

A dark, atmospheric photograph of a complex network of industrial pipes, ducts, and structural beams, likely representing a physical infrastructure system. The lighting is dramatic, with strong highlights and shadows.

ICS ASIA PACIFIC
SUMMIT 2020
#ICSASIAPACIFIC

STRATEGIES FOR DEFENDING THE CYBER-PHYSICAL BATTLEFIELD

Huang Shao Fei, CISO, Singapore Land Transport Authority
President, Singapore Computer Society Cybersecurity Chapter

SANS | GIAC
CERTIFICATIONS



Protocols

BACnet: 10,530
DNP3: 588
EtherNet/IP: 3,943
Modbus: 13,949
Niagara Fox: 23,294
Niagara Fox with SSL: 159
Siemens S7: 2,701

About

The Shodan search engine has started to crawl the Internet for protocols that provide raw, direct access to industrial control systems (ICS). This visualization shows the location of these industrial control systems on the Internet as well as other related data.

INTRODUCTION

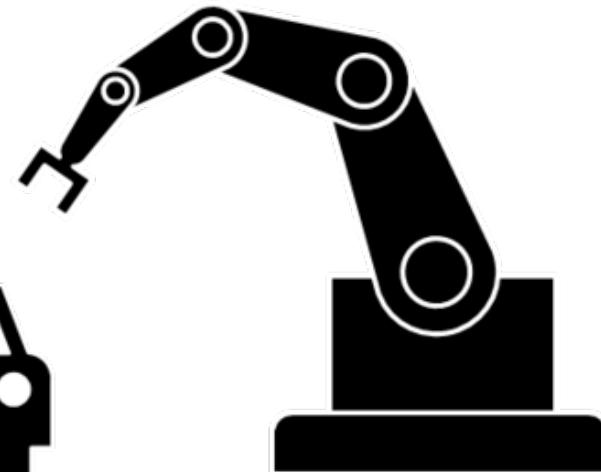
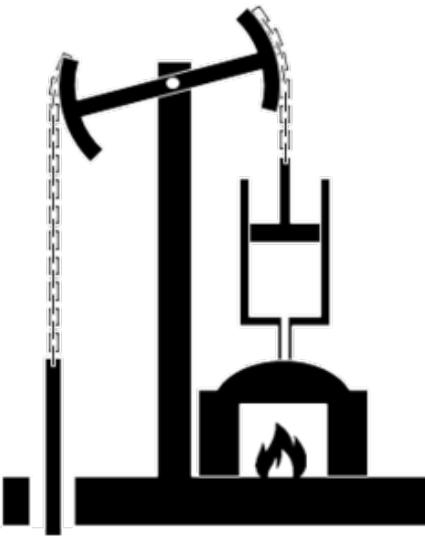
REYKJAVIK

AMSTERDAM

BUCHAREST

SHANGHAI





1st

Mechanization,
water power, steam
power

2nd

Mass production,
assembly line,
electricity

3rd

Computer and
automation

4th

Cyber Physical
Systems



3-5 years
economic lifespan

Standardised systems and
communication protocols

Recovery focuses on data
and system performance

Confidentiality, Integrity & Availability
of Information

Kinetic-Cyber consequences
(critical infrastructure)

