Kaspersky Industrial Cybersecurity Conference

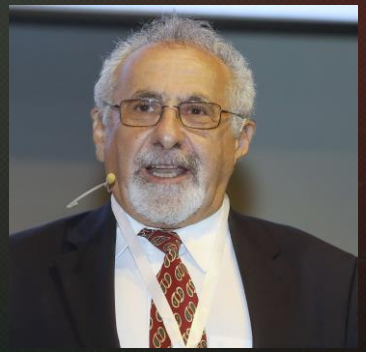
Mitigating ICS Cyber Security Risks through the VLR Triad

kaspersky

kaspersky

……. Presenter's Introduction

- 1976 -1990 Tadiran Inc.
- 1991 - 2011 Motorola Solutions Ltd
- 2011 - 2013 Siemens Israel, Ltd
- 2014 - 2014 Waterfall Security Ltd
- 2014 - SCCE – Consultant
- 2015 - SCCE - Workshop Trainer
- 2018 - SCCE - ISO 27001 Auditor
- 2020 - SCCE - Member ISA 62443 committee
- 2022 - SCCE - OT CEP 2022 Panel Member, Singapore

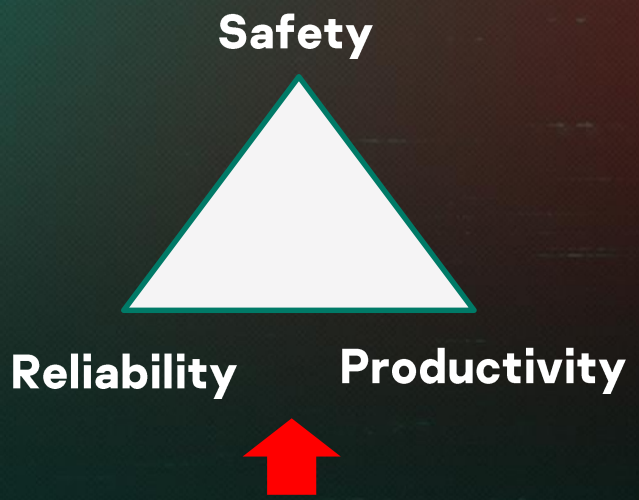


Daniel Ehrenreich

kaspersky

The “Industrial Cyber Security Incident”

- **“Internally Generated attack**
  - Physically inserting a malvertized device
- **Externally Generated Attack**
  - Compromising the IT and later the OT
- **Supply chain-related attack**
  - Downloaded update or a remote service



Any unauthorized internal or external or supply chain initiated electronic or physical activity conducted by an adversary, which directly violates the process run by the ICS-OT and threatens the operating Safety, Reliability, and Productivity (SRP) of the facility.

kaspersky

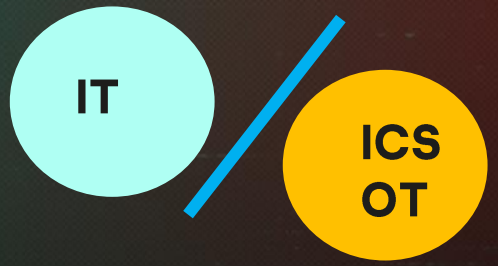
SRP is the goal for ICS-OT Cyber security

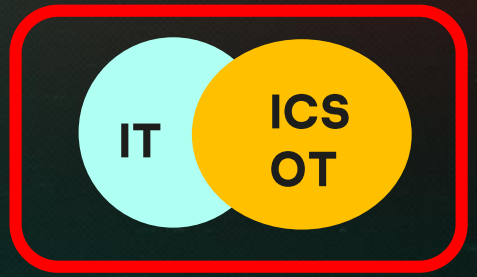
- **Safety Requirement**
  - Machines must not hurt people during their failure or are damaged
  - People must not be allowed in any way to damage the machinery
- **Reliability Requirement**
  - Machines must operate reliably without operating outage or damage
  - Reliability is achieved with correctly designed processes
- **Productivity Requirement**
  - The operation process must deliver the business continuity goal
  - The operation process must assure the quality goals of the plant

