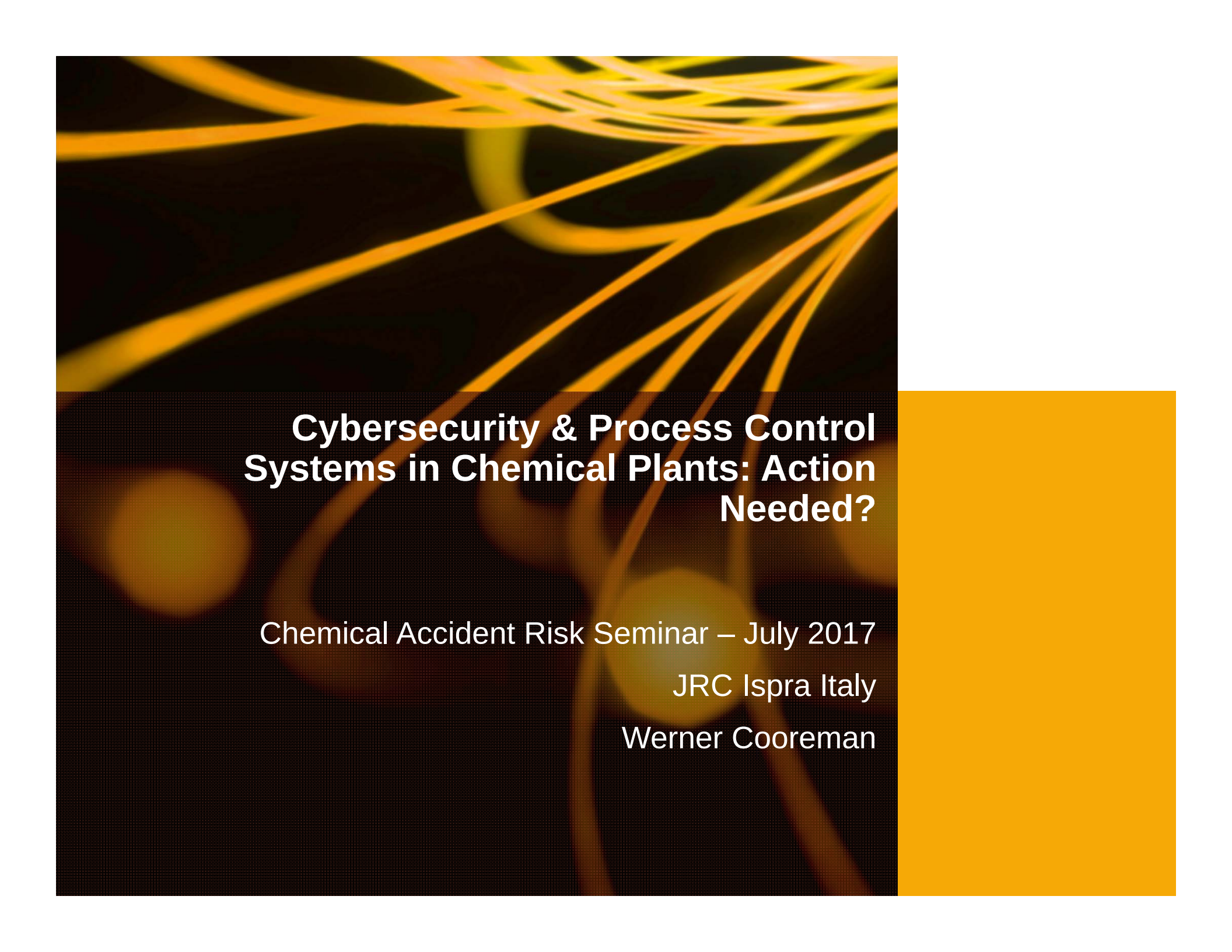


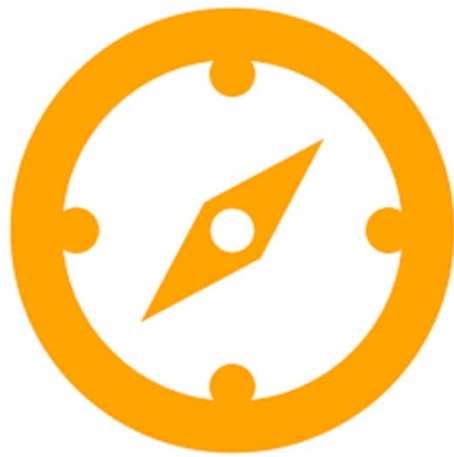


Cybersecurity & Process Control Systems in Chemical Plants: Action Needed?

