Virtual Testbed for Smart Grid Cybersecurity Experiments & Training

PRESENTED BY

Daisuke Mashima

Principal Research Scientist at Illinois at Singapore Pte Ltd

This research is supported in part by the National Research Foundation, Singapore, Singapore University of Technology and Design under its National Satellite of Excellence in Design Science and Technology for Secure Critical Infrastructure Grant (NSoE_DeST-SCI2019-0005) and in part by the National Research Foundation, Singapore (through the National Cybersecurity R&D Lab grant office at the National University of Singapore) via a grant (NCL-2022-01) awarded under the “National Cybersecurity R&D Lab Grant 2021”. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore and the National Cybersecurity R&D Lab grant office at the National University of Singapore.

Outline

1 **What is Smart Grid?**

2 **Cybersecurity Challenges in Smart Grid**

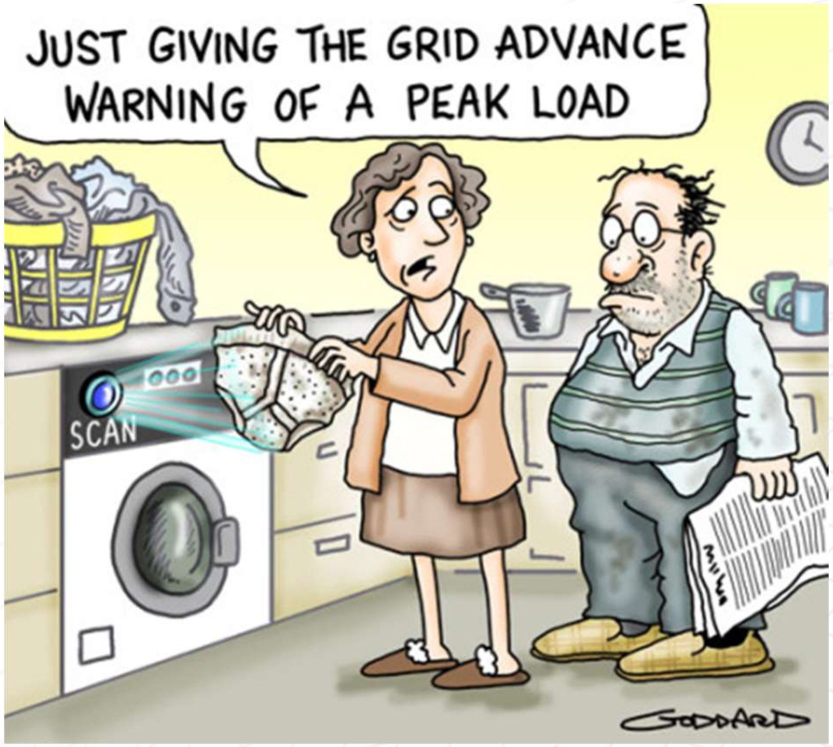
3 **Smart Grid Cyber Security Testbeds**

4 **Smart Grid Cyber Range as a Service (CRaaS)**

What is Smart Grid?

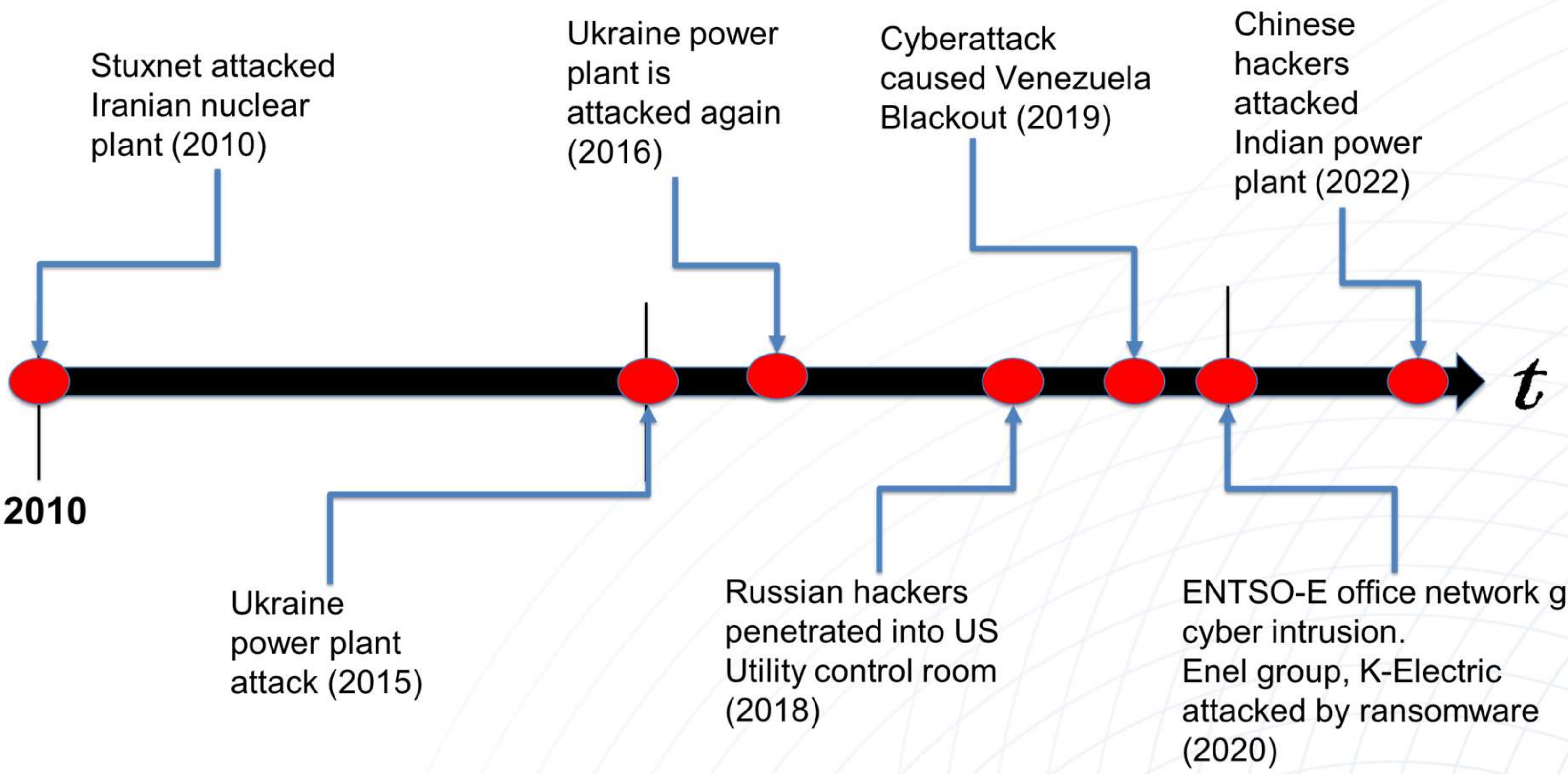
Power Grid enhanced with ICT (Information and Communication Technologies)

