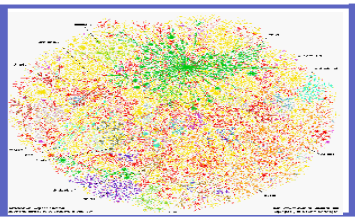
Ein Ansatz zur Intrusion Detection für Prozessautomatisierungssysteme

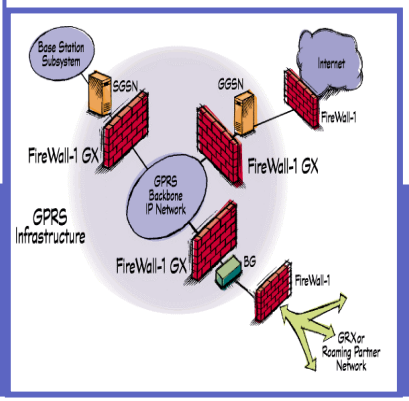
An Approach to Intrusion Detection for Process Control Systems

Martin Naedele

ABB Corporate Research

Baden, Switzerland





Overview

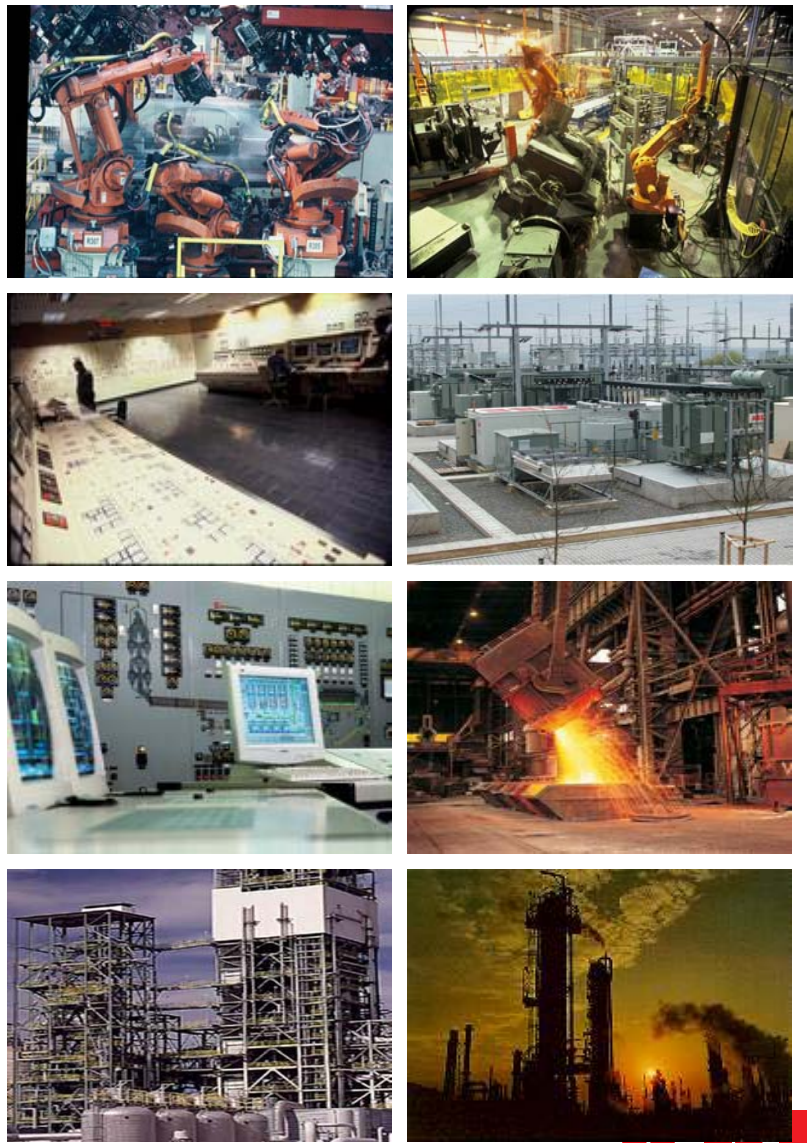
- Motivation
- Industrial automation systems
- IS security / IDS for automation systems
- Proposed approach / prototype

