FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Diplomarbeitspräsentation

AUTOMATION SYSTEMS GROUP

Traffic Control in Industrial Automation Networks

with focus on Paper Machines

Masterstudium:
Technische Informatik

Christian Mauser

Technische Universität Wien
Institut für Rechnergestützte Automation
Arbeitsbereich: Automatisierungssysteme
Betreuer: Ao.Univ.-Prof. Dr. Wolfgang Kastner
Univ.-Ass. Dipl.Ing. Lukas Krammer

Problem Environment

Voith-Pressebild

Industrial Automation Networks

A trend towards **Ethernet-based** automation networks can be observed!

- more and more subsystems share the **same network medium**
- the probability of **unwanted influences** between subsystems rises
- an **Internet connection** is often available
- the network is vulnerable to threats like **intrusion, malware, etc.**

Aim of the Thesis

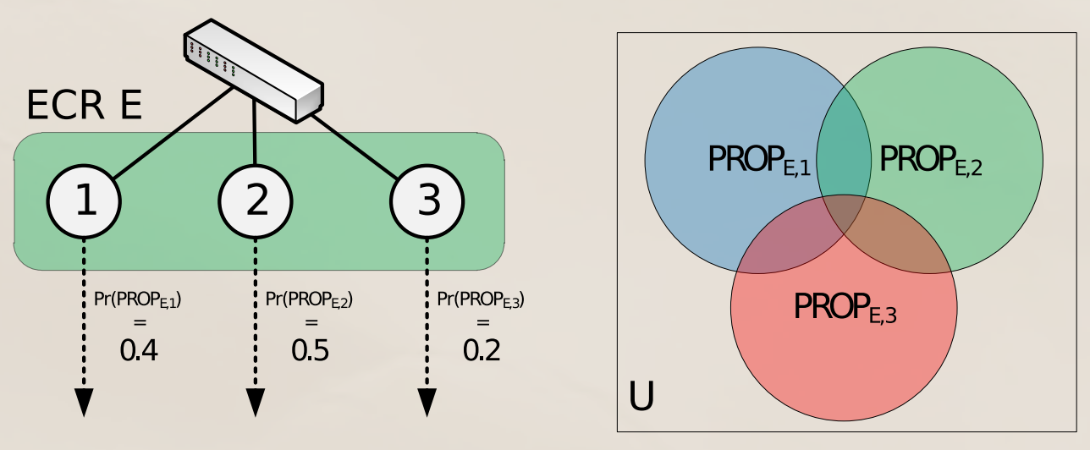
Improvement of **Dependability** and **Security** of industrial automation networks!

Theory

Error — **Unintended state** of the automation network, caused by one or more faulty hosts that pollute the network with **unwanted traffic** (e.g. flooding attack).

Error Propagation Probability (EPP)

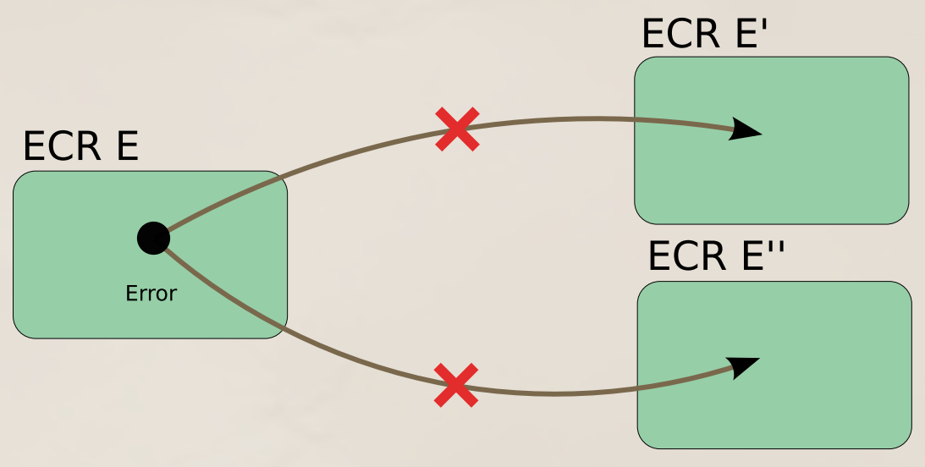
Probability, that an error is propagated from the automation network to its environment (e.g., paper machine).