- Reliability
- Economics
- Efficiency
- Environmental Friendliness
- Safety
- Security



https://alittlefridaystory.com/2016/01/22/solar-power-a-new-hope/

Smart Grid is Under Attack!



Stuxnet attacked Iranian nuclear plant (2010)

Ukraine power plant attack (2015)

Ukraine power plant is attacked again (2016)

Russian hackers penetrated into US Utility control room (2018)

Cyberattack caused Venezuela Blackout (2019)

ENTSO-E office network got cyber intrusion.
Enel group, K-Electric attacked by ransomware (2020)

Chinese hackers attacked Indian power plant (2022)

Stuxnet Worm (2010)

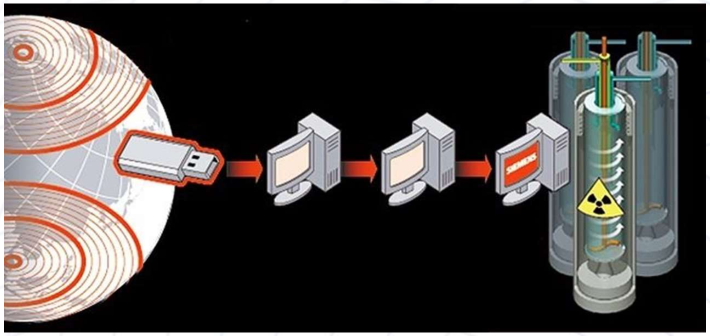
Targeted nuclear plants in Iran

Exploited multiple zero-day vulnerabilities on Windows

Can infect via USB drive

Successfully compromised PLC connected to centrifuge units

Reports fake, apparently normal data to SCADA

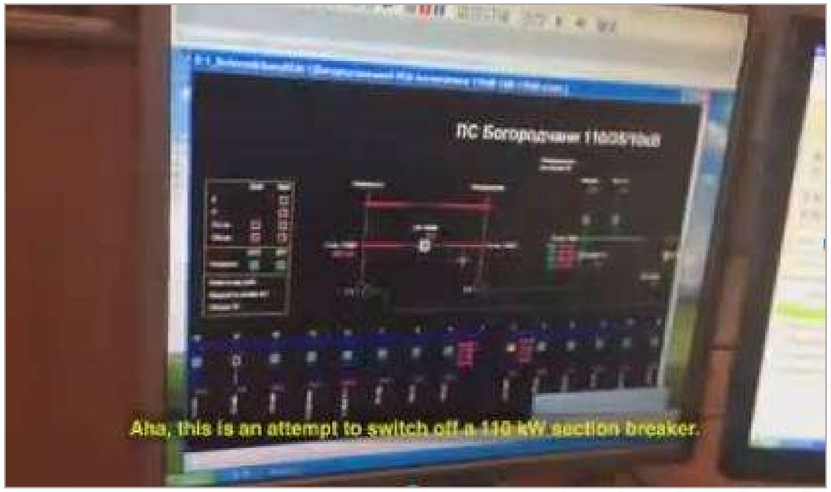


(null-byte.wonderhowto.com)

Ukrainian Power Plant Attack (2015)

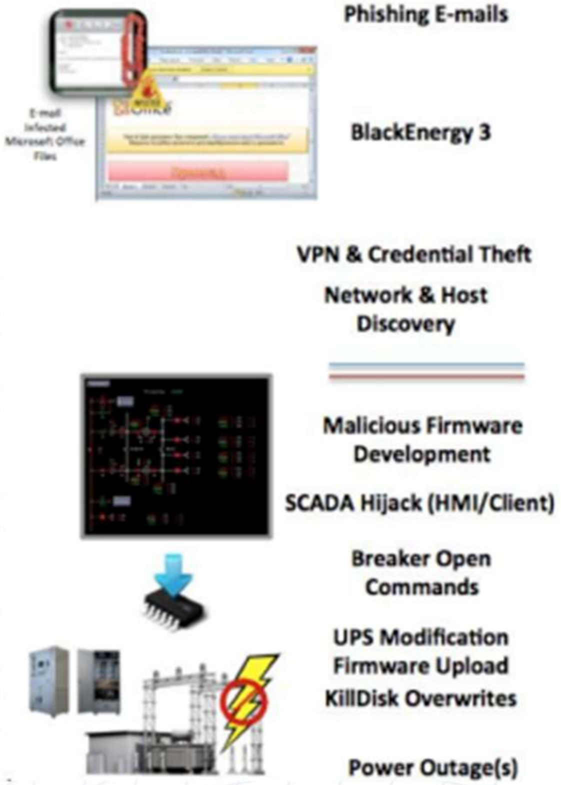
Caused massive power outage in Ukraine

Control system was remotely manipulated!