Automation systems - Examples

- Automation domains

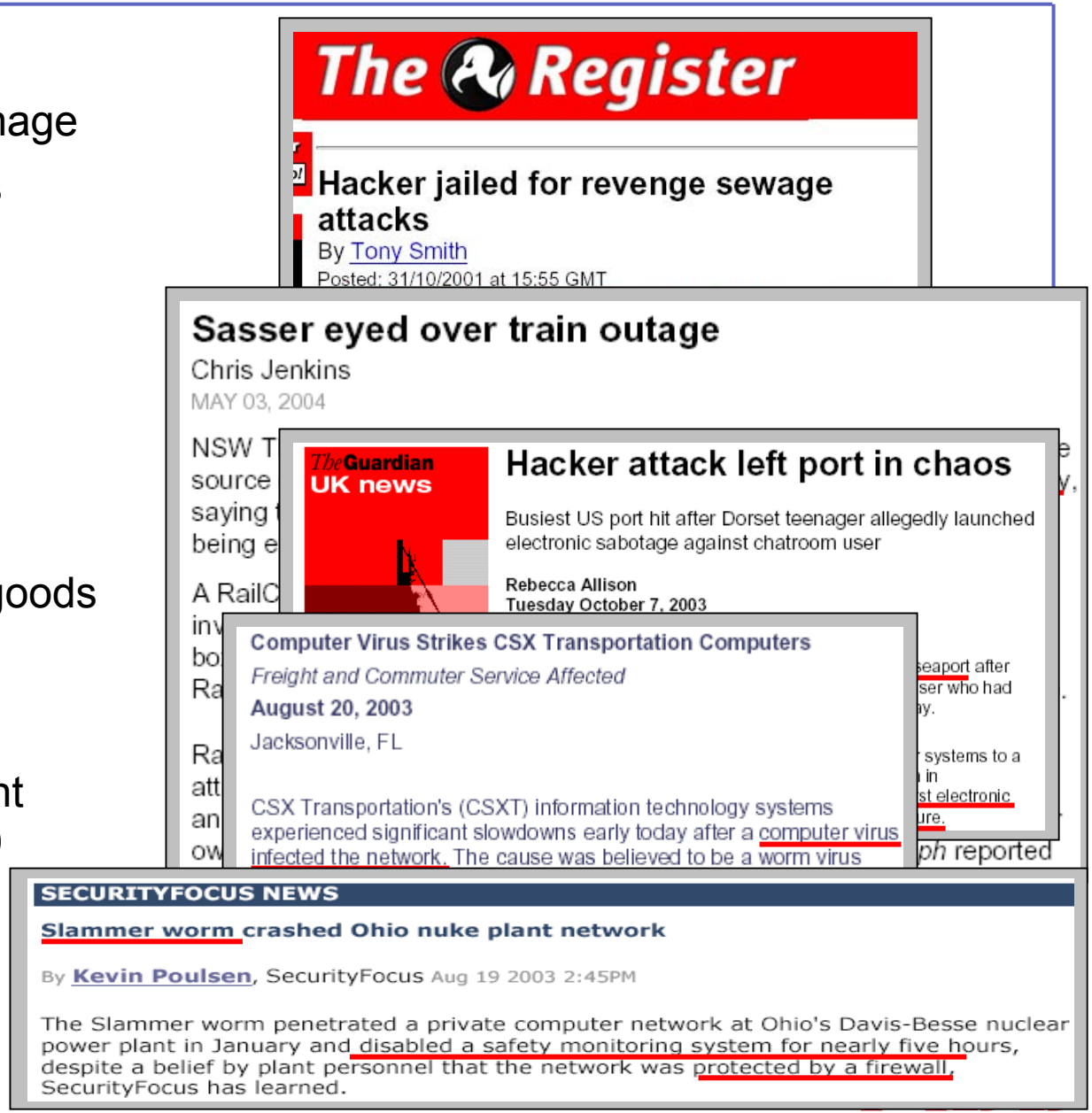
  Steel, paper, cement, pharma, petrochem, power gen/distrib, automotive, food, gas, water, transportation, ….

