Orientation
INDUSTRY revolutions over time

- **Industry 1.0**: Steam-based mechanical production
  - First mechanical loom

- **Industry 2.0**: Electricity-based mass production
  - First assembly line

- **Industry 3.0**: Controller-based automation
  - First programmable controller
  - Ubiquitous production and control
  - Cyberthreats
  - Physical threats

- **Industry 4.0**: Online-ordered mass production in a customizable smart factory

Timeline:
- 1784
- 1870
- 1969
- 2014

Business trends: HIGH to LOW
SECURITY

state of being protected against threat
## THREAT

A person with a malicious intent

<table>
<thead>
<tr>
<th>IEC 62443</th>
<th>Skills</th>
<th>Motivation</th>
<th>Means</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>SL4 Nation-state</td>
<td>ICS Specific</td>
<td>High</td>
<td>Sophisticated (Campaign)</td>
<td>Extended (multi-disciplinary teams)</td>
</tr>
<tr>
<td>SL3 Hacktivist, Terrorist</td>
<td>ICS specific</td>
<td>Moderate</td>
<td>Sophisticated (Attack)</td>
<td>Moderate (groups of hackers)</td>
</tr>
<tr>
<td>SL2 Cyber crime, Hacker</td>
<td>Generic</td>
<td>Low</td>
<td>Simple</td>
<td>Low (Isolated individuals)</td>
</tr>
<tr>
<td>SL1 Careless employee, contractor</td>
<td>No attack skills</td>
<td>Mistakes</td>
<td>Non-intentional</td>
<td>Employee, contractor</td>
</tr>
</tbody>
</table>
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
With each new site, the equipment and layout differs, as technology advances.
Architecture changes as result of manufacturing programs for excellence, quality...

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.

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

Platform architecture may be standard, but system configuration is not.
Require advanced training in combination with process knowledge.
chemical versus other

Source: Cisco Security Research

2016 ATTACK TRAFFIC
large versus small companies

Groups

- More visible as target
- More complex as target
- High security awareness
- Resource availability

SME

- Less visible as target
- Less security awareness
- Resource constraints
objectives are data oriented (so far)

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

Operation Ghoul: Victims of advanced targeted attack

Notable wiper incidents

Data Wiper – Data Theft – Cyber sabotage
Cyber Defenses
• 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
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