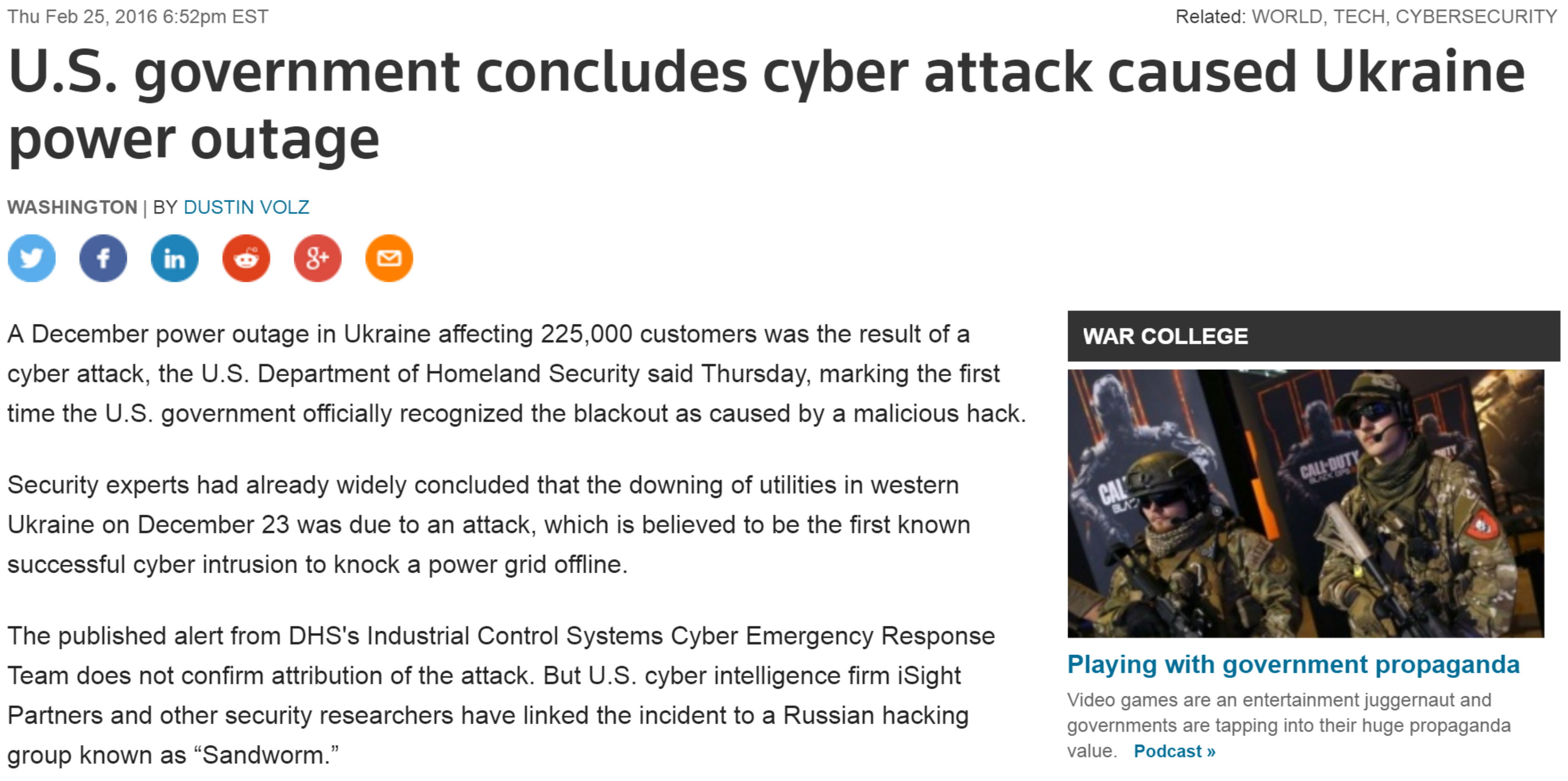
Kritische Infrastrukturen vor Cyber-Bedrohungen schützen

Ralph Langner ▪ Langner Communications GmbH

Cyber-physische Angriffe sind nicht dasselbe wie «Hacking».

