Applied Risk | Critical Infrastructure Made Secure.

How the IEC 62443 can help organisations thrive during the COVID-19 crisis

July 1st, 2020

ISASecure®

APPLIED RISK CONFIDENTIAL

Agenda

01 Introduction

02 Understanding OT cyber risk

03 Cybersecurity challenges and the IEC 62443 requirements

04 Recommendations for Securing OT Assets based on IEC 62443

05 Q&A

About Applied Risk

Applied Risk provides cyber security solutions for securing critical infrastructures, including Industrial Control Systems (ICS) and Industrial Internet of Things (IIoT).

Due to our extensive knowledge and experience we are creating safe, secure and reliable solutions for end users and suppliers throughout the whole lifecycle of their assets.

Our solutions are available worldwide.

Power. Oil & Gas. Chemical.

Manufacturing. Maritime. Healthcare.

Transport. Pharma. Automotive.

Water. Defence. Mining.

CREST

ISASecure®

Who We Are

Jalal Bouhdada

Founder & CEO

Chris Sandford

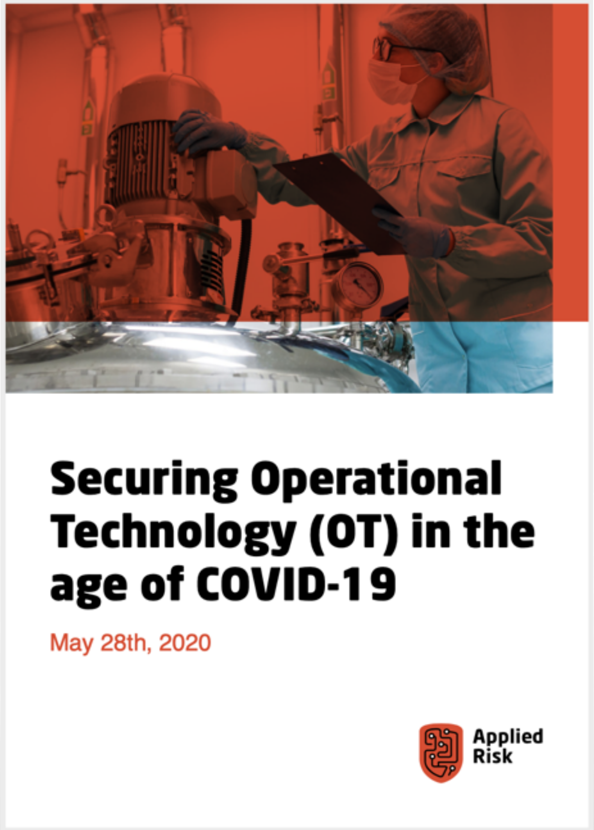
Director, Middle East
OT Security Services

Original White Paper

This webinar provides a summary of the "Securing Operational Technology (OT) in Age of COVID-19" white paper, which was based on:

- Discussions with asset owners and operators
- Examination of third-party material
- Consultation with specialists in critical infrastructure.

Deliverables from this work include a white paper, a 15-page overview with practical recommendations for the industry.



