

# Protecting critical infrastructure against cyber threats

Ralph Langner ▪ Langner Communications GmbH

Langner

Cyber-physical attacks are not „hacking“

They are planned and executed
by engineers, not by „hackers“

Langner

# Example #1: Ukrainean power grid attack

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.”

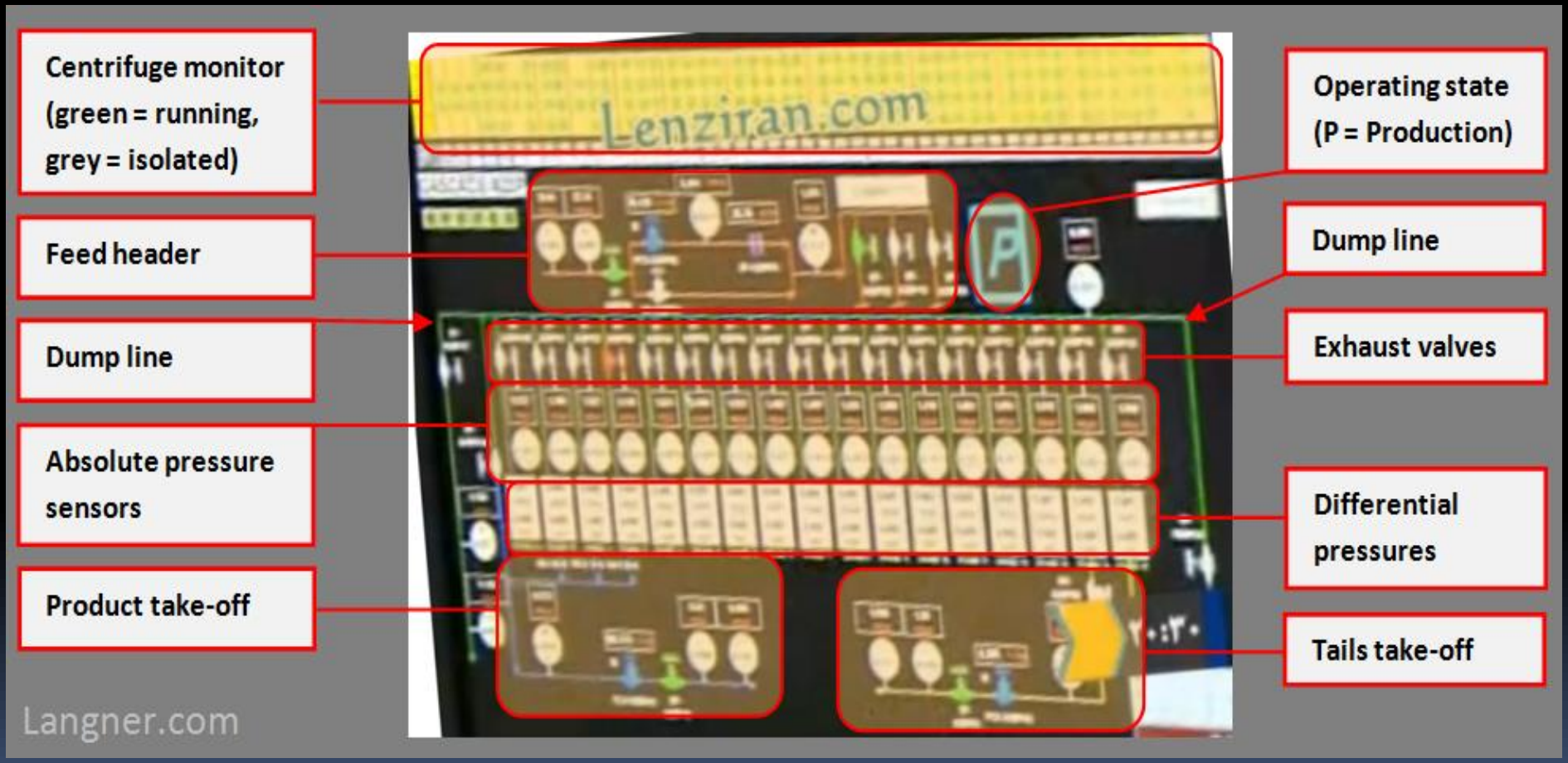
**WAR COLLEGE**

**Playing with government propaganda**

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

Langner

# Example #2: Stuxnet




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

Langner

Cyber-physical attacks are about malicious control

Opportunities for and impacts of malicious control can be analysed

Langner

Let‘s turn this into a research proposition

Focus: Cyber-physical attacks on critical infrastructure with unacceptable impact on national security

Axiom: There is only a very limited number of relevant *structural vulnerabilities*

Benefit: Heuristics to discover those structural vulnerabilities are essential for offense and defense

Langner

Sample problem #1

# Large-scale electric power outage

Sub-problem #1

How many substations are critical?