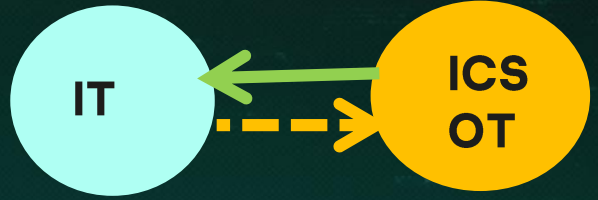
kaspersky

Principles for Creating a Cyber secured ICS

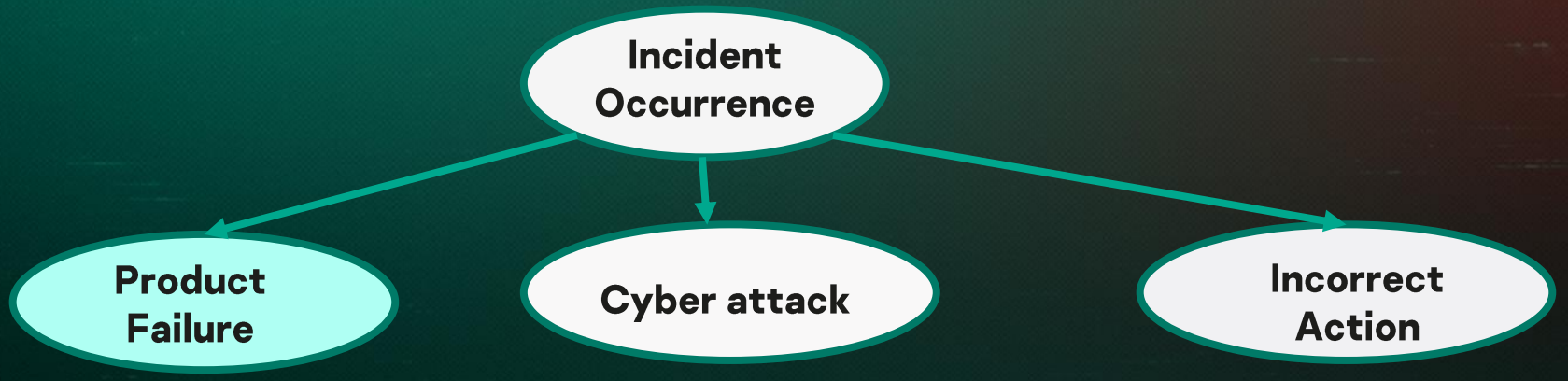
- **ICS –OT and IT architectures must be:**
  - Separately designed with key their key objectives
  - Separately deployed in their dedicated zones
  - Separately tested and commissioned
- **ICS –IT and IT systems Must Not Converge**
  - They can be securely interconnected
  - Using Data Diode, DMZ, Strong firewall, etc.
- **Secured ICS-OT and IT connection:**
  - Improved productivity operations
  - Improved maintenance processes