Lower EPP means **higher level of dependability/security!**

Error Containment Coverage (ECC)

Probability, that an error is detected within an *Error Containment Region* (ECR).

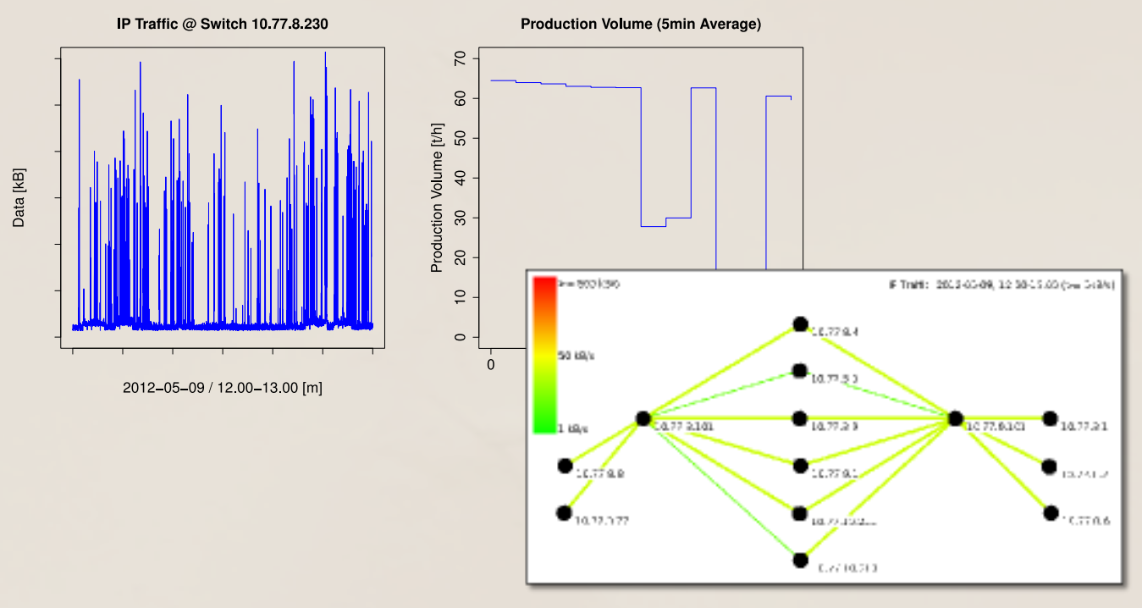


Higher ECC means **higher level of dependability/security!**

