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

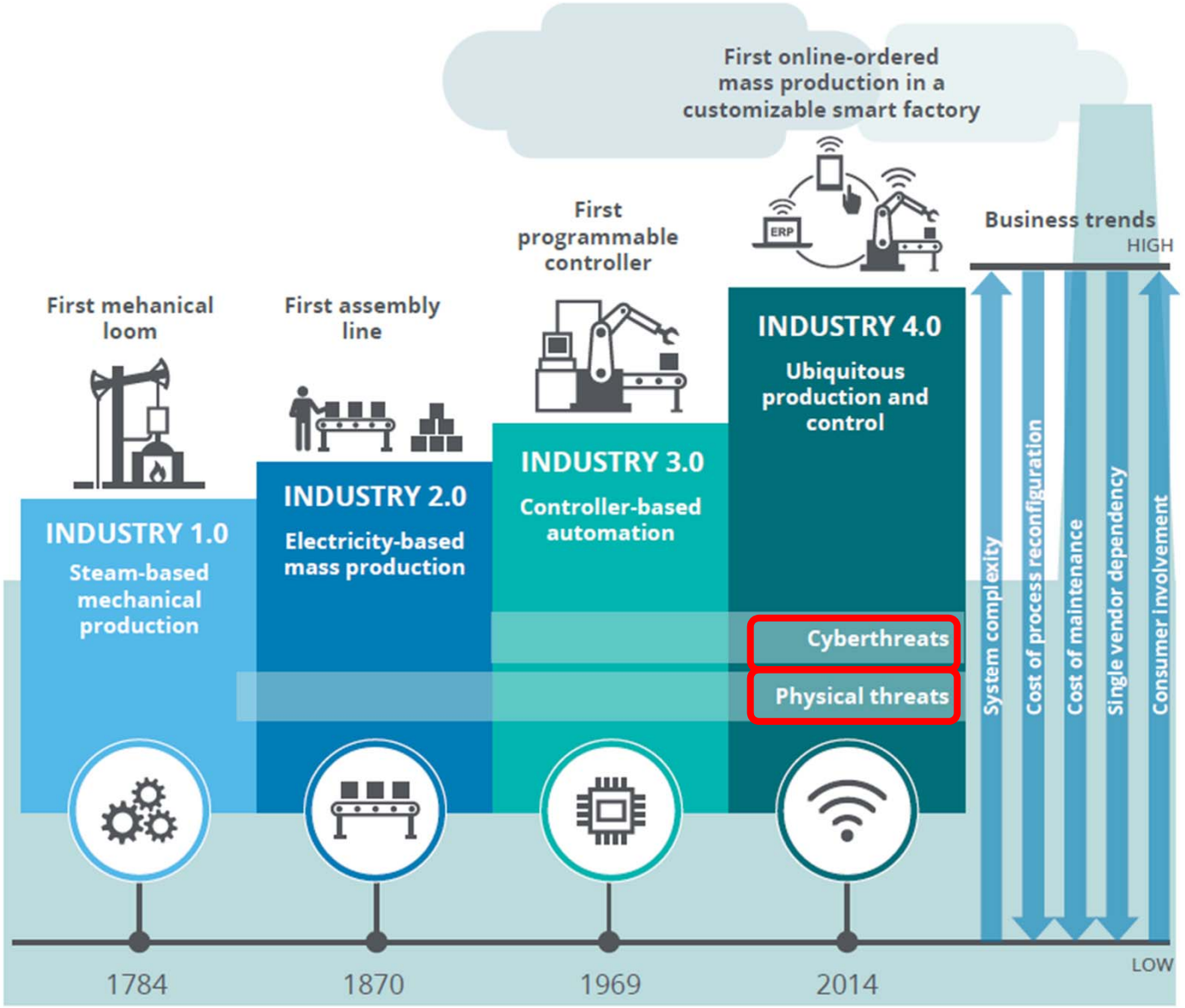
Chemical Accident Risk Seminar – July 2017