- Automation concerns
  - Control of the process
  - Control of the power supply
  - Safety systems



Motivation for protecting automation systems

- Threats (as usual)
  - Random collateral damage
  - Disgruntled employees
  - Economic competition
  - Organized crime
  - Terrorists
  - E-warfare
- Damage potential
  - Loss of semi-finished goods
  - Loss of production
  - Destruction of plant
  - Damage to environment (Release of chemicals)
  - Damage to persons (Explosions)



Motivation for protecting automation systems

- Threats (as usual)
  - Random collateral damage
  - Disgruntled employees
  - Economic competition
  - O
  - Te
  - E-
- Dama
  - Lo
  - Lo
  - De
  - Damage to environment (Release of chemicals)
  - Damage to persons (Explosions)

The Register

Hacker jailed for revenge sewage attacks

By Tony Smith

Competition, a first for power suppliers, has created what IEEE-USA calls "financial incentives for malicious intrusion into computers and communication systems of the electric power industry and marketplace participants."

[Quelle: IEEE-USA, "Legislative agenda for the 107th congress," 2000]

Questioning of captured al-Qaeda operatives also found that the terror group was interested in a class of digital devices involved in DCS and SCADA systems.

[BBC news, 7/2002]

Jacksonville, FL

CSX Transportation's (CSXT) information technology systems experienced significant slowdowns early today after a computer virus infected the network. The cause was believed to be a worm virus