Aha, this is an attempt to switch off a 110 kW section breaker.

(https://www.youtube.com/watch?v=8ThgK1WXUgk)



Phishing E-mails

BlackEnergy 3

VPN & Credential Theft

Network & Host Discovery

Malicious Firmware Development

SCADA Hijack (HMI/Client)

Breaker Open Commands

UPS Modification
Firmware Upload
KillDisk Overwrites

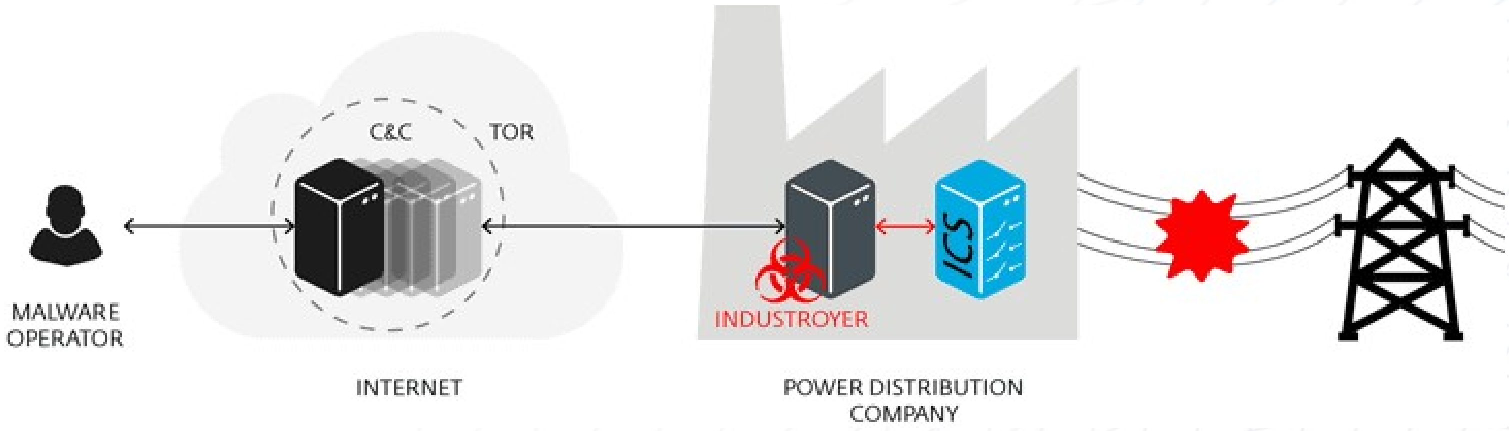
Power Outage(s)

(https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf)

CrashOverride / Industroyer Malware (2016)

Abuses widely-used Industrial Control System protocols, including IEC 60870-5-104 and IED 61850

Capability of issuing valid-looking control commands and measurements



https://gigazine.net/news/20170613-crashoverride/

Aurora Generator Test (2007)

Demonstrated how a cyber-originated attack can damage physical power grid components.

Succeeded in exploding a diesel generator in 3 minutes!

(https://www.youtube.com/watch?v=LM8kLaJ2NDU)

Cybersecurity Solutions to Counter Threats

IEC 62351 (Security standard for smart grid protocols)

Industrial firewall

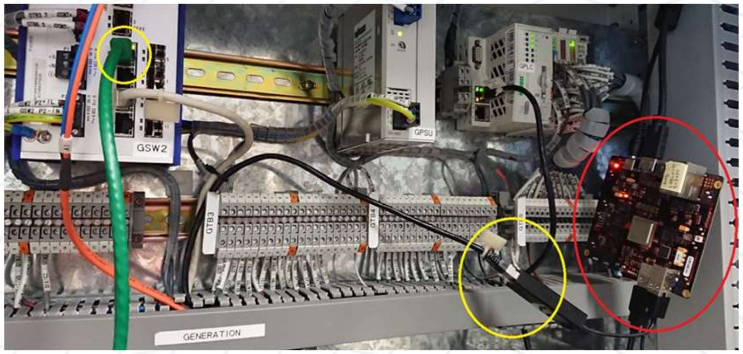
Data Diode

Intrusion Detection Systems

- Signature-based
- Rule-based
- Specification-based
- AI/ML-based
- Physical-based

Bump-in-the-wire (BITW) security appliances

https://www.stengg.com/en/electronics/companies-affiliates/st-electronics-info-security/digisafe-data-diode-solution/



BITW device integrated into EPIC Testbed

How Could We Test / Evaluate?

Industrial firewall is configured appropriately?

How accurate is our intrusion detection system?

Which solution is better for investment?

To what degree is the impact on power grid stability mitigated?

Is the solution compatible with our smart grid infrastructure?

Would the solution affect the performance / availability?

Evaluation in the real system / production environment is NEVER possible!

Hardware-based Testbed?

Testbed using the same hardware as the real system is good for fidelity.