JRC Ispra Italy

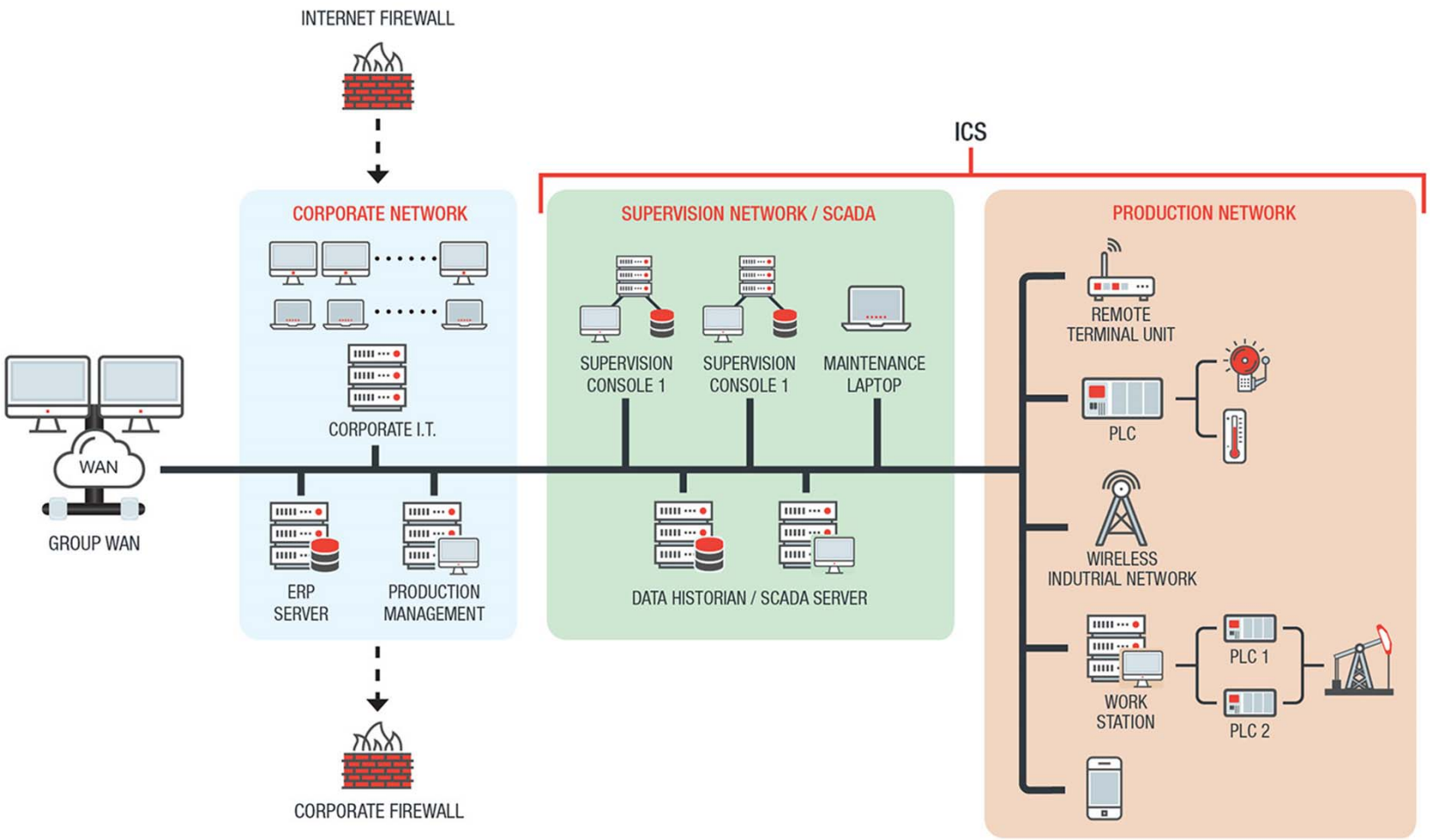
Werner Cooreman

Orientation