Operational impact affecting safety

15-20 years
lifespan

Often outdated, proprietary or special
software and protocols

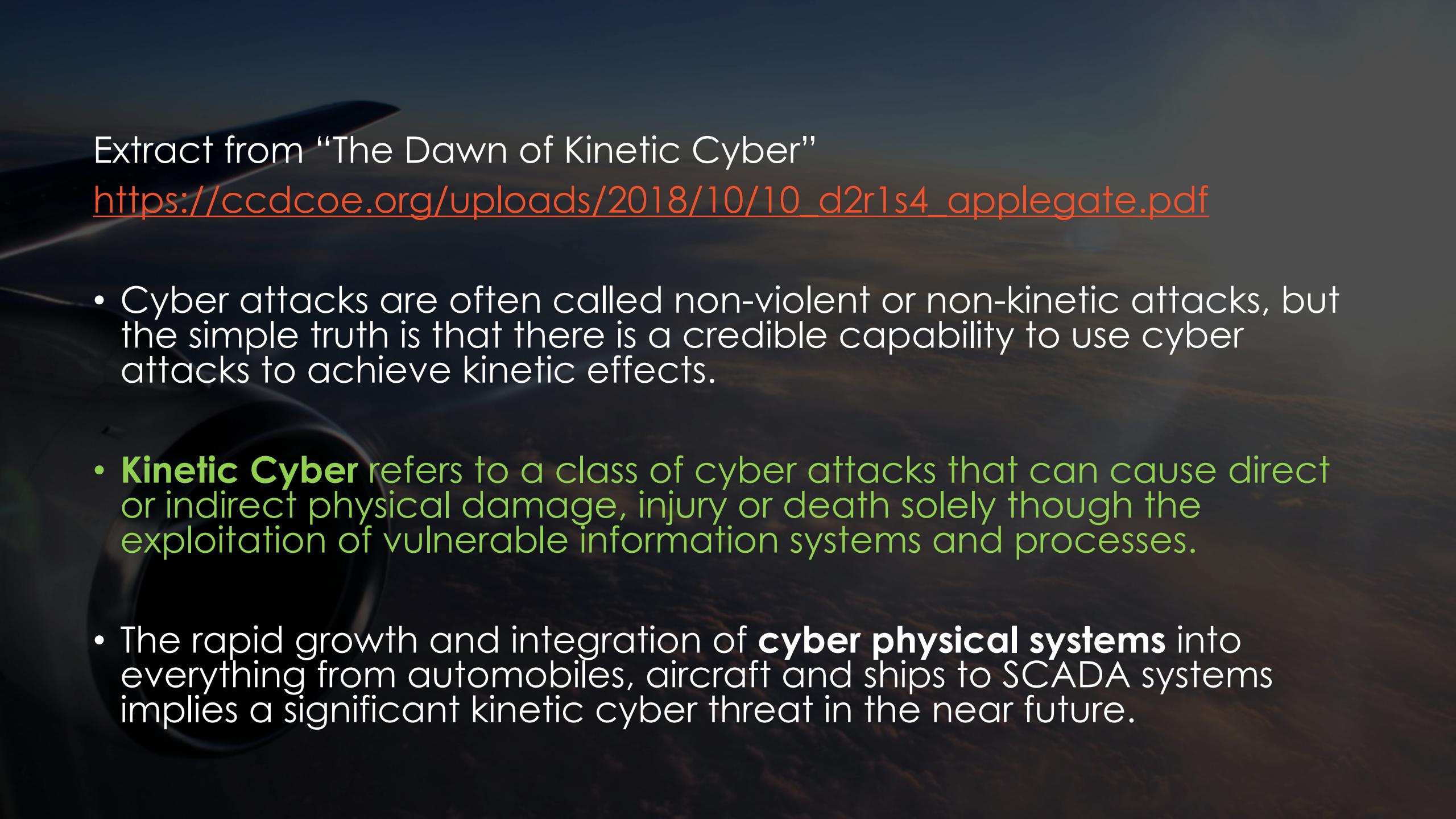
Recovery focuses on process control
and operational continuity

Safety, Processes
and Environment



Information Technology

vs. **Operational Technology**



Extract from “The Dawn of Kinetic Cyber”

https://ccdcoc.org/uploads/2018/10/10_d2r1s4_applegate.pdf

- Cyber attacks are often called non-violent or non-kinetic attacks, but the simple truth is that there is a credible capability to use cyber attacks to achieve kinetic effects.
- **Kinetic Cyber** refers to a class of cyber attacks that can cause direct or indirect physical damage, injury or death solely through the exploitation of vulnerable information systems and processes.
- The rapid growth and integration of **cyber physical systems** into everything from automobiles, aircraft and ships to SCADA systems implies a significant kinetic cyber threat in the near future.

STATE OF OT/ICS CYBERSECURITY - TECH LIMITATIONS

- Not as straightforward as most IT systems - requires specialised domain knowledge e.g. engineering, train operations
- Safety-critical OT components cannot be patched like IT equipment - requires elaborate verification & validation
- Forensic investigations difficult, and in some cases, impossible
- Legacy technology e.g. floppy disk drives, serial-port modems
- Outdated Operating Systems, incompatible software and drivers
- Performance limitations (CPU, memory etc.)

STATE OF OT/ICS CYBERSECURITY - ATTACK SURFACE++

The search engine for Power Plants

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



TOTAL RESULTS
304

TOP COUNTRIES

Country	Count
Spain	131
Italy	48
Estonia	26
Belgium	18
Poland	17

TOP SERVICES

Service	Count
FTP	156
Telnet	70
BACnet	66
2121	6
HTTP(S)	3

TOP ORGANIZATIONS

Organization	Count
Telefónica de España Static IP	102
Vodafone Italia	20
Telia Eesti	17
Vodafone Italy ask to use th...	12
Plus	10

TOP PRODUCTS

Product	Count
Excel Web	66
nginx	4

68.2.219.68

88.88-2-219.staticip.rimaf-fde.net
Telefonica de Espana Static IP
Added on 2019-08-09 00:01:48 GMT
Spain, Burgos

Linux 2.6.15.7-e1inos-249 (xlweb) (2)

217.153.79.213

220- #####
220- #
220- # Welcome to the embedded ftp server
220- #####
220 xlweb FT...

217.153.79.213

220- #####
220- #
220- # Welcome to the embedded ftp server
220- #####
220 xlweb login:

150.140.145.123

University of Patras
Added on 2019-08-08 21:11:43 GMT
Greece, Patras

Linux 2.6.15.7-e1inos-249 (xlweb) (1)

62.197.214.201

SWAN, a.s.
Added on 2019-08-08 21:19:41 GMT
Slovakia, Nitra

220- #####
220- #
220- # Welcome to the embedded ftp server
220- #####
220 xlweb FT...