Sie werden von Technikern und nicht von «Hackern» geplant und ausgeführt.

Beispiel #1: Angriff auf ukrainisches Energievesorgungsnetz



Thu Feb 25, 2016 6:52pm EST

Related: WORLD, TECH, CYBERSECURITY

U.S. government concludes cyber attack caused Ukraine power outage

WASHINGTON | BY DUSTIN VOLZ

A December power outage in Ukraine affecting 225,000 customers was the result of a cyber attack, the U.S. Department of Homeland Security said Thursday, marking the first time the U.S. government officially recognized the blackout as caused by a malicious hack.

Security experts had already widely concluded that the downing of utilities in western Ukraine on December 23 was due to an attack, which is believed to be the first known successful cyber intrusion to knock a power grid offline.

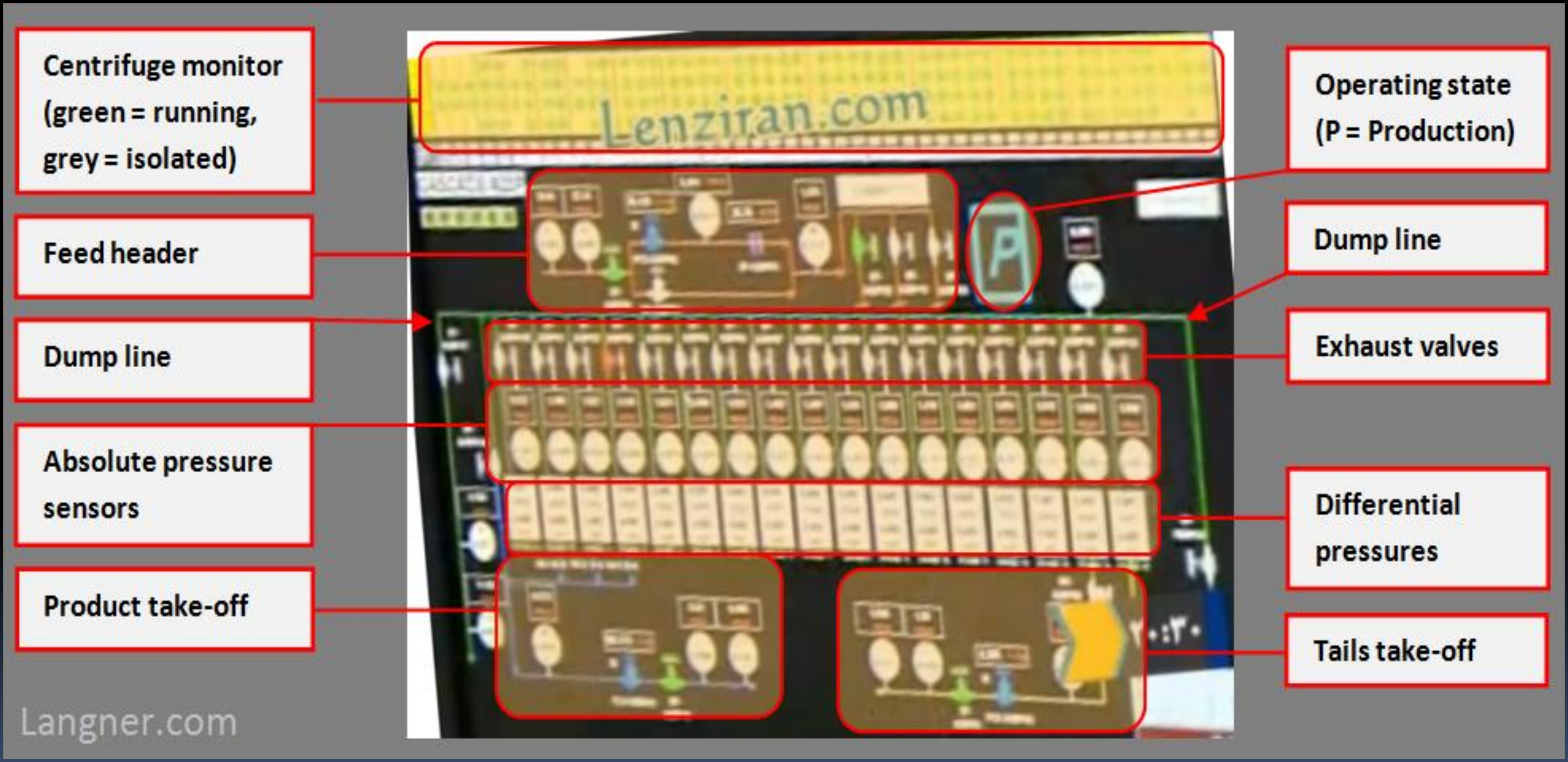
The published alert from DHS's Industrial Control Systems Cyber Emergency Response Team does not confirm attribution of the attack. But U.S. cyber intelligence firm iSight Partners and other security researchers have linked the incident to a Russian hacking group known as "Sandworm."