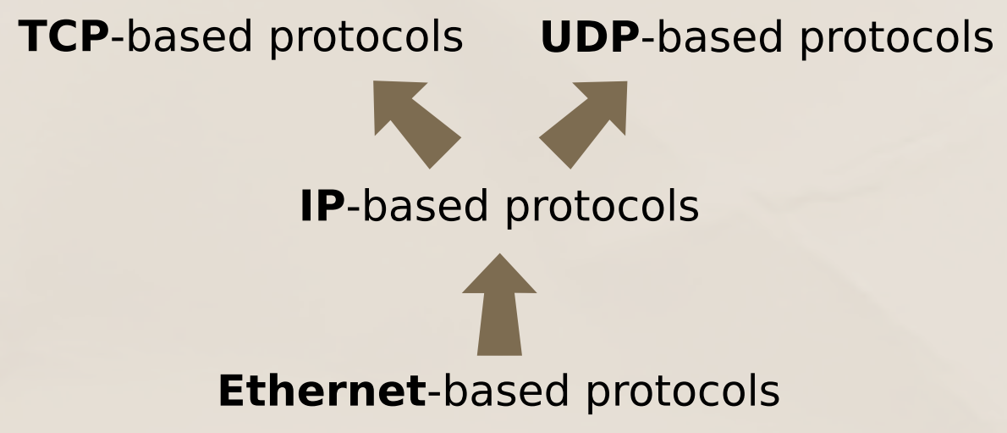
Analysis

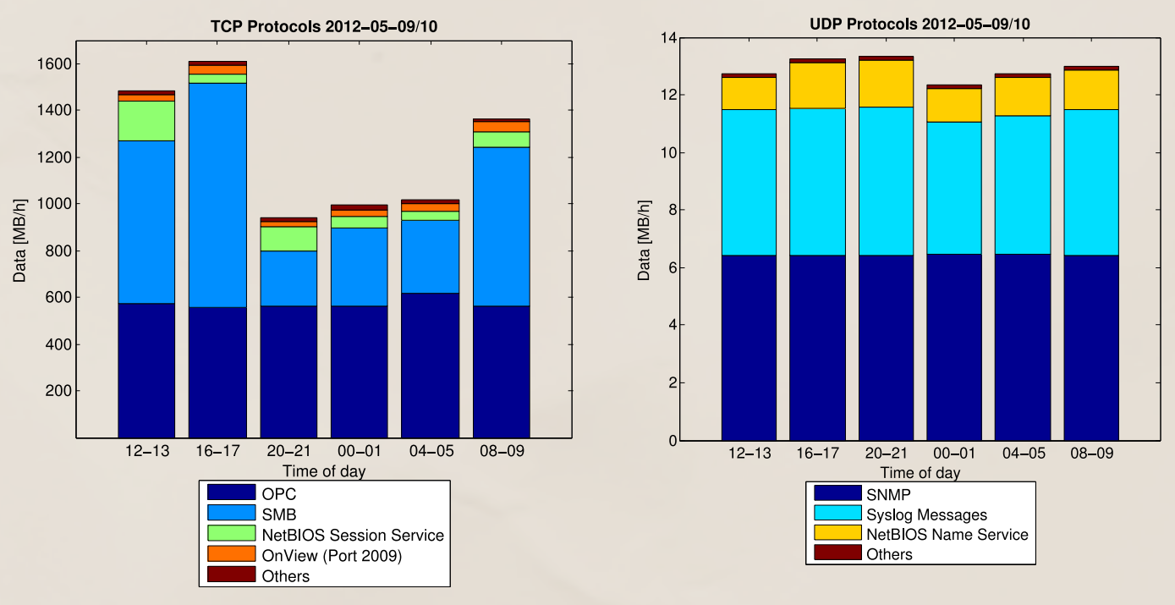
Quantitative Traffic Analysis

- **Traffic Graphs** visualizing cumulated traffic per second
- **Traffic Maps** visualizing point-to-point links