166.102.235.80.staticip.ee

Telia Eesti
Added on 2019-08-08 18:04:01 GMT
Estonia, Tallinn

Instance ID: 3
Object Name: CPU3
Vendor Name: Honeywell
Application Software: 29
Firmware: fw-version=XLWebExe-2-01-04; xlweb-linux-2-01-10; bs-version=XLWebExe-2-01-04
Model Name: Excel Web



Ke2 therm evaporator



Explore Downloads Reports Pricing Enterprise Access

My Account



Share Search

Download Results

Create Report

TOTAL RESULTS

104

TOP COUNTRIES



Japan 77
United States 16
Canada 11

TOP SERVICES

8081 58
8083 36
Splunk 7
8009 2
8880 1

TOP ORGANIZATIONS

NTT 52
VECTANT 6
TOKAI 6
NTT PC Communicati... 6
Fujitsu 5

202.239.246.63

d63.iwateFL1.vectant.jp
VECTANT
Added on 2020-06-21 23:12:57 GMT
• Japan, Morioka

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html
Cache-Control: no-cache
Set-Cookie: ke2=54213;r...
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"><html><head><meta http-equiv="X-UA-Compatible" content="IE...</head><body>

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html
Cache-Control: no-cache
Set-Cookie: ke2=16434;r...
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"><html><head><meta http-equiv="X-UA-Compatible" content="IE=EmulateI...</head><body>

Shodan Retweeted

dalmoz @dalmoz_ · Jun 22

Shodan Dork of the Day:

114 Industrial refrigeration/evaporation units, located in Japan 🇯🇵, USA 🇺🇸, Canada 🇨🇦.

Access to Settings reveal passwords, setpoints. Default creds are pretty consistent.

@shodanhq #shodandork

https://twitter.com/dalmoz_/status/1274939892431228928?s=20

KE2 Province エネコントローラ

(株)大洋アレスコ
054626296042IP ドレス: 10.10.105.27
MAC ドレス: 00:04:A3:CE:4A:0CSite name: Maru Kai Bon Festival
Second Factory NO1
Verbal sele: Japanese

Setting ③

cool down

Temperature in the libr	4.5 °C
Refrigerant:	R-22
Minimum cooling time	2 分間
Minimum stop time:	5 分間
Temperature range:	2.0 °C
Kuneche substitution t	45.0 °C
Subsidyセツタ1:	T1 suction tempe
Subsidyセツタ4:	T4コイルTemperatur
ファンControl:	Broken (wher
ファンspeed	0.0 %
Control in the plural	average temp

Frost

Frost extraction method:	ヒーター
The temperature at the end of fr	5.0 °C
Water cut time:	15 分間
Elongation temperature of フ	6.0 °C
Maximum delay time:	0 分間
Frost take control:	OFF
Frost takes the first move:	Save エネ
ヒーターControl (コイルTemperature	Duan
Frost take ポンプダウン time:	0 分間
Save エネ霜取	
Frost take バラメータ値:	40
Cycle frost	
Frost recovery number/day:	1

デジタルEnergy

Strength ①Func	システムOFF
Force ②function:	invalid
Force ③Function:	invalid

アクティブ Status: オープン loop

アクティブ Status: オープン loop

アクティブ Status: クローズ circ

センサRevision value

PID	
Proportional:	3
Integral:	5
Derivative:	3
Subsidiary temperature	0.0 °C
alarm	
High temperature alarm (temp difference) in the library:	

リモート:

KE2省エネコントローラ

(株)大洋アレスコ
0546296042

IP ドレス: 10.10.105.27

現場名: 丸啓鰹節(株)第二工場 N O 1

MAC ドレス: 00:04:A3:CE:4A:0C 言語選択: 日本語

運転モード
一時停止中庫内温度
+6.2°Cコイル温度
+6.0°C圧縮機
リレーOFF蒸発器ファン
リレーOFF警報
リレーOFF

警報なし

DI
運転中DI
デジタル入力②デジタル入力③
無効T4コイル温度
+6.3°C

AUX

吸入圧力
0.334 MPaT1吸入温度
+3.4°C蒸発温度
-4.1°C弁開度
0.0 %

ホームページ

設定①

設定②

設定③

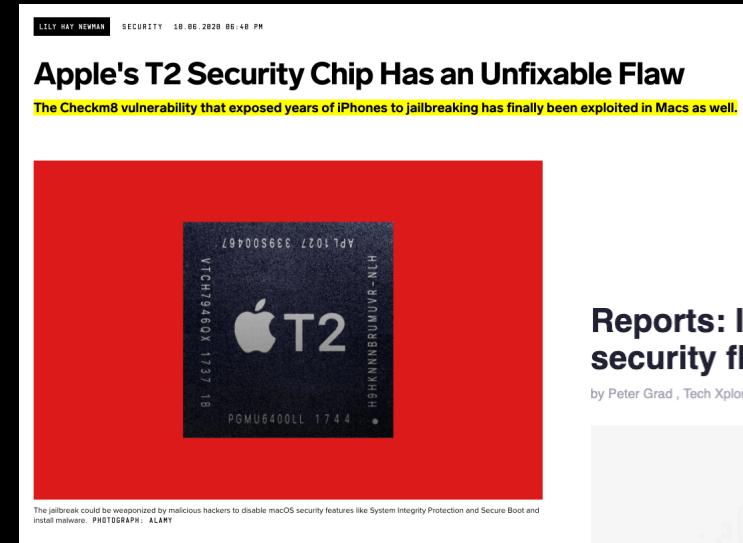
グラフ

接続中ユーザ数: 1

KEP
thermadorbox

STATE OF OT/ICS CYBERSECURITY - SUPPLY-CHAIN RISKS

- Unconventional, chain-linked threats that do not depend on one single attack vector.
- Supply-chain threats include Tier 2 and Tier 3 suppliers and sub-contractors that could compromise security, with organisations being the last one to find out they've been compromised.
- **Supply-chain challenges are especially acute in Operational Technology systems and may become worse.**



Reports: Intel chips have new security flaws

by Peter Grad , Tech Xplore

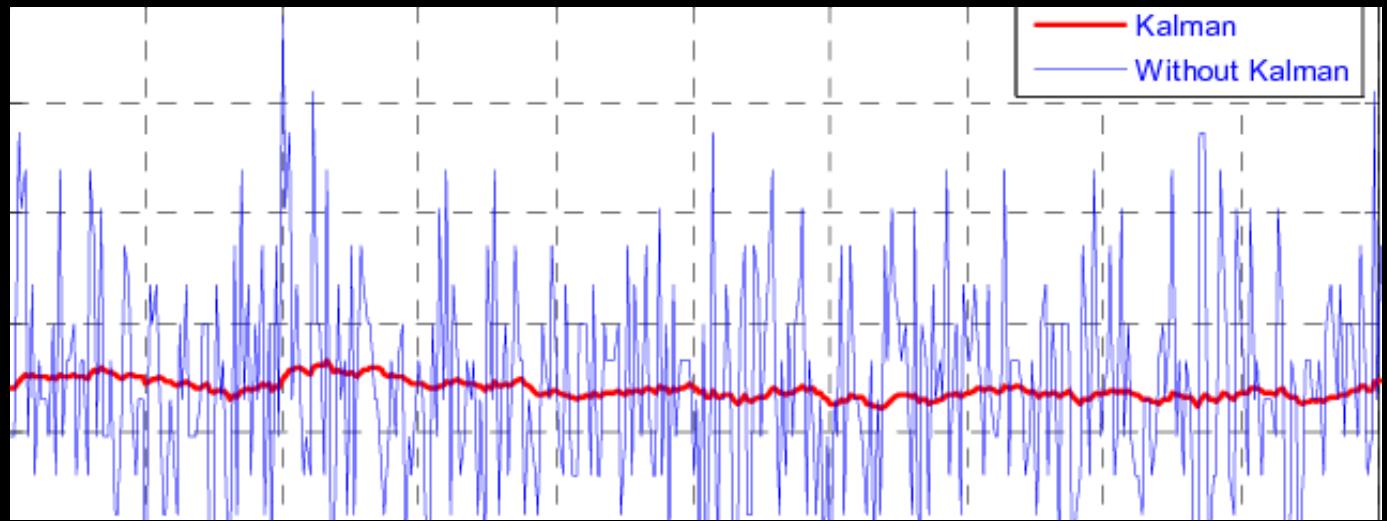


Credit: Pixabay/CC0 Public Domain

A pair of new security threats to Intel-based computer systems have been revealed. The beleaguered semiconductor chip manufacturer has faced a seemingly endless series of vulnerabilities over the past two years.

STATE OF OT/ICS CYBERSECURITY - MONITORING RISKS

- “Noise” tells you about the process and the sensor performance
- Noise is filtered out e.g. Kalman before the Serial-To-Ethernet converter
- Information about nuances of the processes and the sensors are not available for network anomaly detection



Operator's View (post-filter)



```
import time
client = ModbusTcpClient('10.0.21.10', port=502)
client.connect()

result = client.read_coils(1,1)
print('Manual or Auto: ' + str(result.bits[0]))

result = client.read_coils(5,1)
print('Plus/Minus sign: ' + str(result.bits[0]))

Rr = client.read_holding_registers(address=0, count=1, unit=1)
PV = float(Rr.registers[0])
print('PV(mm) = %f' % PV)

client.write_register(address=1,value=5000,unit=1)

# to make fake indicator
client.write_register(address=11,value=20000,unit=1)
client.write_register(address=12,value=0000,unit=1)

time.sleep(1)

# Read value
Svr = client.read_holding_registers(address=1, count=1, unit=1)
SV= float(svr.registers[0])
print('SV(mm) = %f' % SV)

RHR = client.read_holding_registers(address=11, count=1, unit=1)
RH = float(RHR.registers[0])
print('RH(mm) = %f' % RH)

RLR = client.read_holding_registers(address=12, count=1, unit=1)
RL = float(RLR.registers[0])
print('RL(mm) = %f' % RL)
```