Chemical Accident Risk Seminar – July 2017

JRC Ispra Italy

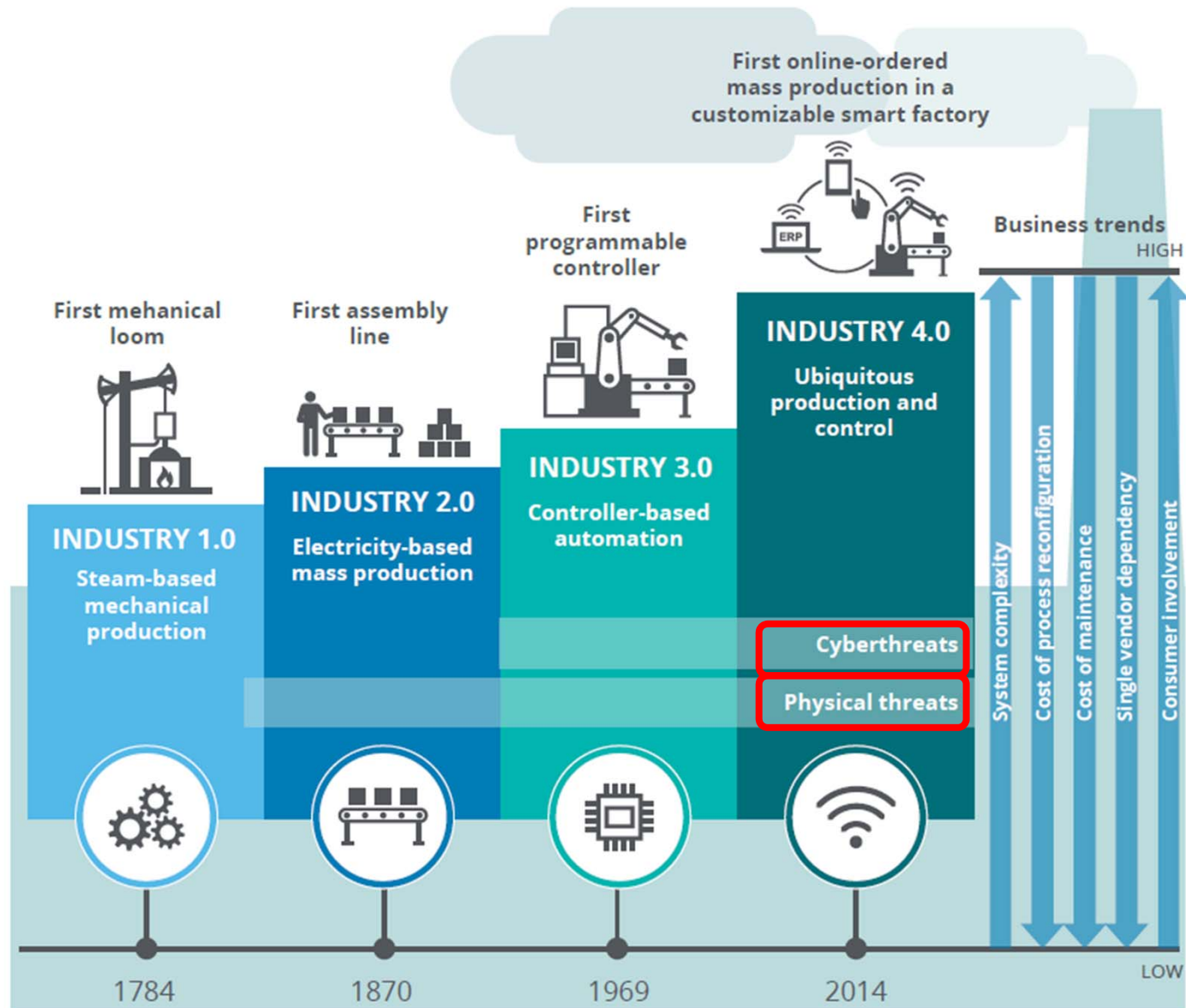
Werner Cooreman

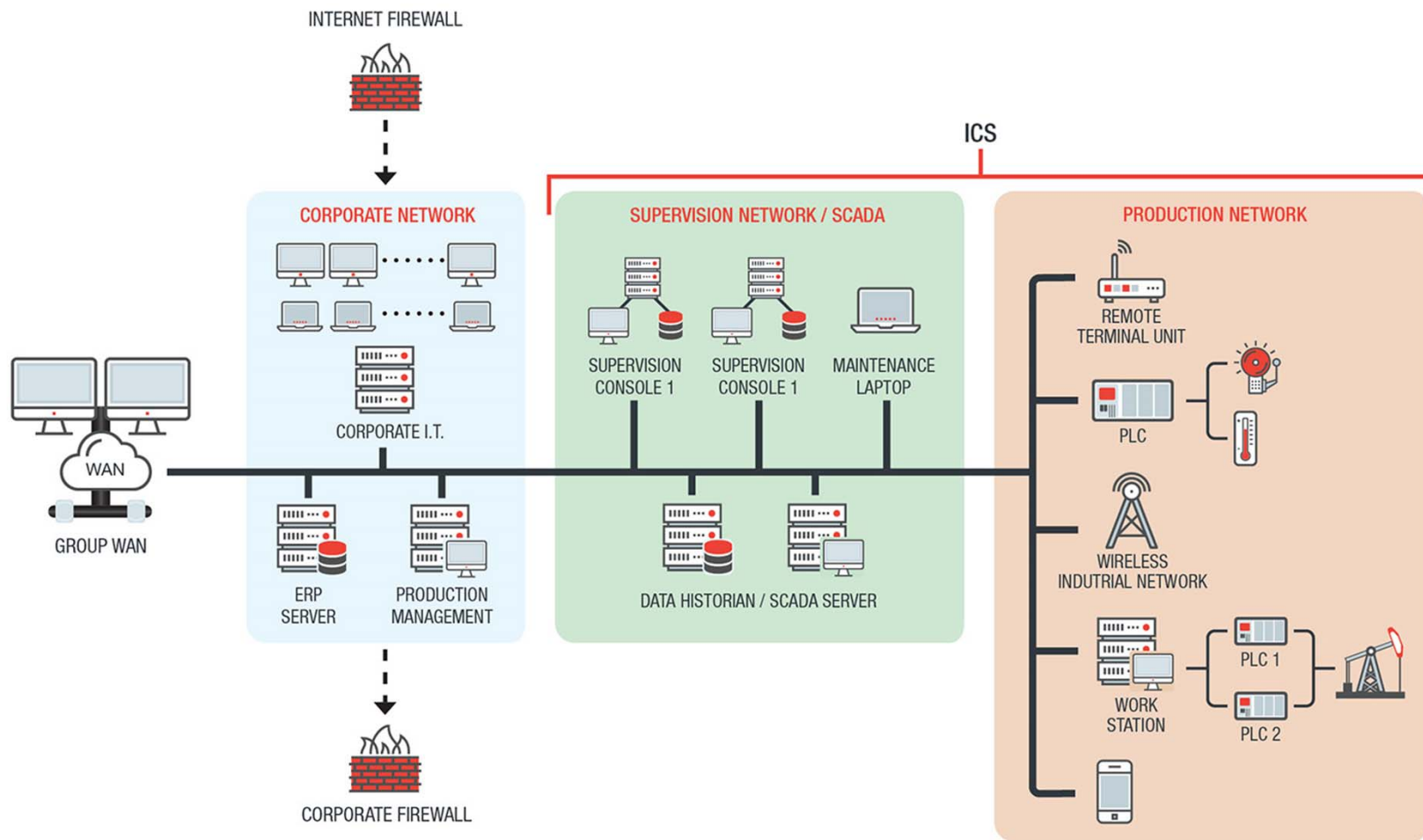


Orientation

INDUSTRY

revolutions over time





SECURITY

state of being protected against threat



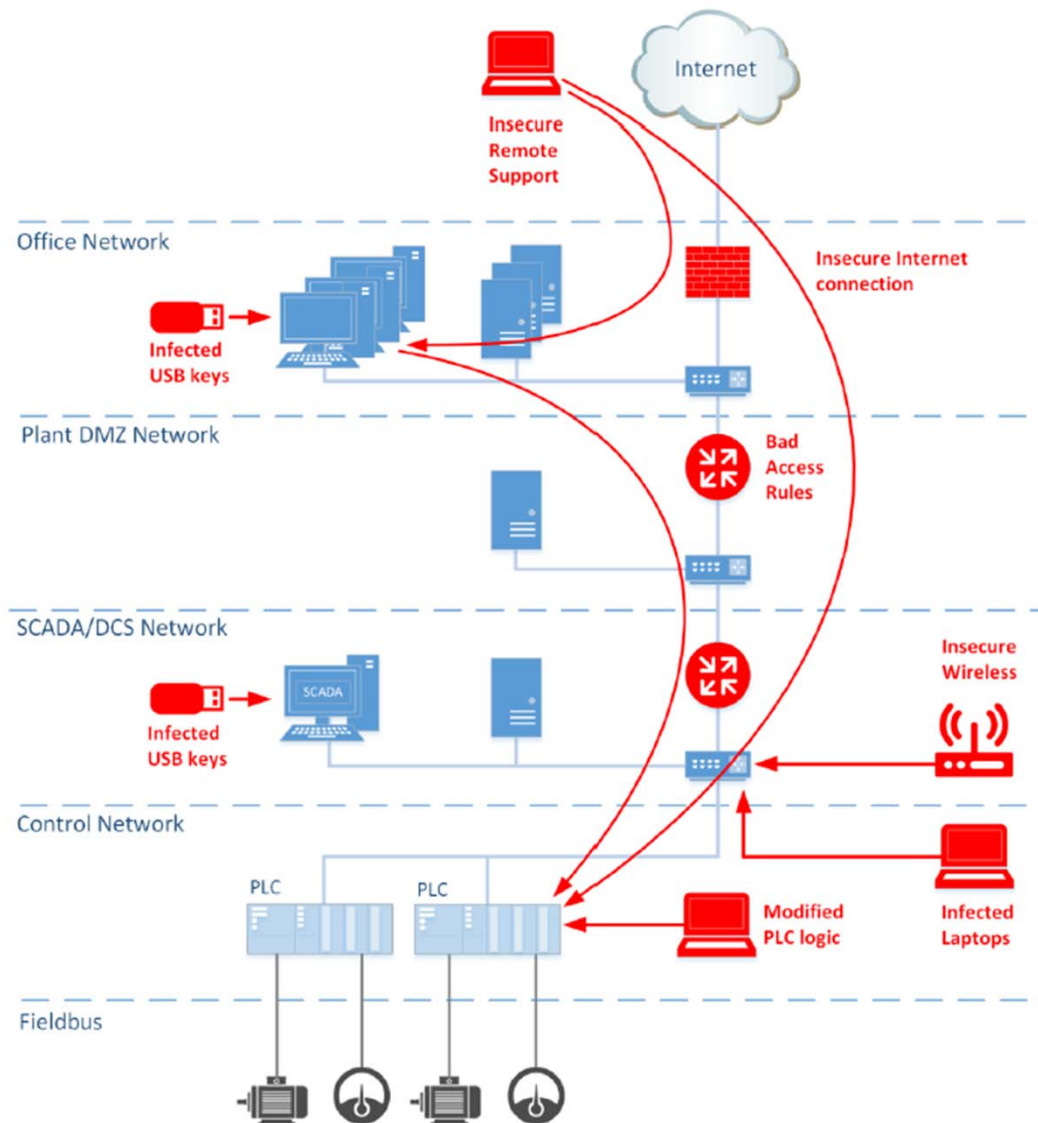
THREAT

a person with a malicious intent

IEC 62443		Skills	Motivation	Means	Resources
SL4	Nation-state APT	ICS Specific	High	Sophisti- cated (Campaign)	Extended (multi- disciplinary teams)
