Toward Open Source Intrusion Tolerant SCADA

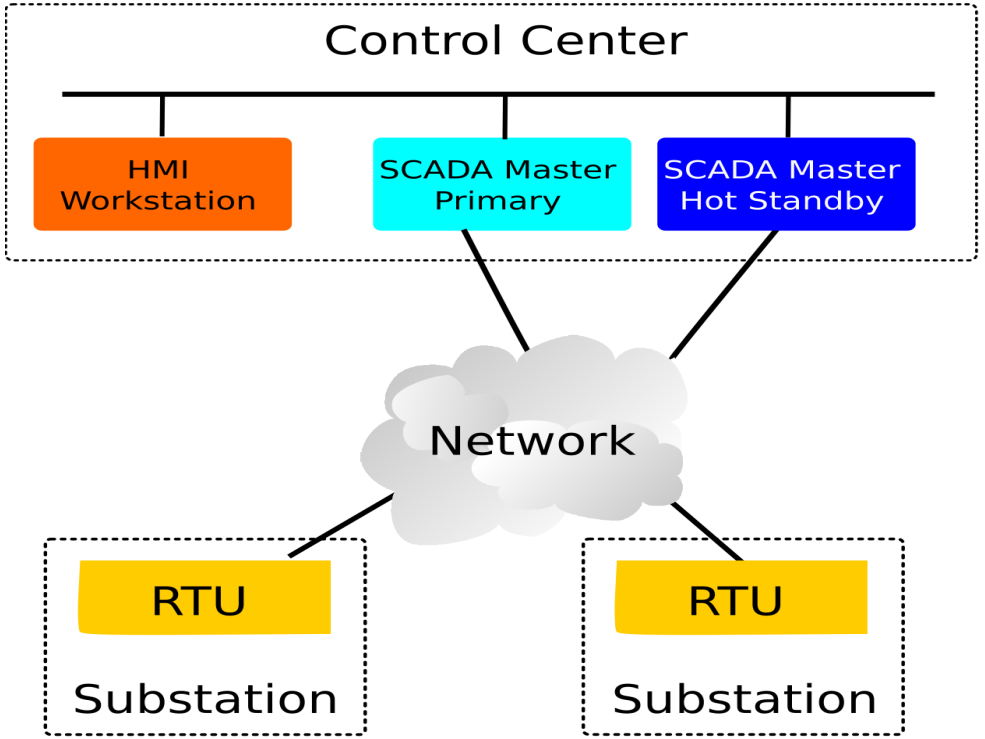
Trevor Aron
JR Charles
Akshay Srivatsan
Mentor: Marco Platania

Outline

- What is SCADA?
- SCADA Vulnerabilities
- What is Intrusion Tolerance?
- Prime
- PvBrowser
- Our Architecture
- Demo
- Future Directions

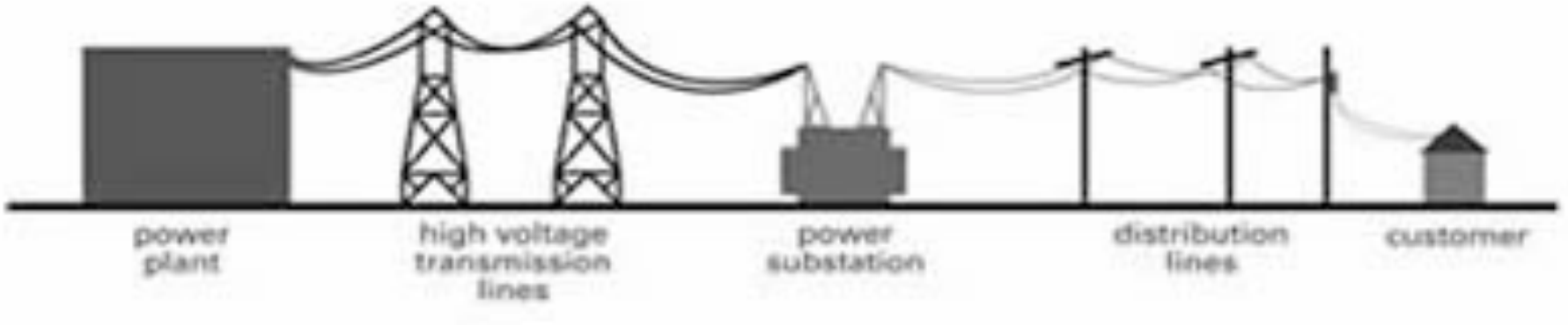
What is SCADA?

- **S**upervisory **C**ontrol and **D**ata **A**cquisition
- Used to supervise and control national infrastructure
- Main components:
  - Master
  - HMI
  - PLCs/RTUs
- Designed to work with propriety hardware and protocols
- Components are connected on private, isolated network



SCADA in Power Grids (1)

- Power grids include generation plants and transmission/distribution substations which are spread across wide areas
  - **Electrical Generation Plant**: generates electrical power to be transmitted across the grid
  - **Transmission Substation**: transforms power for long distance transmission and provides switching between sources/destinations to meet the needs of the grid
  - **Distribution Substation**: receives power from a transmission substation(s) to be distributed on site



SCADA in Power Grids (2)

- SCADA system is used to monitor power substations
- RTUs read data from field devices
  - Transformers
  - Generators
  - Switches
  - …
- Data is processed by the SCADA master and presented to the user through the HMI
- If the values read from RTUs exceed predefined safety threshold, alarms are raised by the master

SCADA Systems moving to the Internet

- Traditional Security Model
  - Perimeter based
  - Security through obscurity
  - Primary/Standby Architecture
- SCADA systems originally designed to run on private networks and are not optimized for security
- In the past decade, SCADA systems witnessed many changes
  - Use of off-the-shelf hardware
  - Standardized protocols
  - Open networks (e.g. Internet)

SCADA vulnerabilities

- Attacks exploiting software vulnerabilities
  - Stuxnet
  - Project SHINE
  - Attacks involving foreign governments

- Current solutions are ineffective against malicious intrusions

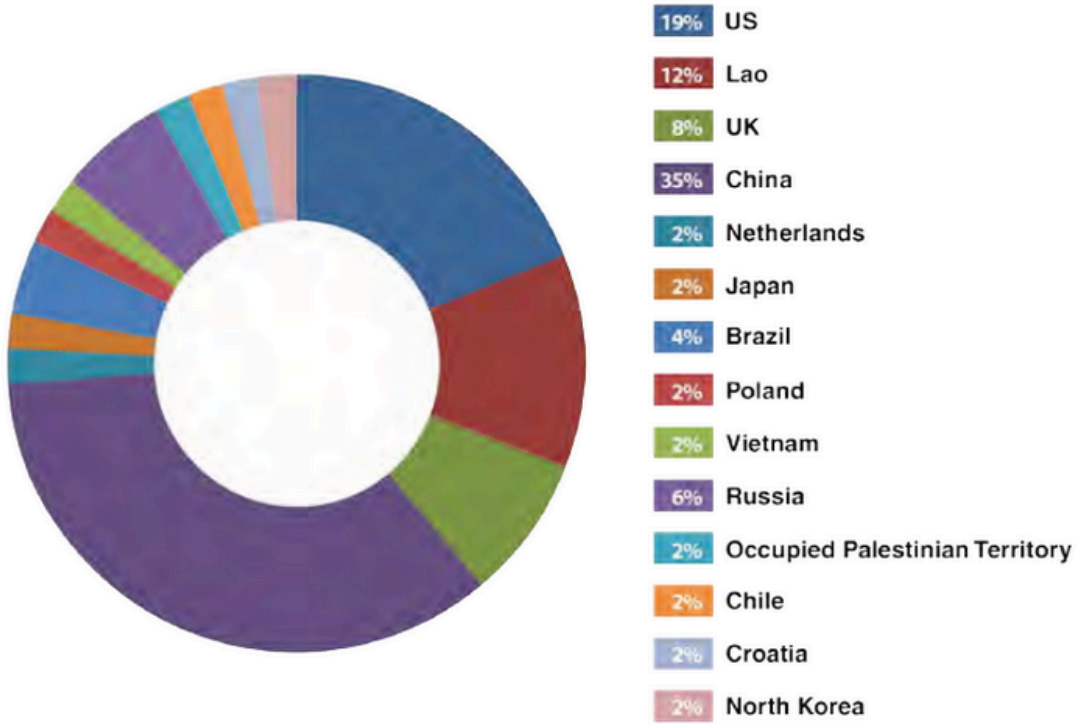
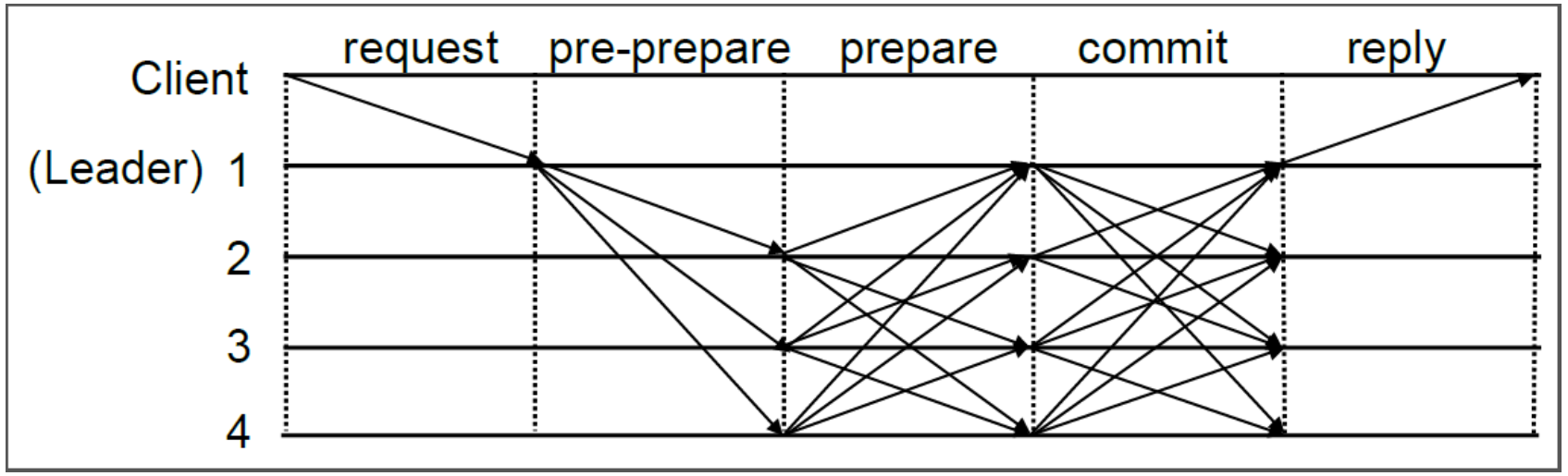