Securing Operational Technology (OT) in the age of COVID-19

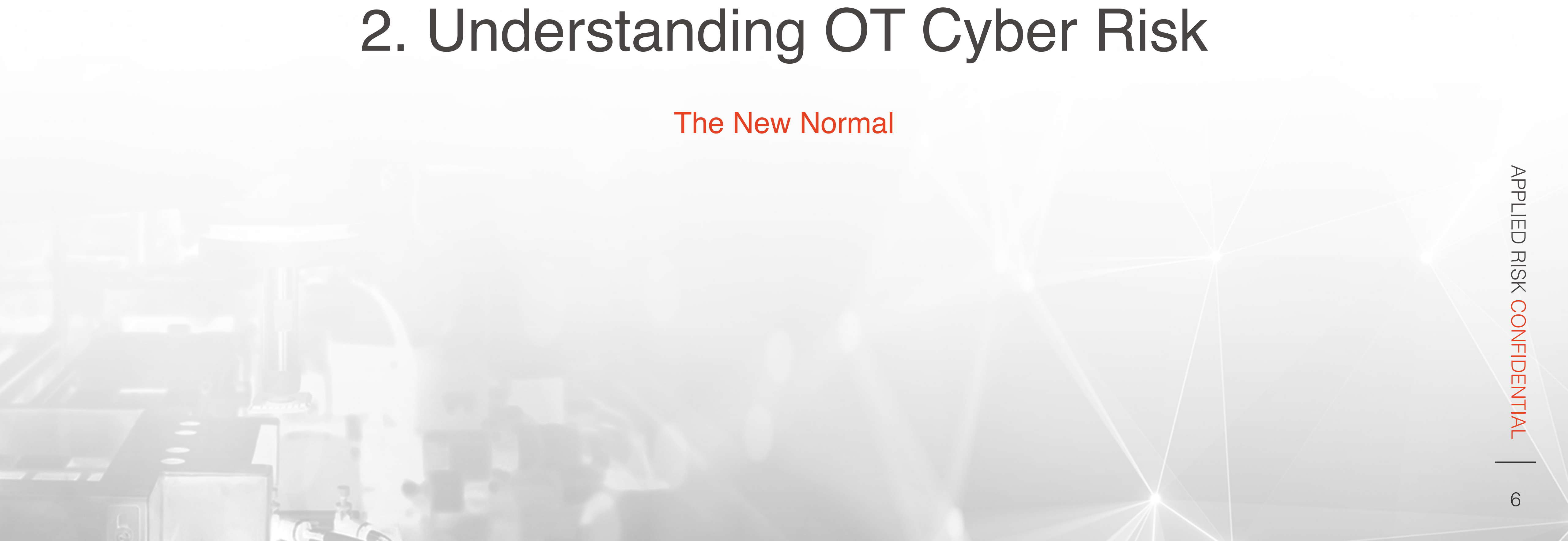
May 28th, 2020

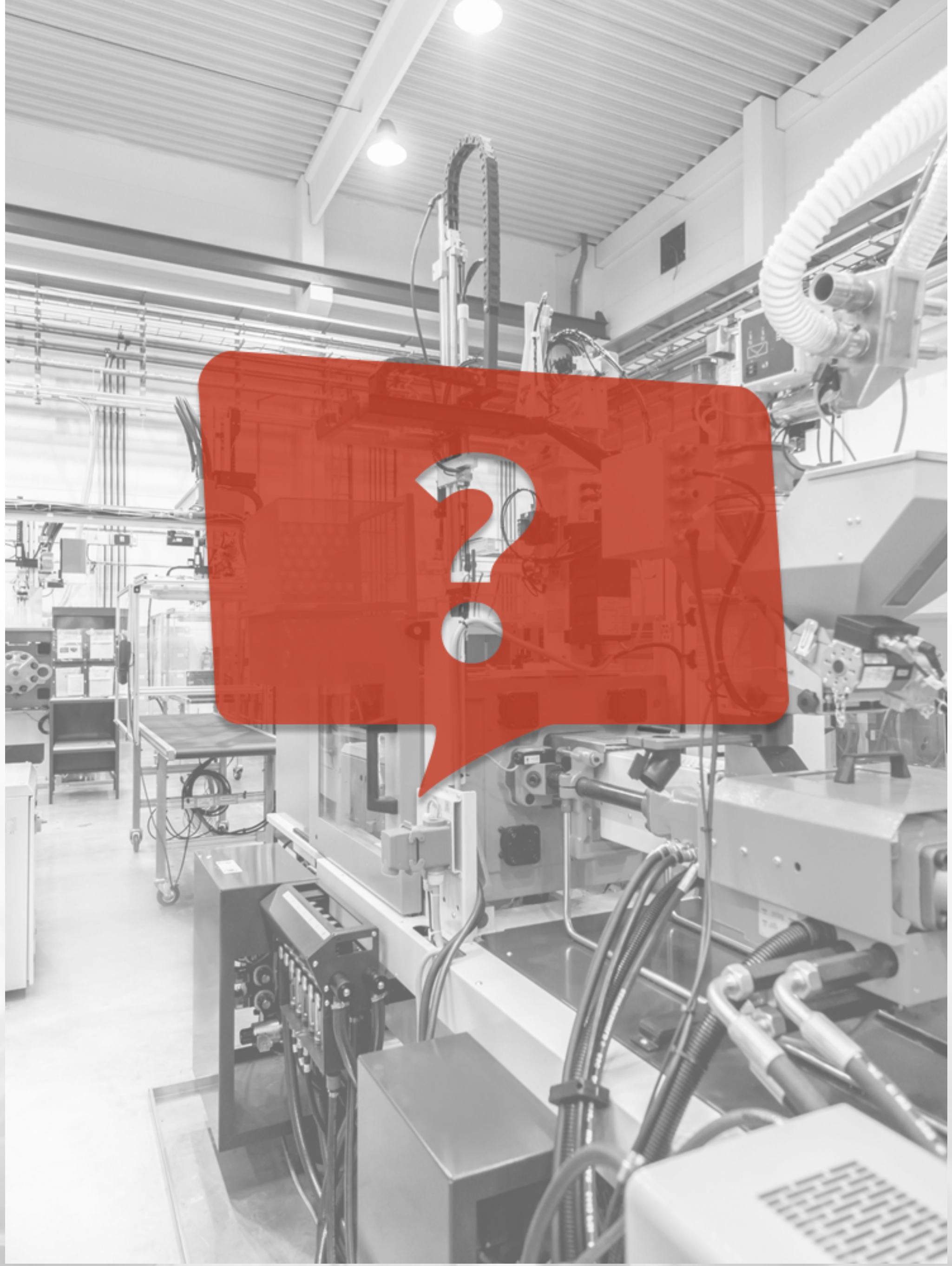
Applied Risk

https://www.applied-risk.com/resources/covid19

2. Understanding OT Cyber Risk

The New Normal





As organisations are you still adopting IEC 62443 standards even in these challenging times?

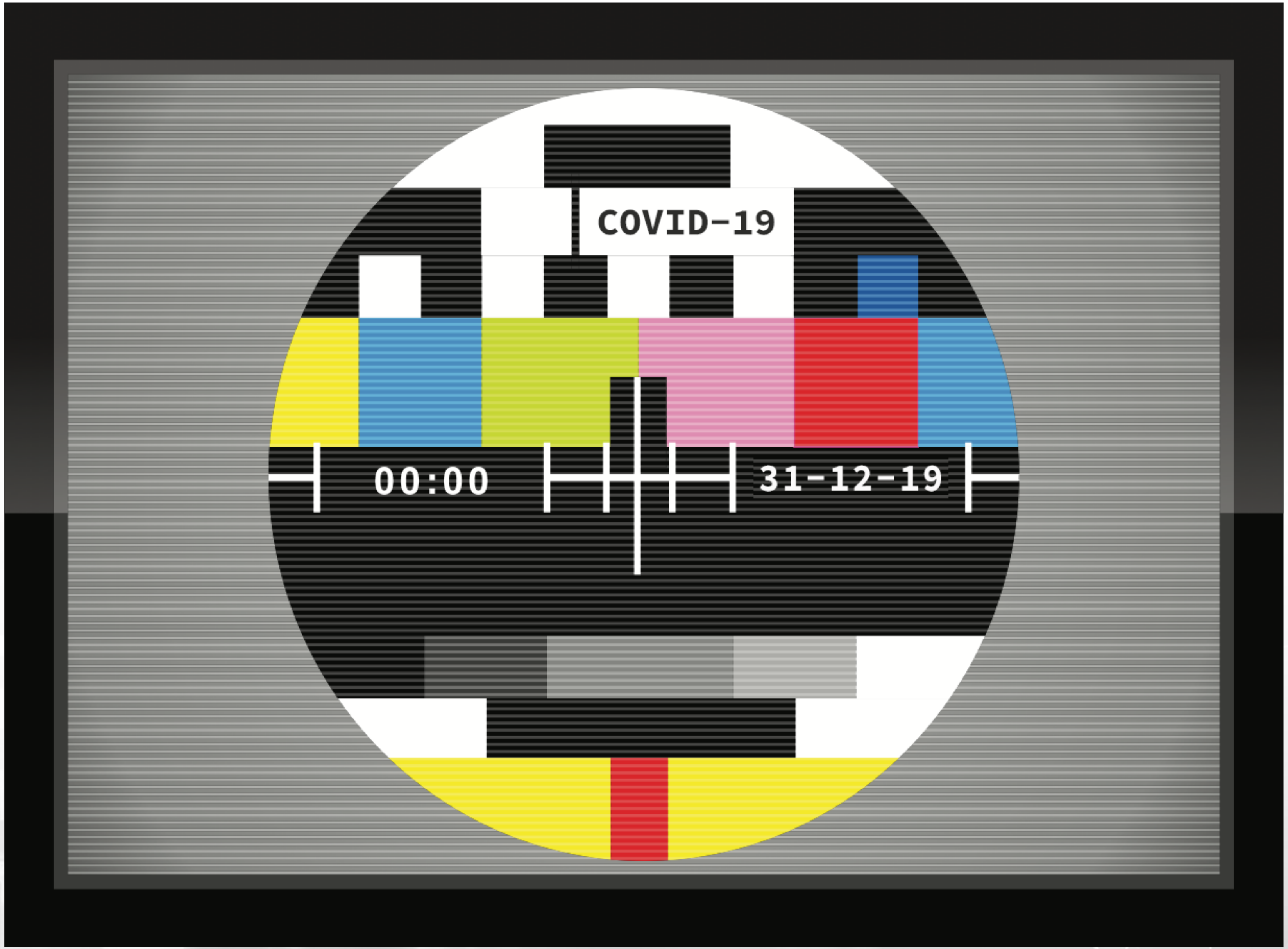
☐ Yes

☐ No

Understanding the New Normal

Balancing the new cyber risks requires new strategies for safeguarding critical safety and operational systems;

- Understanding the new cyber risk,
- Establishing baseline defences,
- Building interoperable defences with partners,
- Resetting overall architecture to accommodate this new reality.
- Understand how the role of information systems in critical infrastructure has changed
  - What has been changed?
  - How to respond to new reality?