systems to a
in
st electronic
ure.
ph reported

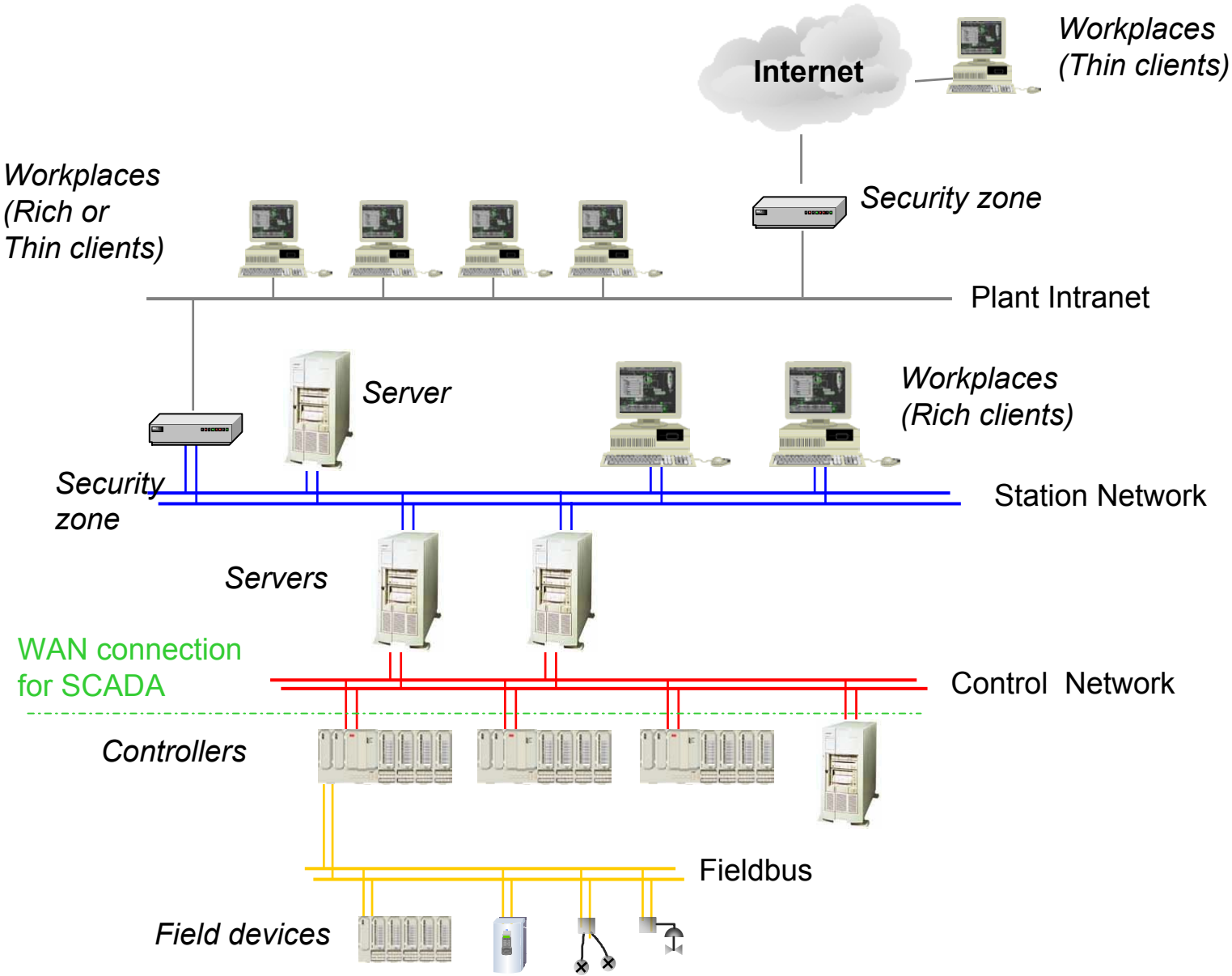
SECURITYFOCUS NEWS

Slammer worm crashed Ohio nuke plant network