FIGURE 10: Country breakdown indicating the number of attack attempts

Source: Trend Micro Incorporated
Who's Really Attacking Your ICS Equipment?

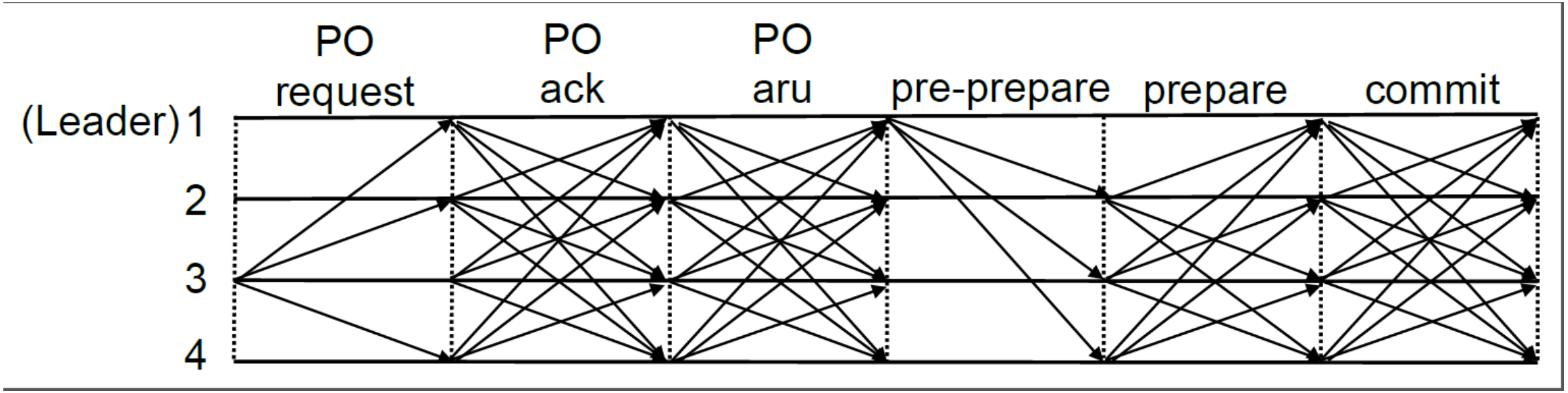
What is Intrusion Tolerance?

- **Intrusion Tolerance**: Executing correct operations even if a part of the system is controlled by an adversary
  - Safety: all correct replicas maintain consistent state
  - Liveness: eventual progress
- There are many algorithms in literature that provide byzantine fault tolerant replication, until less than one third of the system is compromised
  - BFT
  - Zyzzyva
  - Prime
  - Aardvark
  - …



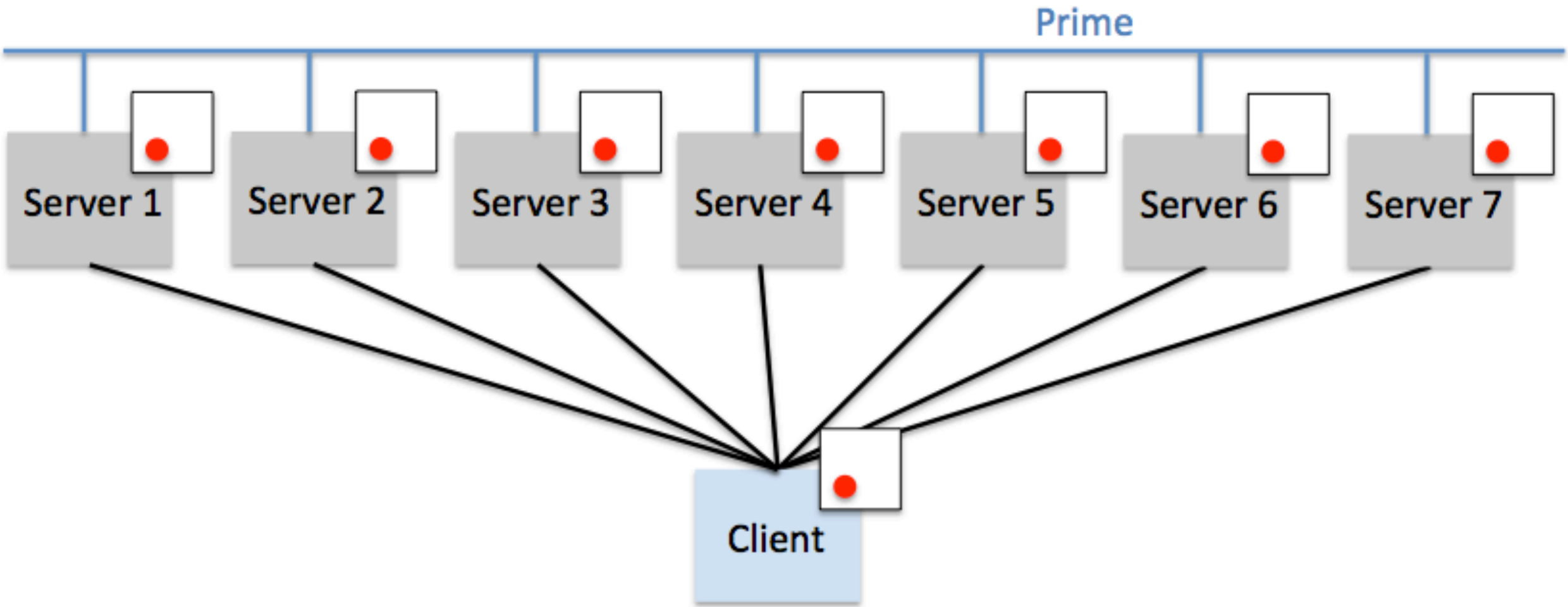
Prime: Byzantine Replication with Performance Guarantees Under Attack

- First BFT protocols to provide performance guarantees while under attack
- Limits the power of a malicious leader to achieve bounded delay performance guarantee



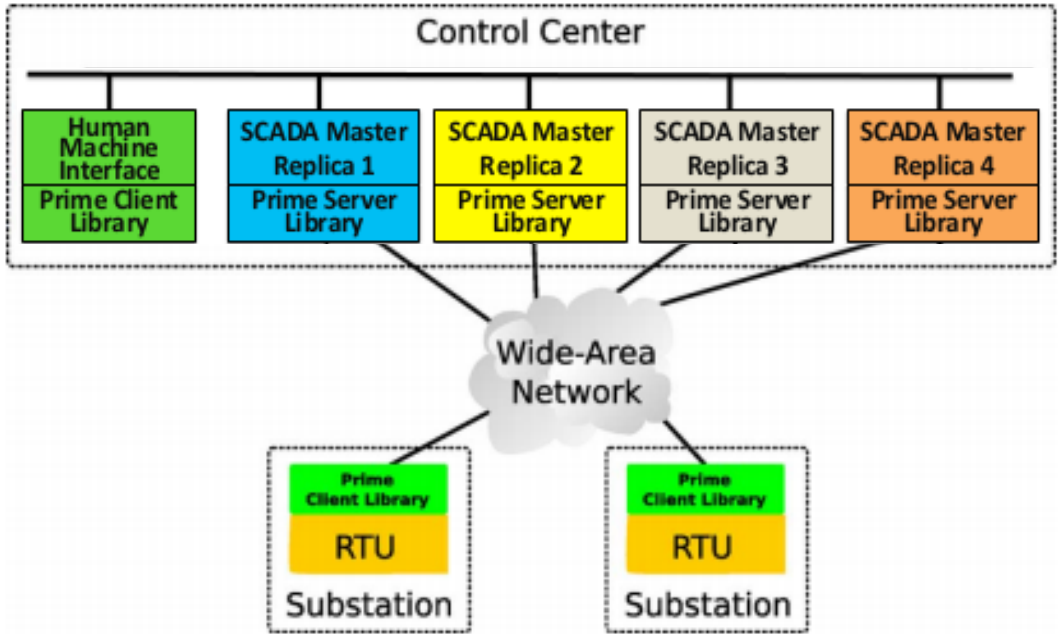
Defense across space and time

- Prime and BFT protocols in general are fragile over long system life time
- Solution
  - Defense Across Space: diversify the execution environment to generate different versions of the same application
  - Defense Across Time: periodic and proactive replica rejuvenation to clean undetected intrusions
  - Diversity + Proactive recovery allow for long lived intrusion tolerant systems