But…

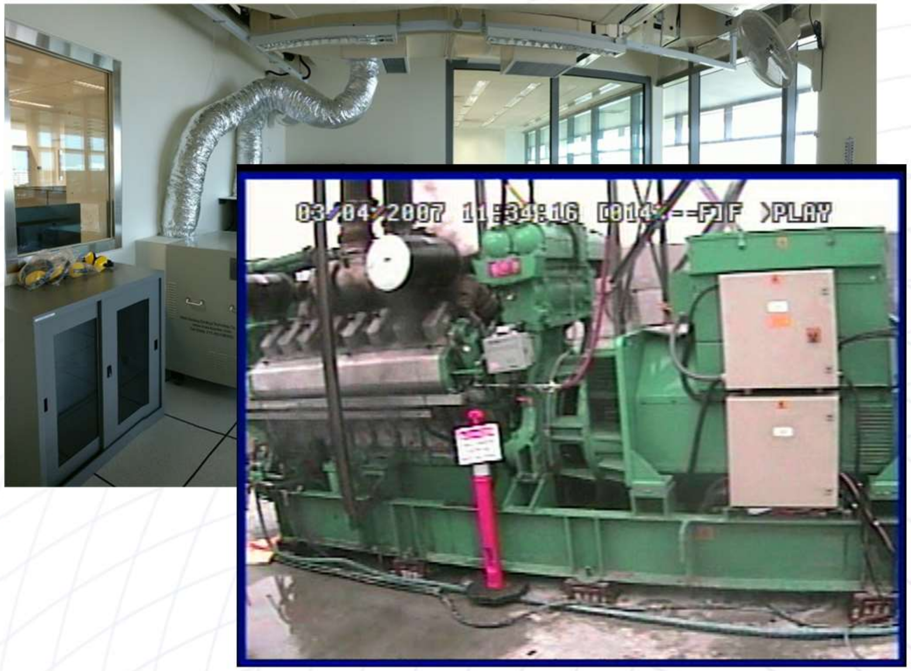
Expensive!

Not configurable or extensible

Not easily accessible

Still has come constraints / restrictions

EPIC Testbed in SUTD
(https://itrust.sutd.edu.sg/testbeds/electric-power-intelligent-control-epic/)



(https://en.wikipedia.org/wiki/Aurora_Generator_Test)

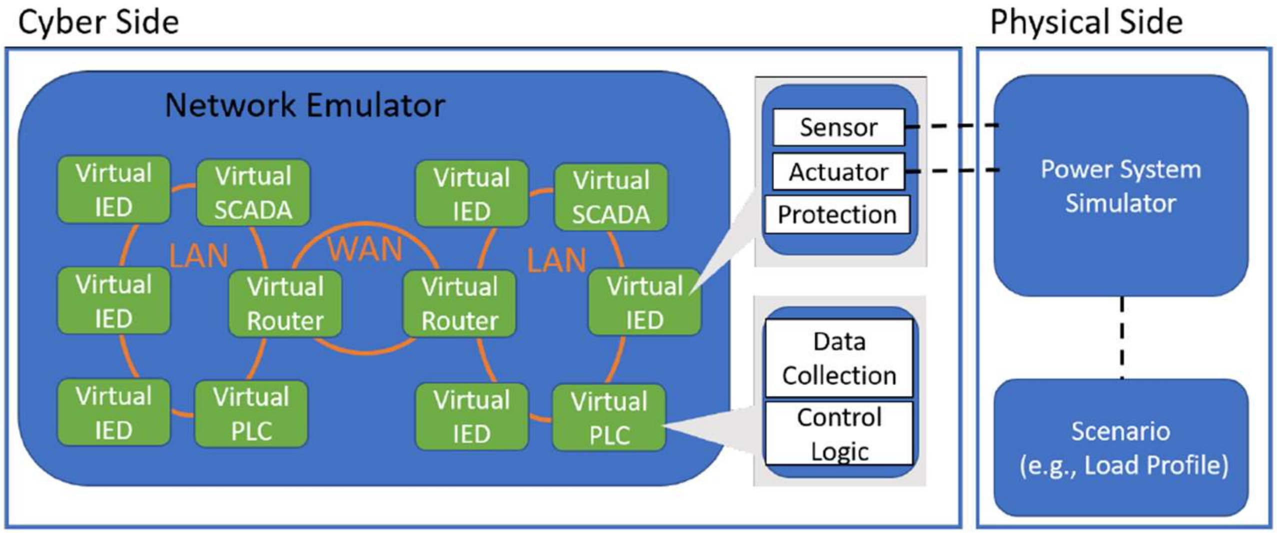
Virtual Testbed (a.k.a Cyber Range)

Emulation of virtual smart grid devices (IEDs, PLCs, SCADA HMI)