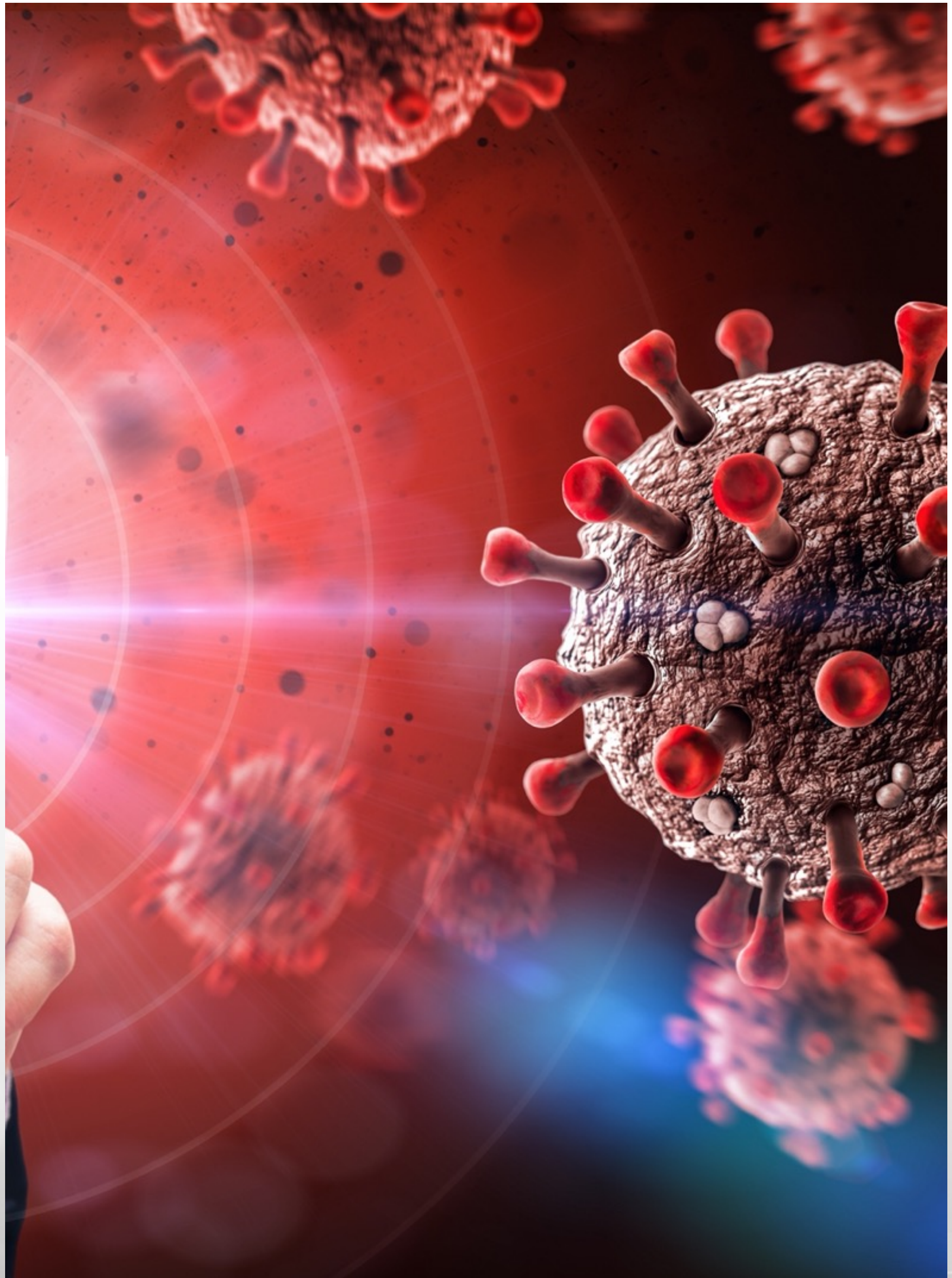

COVID-19
00:00
31-12-19

Situational Awareness

During these unprecedented times, attackers are targeting organizations even more, as they struggle to support a rapidly expanded remote workforce. Furthermore, organizations have a reduction in resources, increasing the need for automation and self-defending application workloads.

Companies are becoming agile to adapt to the new situation.

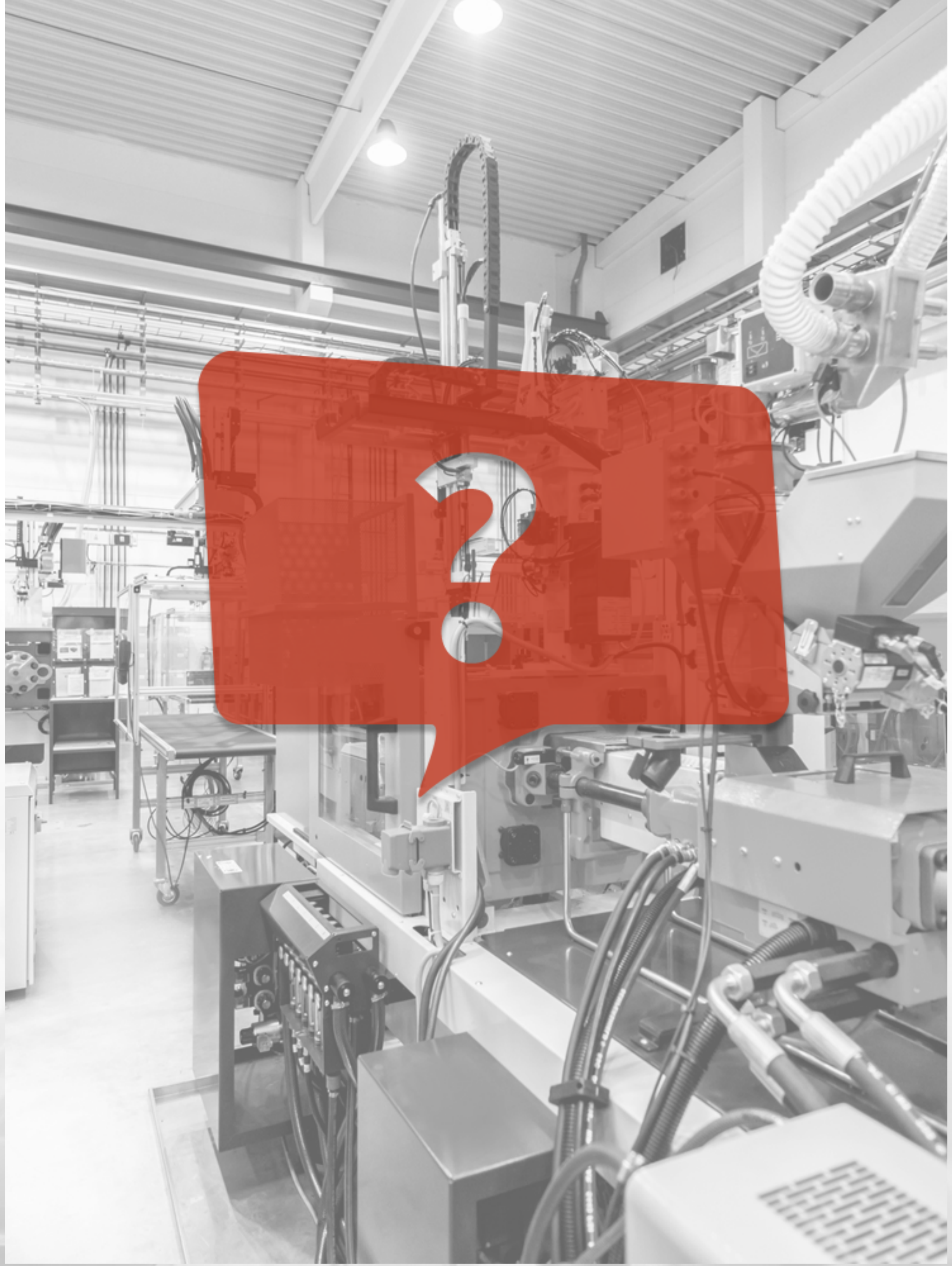
- Attackers are seeking new weak points in organizations' infrastructure to exploit
- Remote working is creating novel cyber risk for OT environment
- Cyber criminals are capitalizing on the COVID-19 (e.g. increased number of phishing, ransomware and DDoS attacks)



Top Priorities

During emergency situations, there is always a shift in focus to maintaining day to day operations. In case of this pandemic, the primary priority is to:

- Keep people and assets safe,
- Continue to operate to meet market demand and suppliers obligations
- Maintain operational efficiency
- Reduce cost



Applied Risk

As an end-user do you envision requiring IEC 62443 certification from your suppliers?

