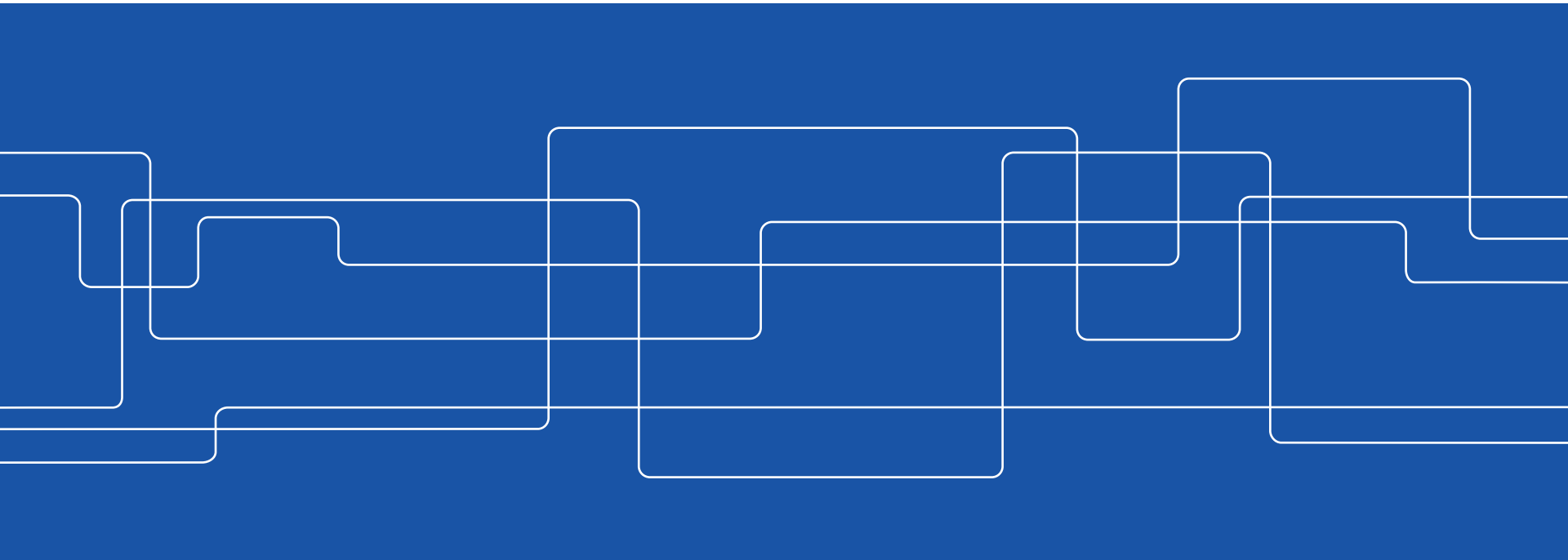
Security Monitoring as a Service for Critical Infrastructures