WAR COLLEGE

Playing with government propaganda

Video games are an entertainment juggernaut and governments are tapping into their huge propaganda value. **Podcast »**

Beispiel #2: Stuxnet



Quelle: To kill a centrifuge (http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf)

Bei cyber-physischen Angriffen geht es um schadhafte Manipulationen.

Möglichkeiten für schadhafte Manipulationen und ihre Auswirkungen können analysiert werden.

Machen wir dies zu einer Forschungsannahme:

Fokus: Cyber-physische Angriffe auf kritische Infrastrukutren mit <u>inakzeptablen Auswirkungen auf die nationale Sicherheit</u>

Axiom: Es gibt nur eine sehr beschränkte Anzahl von entsprechenden *strukturellen Verwundbarkeiten.*

Nutzen: Heuristische Methoden zur Erkennung dieser strukturellen Verwundbarkeiten sind grundlegend für Angriff und Verteidigung.

Problembeispiel #1

Grossflächiger Stromausfall

Unterproblem #1

Wie viele Unterwerke sind kritisch?

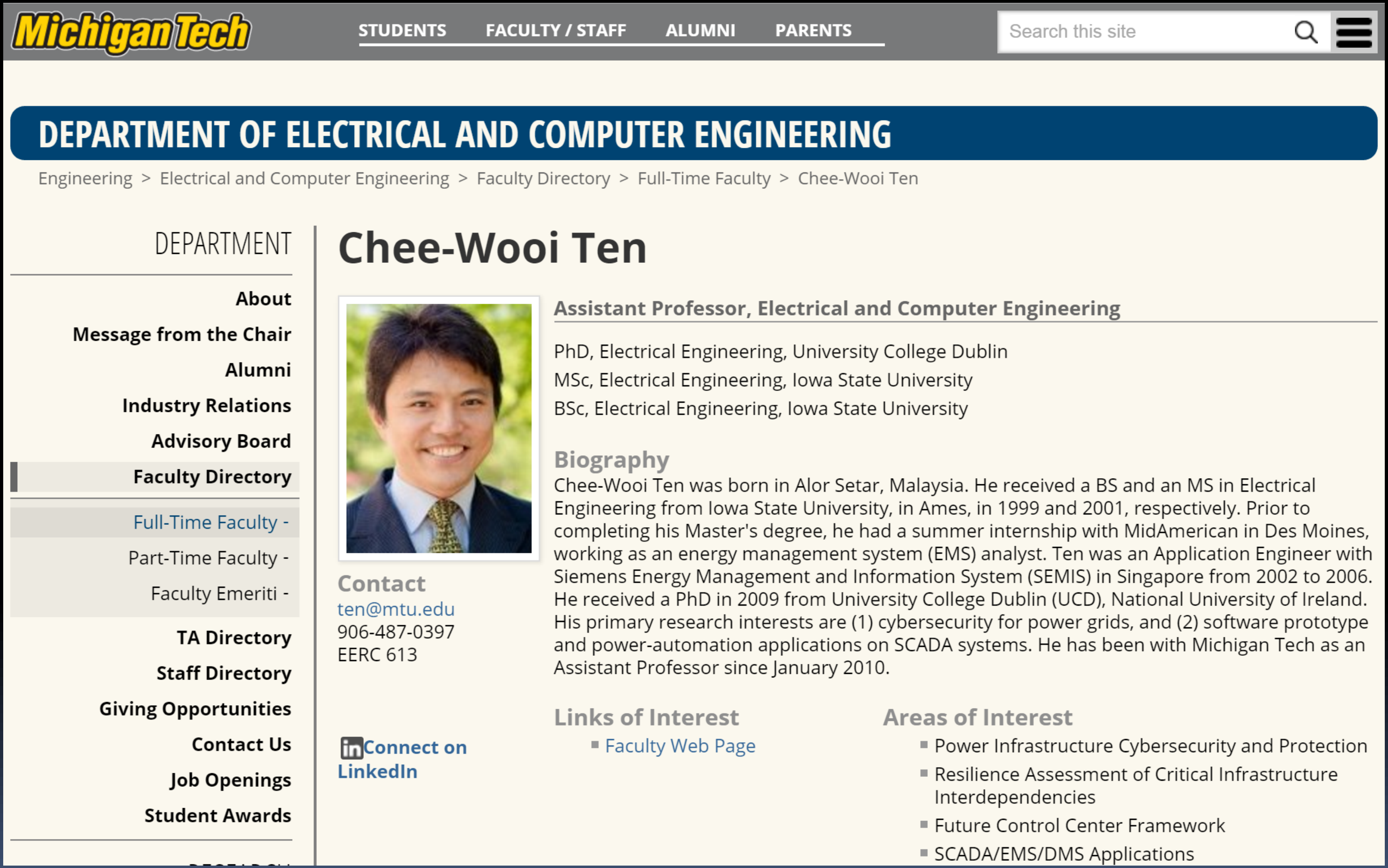
Unterproblem #2

Welches sind diese kritischen Unterwerke?

Unterproblem #3

Wie können Cyber-Angreifer einen langfristigen Unterbruch verursachen?

Laufende Forschung zu diesem Thema von Chee-Wooi Ten



DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Engineering > Electrical and Computer Engineering > Faculty Directory > Full-Time Faculty > Chee-Wooi Ten

Chee-Wooi Ten

Assistant Professor, Electrical and Computer Engineering

PhD, Electrical Engineering, University College Dublin
MSc, Electrical Engineering, Iowa State University
BSc, Electrical Engineering, Iowa State University

Contact
ten@mtu.edu
906-487-0397
EERC 613

Connect on LinkedIn

Biography

Chee-Wooi Ten was born in Alor Setar, Malaysia. He received a BS and an MS in Electrical Engineering from Iowa State University, in Ames, in 1999 and 2001, respectively. Prior to completing his Master's degree, he had a summer internship with MidAmerican in Des Moines, working as an energy management system (EMS) analyst. Ten was an Application Engineer with Siemens Energy Management and Information System (SEMIS) in Singapore from 2002 to 2006. He received a PhD in 2009 from University College Dublin (UCD), National University of Ireland. His primary research interests are (1) cybersecurity for power grids, and (2) software prototype and power-automation applications on SCADA systems. He has been with Michigan Tech as an Assistant Professor since January 2010.