☐ Yes

☐ Thinking about it

☐ No

☐ Not an end-user

3. Cybersecurity challenges and the IEC 62443 requirements

Trends & Challenges

01 Remote Access

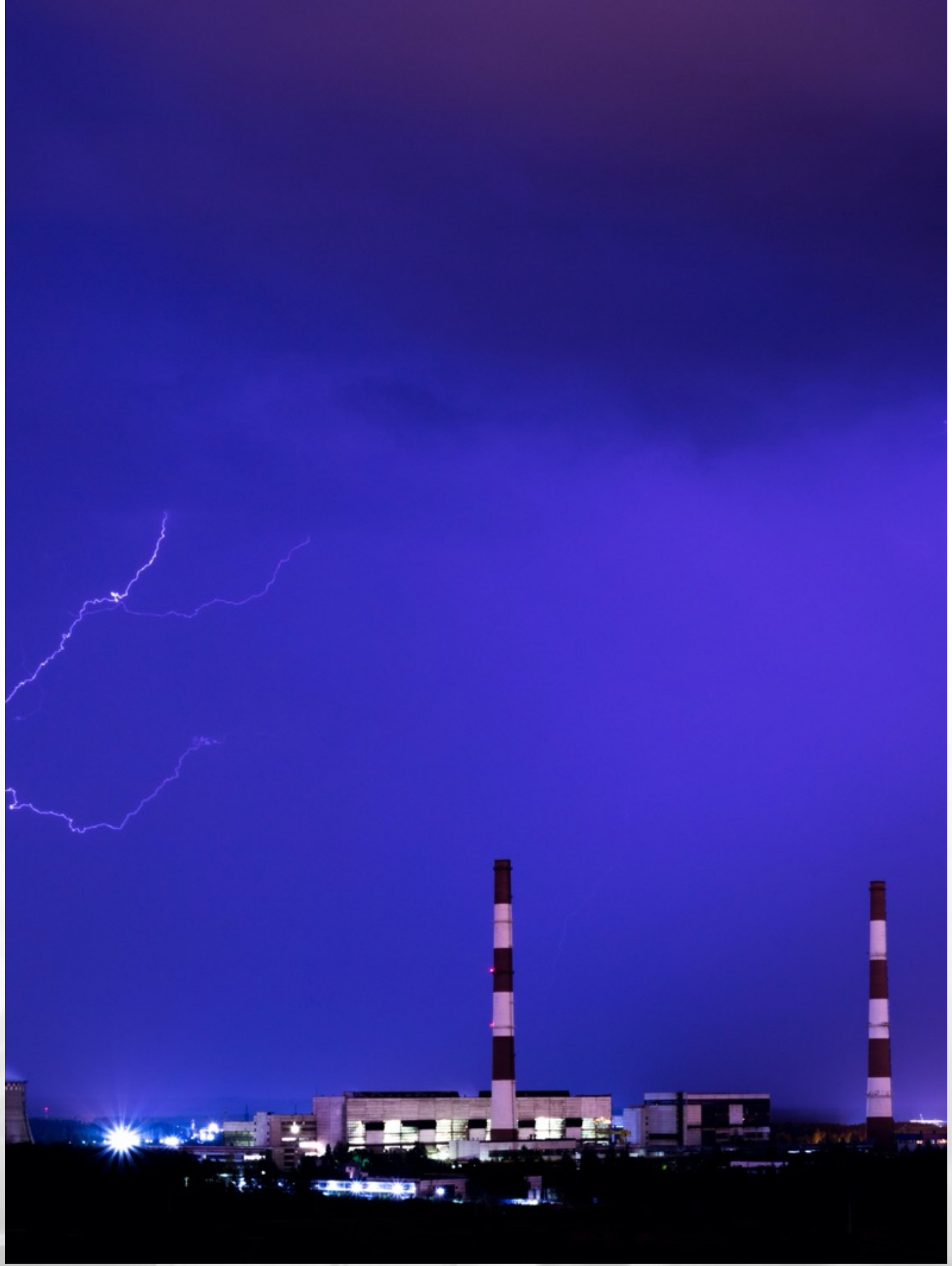
Digitalization of the workplace has been a trendy concept for a while, but quarantine measures are causing it to accelerate. Organisations suddenly had to scale infrastructure to make sure workers have the right conditions to do their job, while trying to keep standard levels of security.

02 Infrastructure and Maintenance Gaps

During emergency situations there is always a shift in focus to maintaining day to day operations. Organizations are having to react quickly to provide remote employees with the tools and information they need to do their work and keep things running during the crisis while suffering budget cuts and halt in recruiting.

03 Shortage of Resources

As much as efforts are doubled to protect personnel, new peaks of infection could still cause staff to be ill and absent. But delivery of critical services such as electricity, natural gas and water must remain dependable and consistent, even if a health emergency severely limits the number of employees and contractors who are able to work.



Threat Landscape

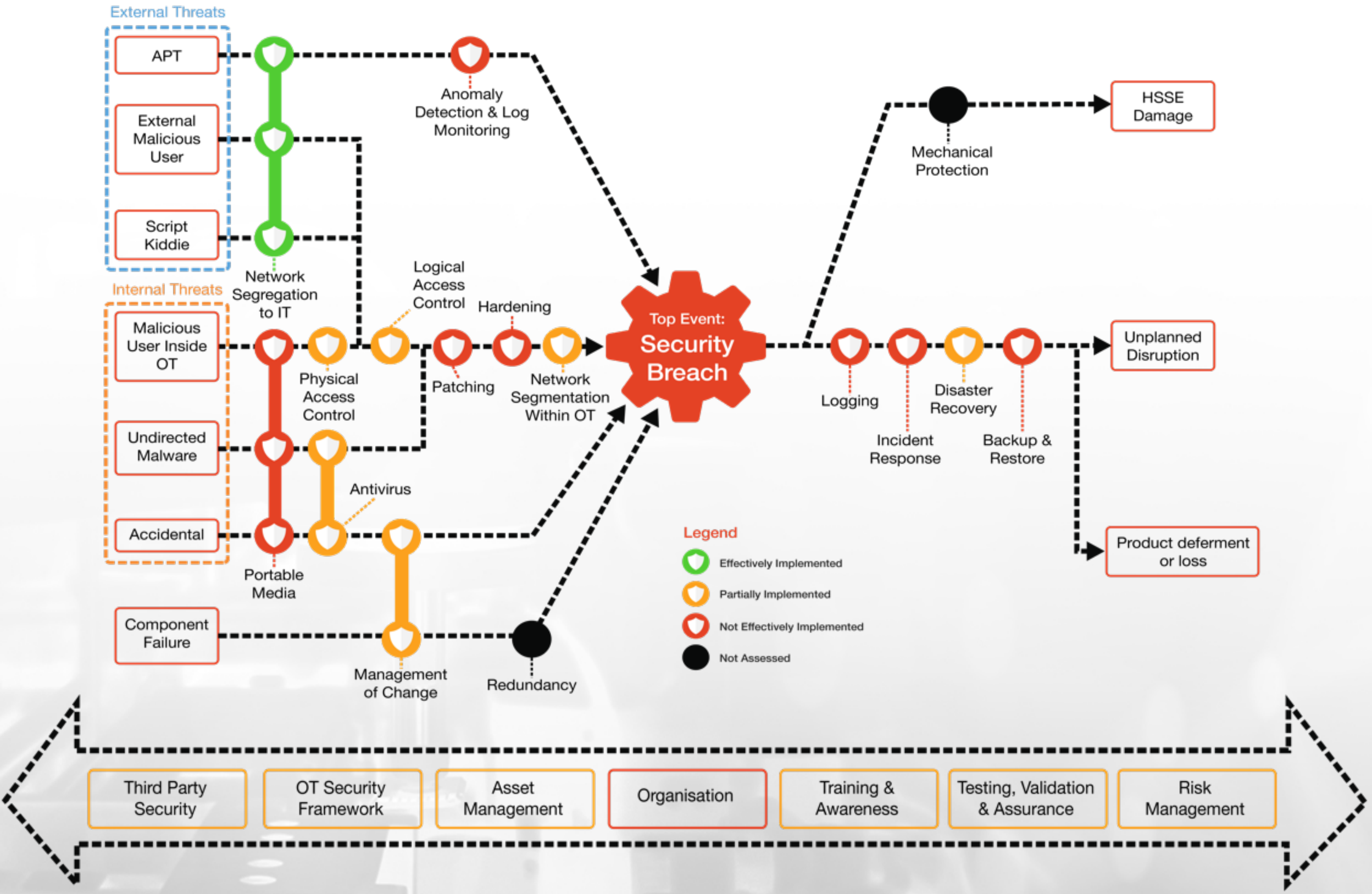
The dependency critical infrastructure has on industrial control systems introduces a variety of security issues that can have a significant impact on the resilience and reliability of OT assets.