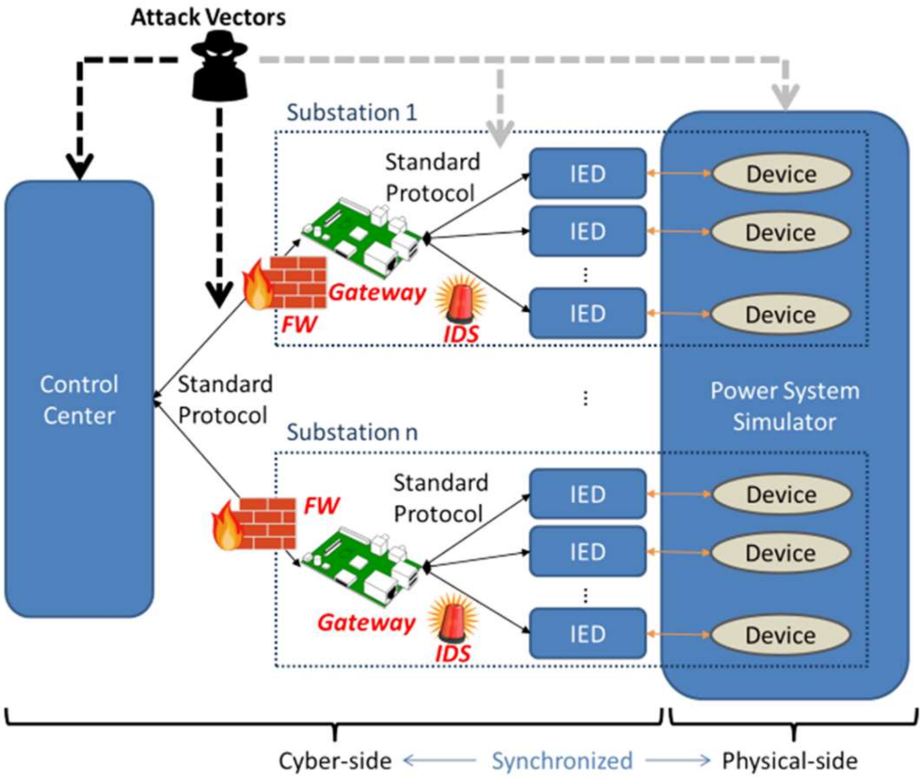
Emulation of cyber network topology

Simulation of physical power system behavior

Configurable, extensible, scalable, and portable



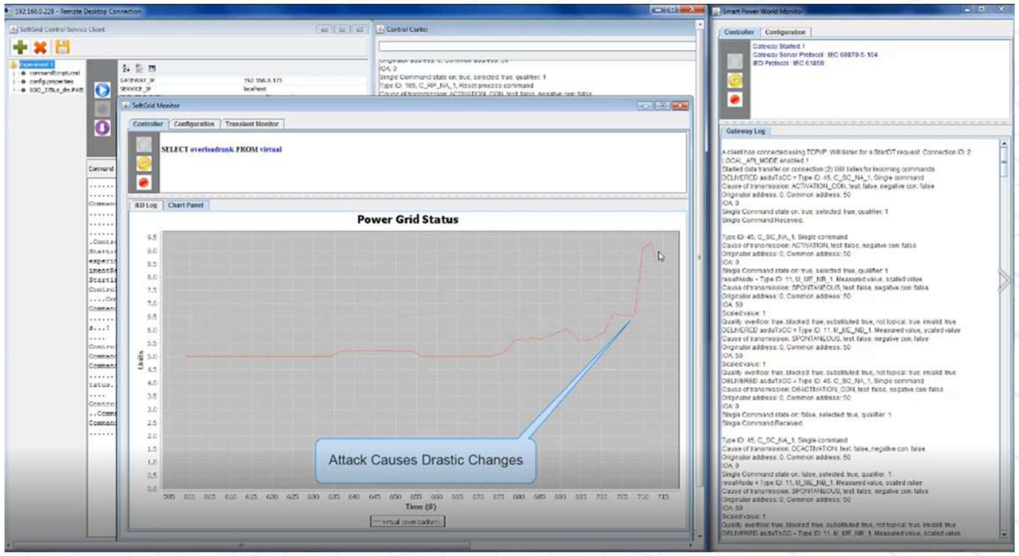
IEC Standard Based Virtual Substation Testbed



(URL: http://www.illinois.adsc.com.sg/softgrid)

SoftGrid (2016)

- Software-based testbed for emulating IEC 61850 based smart grid system.



```
GATEWAY_IP        192.168.0.173
SERVICE_IP        localhost
```

```
IOA: 0
Single Command state on: true, selected: true, qualifier: 1
Type ID: 105, C_RP_NA_1, Reset process command
Cause of transmission: ACTIVATION_CON, test false, negative con: false
```

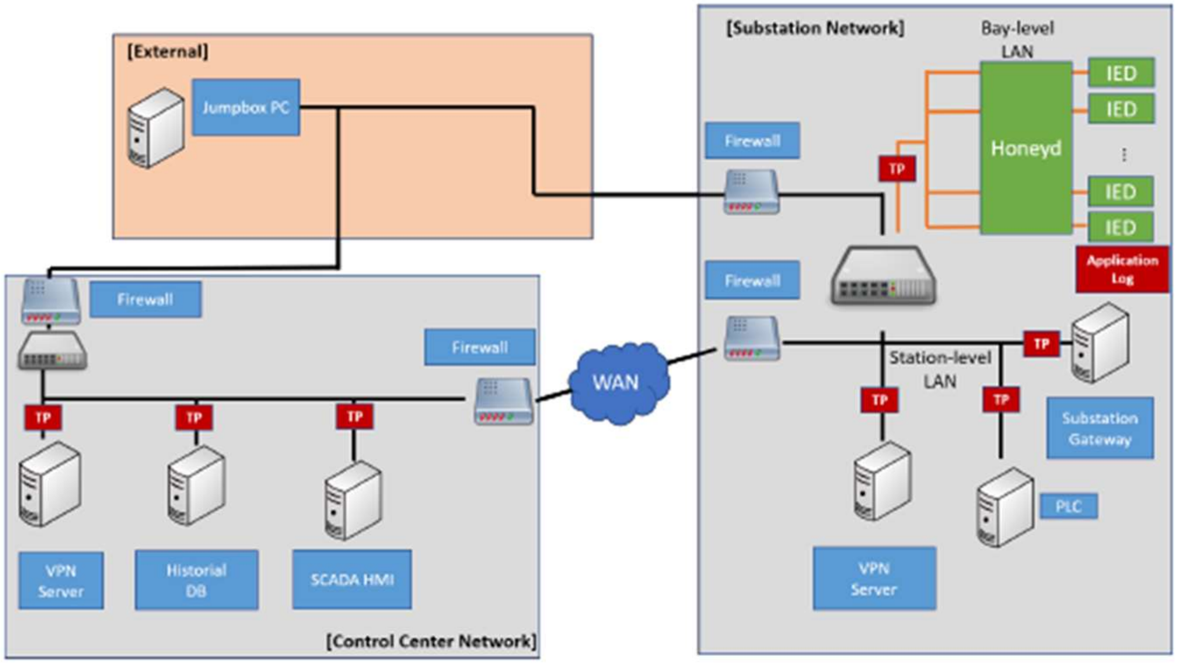
```
SELECT overloadrank FROM virtual
```