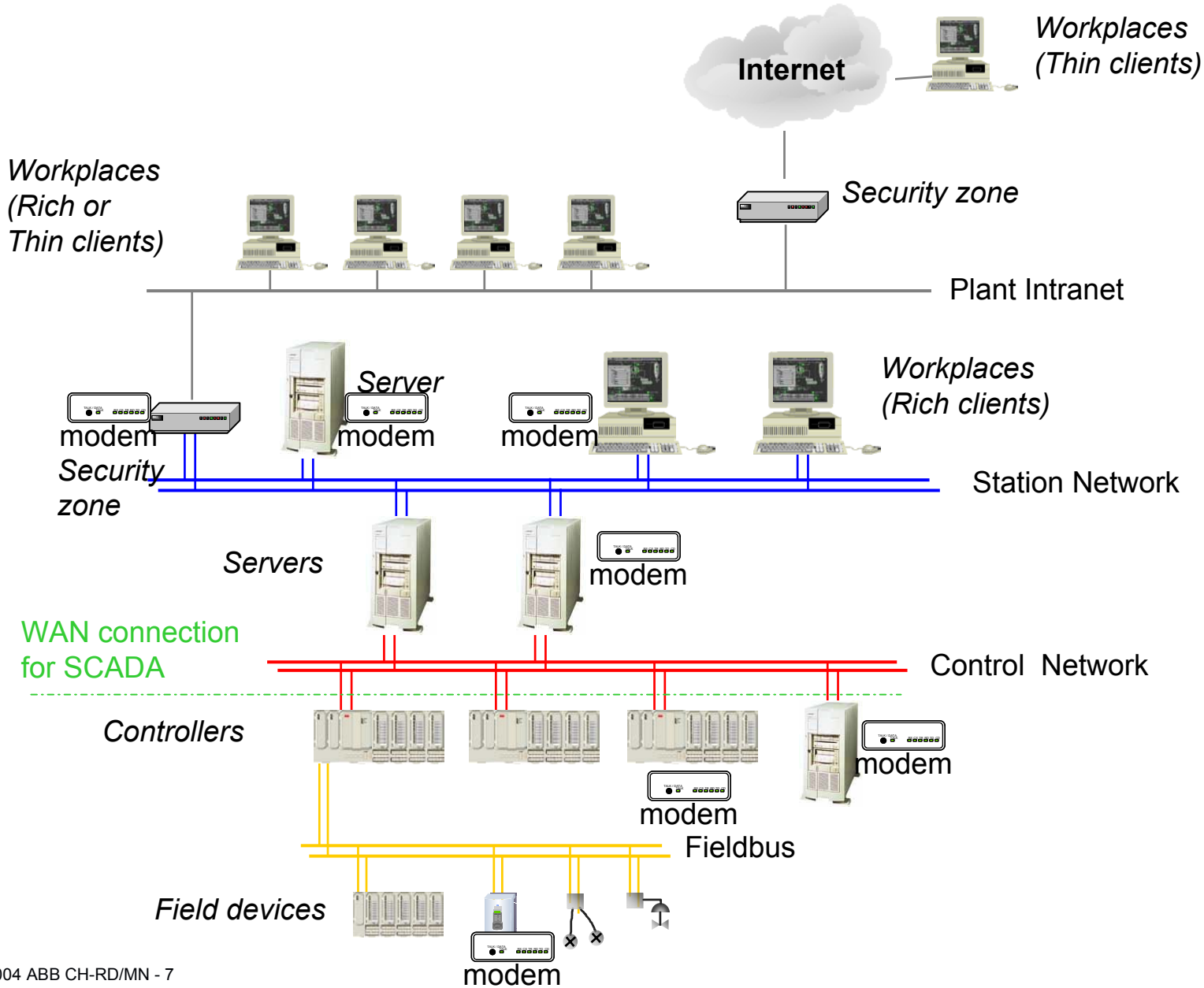
By Kevin Poulsen, SecurityFocus Aug 19 2003 2:45PM

The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall, SecurityFocus has learned.