Hacker's View



Factory Floor (Process Data)

OT cyber monitoring is not sufficient to identify many significant control system cyber incidents

Submitted by Joe Weiss on Mon, 01/27/2020 - 23:01

A major news organization contacted me about my control system cyber incident database. I have been very clear the database is not public but I could provide sanitized information. Until now, that was not sufficient to get media interest as they wanted names. Since this news organization was willing to go without names, I provided sanitized summaries of 20 actual cases. I chose a combination of cases representing domestic and international, unintentional and malicious, multiple industries (e.g., power, water, pipelines, transportation, etc.), and various levels of impact (e.g., business disruption, major environmental spills, major blackouts, catastrophic failures including deaths, etc.) An important finding was many cases would NOT have been detected from OT network monitoring as these were control system cyber incidents. This is a clarion cry for training the control system engineers to question when incidents happen if they could be cyber-related. This becomes very important as sophisticated hackers can, and have, made cyber attacks look like equipment malfunctions.

Joe Weiss

STATE OF OT/ICS CYBERSECURITY - LACK OF CAPACITY & SKILLS

digital workforce

Cybersecurity
workforce

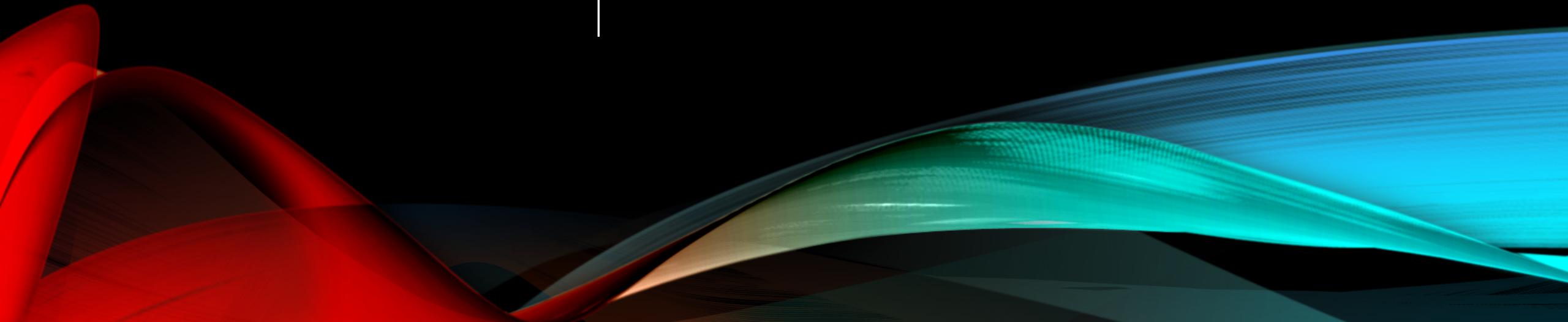
engineering
workforce

ICS/OT Cybersecurity Workforce

STATE OF OT/ICS CYBERSECURITY - CULTURE & MINDSET



IMPLEMENTING AN OT CYBER DEFENCE STRATEGY



Recap of OT Cybersecurity Masterplan

- ✓ Announced at the opening of SICW 2019
- ✓ Outlined efforts to **enhance the cyber resilience** of OT stakeholders, **improve cross-sector responses** and **strengthen partnerships with industry and stakeholders** by driving multiple OT cybersecurity initiatives to address key challenges and emerging cyber threats in the OT environment



"The Masterplan will guide the development of capabilities to secure systems in the OT environment, and mitigate emerging OT cyber threats."

SM Teo Chee Hean - SICW 2019

Overview of Masterplan's Key Thrusts

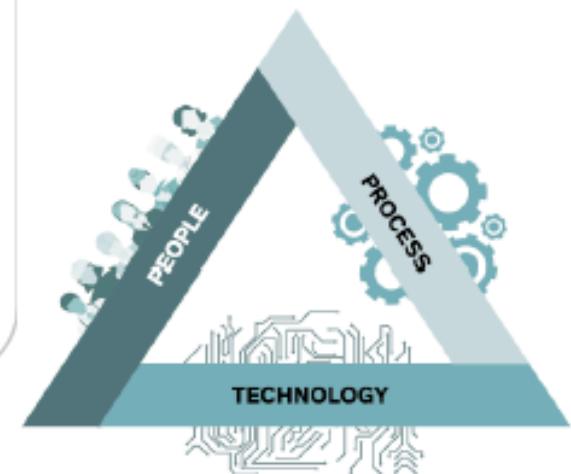
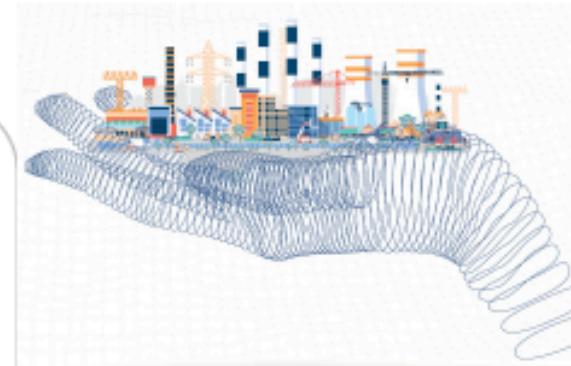
The OT cybersecurity masterplan outlines the key thrusts to uplift the cybersecurity posture of people, process and technology of OT stakeholders. Key thrusts include:

Key Thrust 1: OT Cybersecurity Training

Key Thrust 2: OT Cybersecurity Information Sharing and Analysis Center (OT-ISAC)

Key Thrust 3: Strengthening Policies and Processes

Key Thrust 4: Adopting Technologies for Cyber Resilience



KEY THRUST 1: OT CYBERSECURITY TRAINING

1

Make cybersecurity training an organization-level priority.

2

Focus on incremental efforts, do not try to change the world overnight.

3

Reward and reinforce positive behaviours.

4

Make content engaging and relatable.

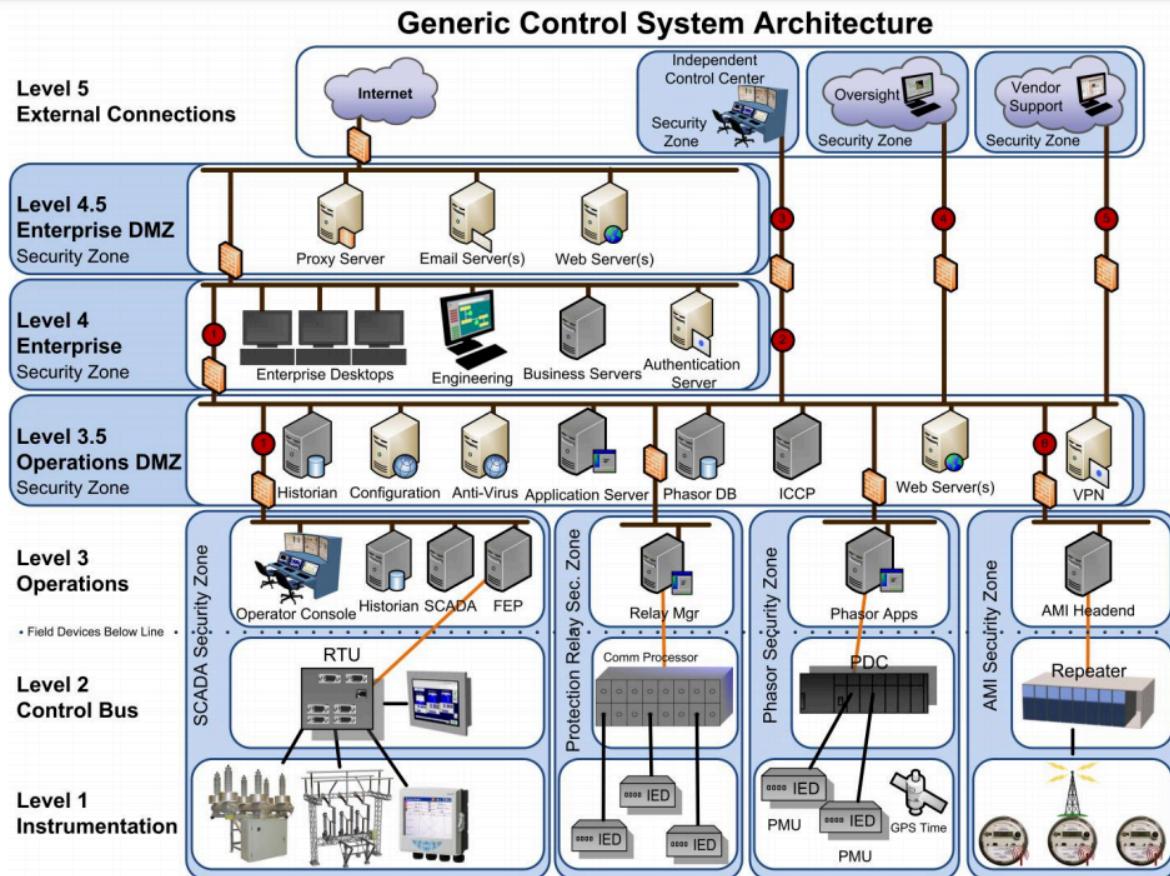
KEY THRUST 3: STRENGTHEN POLICIES AND PROCESSES

- Framework focusing on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.
- Knowing where you / your organisation is at (in terms of cyber maturity) is important, but do not set unrealistic goals.
- **NIST Cybersecurity Framework Version 1.1**



<https://www.nist.gov/cyberframework/framework>

SURVEY THE BATTLEFIELD



- Inventorize and understand what needs to be protected
- Differentiate between end-points that need raw data and those that need information
- Consider carefully decisions related to safety-critical equipment, and involve stakeholders early

The consensus of the Commission and participating investigative agencies is that the loss of the Space Shuttle Challenger was caused by a failure in the joint between the two lower segments of the right Solid Rocket Motor. The specific failure was the destruction of the seals that are intended to prevent hot gases from leaking through the joint during the propellant burn of the rocket motor.