Semantic Traffic Analysis

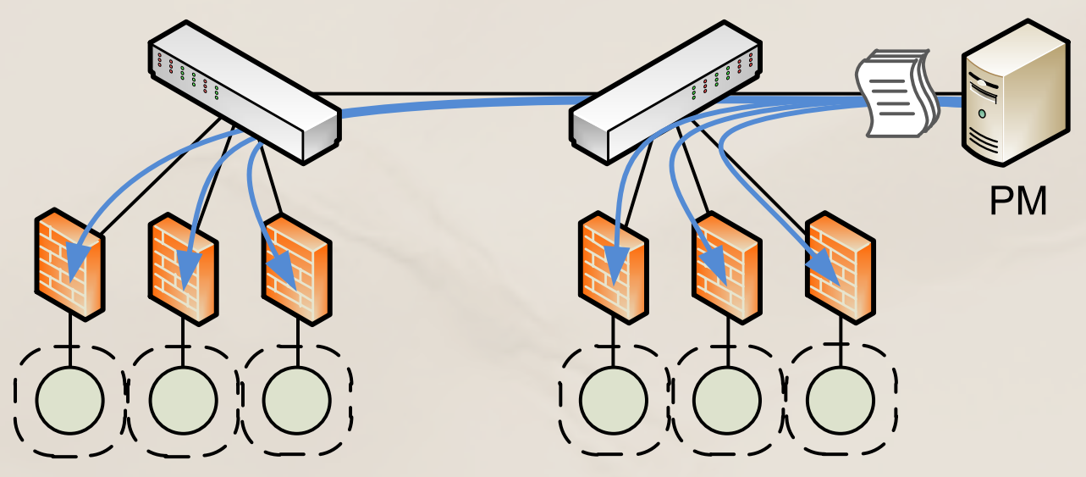


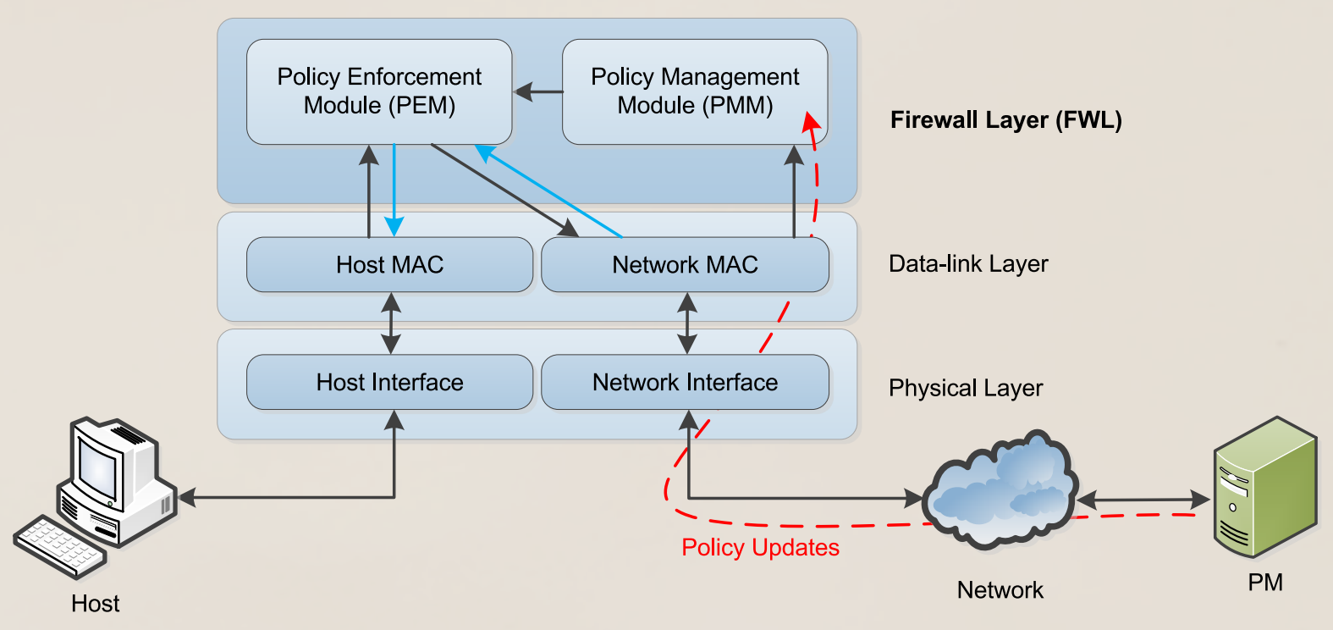


Approaches

Distributed Firewall

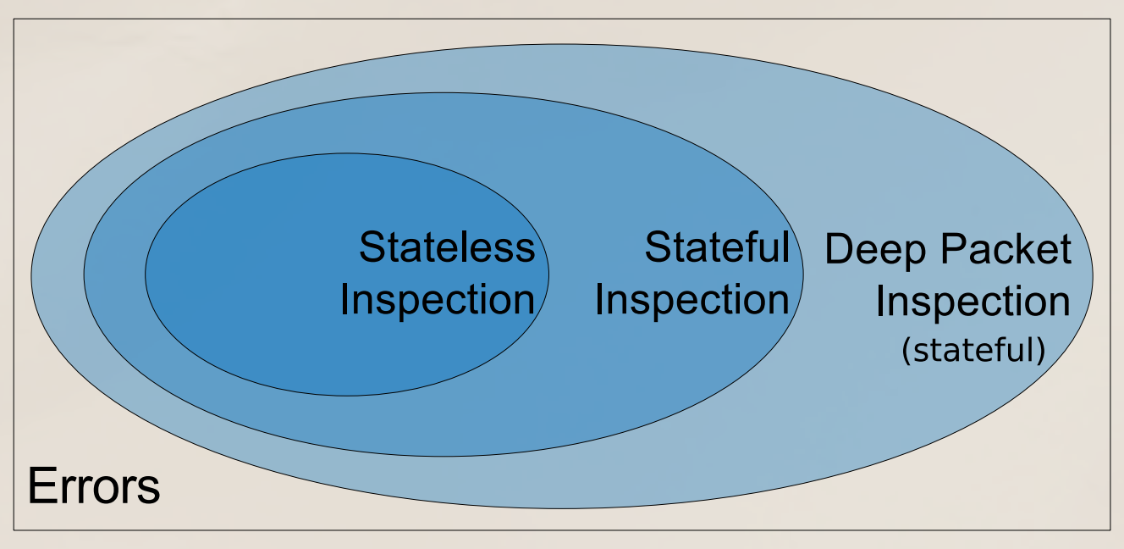
- **Distributed** policy **enforcement** by Local Firewalls (LFWs)
- **Central** policy **definition** by Policy Manager (PM)