Regardless of whether the supporting OT are centralised, stand-alone or embedded they can be exposed to:

- external threats (eg hacking, espionage, denial of service attacks, sabotage)
- internal threats (eg misuse by disgruntled employees, fraud, theft and human error)
- natural disasters (eg storm and flood damage)

Applied Risk

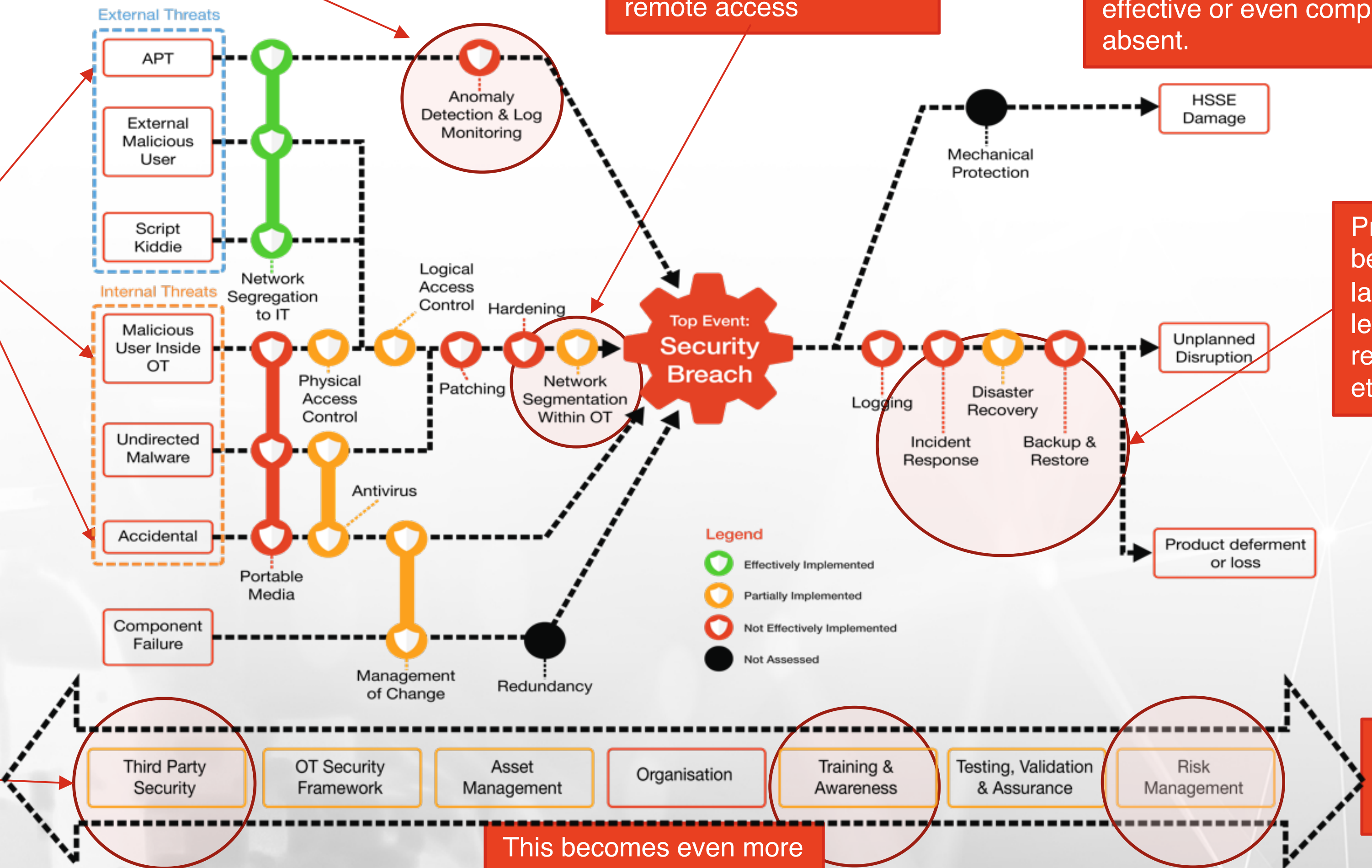
OT Security Bow-Tie Model



Security Control	IEC 62443-2-1 Req
Network Segmentation	4.3.3.4
Access Control	4.3.3.5
System Hardening	4.3.4.3
Patch Management	4.3.4.3
Logging & Monitoring	4.3.4.3
Incident Management	4.3.4.5
Backup & Recovery	4.3.4.3
Business Continuity	4.3.2.5
Asset Management	4.3.4.3
Governance	4.3.2.3
Training & Awareness	4.3.2.4
Risk Management	4.2.4; 4.3.4.2
Physical Security	4.3.3.3

APPLIED RISK CONFIDENTIAL

How COVID-19 Changes the OT Security Bow-Tie



Network traffic will show different patterns.

Network segmentation might need to be reconsidered due to remote access

The residual risk might change due to the fact that controls might be less effective or even completely absent.

Threats might change or likelihood of threats change

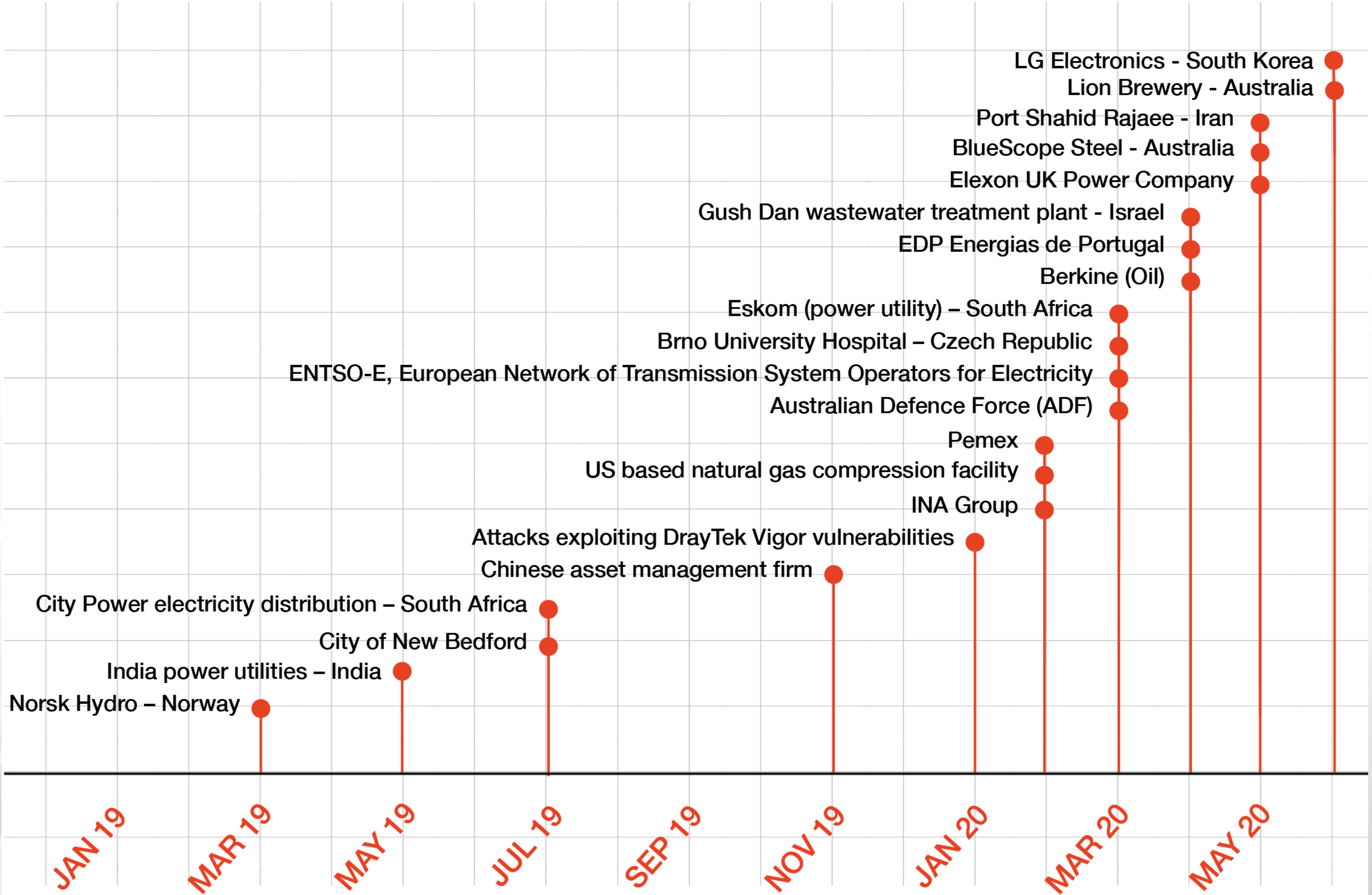
Procedures might need to be reconsidered due to lack of on-site presence, less people on-site, slower replacement processes, etc.