EXPLOIT POWER OF DATA

A major malfunction

Challenger's brief flight

.678 seconds

Following Challenger's liftoff, a puff of black smoke — seen only by automatic launch cameras — indicates a problem with one of the O-ring seals at the joint between segments of the shuttle's right-hand solid rocket booster. No human eyes see the smoke, and there would have been no way to abort the flight if they had.

58 seconds

A small jet of smoke and flame bursts through the side of the booster and quickly grows.

73 seconds

The flame burns through the strut attaching the solid rocket booster to the external fuel tank, causing the booster to swivel into the side of the tank. The resulting massive explosion destroys the space shuttle.

Full thrust

Once the boosters ignite, there is no way to shut them off.

3 minutes, 58 seconds

Challenger's crew compartment, which appeared to come away from the exploding shuttle more or less intact, smashes into the Atlantic Ocean at 200 mph.

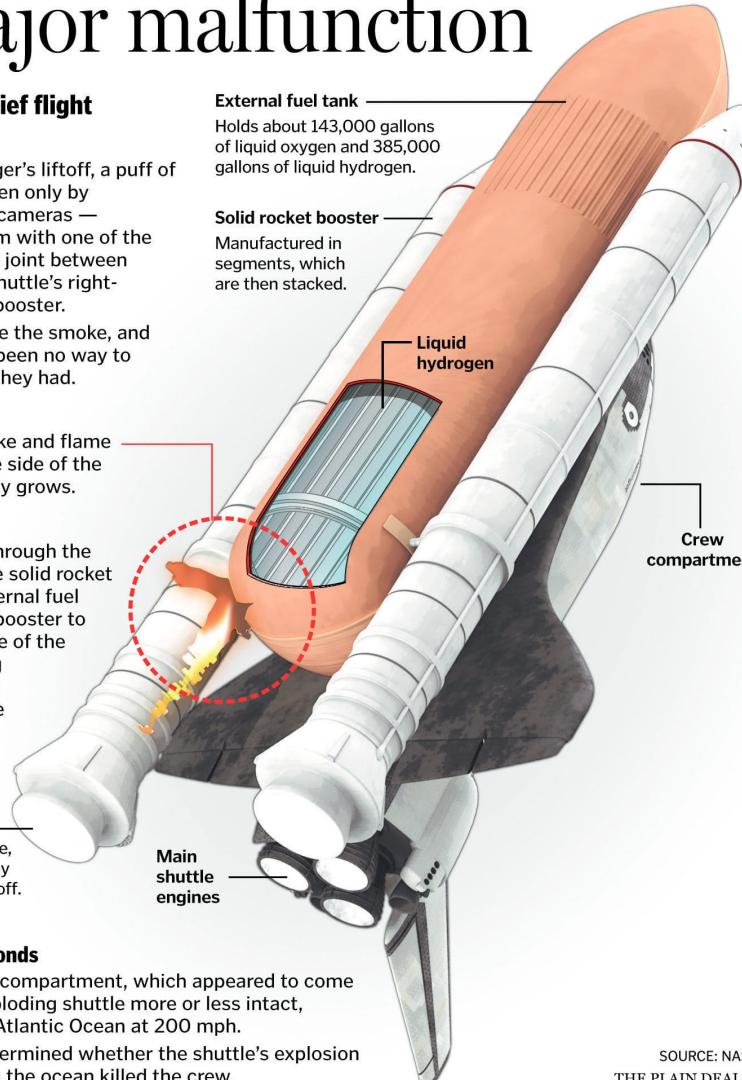
Officials never determined whether the shuttle's explosion or the impact with the ocean killed the crew.

External fuel tank
Holds about 143,000 gallons of liquid oxygen and 385,000 gallons of liquid hydrogen.

Solid rocket booster
Manufactured in segments, which are then stacked.