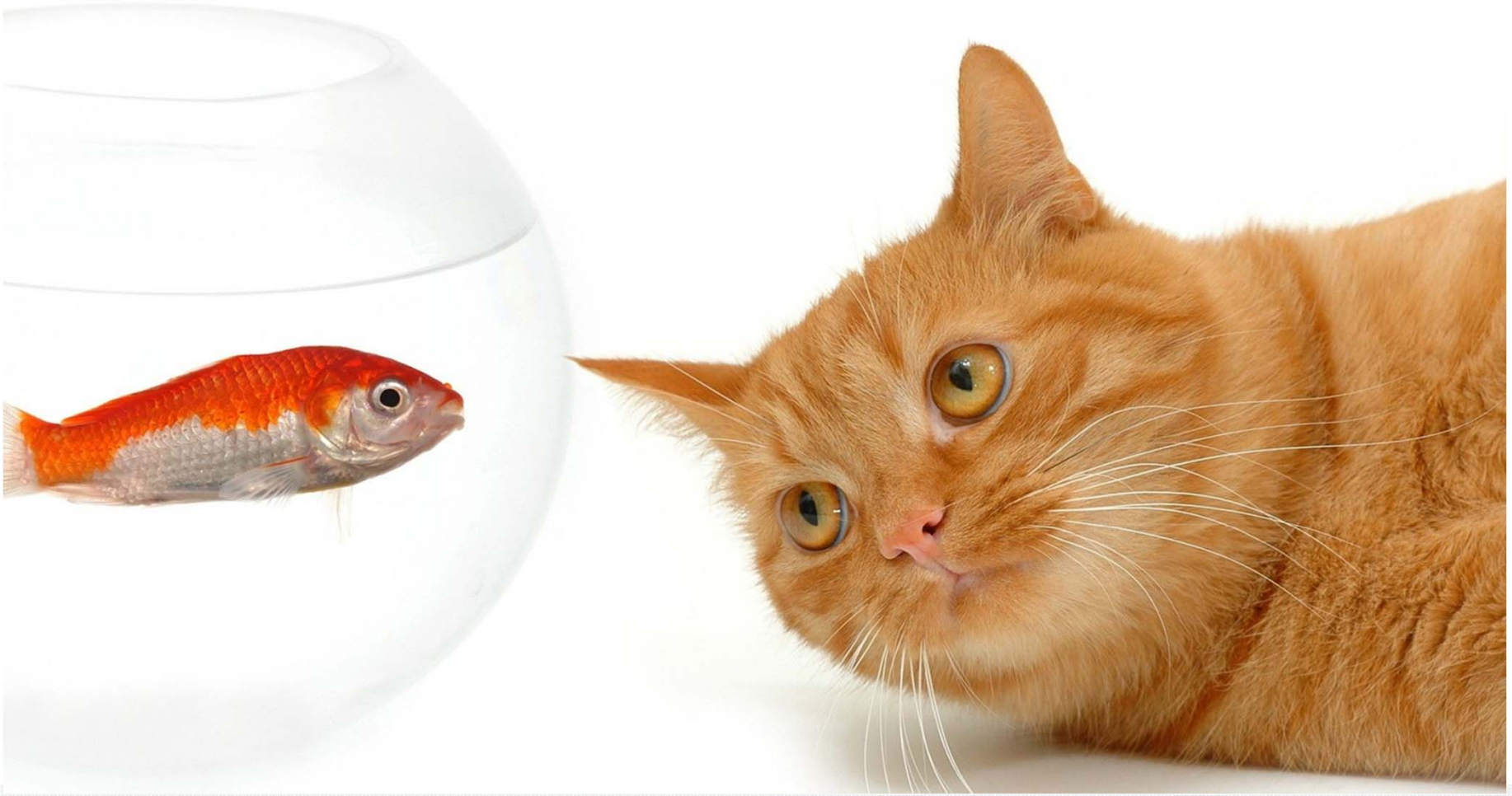
INDUSTRY revolutions over time



INDUSTRY Industrial Control Systems