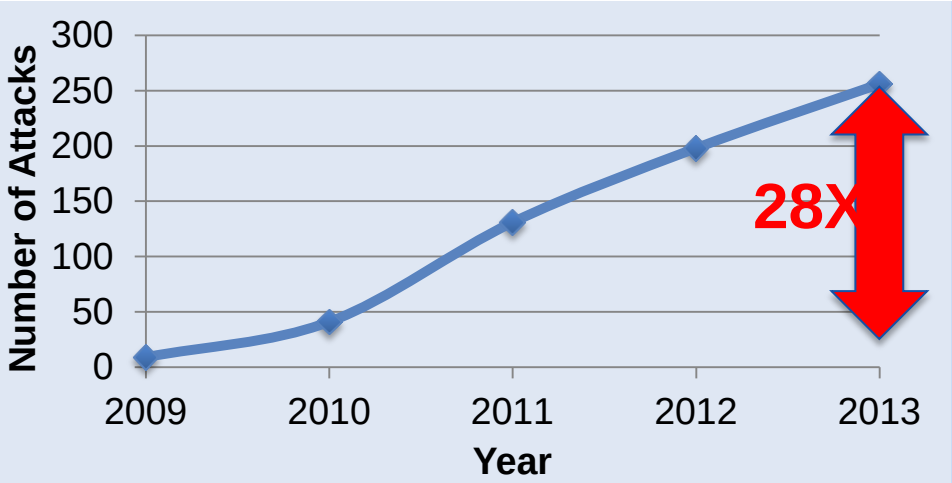
György Dán

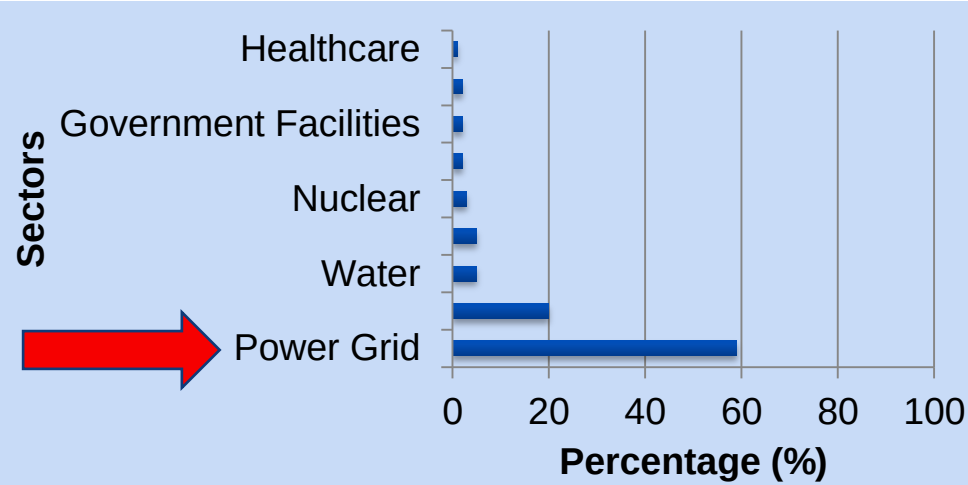
Department of Communication Networks

KTH Royal Institute of Technology

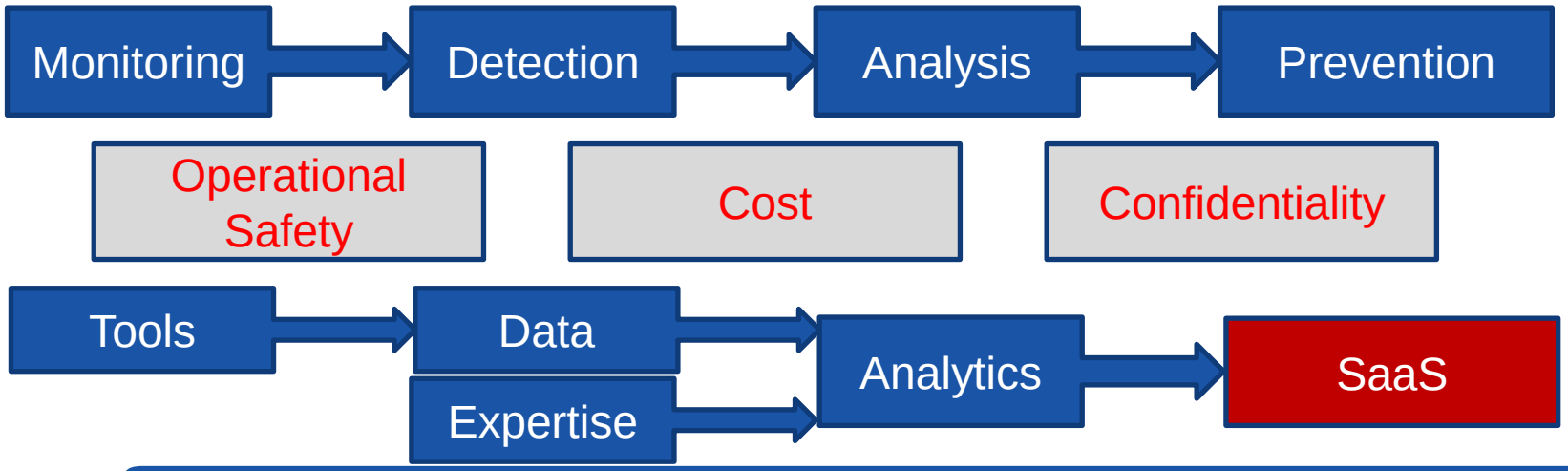


Security Monitoring is Essential

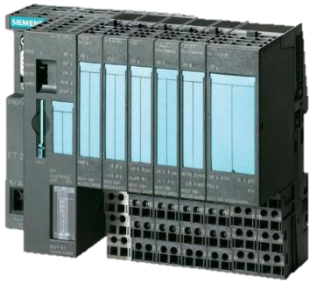




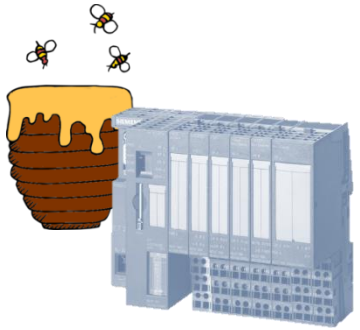
ICS-Cert



Solution - PLC honeypot and gateway



- Programmable Logic Controller (PLC)
  - Networked device for industrial control with guaranteed real-time responses
  - Widely used for substation automation