Prime
Server 1
Server 2
Server 3
Server 4
Server 5
Server 6
Server 7
Client

Intrusion tolerant SCADA

- Use Prime to replicate SCADA masters
- SCADA master works correctly if no more then *f* replicas out of *3f+1* replicas have been intruded
- Diversity and proactive recovery allow for the system to function for a long time
- An earlier version of Prime was integrated by Siemens into their SCADA product for the power grid, but it does not include diversity and proactive recovery (no protection across space and time)



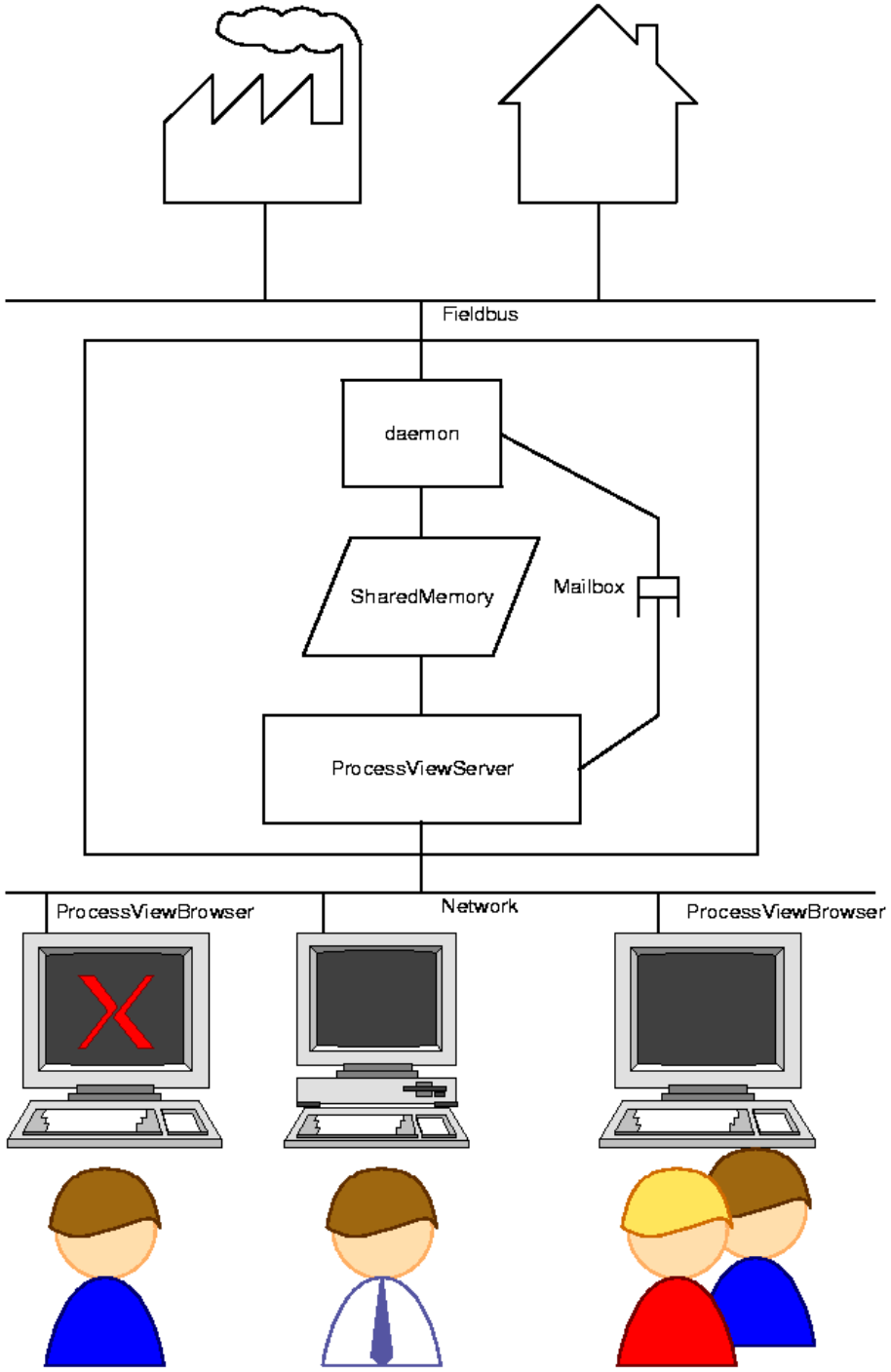
Our Goals

- To develop a proof-of-concept of an open source intrusion tolerant SCADA

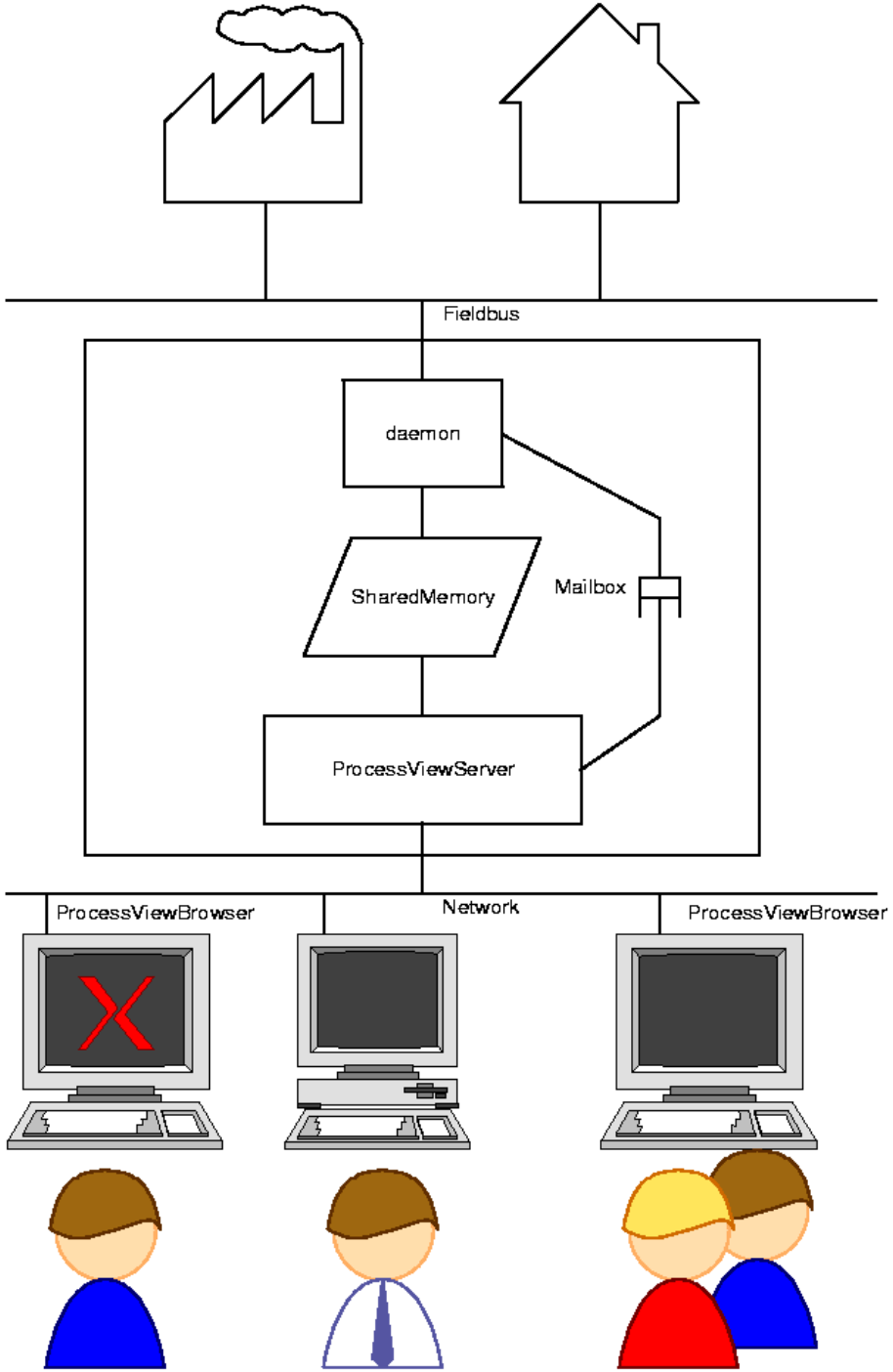
- Components:
  - **PvBrowser**: Open source SCADA software
  - **Prime**: Intrusion tolerant replication with performance guarantees under attack
  - **RTU emulator**: simulates data generation from field devices

PvBrowser

- Open source SCADA Master and HMI server
- Architecture
  - Master
    - **Data acquisition daemon** (DAD): communicates with RTUs/PLCs
    - **Shared memory**: medium for communication between DAD and Pvserver
    - **ProcessViewServer**: visualizes data from DAD and communicates with HMI
  - HMI
    - **ProcessViewBrowser**: presents information from the visualizer to user