SL3	Hacktivist, Terrorist	ICS specific	Moderate	Sophisti- cated (Attack)	Moderate (groups of hackers)
SL2	Cyber crime, Hacker	Generic	Low	Simple	Low (Isolated individuals)
SL1	Careless employee, contractor	No attack skills	Mistakes	Non- intentional	Employee, contractor

THREAT

cyberattack vectors



IMPACT

attack outcomes on process

Component Damage

- *Equipment overstress*
- *Safety limits violation*



Production Damage

- *Product quality*
- *Production rate*
- *Operating costs*
- *Maintenance efforts*



Compliance Violation

- *Safety*
- *Pollution*
- *Contractual treaties*



NOT considered:

- **Theft or manipulation of information**
- **Attack on physical security systems**



Vulnerability Assessment

Variance

- With each new site, the equipment and layout differs, as technology advances
- Architecture changes as result of manufacturing programs for excellence, quality...

Safety

- Physical safeguards for process deviations can mitigate loss of control systems to an extent
- Safety culture provides enhanced vigilance
- Process overwatch
- Response plans exist for out-of-control processes

Security

- Responsible Care codes include security commitments
- Corporate Security programs include ICS security
- Firewall, IAM, access rules, physical security...
- ICS providers include security (Siemens, Honeywell...)

ICS systems

- Platform architecture may be standard, but system configuration is not
- Require advanced training in combination with process knowledge

