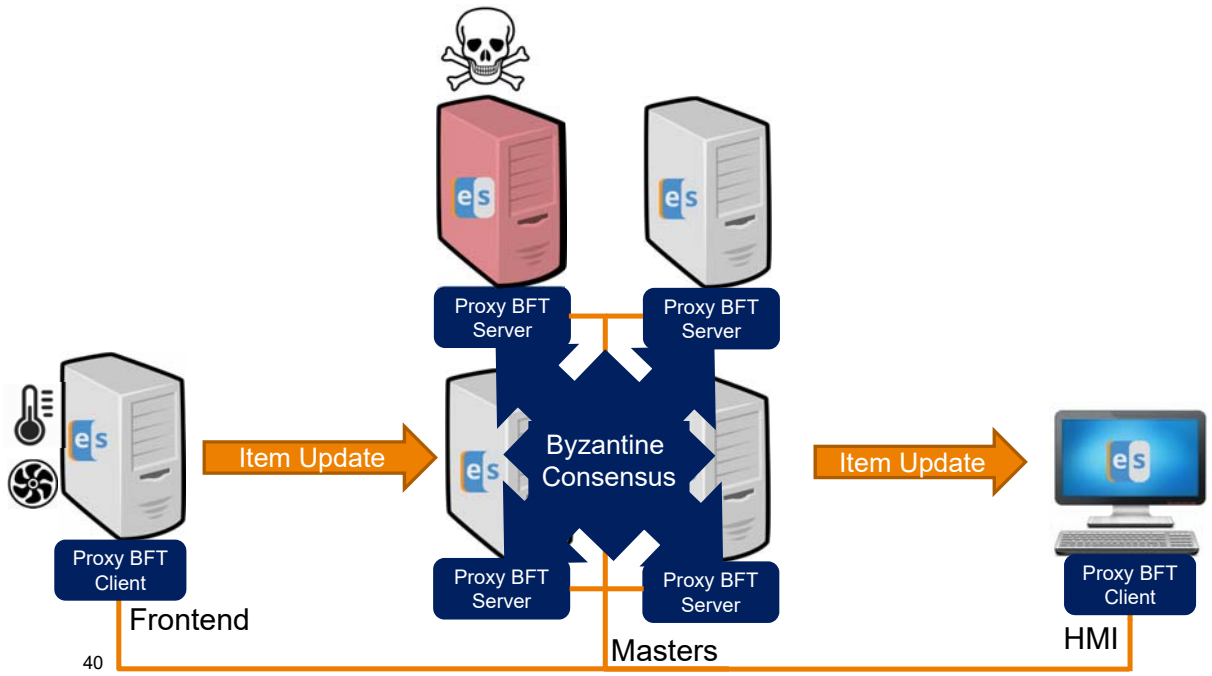
The Demonstration: 4 Steps

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

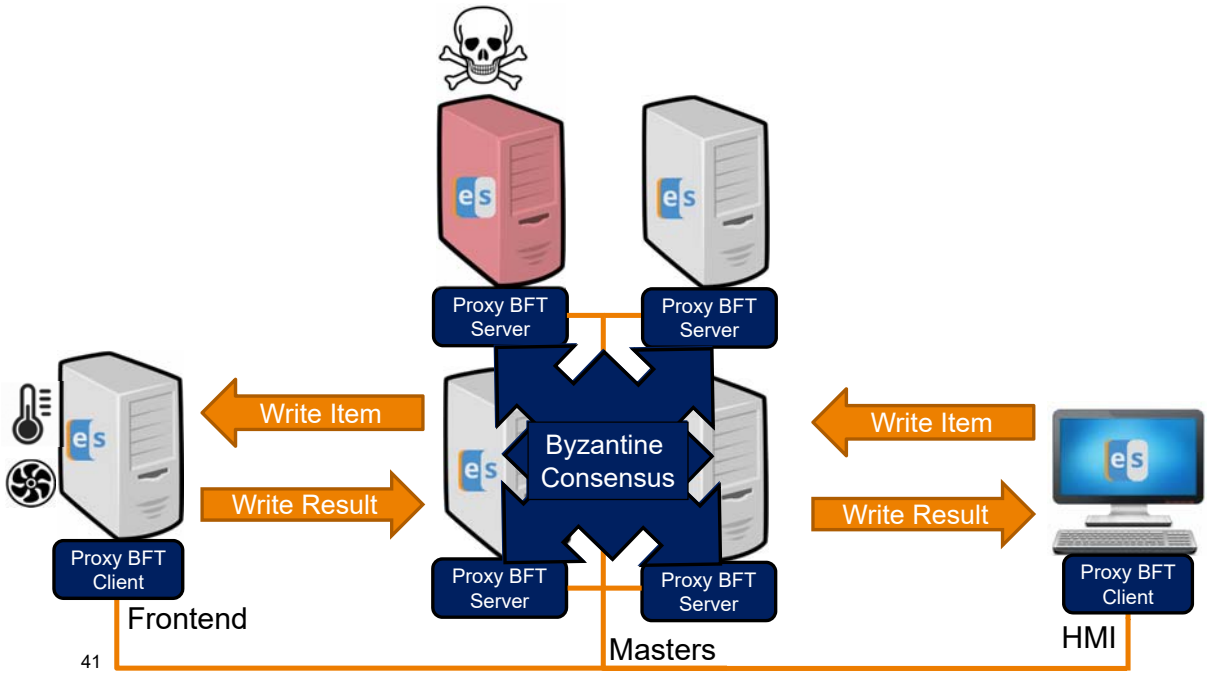
Attack scenario

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

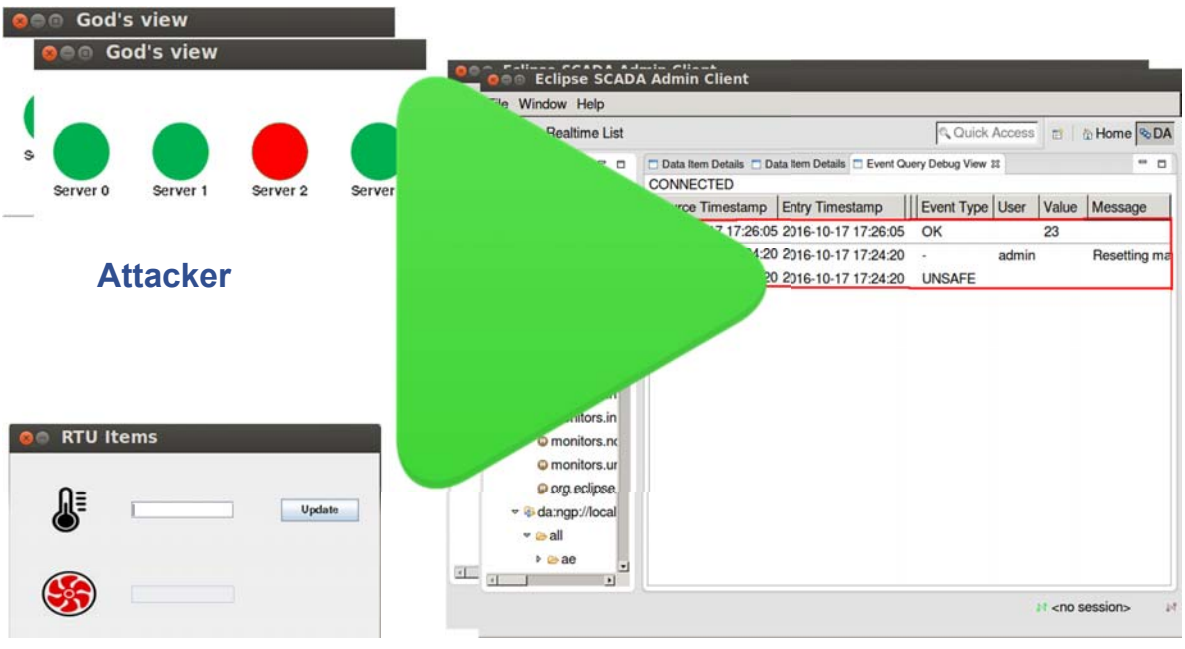
Thermometer Item use case



Turbine Item use case

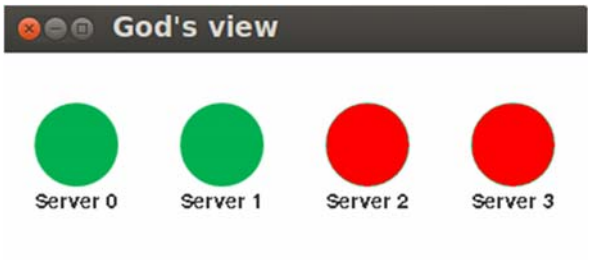


Demo



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

Thank you! Any questions?

This was:

Intrusion-Tolerant SCADA

Web: http://segrid.eu

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