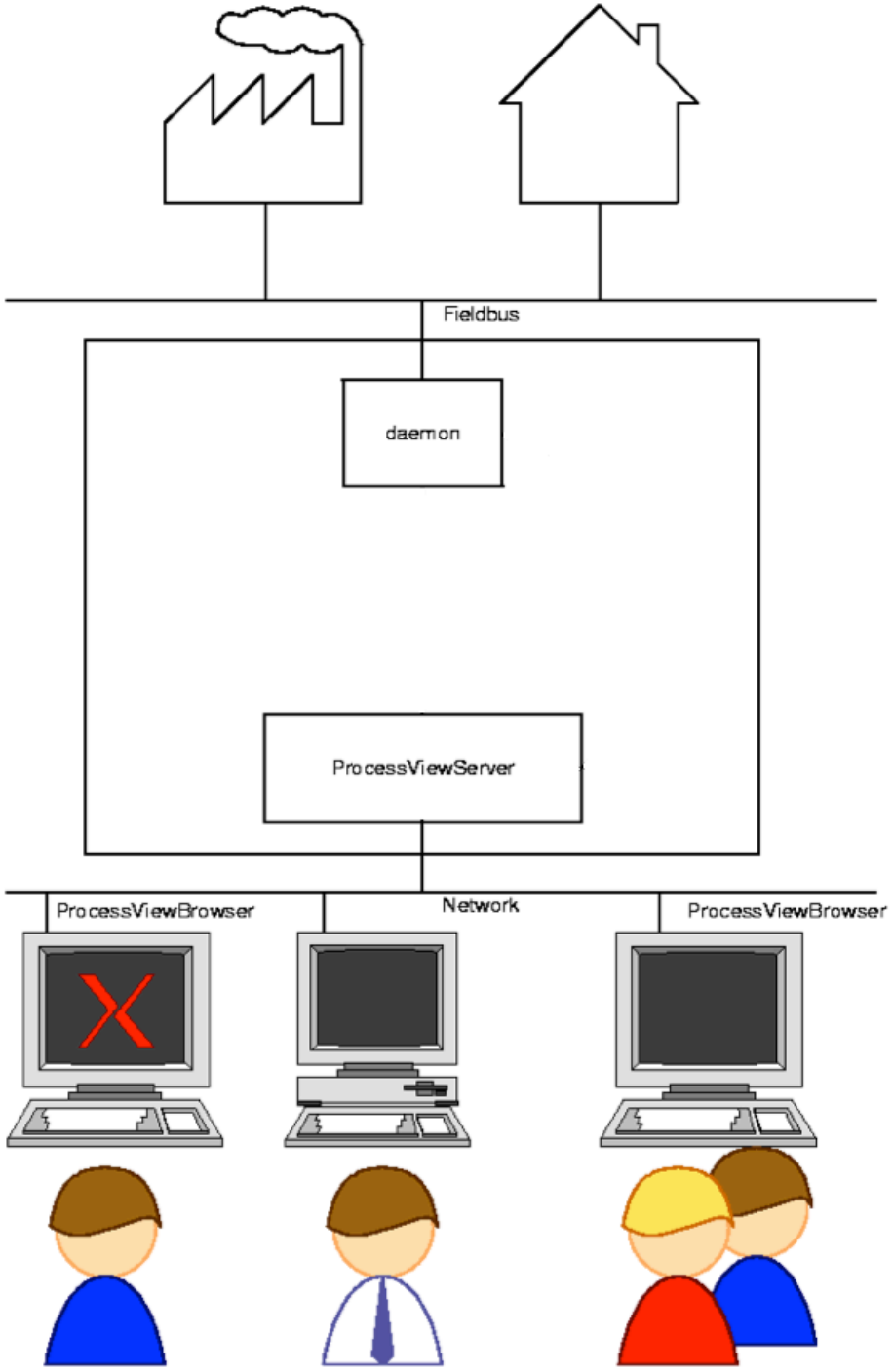


PvBrowser (Modifications)



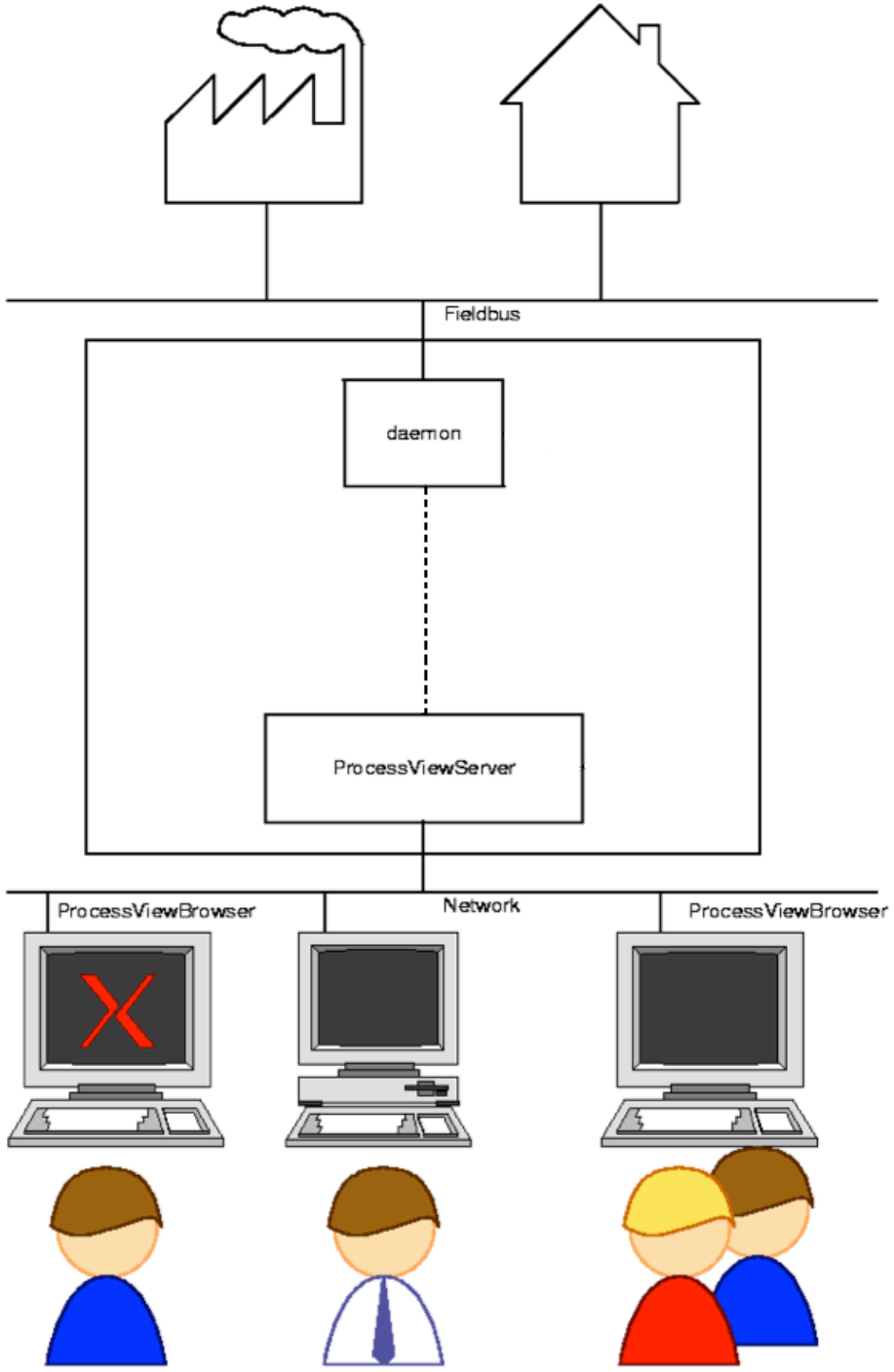
PvBrowser (Modifications)