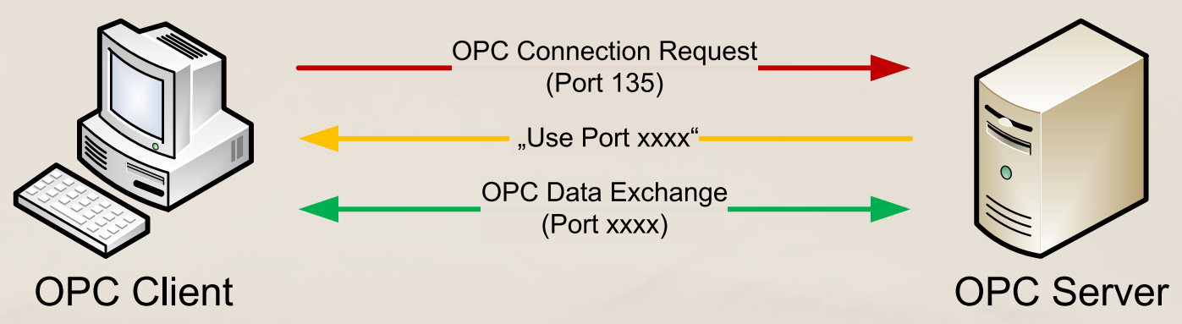
- Minimal size of Error Containment Regions (ECRs)
- **Improved Error Propagation Probability** (EPP)!

Smart Packet Filtering



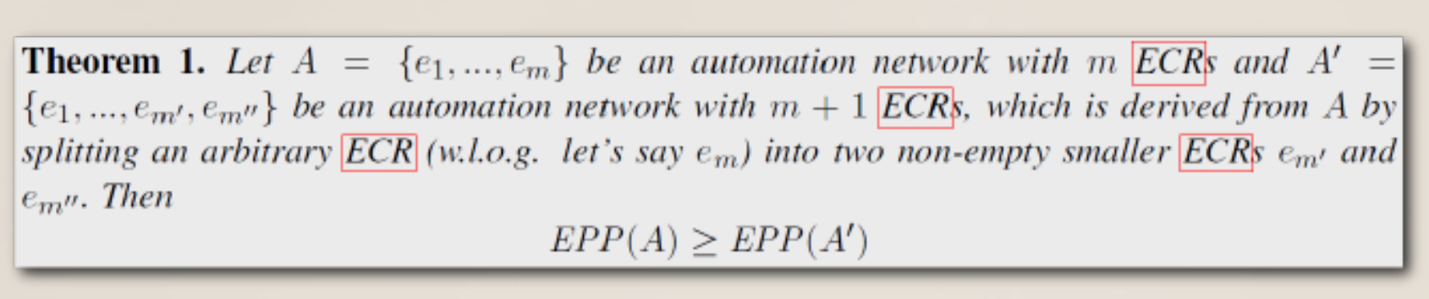
- **Deep Packet Inspection** detects more error events than common filtering techniques
- **Improved Error Containment Coverage** (ECC)!