Liquid hydrogen

Crew compartment



SOURCE: NASA
THE PLAIN DEALER

Dataset	Inference from data	Decision	Result
Selective Data (actuality)	Low temperatures have little to no effect on O-ring failure rate	Allow space shuttle launch at low temperatures	Space Shuttle Challenger explosion leading to 7 deaths
All Data (ideal)	Low temperatures have a substantial effect on O-ring failure rate, especially as all launches below 65° had O-ring issues	Don't allow space shuttle launch at low temperatures, due to the substantially elevated risk of failure	Unknown; likely, significantly lower risk of O-ring failure and subsequent explosion

<https://priceconomics.com/the-space-shuttle-challenger-explosion-and-the-o/>

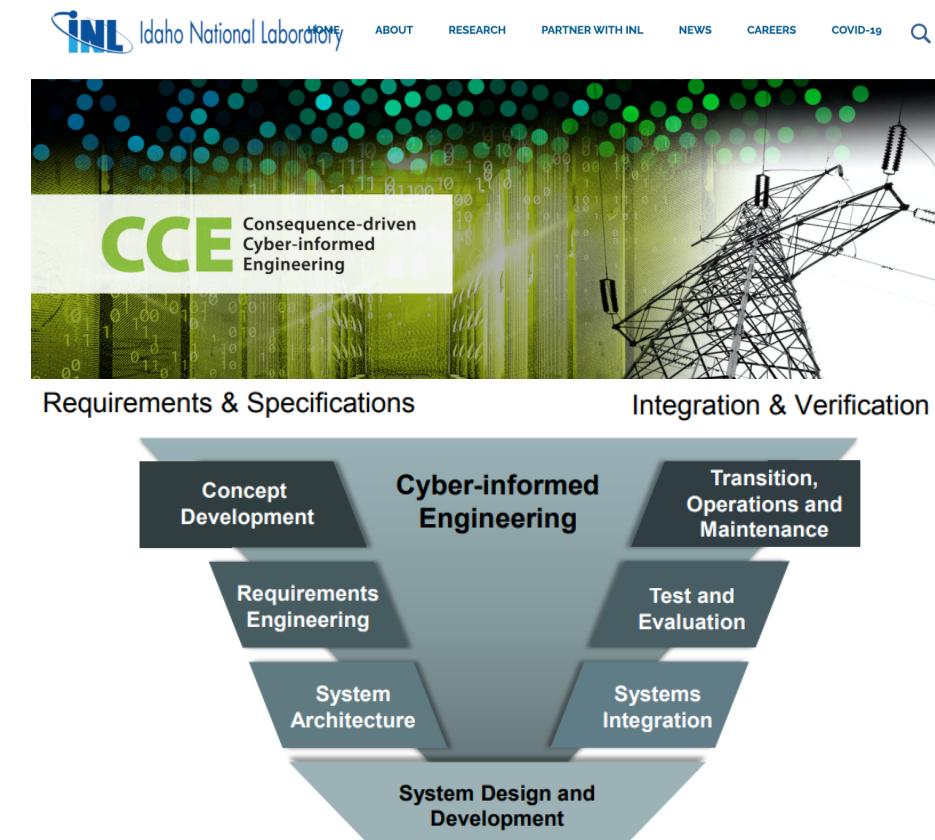
- The problem with most ICS/OT environments today is not the lack of data, but the overwhelming volume of “dirty” data
- Focus on building up cyber threat detection and response capability (and importantly, data analytics)
- Detecting “signals” from the noise

ALIGN YOUR STRATEGY

- ICS/OT systems generally engineered against **deterministic** outcomes, backed by evidence
 - Safety cases are a good example of this (https://en.wikipedia.org/wiki/Safety_case)
 - “A vehicle safety case may show it to be acceptably safe to be driven on a road, but conclude that it may be unsuited to driving on rough ground, or with an off-center load for example, if there would then be a greater risk of danger e.g. a loss of control or an injury to the occupant.”
- Cyber-attacks (i.e. rogue threats) often produce **random** outcomes, never observed before during testing
- Strategies must be ALIGNED to operational and safety risks, and remain reasonably practical

KEY THRUST 4: ADOPT TECH FOR RESILIENCE

- **Consequence-driven Cyber-informed Engineering (CCE)** is a methodology focused on securing the nation's critical infrastructure (CI) systems
- Developed at Idaho National Laboratory, CCE begins with the assumption that if CI is targeted by a skilled and determined adversary, the targeted operation can – and will – be sabotaged
- Consequences in ICS/OT are largely engineering and domain-specific. Compare to information security (C.I.A. triad)
- Manage legacy tech by focusing on safety-directed cybersecurity goals i.e. reach a **Safe State**



<http://inl.gov/cce>

- Institutionalize cybersecurity policies & processes to inculcate good cybersecurity hygiene.

Cyber Processes



- Stand up CERT capabilities to defend systems and skills to face cyber threats.

Cyber Capacity



- Conduct training to educate people and suppliers with awareness and skills to face cyber threats.

Cyber Competency



- Equip systems with cyber tools to protect networks and repulse cyber attacks.

Cyber Tools



- Explore and adopt advanced technologies to sharpen cybersecurity capabilities and operational readiness.

Cyber Technology



No 100% Cybersecurity -
Multi-Layered Strategy is Key!





“Think like a **hacker**, but act like an **engineer**”

- Marty Edwards, former Director, US ICS CERT



THANK YOU

And Stay Safe And Healthy!

Connect with me on LinkedIn -
<http://www.linkedin.com/in/shaofei>