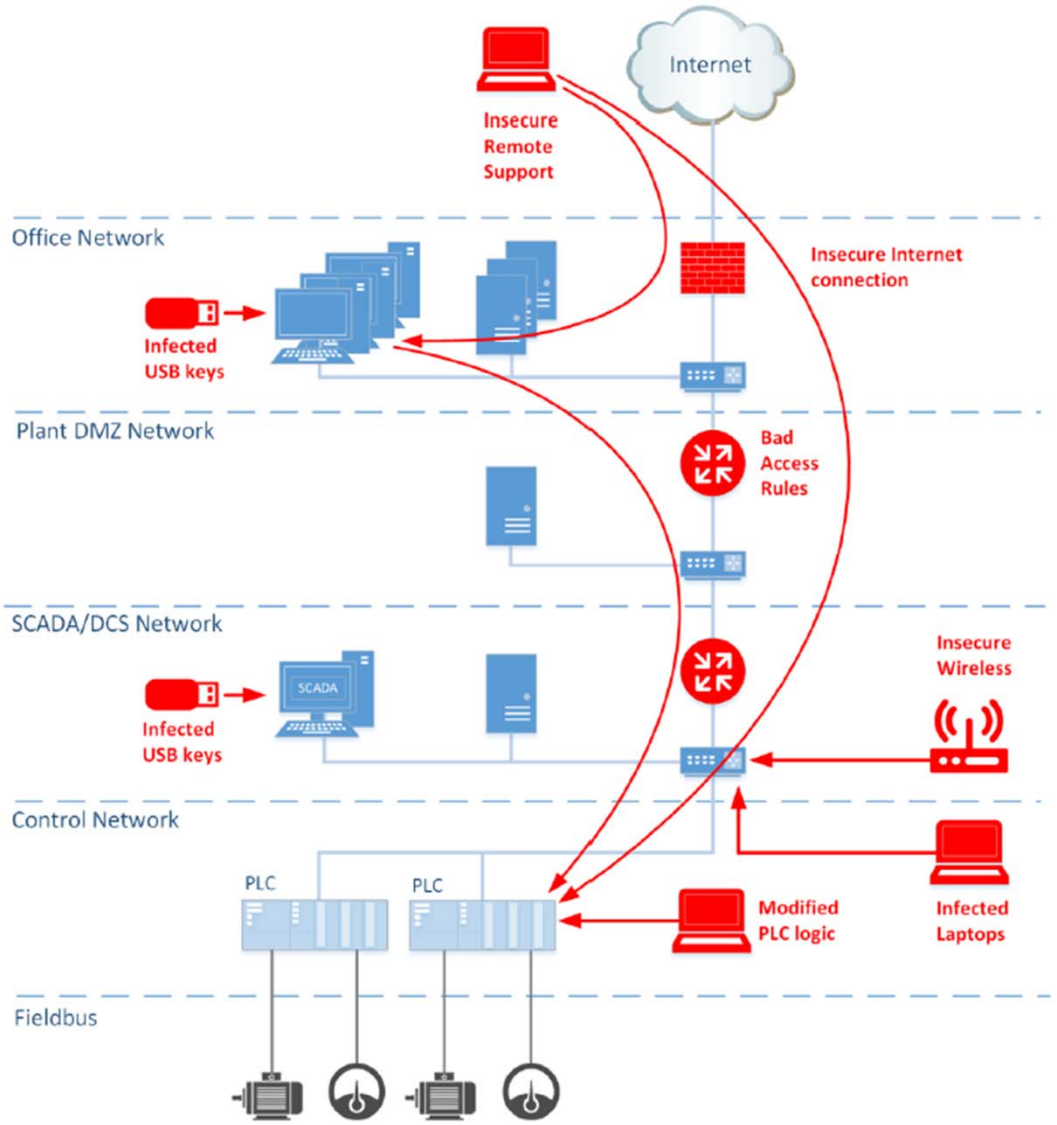
SECURITY state of being protected against threat