Attack Causes Drastic Changes

```
Gateway Started: 1
Gateway Server Protocol : IEC 60870-5-104
IED Protocol : IEC 61850
```

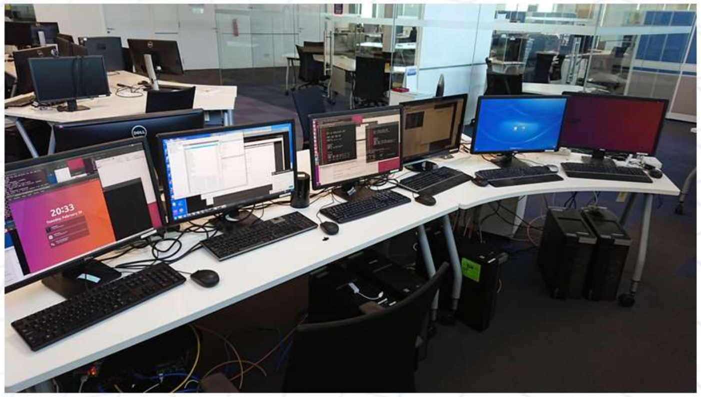
```
A client has connected using TCP/IP. Will listen for a StartDT request. Connection ID: 2
LOCAL_API_MODE enabled 1
Started data transfer on connection (2) Will listen for incoming commands
DELIVERED asduToCC = Type ID: 45, C_SC_NA_1, Single command
Cause of transmission: ACTIVATION_CON, test false, negative con: false
Originator address: 0, Common address: 50
IOA: 0
Single Command state on: true, selected: true, qualifier: 1
Single Command Received.

Type ID: 45, C_SC_NA_1, Single command
Cause of transmission: ACTIVATION, test false, negative con: false
Originator address: 0, Common address: 50
IOA: 0
Single Command state on: true, selected: true, qualifier: 1
resultAsdu = Type ID: 11, M_ME_NB_1, Measured value, scaled value
Cause of transmission: SPONTANEOUS, test false, negative con: false
Originator address: 0, Common address: 50
IOA: 50
Scaled value: 1
Quality: overflow: true, blocked: true, substituted: true, not topical: true, invalid: true
DELIVERED asduToCC = Type ID: 11, M_ME_NB_1, Measured value, scaled value
Cause of transmission: SPONTANEOUS, test false, negative con: false
Originator address: 0, Common address: 50
IOA: 50
Scaled value: 1
Quality: overflow: true, blocked: true, substituted: true, not topical: true, invalid: true
DELIVERED asduToCC = Type ID: 45, C_SC_NA_1, Single command
Cause of transmission: DEACTIVATION_CON, test false, negative con: false
Originator address: 0, Common address: 50
IOA: 0
Single Command state on: false, selected: true, qualifier: 1
Single Command Received.

Type ID: 45, C_SC_NA_1, Single command
Cause of transmission: DEACTIVATION, test false, negative con: false
Originator address: 0, Common address: 50
IOA: 0
Single Command state on: false, selected: true, qualifier: 1
resultAsdu = Type ID: 11, M_ME_NB_1, Measured value, scaled value
Cause of transmission: SPONTANEOUS, test false, negative con: false
Originator address: 0, Common address: 50
IOA: 50
Scaled value: 1
Quality: overflow: true, blocked: true, substituted: true, not topical: true, invalid: true
DELIVERED asduToCC = Type ID: 11, M_ME_NB_1, Measured value, scaled value
```

Comprehensive Smart Grid Cyber Range



Smart Grid Cyber Range (2020)

- Emulates comprehensive model for control center and substation
- Deployable on National Cybersecurity R&D Lab at scale

