IARIA

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CRITICAL INFRASTRUCTURE PROTECTION – NOVEL CONCEPTS AND TECHNOLOGIES

SECURWARE – Special Track CIP-NCT

Stefan Schauer, AIT Austrian Institute of Technology, stefan.schauer@ait.ac.at
Martin Latzenhofer, AIT Austrian Institute of Technology, martin.latzenhofer@ait.ac.at

SECURWARE 2020: The Thirteenth International Conference on Emerging Security Information, Systems and Technologies (IARIA)
Valencia, November 23-26, 2020

STEFAN SCHAUER

Education and Training

- University of Klagenfurt, Computer Science, Graduate Engineer
- ETH Zürich, Computer Science, semester abroad
- Technical University Vienna, Theoretical Physics, PhD

Work Experience

- AIT, Senior Scientist, project management, research
- External lecturer at University of Vienna and University of Klagenfurt

Certificates

- Project Management IPMA-Level D, Certified Information Security Manager

MARTIN LATZENHOFER

Education and Training

- Polytechnic Highschool Vienna 22, Electronic Data Processing and Organization
- University of Stockholm, Computer and Systems Sciences, semester abroad
- University of Vienna, Business Informatics, Master’s degree

Work Experience

- T-Mobile Austria, mobile telecommunication, IT security management
- KPMG Austria, public accounting, ICT audits and consulting
- ACP IT Solutions, IT solution provider, IT service management
- ITSM Partner Consulting, consulting and training
- AIT, Senior Research Engineer, project management, research
- External lecturer at University of Vienna, Remote University of Applied Studies Vienna

Certificates

- ITIL Expert, CISA, CISM, CRISC, CIPM, Certified Information Security Manager

RESEARCH INTERESTS
S. SCHAUER & M. LATZENHOFER

Risk Management for Critical Infrastructure Protection

- Hybrid Risk Management approach provides a holistic view on critical infrastructures
- Large-scale cascading effects can arise from inherent interdependencies
- Complex simulation approaches, mathematical approaches
  (stochastic distribution, propagation, game theory, etc.)
- Critical infrastructures require a comprehensive view on physical and cyber domain

Cybersecurity

- Novel concepts of perimeter security, ICT interrelating with cyber physical systems
- Attack forms involving the human factor, processes, social aspects
- Interdependencies on digitalization, evolution of internet of things (IoT)
- Communication structures in federal crisis management

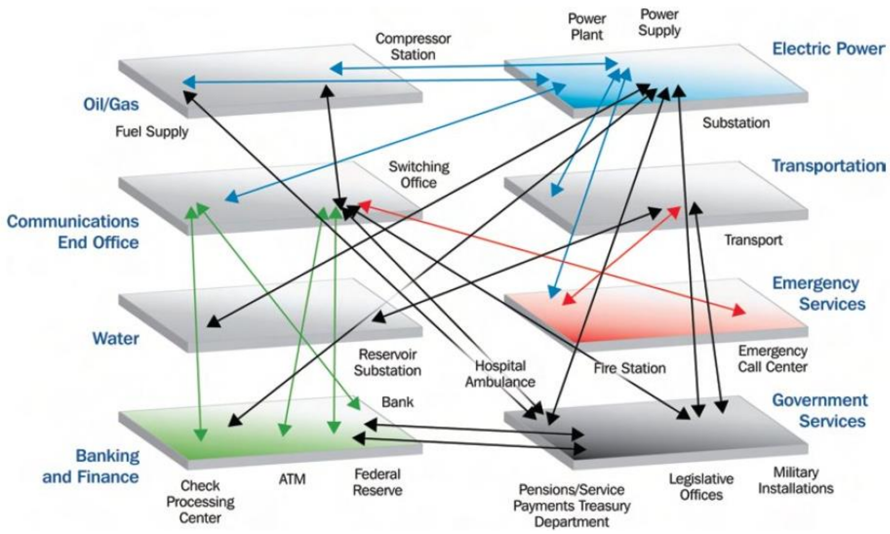
Automotive Security

- Reference architecture for cooperative intelligent transport systems (C-ITS)
- Infrastructure’s perspective, risk management methodologies, legal aspects