Sub-problem #2

Which are those substations?

Sub-problem #3

How can a cyber attacker cause long-term disruption?

Langner

# Existing research on the topic by Chee-Wooi Ten

Michigan Tech | STUDENTS | FACULTY / STAFF | ALUMNI | PARENTS | Search this site

## DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

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

DEPARTMENT

- About
- Message from the Chair
- Alumni
- Industry Relations
- Advisory Board
- Faculty Directory
  - Full-Time Faculty -
  - Part-Time Faculty -
  - Faculty Emeriti -
- TA Directory
- Staff Directory
- Giving Opportunities
- Contact Us
- Job Openings
- Student Awards

# 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

### 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.

### Contact

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

Connect on LinkedIn

### 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

Langner

Sample problem #2

# Killing civilians / creating environmental disaster

Scenario 1

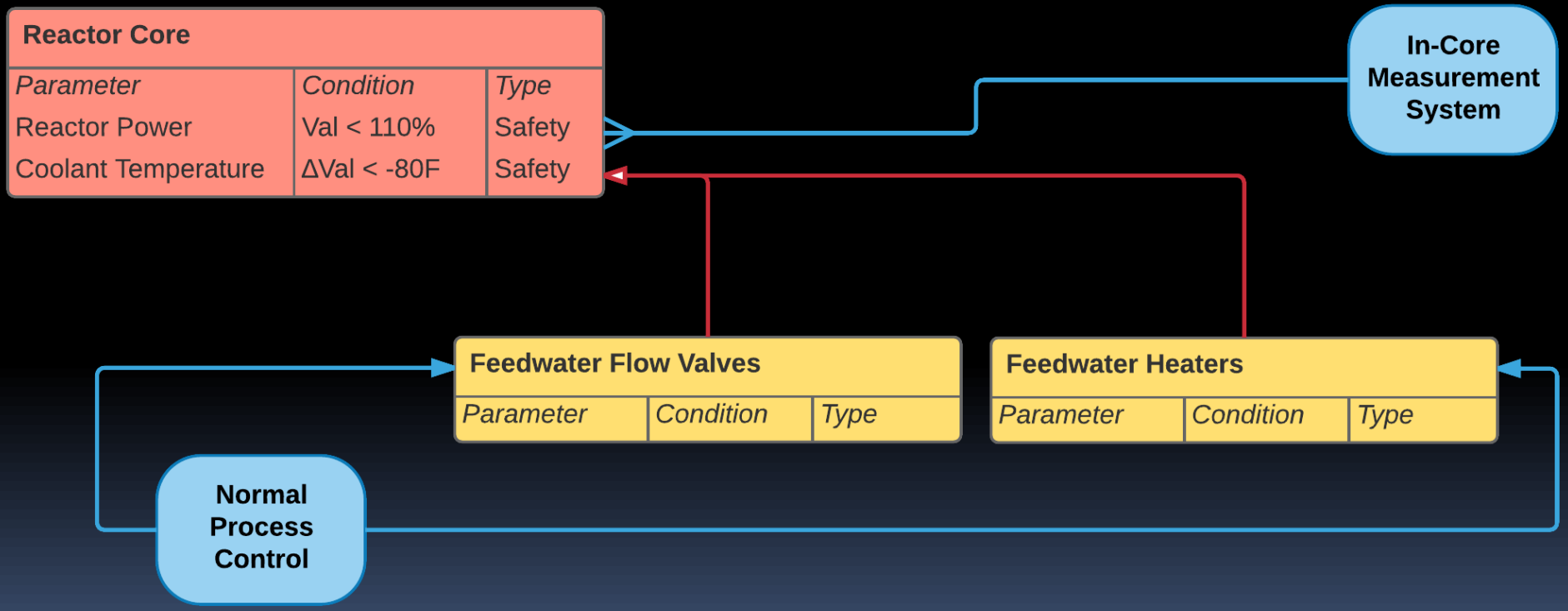
# Compromise digital safety systems

Scenario 2

# Circumvent (digital or analog) safety systems

Langner

# Nuclear safety example:
# Causing a nuclear reactivity accident by circumventing the safety systems‘s design basis assumptions




Langner

# Q&A

**Langner Communications GmbH**

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