2

chemical versus other

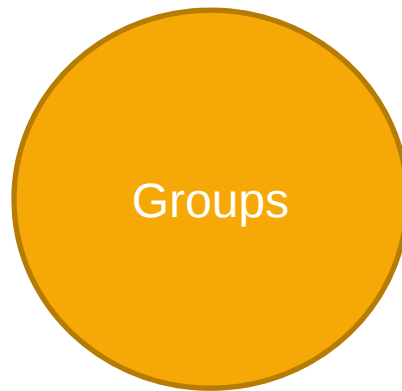


Source: Cisco Security Research

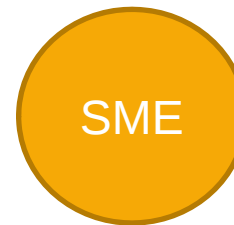
2016 ATTACK TRAFFIC

3

large versus small companies



Groups



SME

More visible as target

More complex as target

High security awareness

Resource availability

Less visible as target

Less security awareness

Resource constraints

4

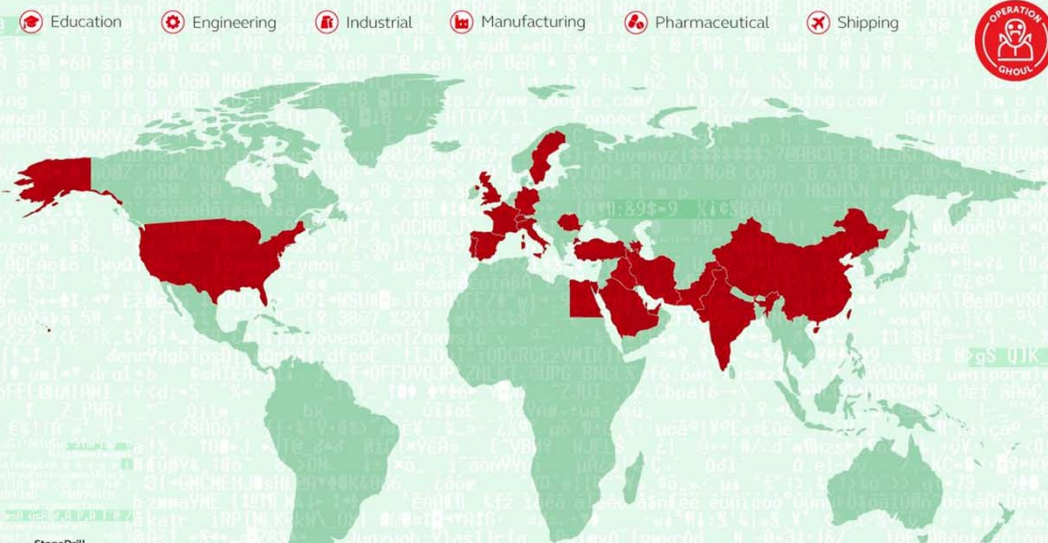
objectives are data oriented (so far)

Blue Termite cyber-espionage campaign targets hundreds of organizations in Japan

The attackers hunting confidential information utilizing a zero-day Flash player exploit and a sophisticated backdoor, customized to each victim. They have been active at least since 2013.



Operation Ghoul: Victims of advanced targeted attack



Notable wiper incidents

Narilam	Shamoon	Groove Monitor	Dark Seoul (Lazarus)	Sony (Lazarus)	BlackEnergy	Shamoon 2.0	StoneDrill
2008 - 2012	2012	2012	2013	2014	2015 - 2016	2016 - 2017	2016 - 2017
Middle East	Middle East	Middle East	South Korea	USA	Ukraine	Middle East	Middle East
Self spreading, affects database software through slow corruptions	Targets in the energy sector, oil, critical infrastructure	Time bomb (predefined dates), deletes files on all disks	Targets in financial and media sectors	Similarities with Shamoon, (EldoS raw disk driver)	Targets in the energy sector, media, transportation, government	Malware repackaged from first wave in 2012. Most victims in Saudi Arabia, with top targets including government, industry, transport, telecoms	Style similarities with Shamoon 2.0. Heavy use of evasion techniques to avoid detection by sandboxes

Egypt
India
Pakistan
UAE
Great Britain

Gibraltar
Germany
Spain
USA
China

France
Iran
Iraq
Italy
Saudi Arabia

Portugal
Qatar
Romania
Sweden
Switzerland

Taiwan
Turkey

sky Lab. All Rights Reserved.

GREAT KASPERSKY

© 2017 Kaspersky Lab. All Rights Reserved.

Data Wiper – Data Theft – Cyber sabotage



- Protect the perimeter
- Maintain updated defenses
- Strengthen access control
- Harden remote access
- Harden ICS features
- Monitor for incidents
- Intrusion detection
- Physical protection





Government Role Considerations

some considerations

DO

- Maintain a risk- & performance based approach
- Strengthen collaboration between private and public sector
 - Bi-directional education
 - Co-creation of rules should rules be considered
 - Timely threat information exchange
- Engage in pursuit and prosecution of cyber criminals
- Avoid prescriptive regulation on specific technologies or methods
- Consider liability protection for the private sector in case of cyber attack (as long as appropriate management systems have been applied)

CONCLUSIONS

- Industrial Control Systems will continue to be incrementally exposed to cyber threats
- Currently, the risk of a disaster with a cyber-attack is real but not high, compared to other security risks
- For chemical industry, the risk of information theft and/or process interruption is more relevant at present (R&D information)
- BUT, we should increase attention to prepare for what might be next, by enhancing collaboration and education