- Break Shared Memory



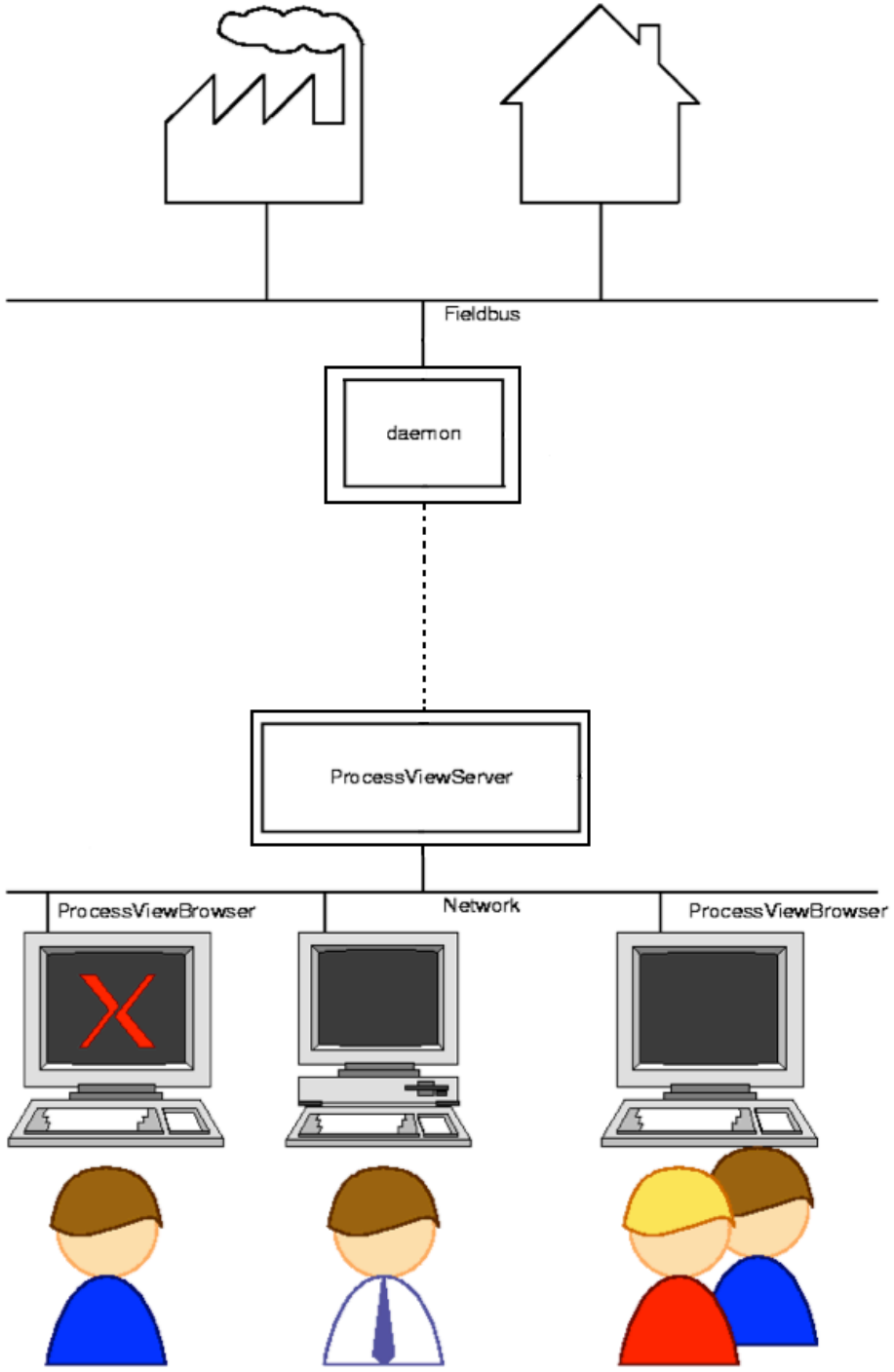
PvBrowser (Modifications)

- Break Shared Memory
- Implement message passing between DAD and PVServer
- Allows us to:
  - Eliminate nondeterministic behavior



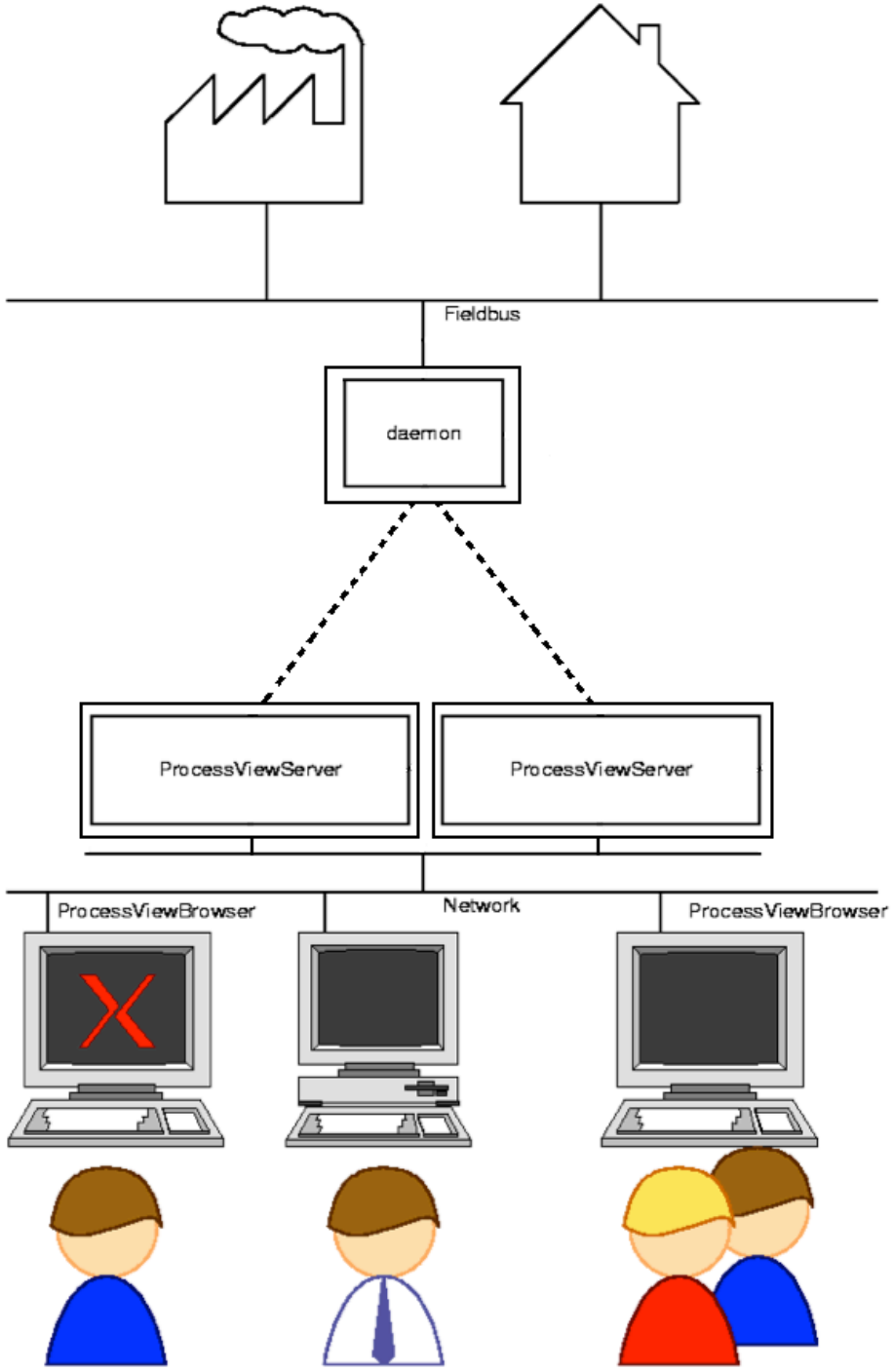
PvBrowser (Modifications)

- Break Shared Memory
- Implement message passing between DAD and PVServer
- Allows us to:
  - Eliminate nondeterministic behavior
  - Run processes on different machines



PvBrowser (Modifications)

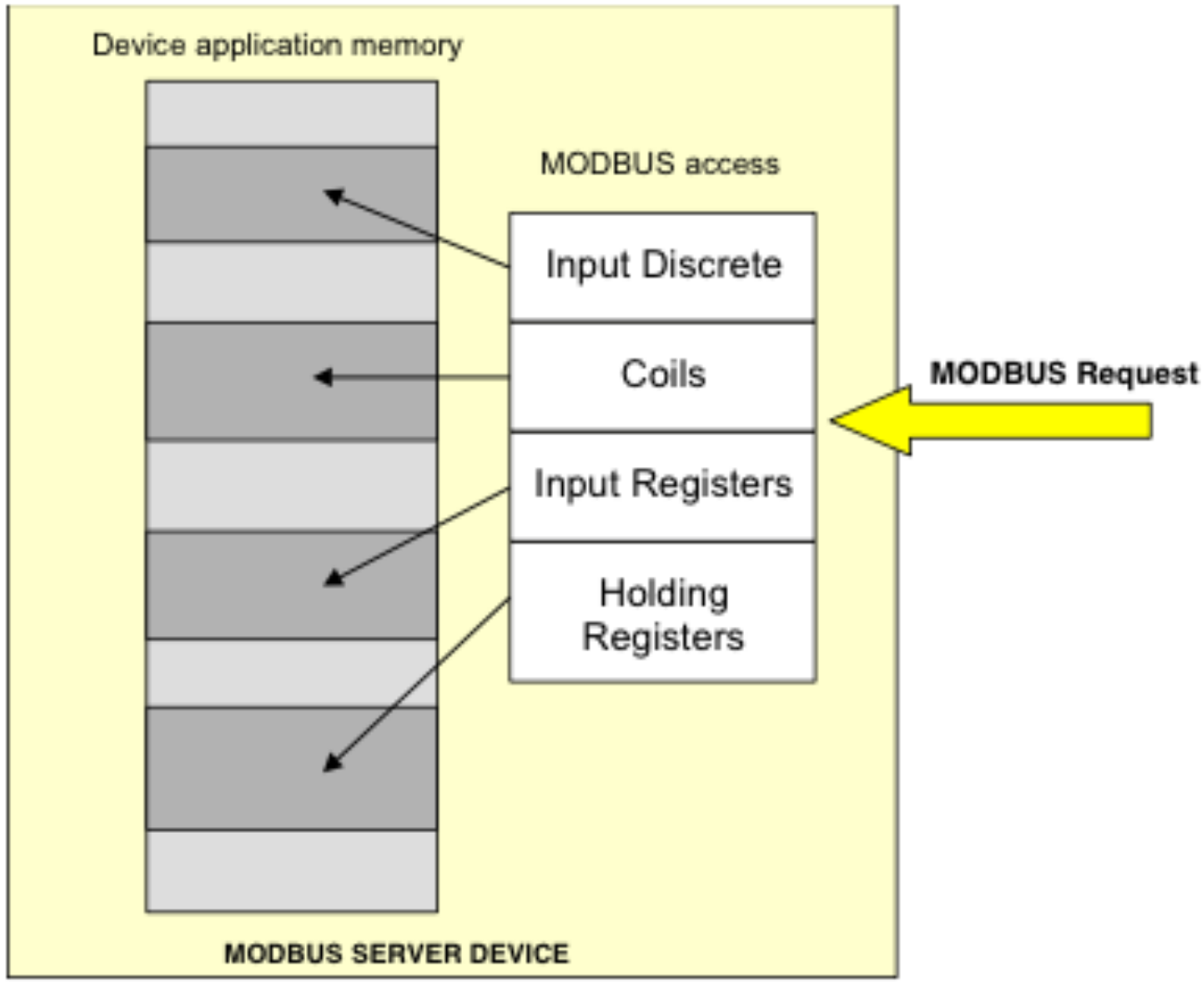
- Break Shared Memory
- Implement message passing between DAD and PVServer
- Allows us to:
  - Eliminate nondeterministic behavior
  - Run processes on different machines
  - Implement replication