- Higher computational effort than common techniques
- Application-specific knowledge necessary
- Reasonable if port-based filtering is not possible, e.g. OPC

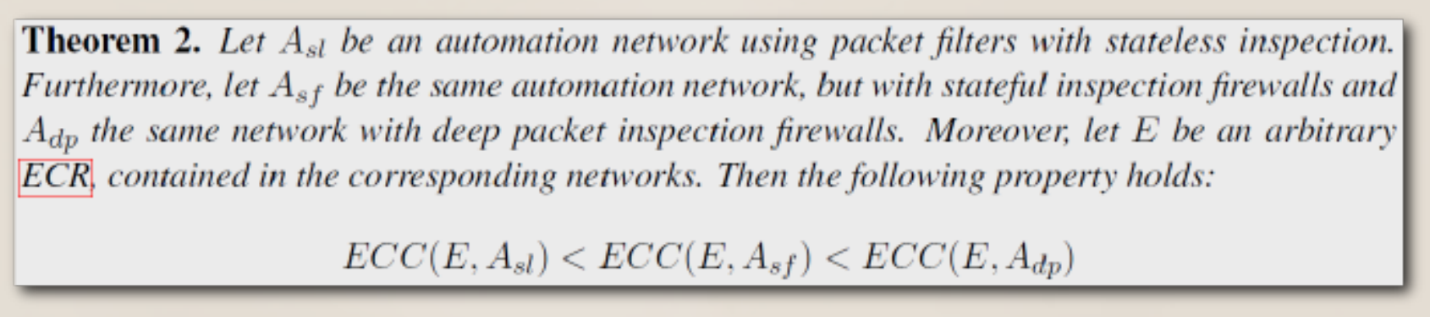

OPC Connection Request (Port 135)
„Use Port xxxx"
OPC Data Exchange (Port xxxx)
OPC Client
OPC Server