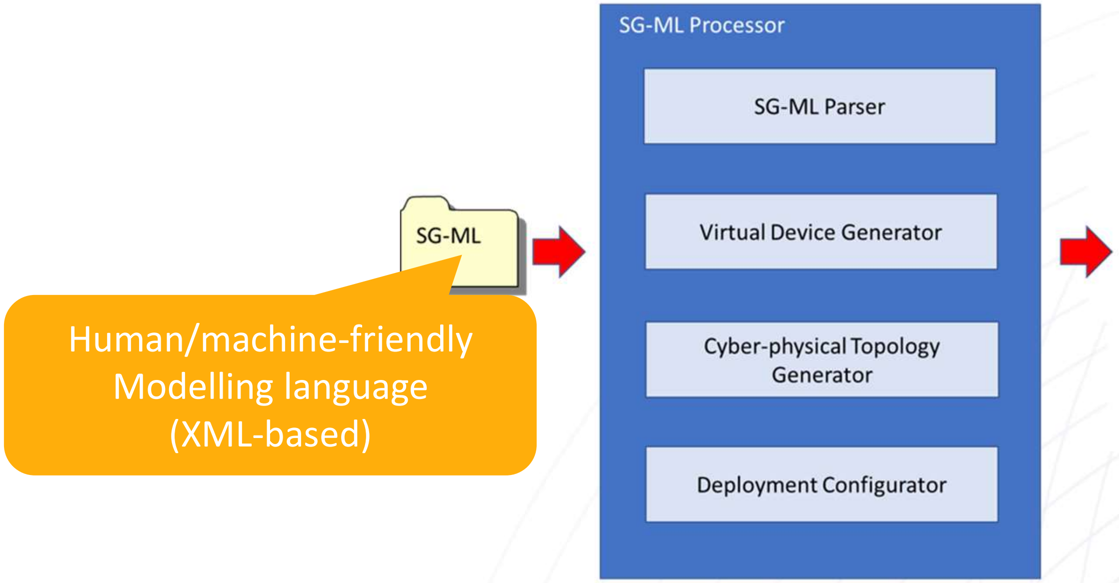


(URL: https://www.illinois.adsc.com.sg/spotify/index.html)

SG-ML: Automated Generation of Smart Grid Cyber Range

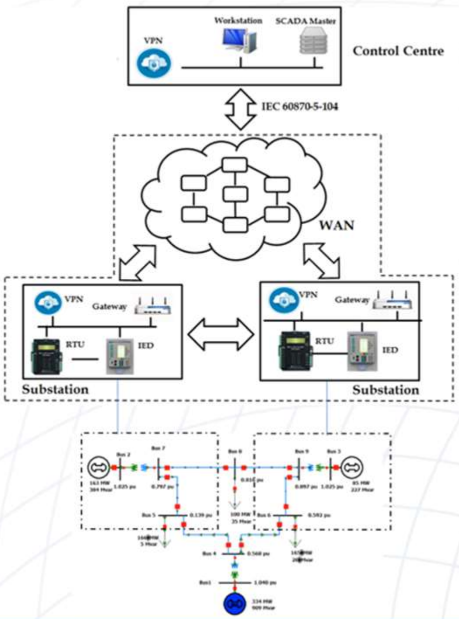
Design and development of cyber range still requires intensive domain knowledge in both cyber and physical sides.

Intensive effort/manpower for implementation and maintenance is needed.



Human/machine-friendly Modelling language (XML-based)

Smart Grid Cyber Physical Range



Daisuke Mashima, Muhammad M. Roomi, Bennet Ng, Zbigniew Kalbarczyk, Suhail Hussain, and Ee-Chien Chang, "Towards Automated Generation of Smart Grid Cyber Range for Cybersecurity Experiments and Training." To appear at DSN 2023 (Industry Track).

Translation to Real-World Usage

Organised by

iTrust Centre for Research in Cyber Security

MINDEF SINGAPORE

Supported by

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE
Research . Innovation . Enterprise

CSA SINGAPORE

National Cybersecurity R&D Laboratory

Organised by

Main Partners

CSA SINGAPORE

iTrust Centre for Research in Cyber Security

National Cybersecurity R&D Laboratory

Technical Partners

ST Engineering

KEYSIGHT

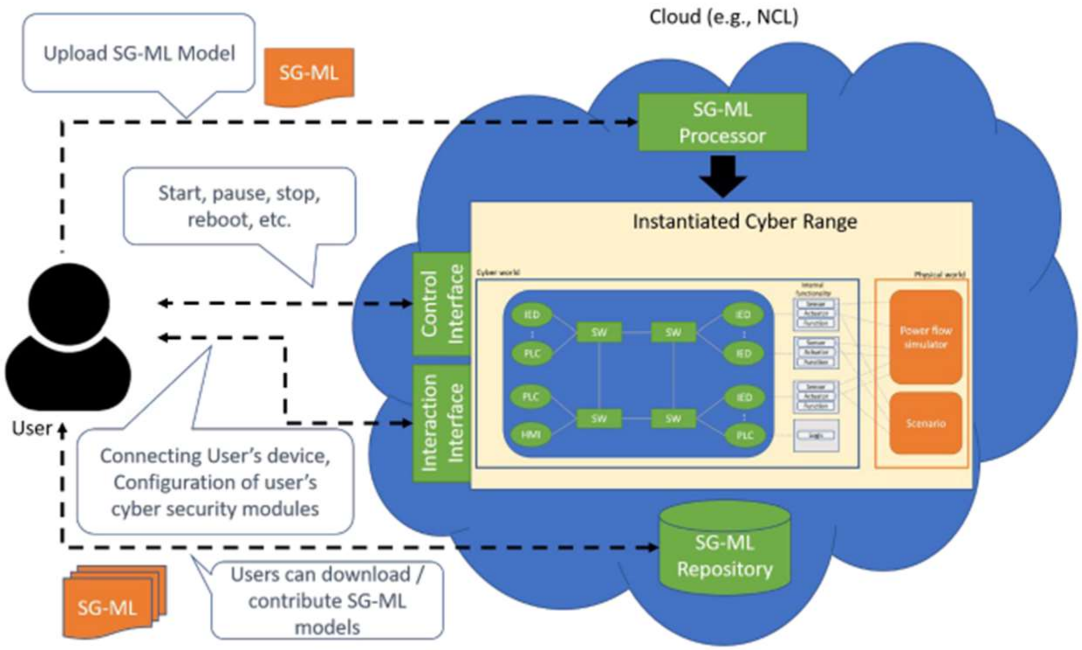
https://itrust.sutd.edu.sg/

Smart Grid Cyber Range as a Service (CRaaS)

Making SG-ML available on the cloud!