Modbus

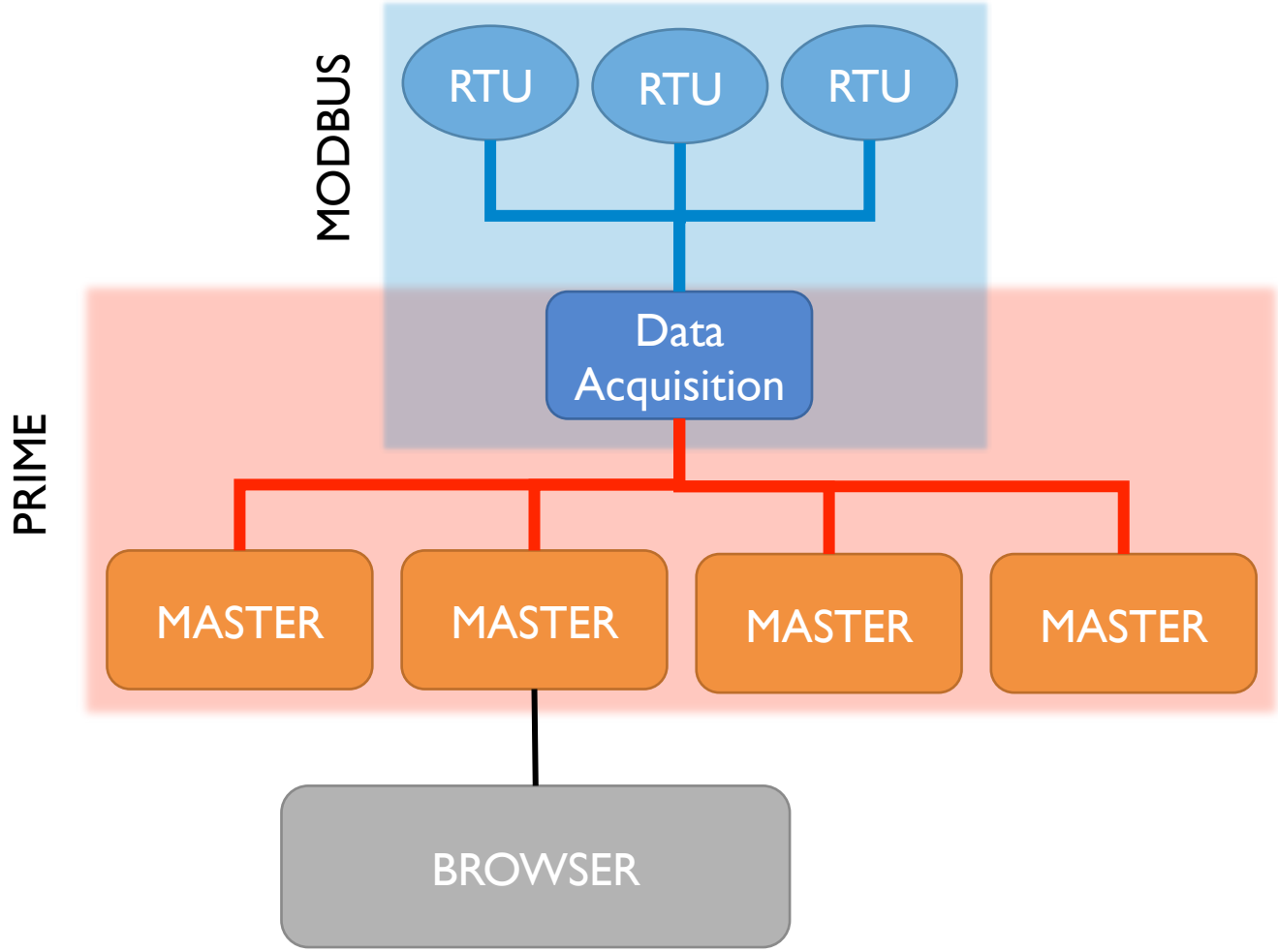
- Standardized communication protocol used by many SCADA systems around the globe
- Used to communicate with Remote Terminal Units (RTUs)
- Values stored in memory registers, organized as:
  - **Input Registers**: analog inputs of different types (e.g. voltage, amperage)
  - **Input Status**: digital input used to represent dichotomous values (e.g. electrical breakers, switches)
  - **Coil Status**: digital output used to switch voltage in a relay (e.g. switch power ON/OFF to field device)
  - **Holding Registers**: store additional data the can be used by other devices; less commonly used

Modbus Example



Our Architecture

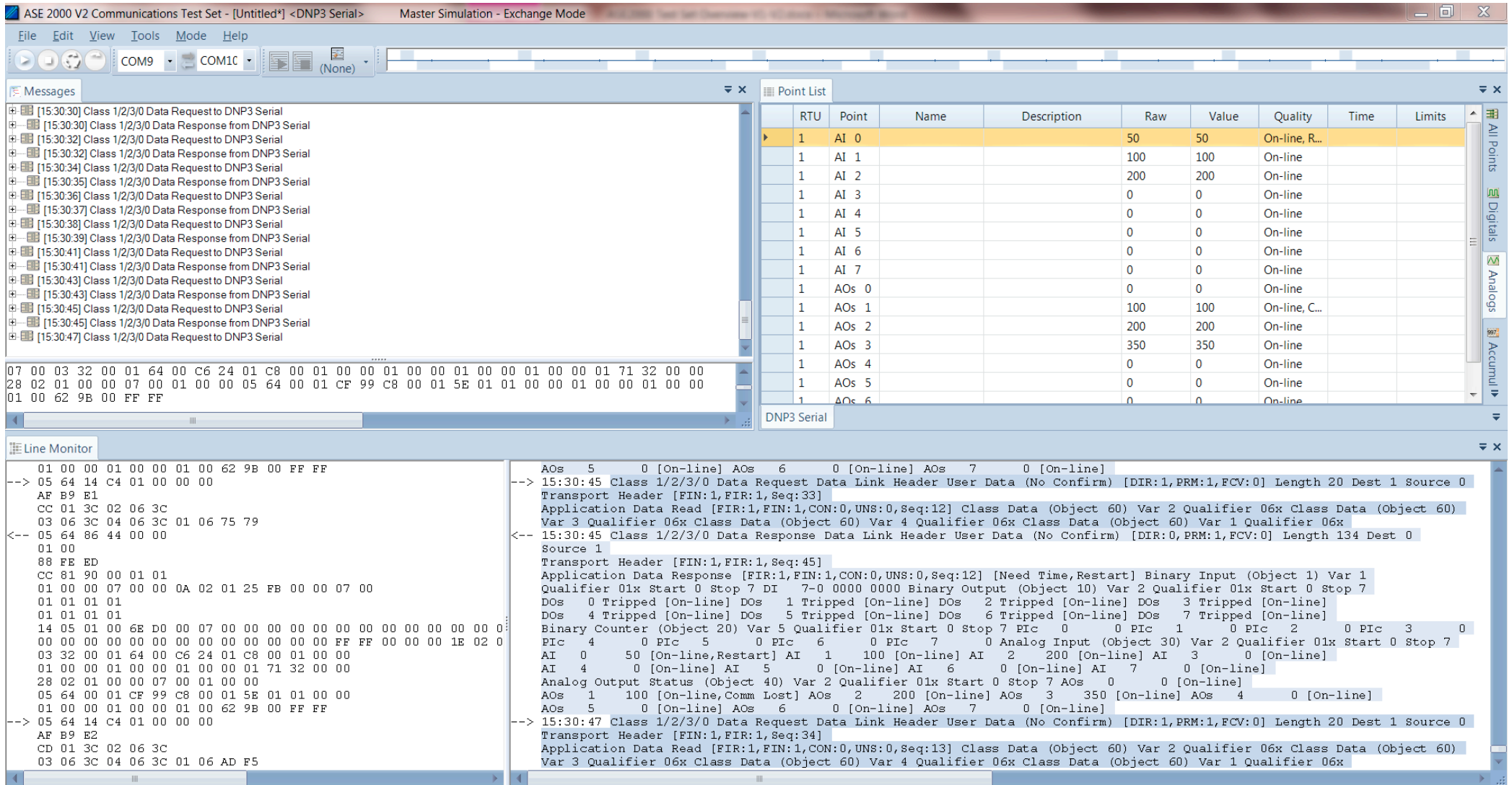
- DAD and 3f+1 PVServers all run on different physical machines
- DAD polls RTUs and communicates data to servers via message passing
- Data polled from field units is replicated consistently across all servers using Prime
- HMI can connect to any server and observe consistent data at each correct replica