Evaluation

Formal Proofs

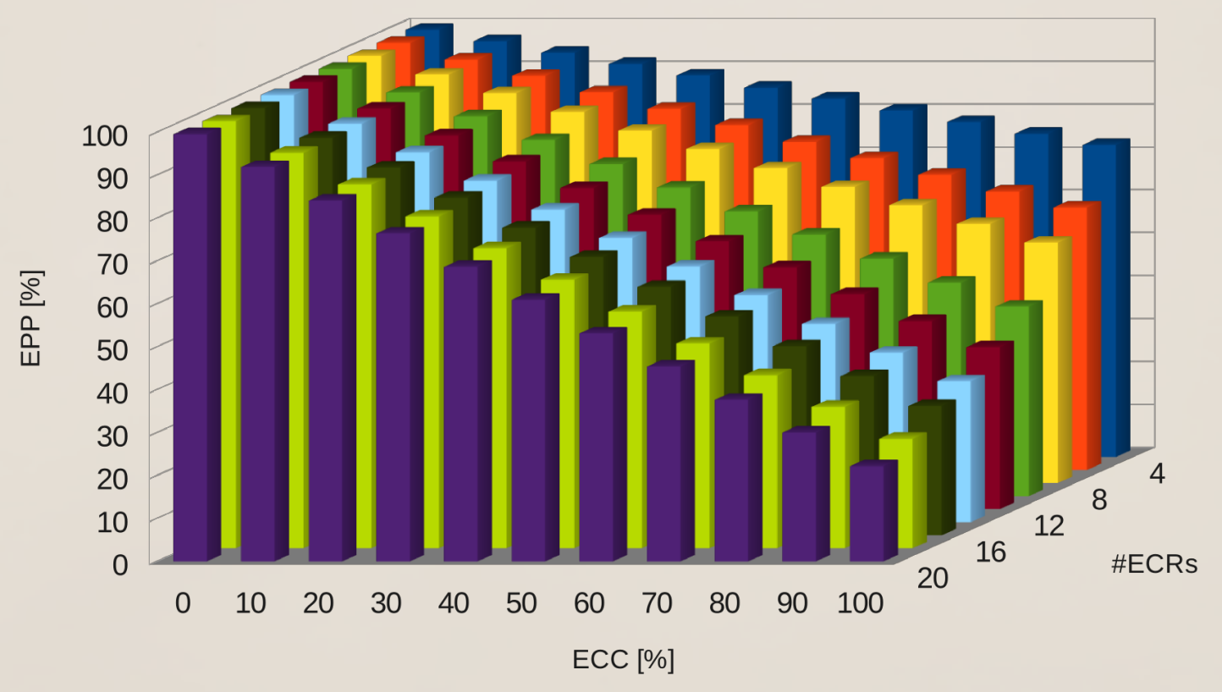

Theorem 1. *Let $A = \{e_1, ..., e_m\}$ be an automation network with m ECRs and $A' = \{e_1, ..., e_{m'}, e_{m''}\}$ be an automation network with $m+1$ ECRs, which is derived from A by splitting an arbitrary ECR (w.l.o.g. let's say e_m) into two non-empty smaller ECRs $e_{m'}$ and $e_{m''}$. Then*

$$EPP(A) \geq EPP(A')$$

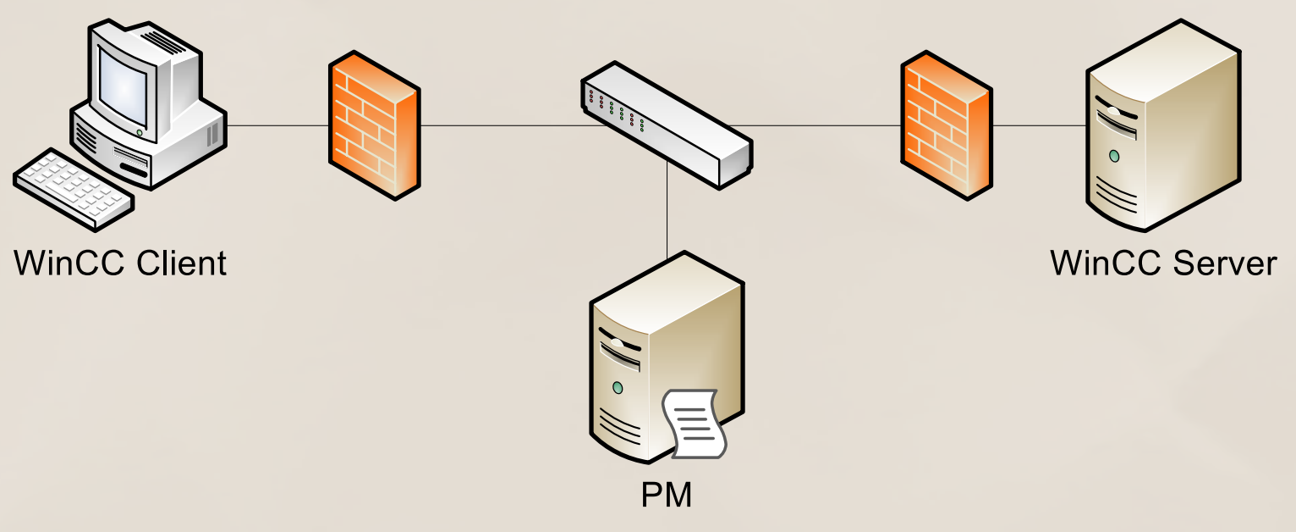

Theorem 2. *Let A_{sl} be an automation network using packet filters with stateless inspection. Furthermore, let A_{sf} be the same automation network, but with stateful inspection firewalls and A_{dp} the same network with deep packet inspection firewalls. Moreover, let E be an arbitrary ECR contained in the corresponding networks. Then the following property holds:*

$$ECC(E, A_{sl}) < ECC(E, A_{sf}) < ECC(E, A_{dp})$$

Simulation



Prototypical Implementation



Evaluation Results

Formal Proofs, Simulation

- **Distributed Firewall** minimizes the number of ECRs, and therefore **decreases EPP**
- **Deep Packet Inspection** improves ECC and thus **decreases EPP** also

Prototypical Implementation

- Combination of Distributed Firewall and Deep Packet Inspection is **realizable**

Contact: cmauser@auto.tuwien.ac.at