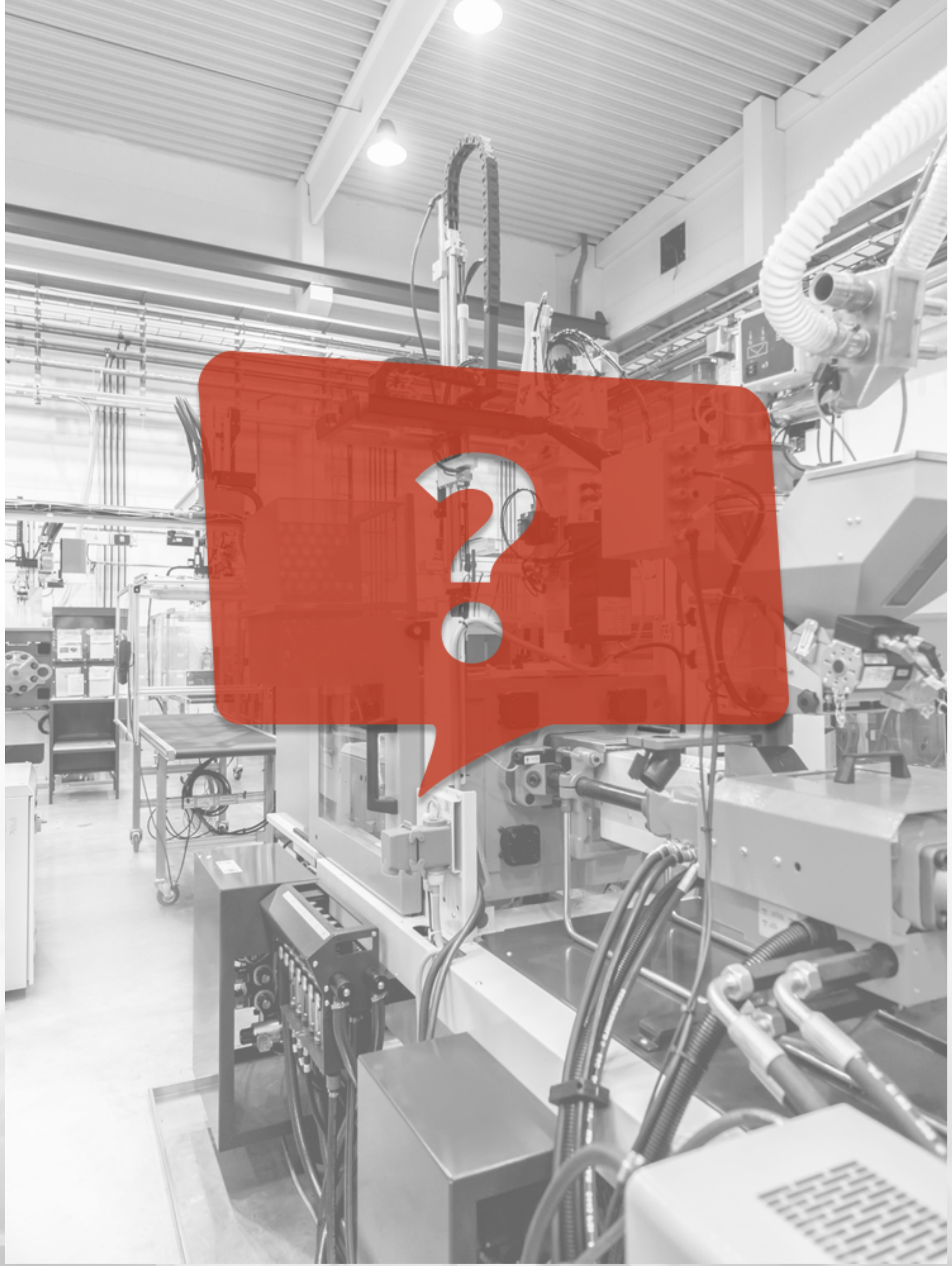
Third party security becomes even more important since these third-parties will work remotely as well. No visibility/control on-site

This becomes even more important for the limited staff that is still on duty

Risk analysis should be updated, considering the new reality

Relevant Cybersecurity Incidents – 2019/2020





Has your organisation made any changes to the incident response plan due to COVID-19?

□ No changes

□ Slight changes

□ Drastic changes

□ Don’t have a cyber incident response plan

□ N/A (not applicable)

Potential Impact to Industrial Environments

Threats can affect OT assets in…	Which can lead to…
Production line machinery that control machine tools and robots and to automate the assembly of products (eg using computer-aided manufacturing (CAM) systems)	• Assembly line failure • Wasted materials and faulty products • Extended operational delays and loss of productivity
Industrial equipment that control the movement of large equipment, direct equipment with requirements for precision, and guide lifting apparatus and transportation equipment	• Failure of automated picking equipment • Inability to locate products • Delayed movement of products
Processing equipment that help gather and process information from sensors in factories, plants and remote locations, often using process control or SCADA systems	• Disruption or failure of processing equipment • Inability to control SCADA devices • Compromise of product quality
Maintenance equipment that support activities such as monitoring readings, processing diagnostic information and test data settings, and configuring equipment (eg production and industrial equipment)	• Degraded performance • Complete failure of maintenance equipment • Unauthorised access to the corporate network