Links of Interest

- Faculty Web Page

Areas of Interest

- Power Infrastructure Cybersecurity and Protection
- Resilience Assessment of Critical Infrastructure Interdependencies
- Future Control Center Framework
- SCADA/EMS/DMS Applications

Problembeispiel #2

Zivilisten töten / Umweltkatastrophe verursachen

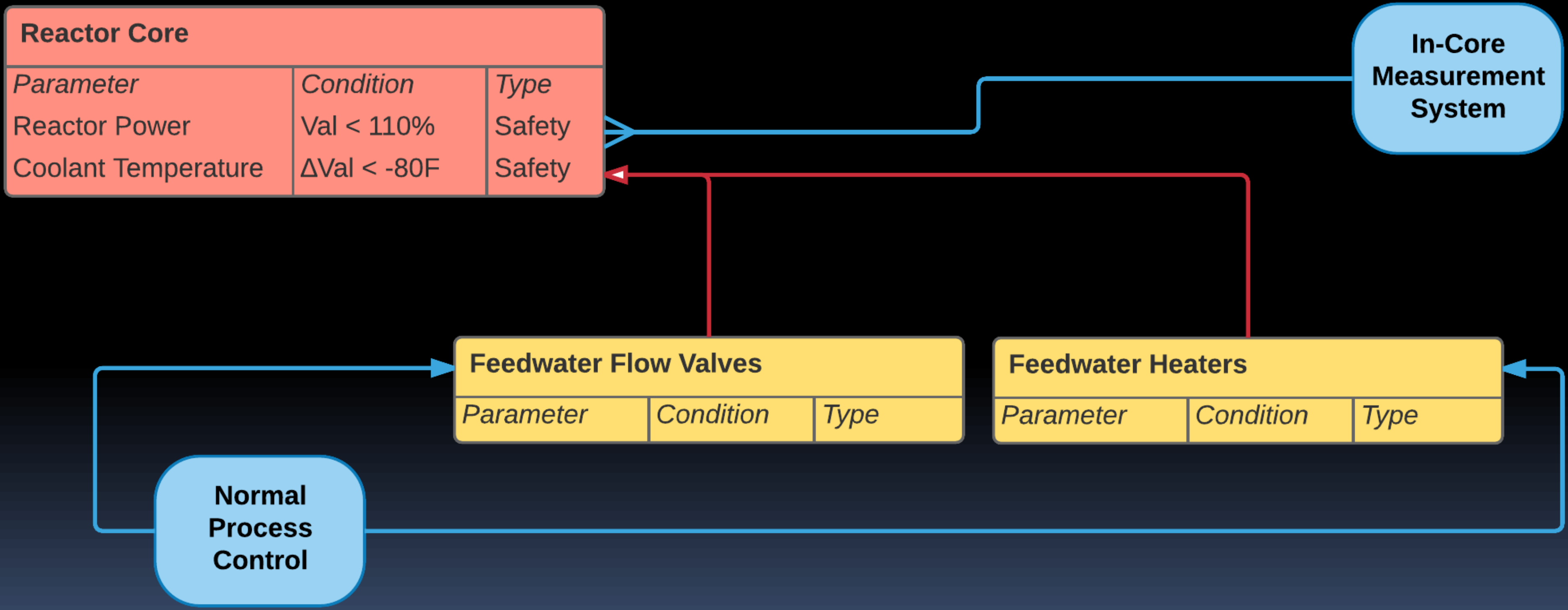
Szenario 1

Digitale Sicherheitssysteme beeinträchtigen

Szenario 2

(Digitale oder analoge) Sicherheitssysteme umgehen

Beispiel Nuklearsicherheit:
Durch Umgehen der Grundannahmen des Sicherheitssystems einen nuklearen Unfall verursachen



Reactor Core

Parameter	*Condition*	*Type*
Reactor Power	Val < 110%	Safety
Coolant Temperature	ΔVal < -80F	Safety

In-Core Measurement System

Feedwater Flow Valves

Parameter	*Condition*	*Type*

Feedwater Heaters

Parameter	*Condition*	*Type*

Normal Process Control

F&A

Langner Communications GmbH

www.langner.com ▪ info@langner.com
Tel +49-40-6090110