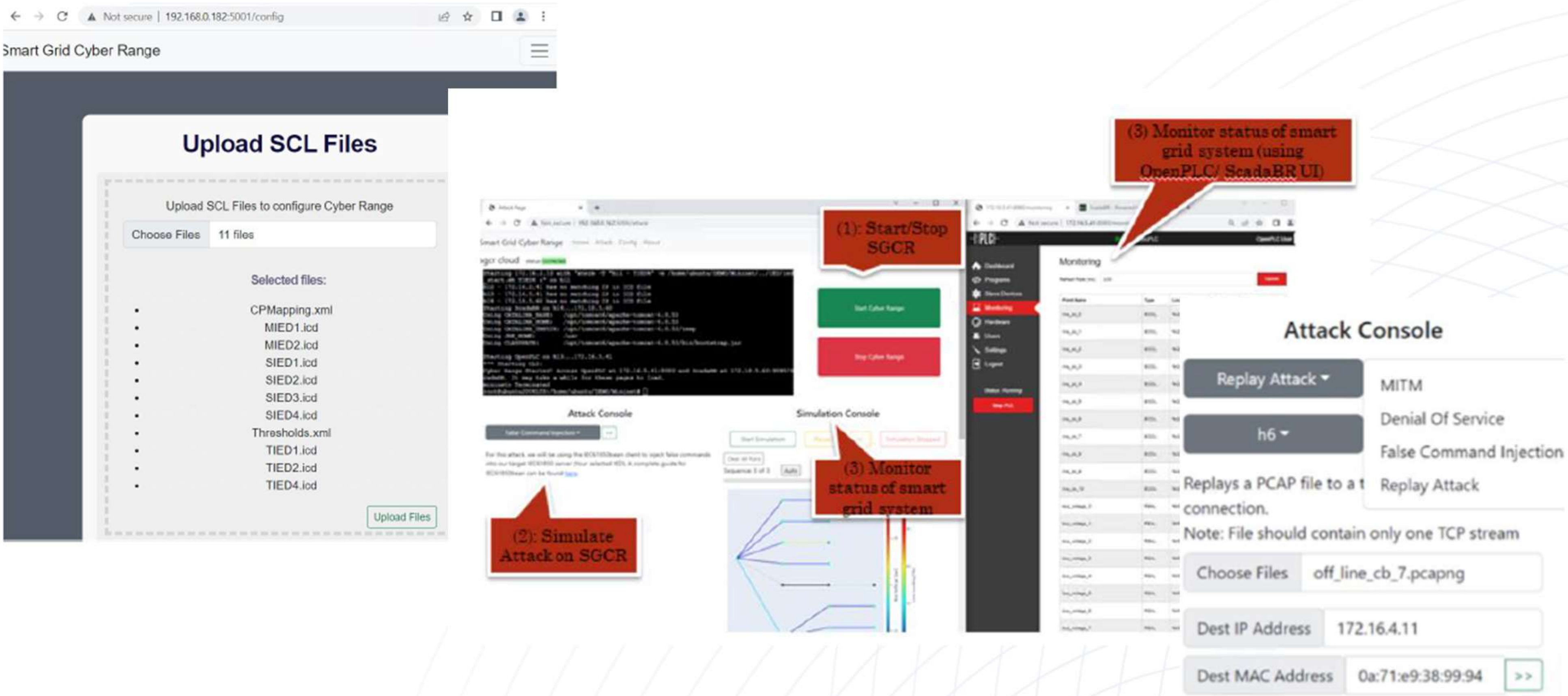
- Remotely accessible/sharable
- Enhanced scalability
- Lower infrastructure cost

To be deployed on OpenStack-based National Cybersecurity R&D Lab (NCL) testbed



This research is supported by the National Research Foundation, Singapore (through the National Cybersecurity R&D Lab grant office at the National University of Singapore) via a grant (NCL-2022-01) awarded under the "National Cybersecurity R&D Lab Grant 2021".

CRaaS Prototype



Not secure | 192.168.0.182:5001/config

Smart Grid Cyber Range

Upload SCL Files

Upload SCL Files to configure Cyber Range

Choose Files 11 files

Selected files:

- CPMapping.xml
- MIED1.icd
- MIED2.icd
- SIED1.icd
- SIED2.icd
- SIED3.icd
- SIED4.icd
- Thresholds.xml
- TIED1.icd
- TIED2.icd
- TIED4.icd

(1): Start/Stop SGCR

(2): Simulate Attack on SGCR

(3) Monitor status of smart grid system

(3) Monitor status of smart grid system (using OpenPLC/ ScadaBR UI)

Attack Console

Replays a PCAP file to a t connection.

Note: File should contain only one TCP stream

Choose Files off_line_cb_7.pcapng

Dest IP Address 172.16.4.11

Dest MAC Address 0a:71:e9:38:99:94

Summary

Virtual testbed for smart grid cybersecurity is valuable not only for academic researchers but also industry players.

Automated generation of cyber range can reduce difficulty of design and development as well as address challenges in terms configurability, extensibility, and accessibility.

Cloud-based, Smart Grid Cyber Range as a Service is on the way!

Contact

Daisuke Mashima (Illinois at Singapore Pte Ltd)

Email: daisuke.m@adsc-create.edu.sg

Web Site: https://www.mashima.us/daisuke

Company Web Site: https://adsc.illinois.edu/