Potential Impact to Industrial Environments

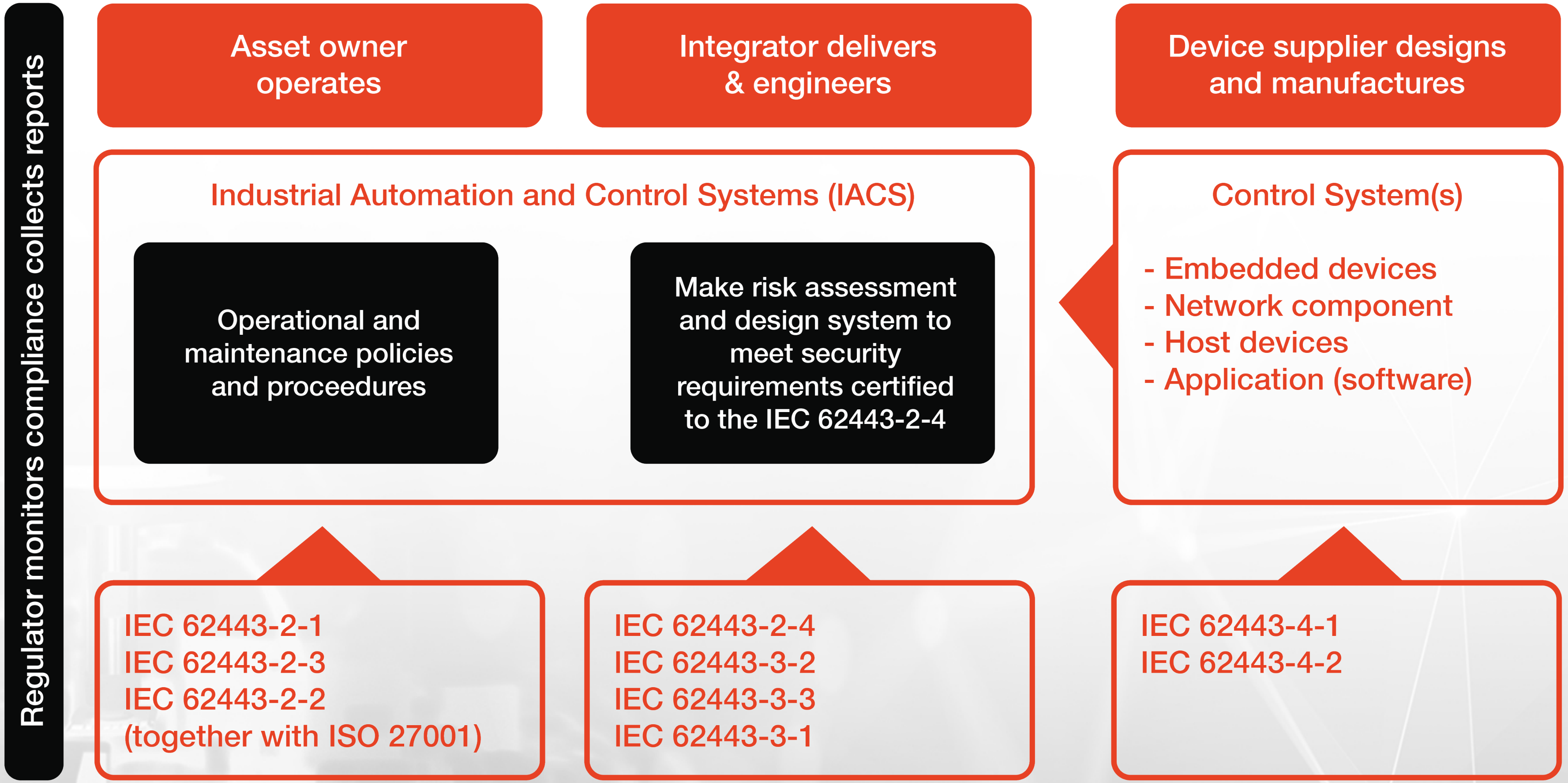
Threats can affect OT assets in…	Which can lead to…
Water processing equipment that support equipment that treats water (eg filter and purify), monitors the quality of water and prepares water for distribution and consumption	• Uncontrolled release of effluent into river • Disruption or loss of water supply to the community • Water contamination
Supply pipeline equipment that control the equipment (eg pumps and valves) that supplies water, oil and gas, and manages elements such as quantity, flow and pressure through the pipeline	• Failure or destruction of pipeline equipment • Major environmental impact • Serious injury or loss of life
Electricity supply equipment that run equipment that controls distribution and quality of electricity supply across the national grid (ie network of power lines across a region or country)	• Disruption or loss of the electricity power grid • Extended periods without electricity supply • Brownouts and unstable supply of electricity to large regional areas

Potential Impact to Industrial Environments

Threats can affect OT assets in…	Which can lead to…
Transport that perform vehicle tracking, handle real-time navigation and communication (eg flight systems), and check the location and function of automated logistic systems (eg in distribution centres and warehouses)	• Difficulty scheduling deliveries and optimising routes • Inability to track goods in the supply chain • Harm to drivers, passengers and goods
Transport control equipment that control or assist the movement of vehicles on roads (eg using traffic lights), trains on the rail infrastructure, ships in a harbour, and airplanes during flight (eg air traffic control)	• Accidents resulting in serious injury or loss of life • Failure to deliver products • Significant delays in public transport
Healthcare equipment that control medical equipment, monitor real-time patient-related information, process testing results and communicate information between medical staff	• Delays in the treatment of patients • Serious injury to patients or loss of life • Disclosure of confidential patient information

4. Recommendations for Securing OT Assets based on IEC 62443

IEC-62443 Series of Standards (Timeless)



Regulator monitors compliance collects reports

Asset owner operates

Integrator delivers & engineers

Device supplier designs and manufactures

Industrial Automation and Control Systems (IACS)

Operational and maintenance policies and proceedures

Make risk assessment and design system to meet security requirements certified to the IEC 62443-2-4

Control System(s)

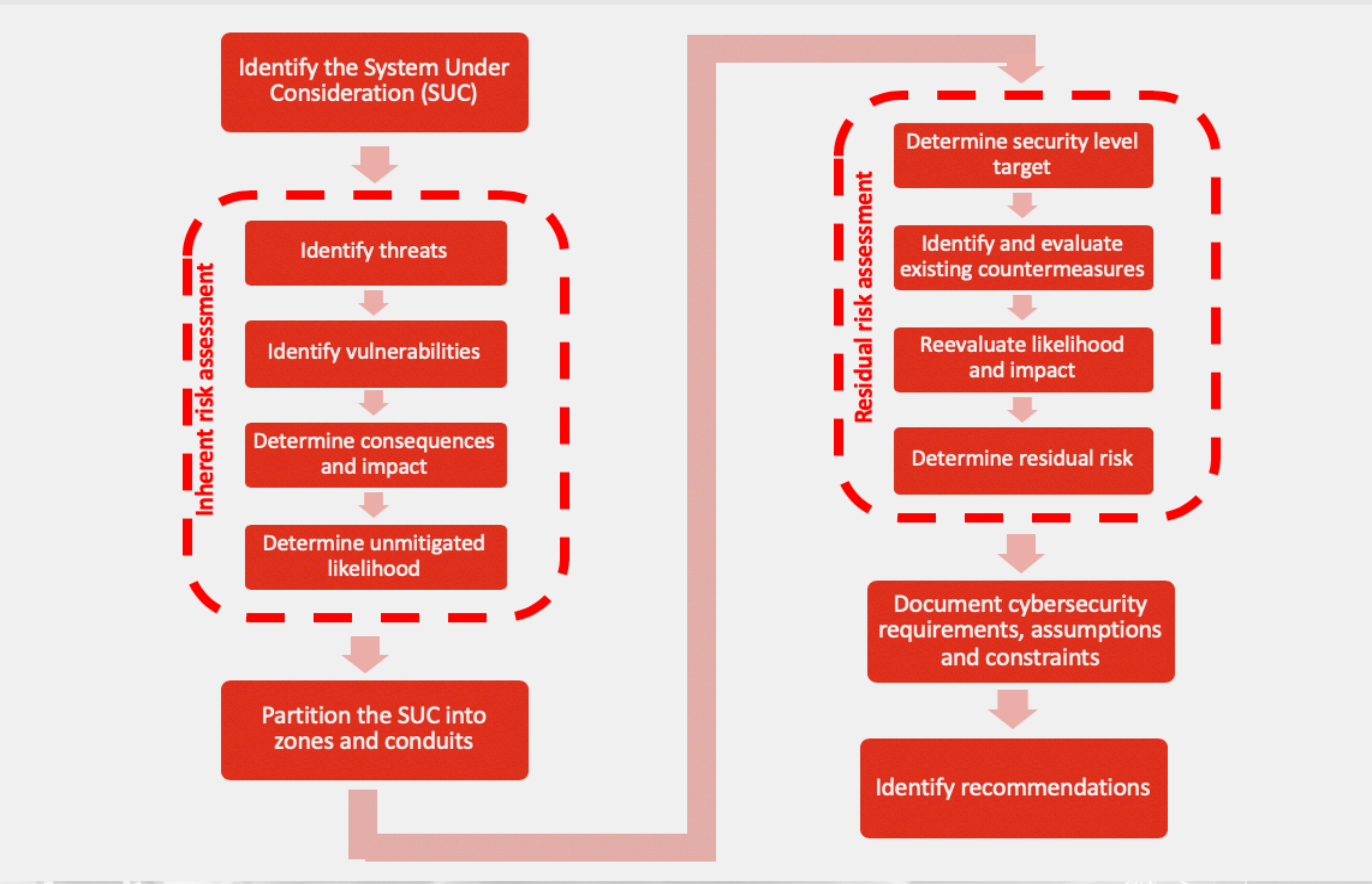
- Embedded devices
- Network component
- Host devices
- Application (software)

IEC 62443-2-1
IEC 62443-2-3
IEC 62443-2-2
(together with ISO 27001)

IEC 62443-2-4
IEC 62443-3-2
IEC 62443-3-3
IEC 62443-3-1

IEC 62443-4-1
IEC 62443-4-2

Risk Assessment in Action (IEC 62443-3-2)



Identify the System Under Consideration (SUC)

Inherent risk assessment

Identify threats

Identify vulnerabilities

Determine consequences and impact

Determine unmitigated likelihood

Partition the SUC into zones and conduits

Residual risk assessment

Determine security level target

Identify and evaluate existing countermeasures

Reevaluate likelihood and impact

Determine residual risk

Document cybersecurity requirements, assumptions and constraints

Identify recommendations

Security Level Vectors

FOUNDATIONAL REQUIREMENTS

1. Identification and authentication control (IAC)
2. Use control (UC),
3. System integrity (SI),
4. Data confidentiality (DC),
5. Restricted data flow (RDF),
6. Timely response to events (TRE), and
7. Resource availability (RA).

