Traffic Control in Industrial Automation Networks
with focus on Paper Machines

Christian Mauser

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!

Error
Unwanted 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 machines).

Error Containment Coverage (ECC)
Probability that an error is contained within an Error Containment Region (ECR).

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)

Formal Proofs

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

Combination of Distributed Firewall and Deep Packet Inspection is realizable

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

Semantic Traffic Analysis
- TCP-based protocols
- UDP-based protocols
- IP-based protocols
- Ethernet-based protocols

Contact: cmauser@auto.tuwien.ac.at