RTU Emulator

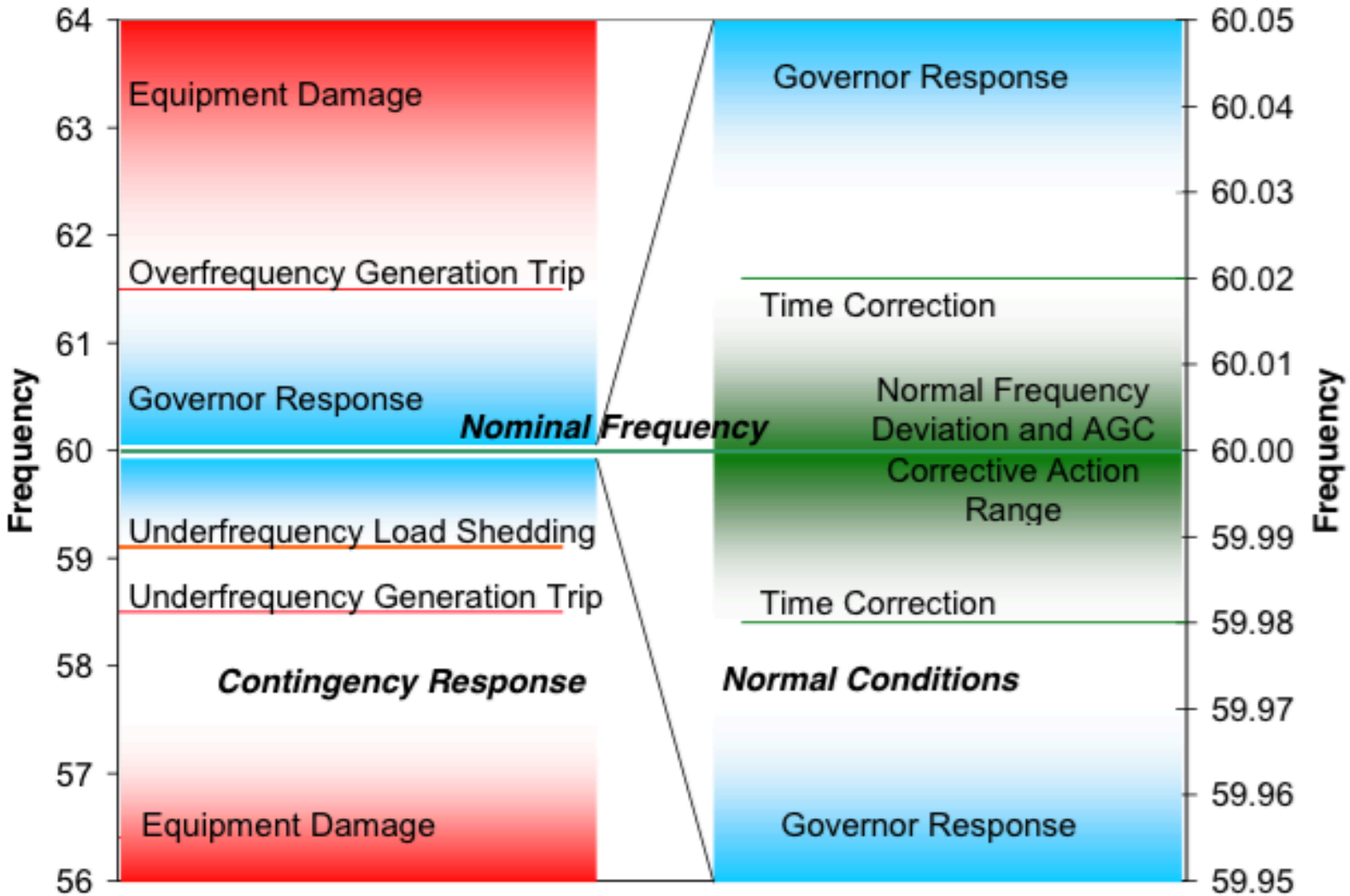
- ASE2000 Version 2 RTU Test Set
- Allows the user to define RTUs
- For each RTU, it is possible to specify communication protocol (e.g. Modbus) and the number of registers
- Used to test how the SCADA master responds to events (e.g. change of values/states)
- Allows testing of newly implemented protocols (e.g. DNP3)

RTU Emulator Example



Frequency Regulation

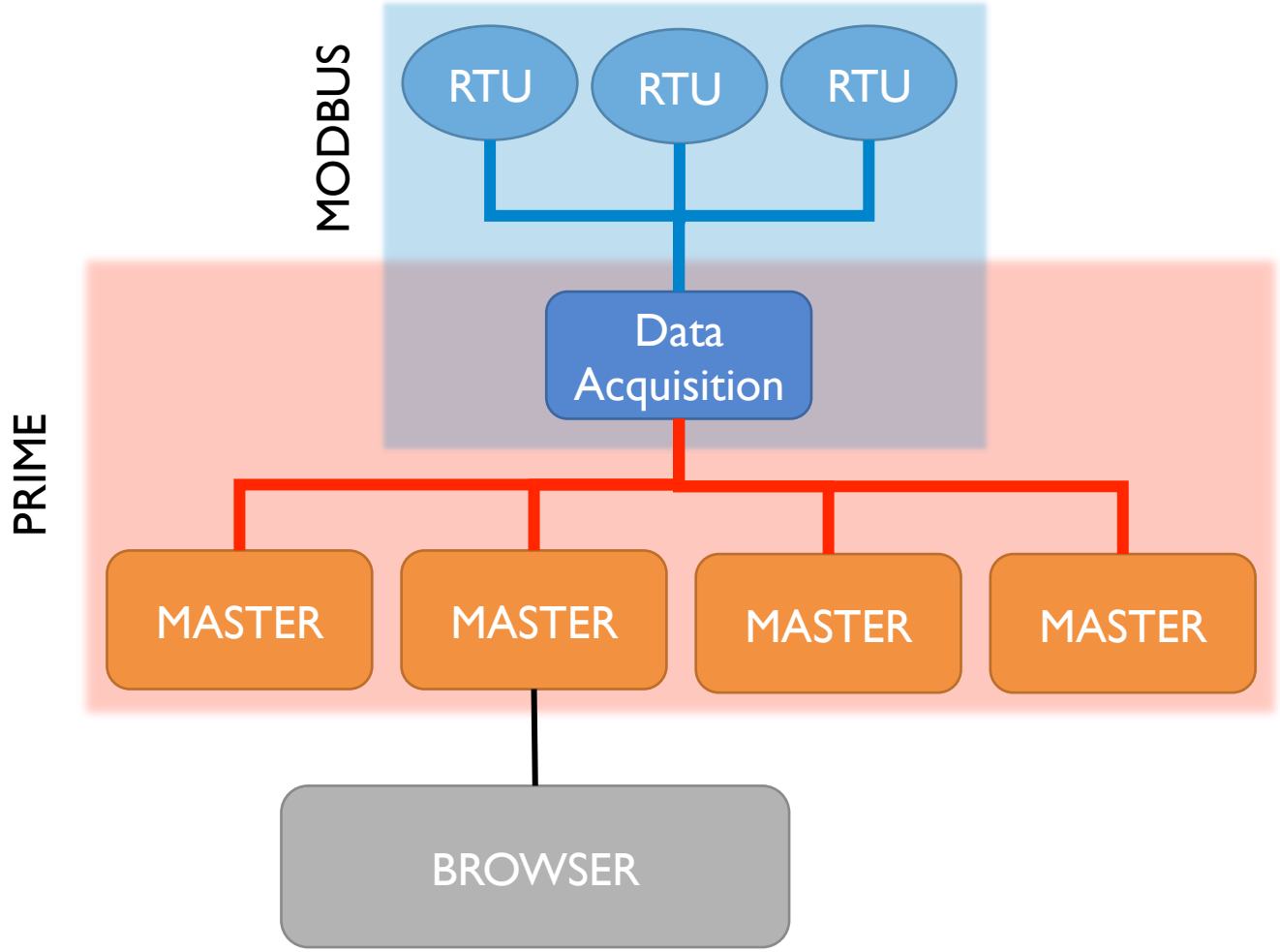
Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965



https://cdn.fbsbx.com/hphotos-xap1/v/t59.2708-21/1117070697_1020661542456794 7_1652314067_n.pdf/PowerGridOverview-Dagle.pdf?oh=a311fd53c7bdbe0459294bafa930067f&oe=5547523F&dl=1