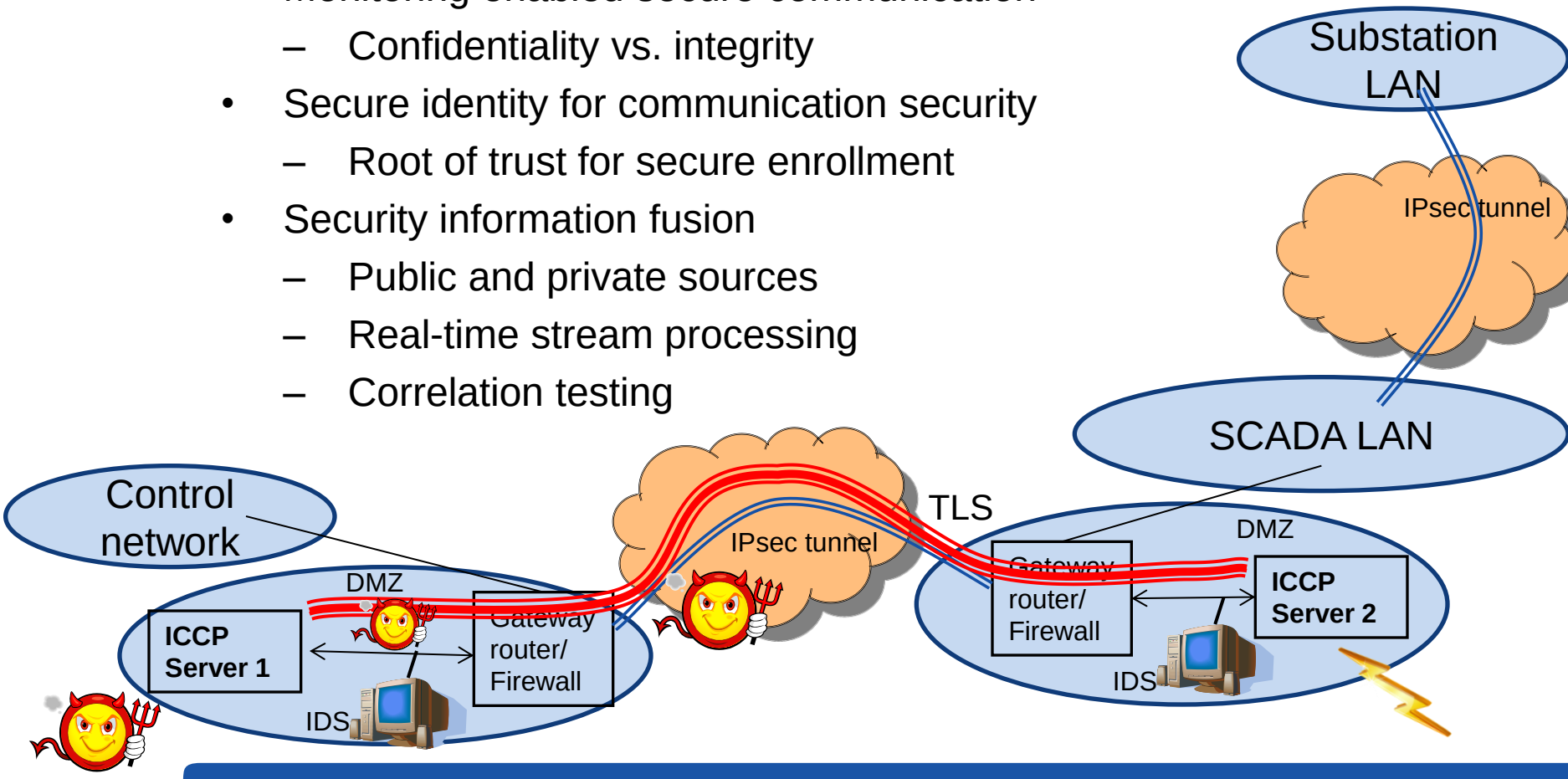
- Honeypot
  - Act as real system toward attacker
  - Log attacker activity to observe strategy

- Monitoring Framework
  - Monitor and manage honeypots
  - Log data sanitization for sharing

- Gateway for redirection to honeypot

Solution - Architecture and Data Sharing

- Monitoring enabled secure communication
  - Confidentiality vs. integrity
- Secure identity for communication security
  - Root of trust for secure enrollment
- Security information fusion
  - Public and private sources
  - Real-time stream processing
  - Correlation testing



Security Monitoring as a Service for Critical Infrastructures

György Dán

Department of Communication Networks

KTH Royal Institute of Technology