Automation systems – System topology



Automation systems – Generic System topology



Automation systems – ISS relevant characteristics

- Security objective
  - Prevent damages to humans and environment
  - Technically: availability – maintain control over the process at all times
- Network topology
  - Relatively small networks
  - Most important hosts not in the core, but at periphery
  - Multiple zones in network
  - Dial-up remote access
- Components
  - Bounded reaction times required (hard real-time)
  - Real-time operating systems w/o security mechanisms
  - Operational environment: temperature, dust, humidity, vibration,…
  - System life time 20 to 30 years
  - Rare maintenance slots

IDS for automation systems

- Challenges
  - Special industrial protocols
  - Operators are no IT/security experts
  - IT experts not on site
  - High number of false alarms not acceptable

=> Today: IDSs not used in automation systems

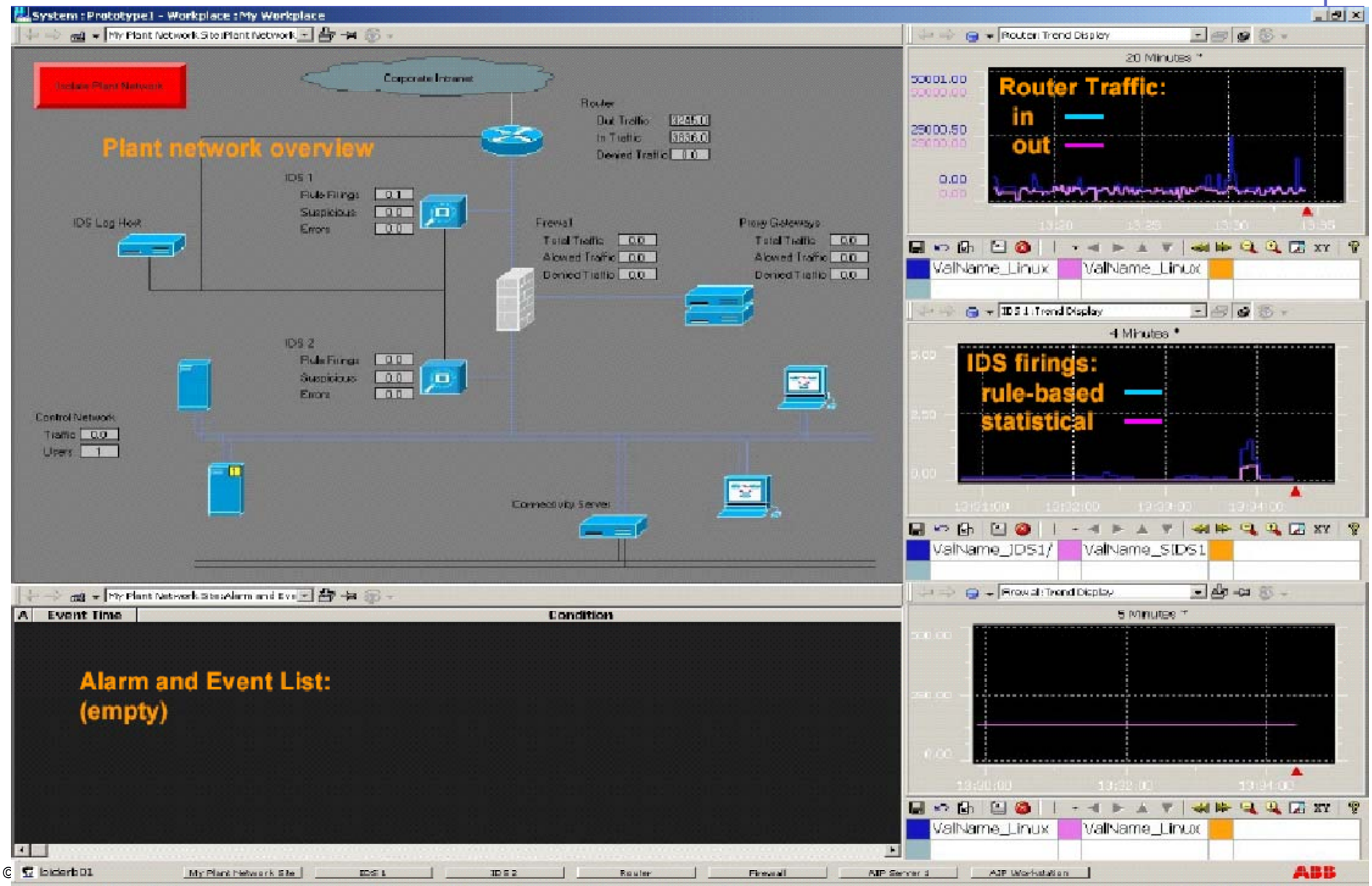
- Chances
  - Static Topology
  - Few applications and services
  - Deterministic network traffic and system state
  - Isolation is often a suitable first response
  - Process monitored 24x7