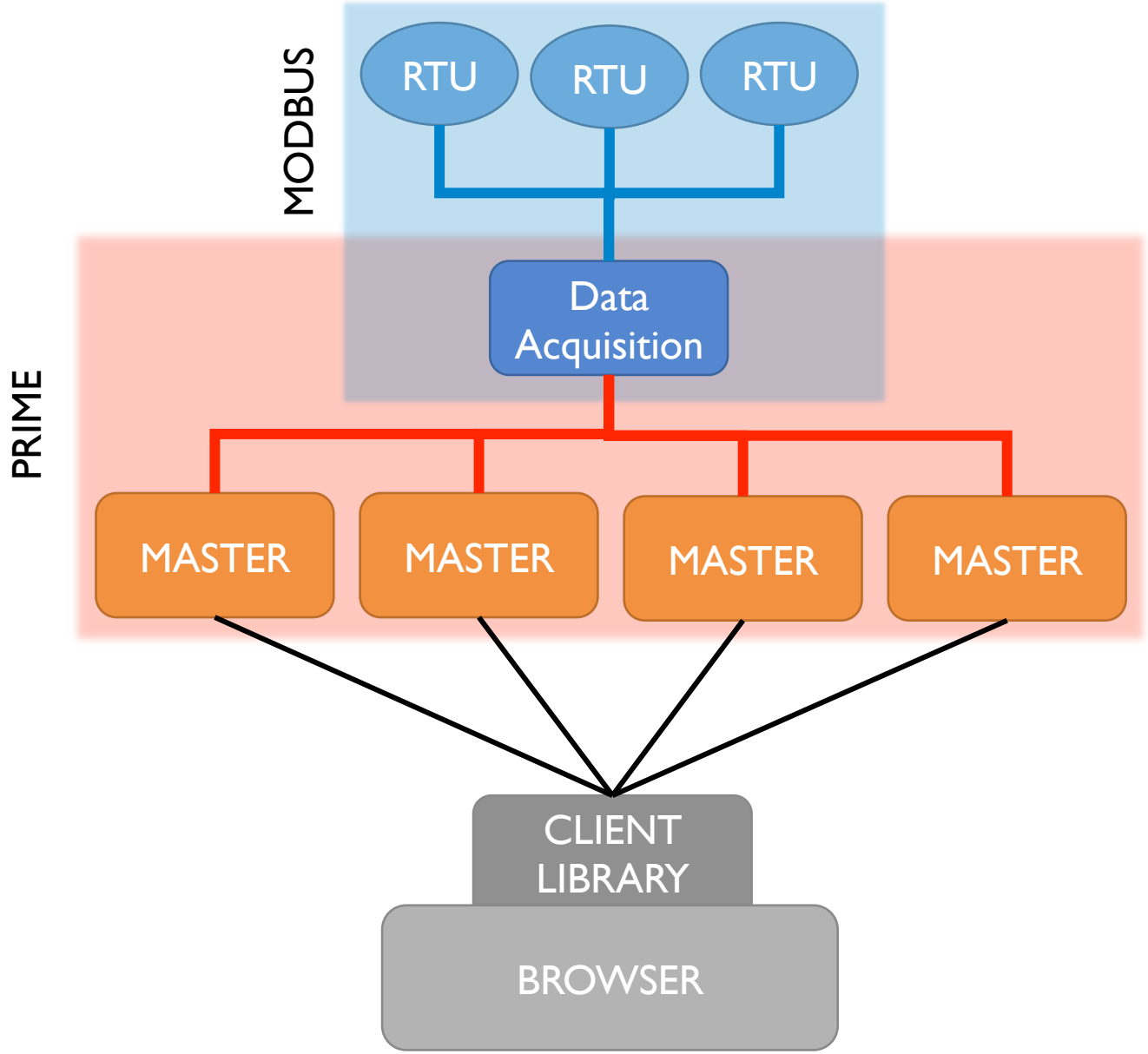
Future Directions

- Our Architecture provides intrusion tolerant replication of the data used by the SCADA Master



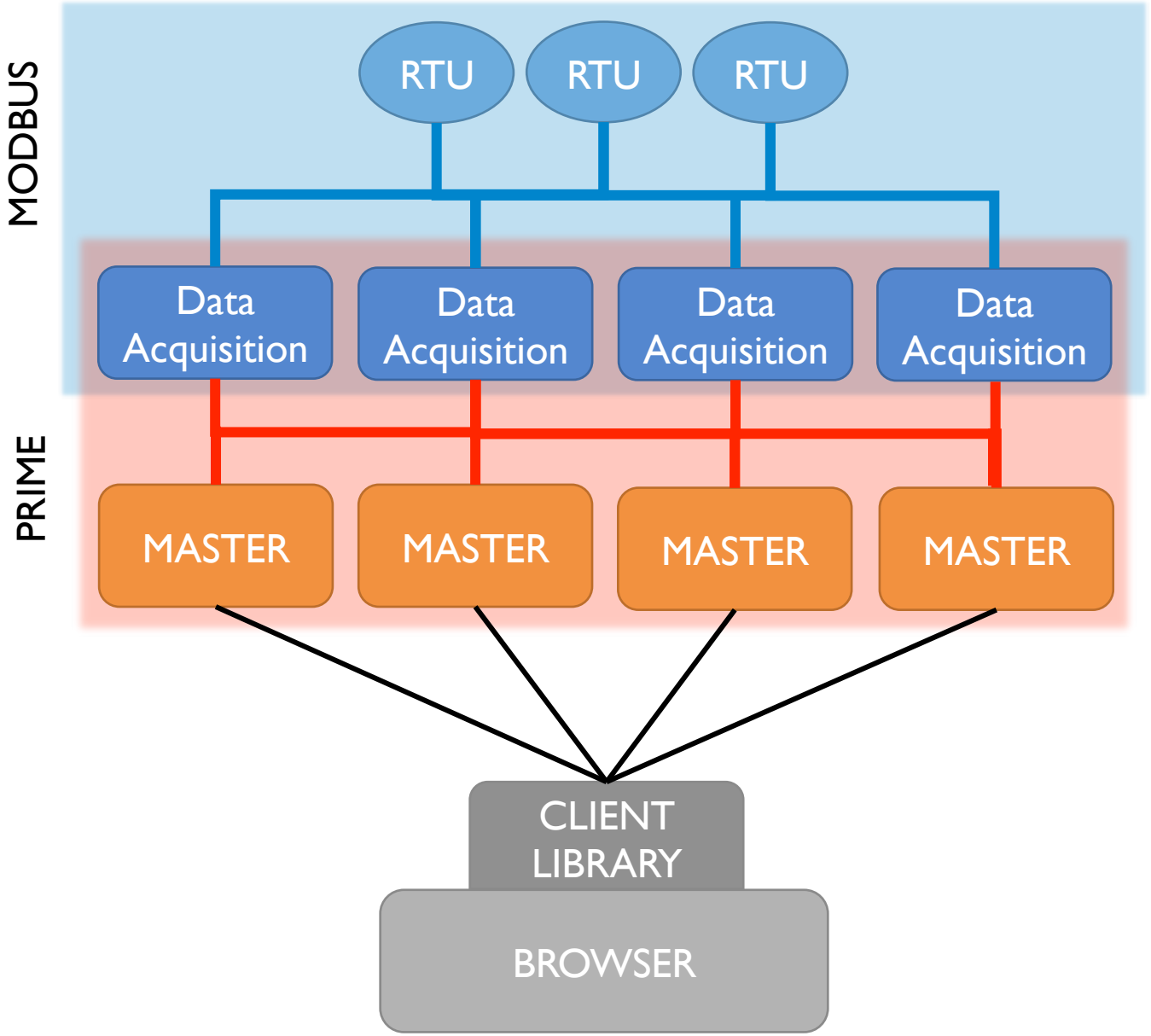
Future Directions

- Our Architecture provides intrusion tolerant replication of the data used by the SCADA Master
- Additional components:
  - Replication of all events involving the SCADA master, allowing a client to compare the state of each server and determine the *correct* state (with f+1 consistency)



Future Directions

- Our Architecture provides intrusion tolerant replication of the data used by the SCADA Master
- Additional components:
  - Replication of all events involving the SCADA master, allowing a client to compare the state of each server and determine the *correct* state (with f+1 consistency)
  - Implementing intrusion tolerance for data acquisition
    - Replicating DAD
    - Using Prime to synchronize and order data polled from RTUs/ PLCs



Special Thanks

- Johns Hopkins DSN Lab
- Dr. Yair Amir
- Dr. Marco Platania

Intrusion tolerance: the time is now!

- Critical Infrastructures (power grids, water plants, transportation systems, …) are at the heart of human society
- Power grids are particularly important because other Critical Infrastructures, systems, and human activities rely on them
- This is one of the factors that make power grids an increasingly important target for cyber attacks
  - In 2013 DHS reported that in 2012 the 40% of cyber attacks targeted the energy sector

"Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy"

Barack Obama, State of the Union 2013

Breaking the barriers

- Power service industry is highly regulated
- Power companies strictly follows the regulation requirements
- SCADA system manufacturers have no (or little) incentive to develop capabilities that are not demanded by power companies
- Because intrusion tolerance is not on the regulations, power companies and SCADA system manufacturers are not interested in working on intrusion tolerant solutions
- The first prototype of intrusion tolerant SCADA produced by Siemens was never translated to a product in the field, lacking customer demand and regulatory requirements

Our goal

- Building the first survivable intrusion tolerant open source SCADA system
- Impact on the energy ecosystem:
  - Showing to regulators, power companies, and SCADA manufacturers the importance of intrusion tolerance and that the problem is solvable
  - Making intrusion tolerant a regulatory requirement
  - Showing and teaching SCADA manufacturers how to integrate intrusion tolerance in their own systems via open source
  - Involving other researchers so to enlarge the SCADA community and increase the impact that it can have