CIP-NCT INTRODUCTION

- Critical infrastructures (CIs) and in particular utility networks represent a backbone of todays society

- Utility providers have become a major target of hackers, cyber criminals and cyber terrorists
  - Targeted attacks
    Hacking and shutdown of Ukrainian Power Grid (2015 & 2016)
    Operation Dust Storm on critical infrastructures in Japan (2016)
  - Infection with ransomware
    Hundred thousand of infected systems by WannaCry and (Not-)Petya (2017)
    Power providers, hospitals and supply chains have been disrupted
  - Ongoing social engineering and phishing attempts

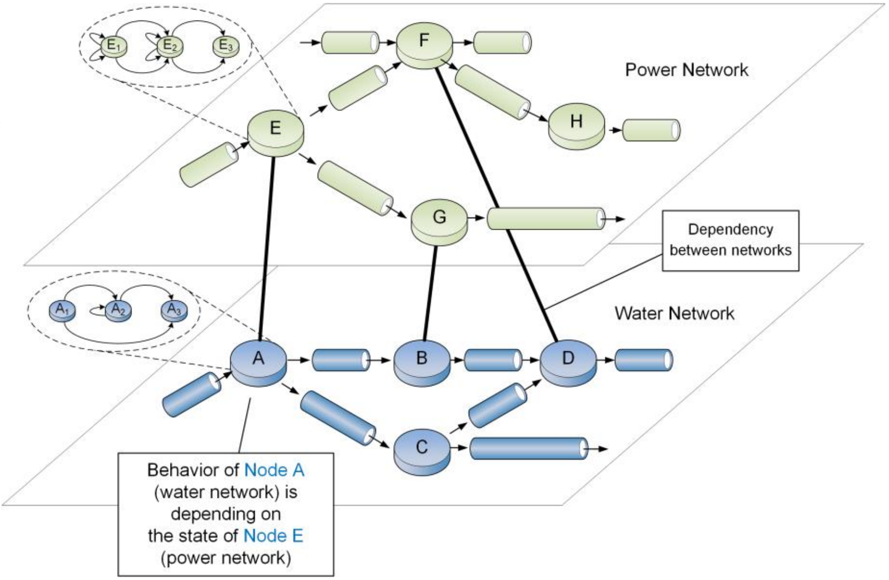


Source: Department of Homeland Security, National Infrastructure Protection Plan

CIP-NCT INTRODUCTION

- Novel approaches towards risk management are required to identify and assess potential consequences of these attacks

- Focus shifts towards a cross-domain simulation framework
  - Parallel simulation of different infrastructure networks
  - One network is influenced by the state of (components of) other infrastructure networks



Dependency between networks

Behavior of Node A (water network) is depending on the state of Node E (power network)

- Highly complex nature of infrastructure networks requires
  - Detailed overview on the information flow among infrastructure assets
  - Adaptive and comprehensive representation of analysis data and results

CIP-NCT CONTENT PAPERS

„An Information Flow Modelling Approach for Critical Infrastructure Simulation“
*Denise Gall, **Christian Luidold**, Gregor Langner,*
Thomas Schaberreiter, Gerald Quirchmayr

This paper provides an innovative approach for conceptualization and implementation of an information flow model as a foundation for the subsequent development of a multi-layered risk model

„A Gap Analysis of Visual and Functional Requirements
in Cybersecurity Monitoring Tools “
***Christian Luidold**, Thomas Schaberreiter*

The second paper conduct a trend analysis of latest research contributions in terms of visualization techniques and functional requirements compared to current state-of-the-art research

THANK YOU!

Stefan Schauer

Martin Latzenhofer

November 23-26, 2020