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 treatles*

NOT considered:

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

Vulnerability Assessment

1 complexity

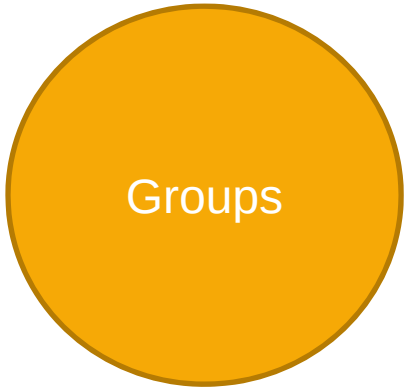
Variance	• With each new site, the equipment and layout differs, as technology advances • Architecture changes as result of manufacturing programs for excellence, quality…
Safety	• Physical safeguards for process deviations can mitigate loss of control systems to an extent • Safety culture provides enhanced 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

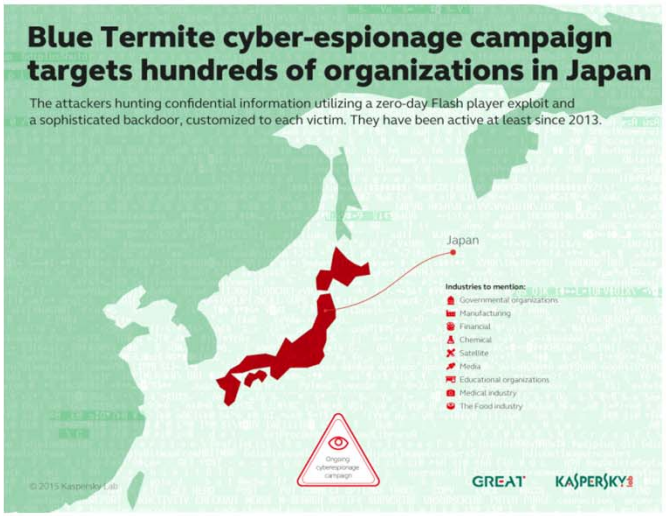
2016 ATTACK TRAFFIC

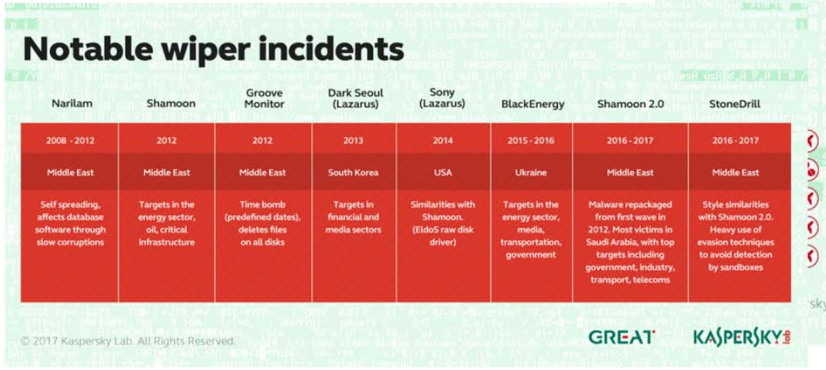
3 large versus small companies



Groups	SME
More visible as target	Less visible as target
More complex as target	Less security awareness
High security awareness	Resource constraints
Resource availability	

4 objectives are data oriented (so far)





Data Wiper – Data Theft – Cyber sabotage

Cyber Defenses

SECURITY best practices

- 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