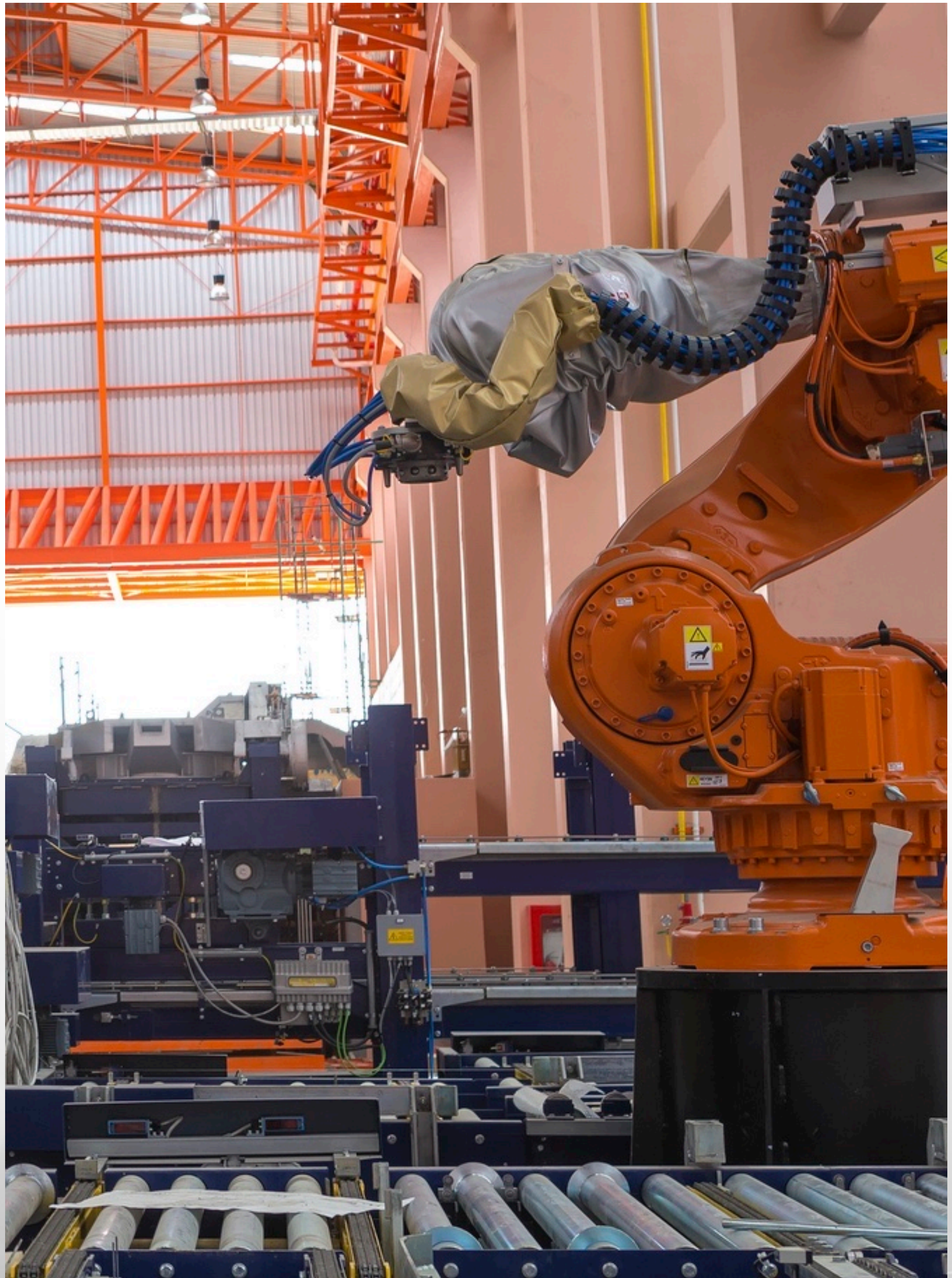
SECURITY LEVELS

SL 0	Does not set specific requirements or specify cybersecurity protections.
SL 1	Requires protection against casual violations.
SL 2	Requires protection against intentional violations with low resources, general knowledge and low motivation.
SL 3	Requires protection against intentional violations with sophisticated resources, specific knowledge of automation and control systems, and moderate motivation.
SL 4	Requires protection against intentional violations with sophisticated resources, advanced knowledge of automation and control systems, and high motivation.

Recommendations for Securing OT Assets

Understanding OT cyber risk and situational changes become imperative in light of the COVID-19 crisis. These are some practical recommendations that will help your organisation survive these unprecedent times and keep your assets safe and reliable:

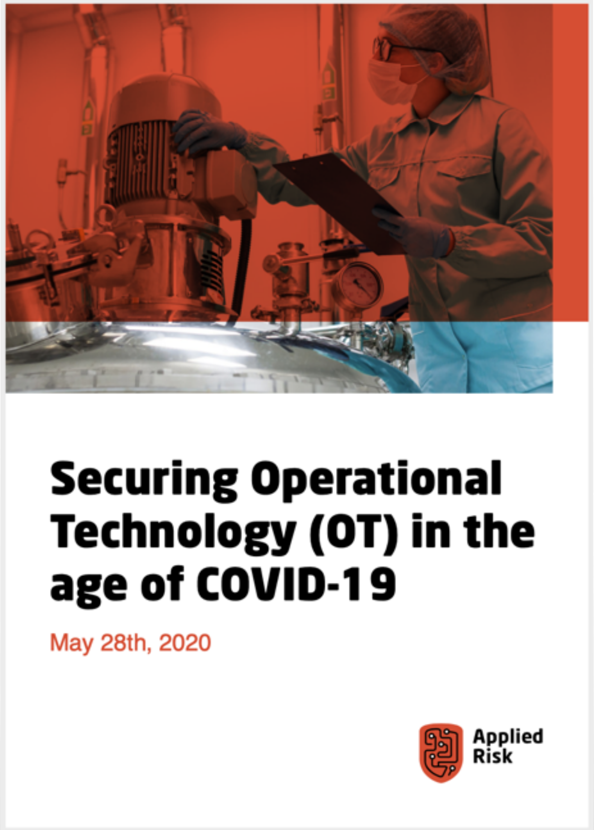
1. Understanding the new OT cyber risk
2. Establish security baseline appropriate to remote work
3. Enhance security capabilities with focus on prevention and response
4. Refresh the security reference architecture (Zone, Conduits and Channels)
5. Review Incident Response Plan



Download the white paper

Download

applied-risk.com/resources/covid19



Securing Operational Technology (OT) in the age of COVID-19

May 28th, 2020

Applied Risk

Questions?

Applied Risk | Critical Infrastructure Made Secure.

Contact

+31 (0) 20 844 4020
info@applied-risk.com
www.applied-risk.com
Teleportboulevard 110, 1043 EJ
Amsterdam The Netherlands