Proposed approach

- Operator as pattern matcher and decider
  - Trained for detection of patterns in trends
  - Knows reasons for certain deviations (e.g. maintenance)
- Security mechanisms have to follow process operation paradigms
  - Few alarms
  - Trend displays
  - Process pictures
- IDS user interface has to be integrated into PCS HMI
  - Industry standard data exchange protocols (OPC)
- Quantitative data sources
- Related work: NCSA/UIUC on large scale visualization for IDS

=> Prototype/ feasibility study using ABB process control system

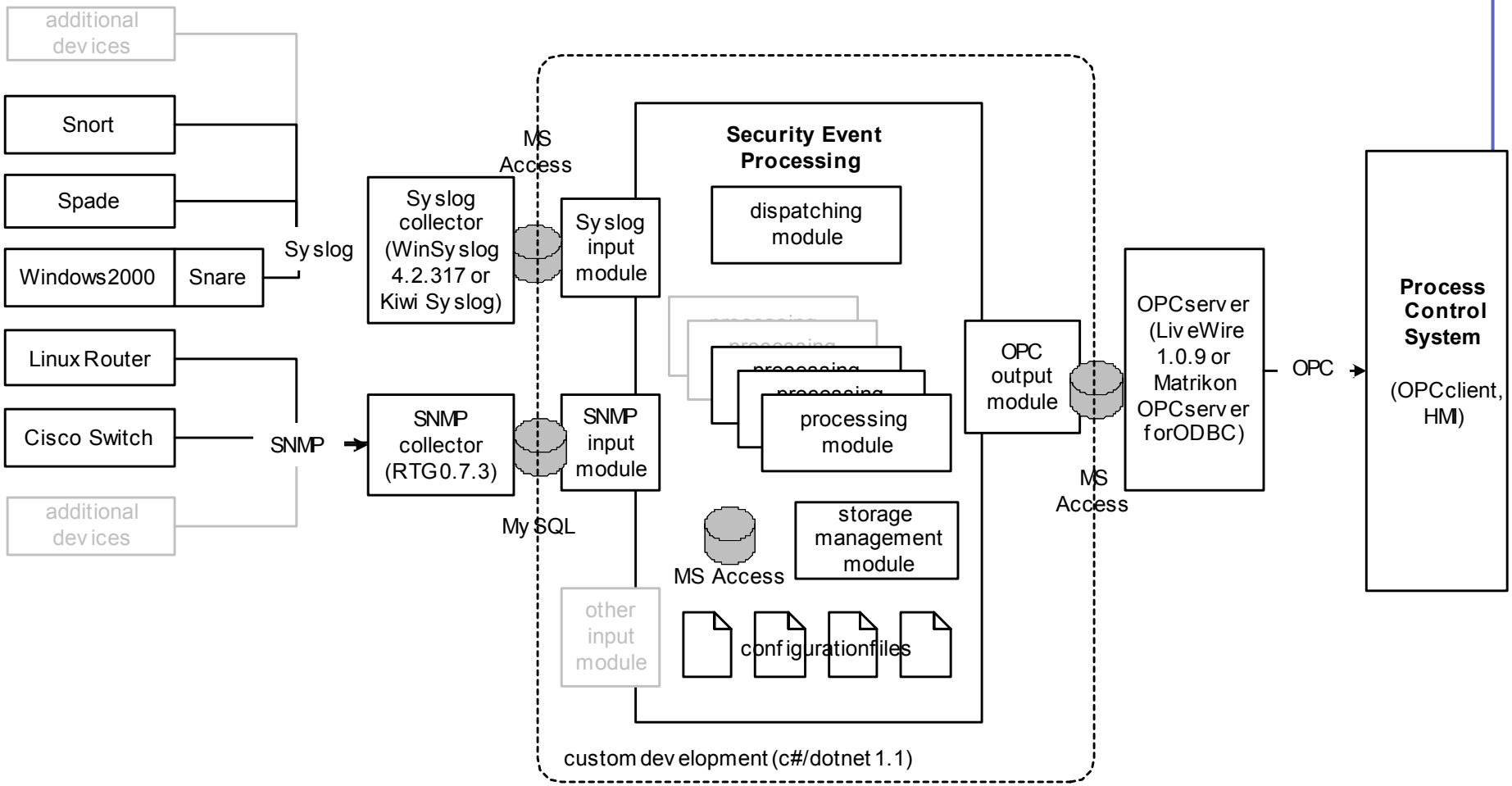
Prototype – User interface



Prototype: Data sources

- Security relevant data
  - Routers, FWs
    - Incoming/outgoing traffic
    - Management activity, rule changes
  - Network, Switches
    - Incoming/outgoing traffic; bandwidth saturation
  - Hosts
    - Successful/failed log-in
    - Management activity
    - Processor load, uptime, resource usage
  - Applications
    - Successful/failed log-in
    - Internal performance parameters
  - …

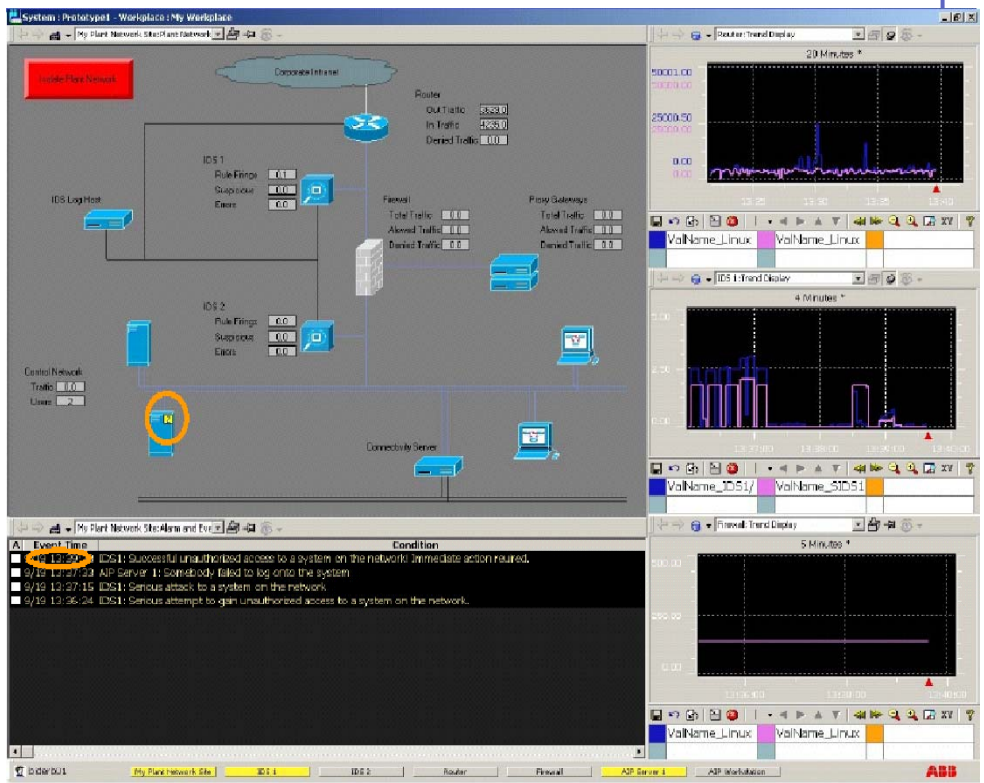
Prototype: System architecture



data generation	input handling	processing	output handling	presentation

Summary/Conclusions

- Industry has need for IDS for automation systems
- Involving process operators offers chance for a practically usable system
- Prototype for experiments
  - Limitations
  - Not yet production quality
- First results promissing
- Further work
  - Most suitable data sources
  - Ergonomic user interface
  - Field trial



ABB