How Industrial Incidents Might Happen



- Controllers
- Software
- Sensors

- Internal
- External
- Supply Chain

- Mistake
- Sabotage
- Remote access

kaspersky

Factors driving the Industrial Incidents

Incident Occurrence

Unsolved Vulnerabilitie

- Legacy Hardware
- Legacy Software
- Perimeter security

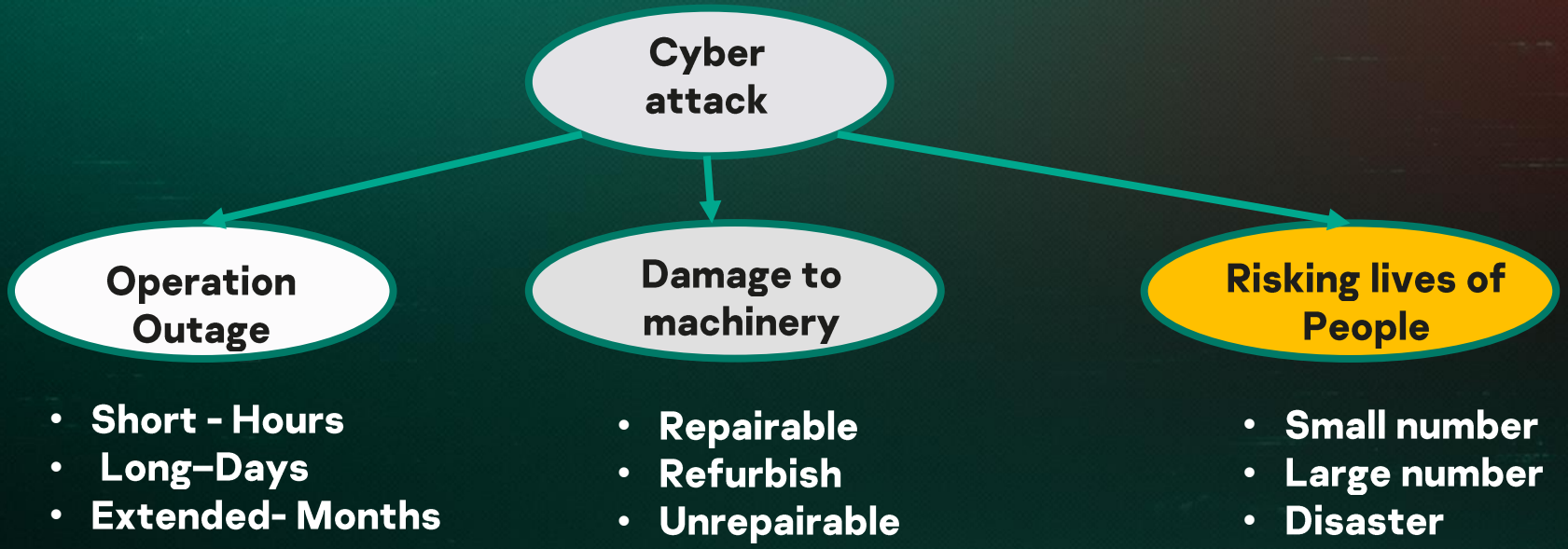
Someone has a Motivation

- Driven by a Reward
- Driven by Revenge
- Forced to do that

Likelihood to Succeed

- Technology Available
- Task is not complex
- Happened before

Consequences of an ICS-OT Cyberattack



kaspersky

Defining the Impact caused by the attack

- **Low impact**
  - Operation outage just for a short time (minutes – hours)
  - Operation outage causing minor impact
- **Medium impact**
  - Repairable damage to industrial machinery
  - Damage to machinery – Replacement is required
- **High Impact**
  - People are significantly hurt during the incident
  - Explosion or fire risking lives of people

ICS Related Impacts:

- Operating Outage
- Damage to Machines
- Hurting people

kaspersky

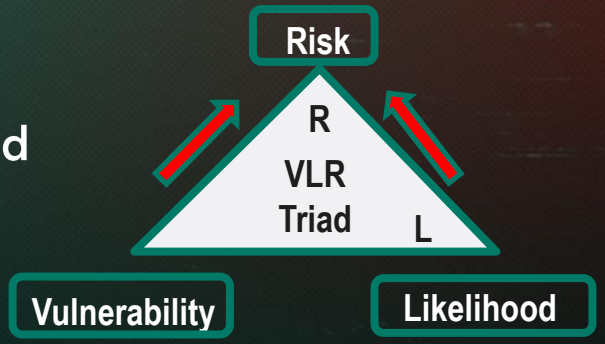
Defining the Vulnerability and Likelihood

- **Defining the Vulnerability**
  - Unknown/ 0 day: It was never published as it was not detected
  - Known / Unsolved: Published, but correction was not implemented
  - Caused by Failure: Unexpected SW of HW failure expose the ICS
- **Defining the Likelihood**
  - Someone has an intention and/or motivation to conduct the attack
  - Cyber capability means having the needed expertise and tools
  - Resources: Someone is financing the whole attack attempt

kaspersky

Defining the VLR Triad

- **Existing Vulnerability**
  - Rated on the scale of 1 (low) to 5 (very high)
  - Makes the attack easier to conduct.
  - May be internal , external or supply chain related



- **Existing Likelihood**
  - Rated at the scale of 1 (low) to 5 (very high)
  - Someone provides the needed resources / financing
  - Capability is created by technical knowledge

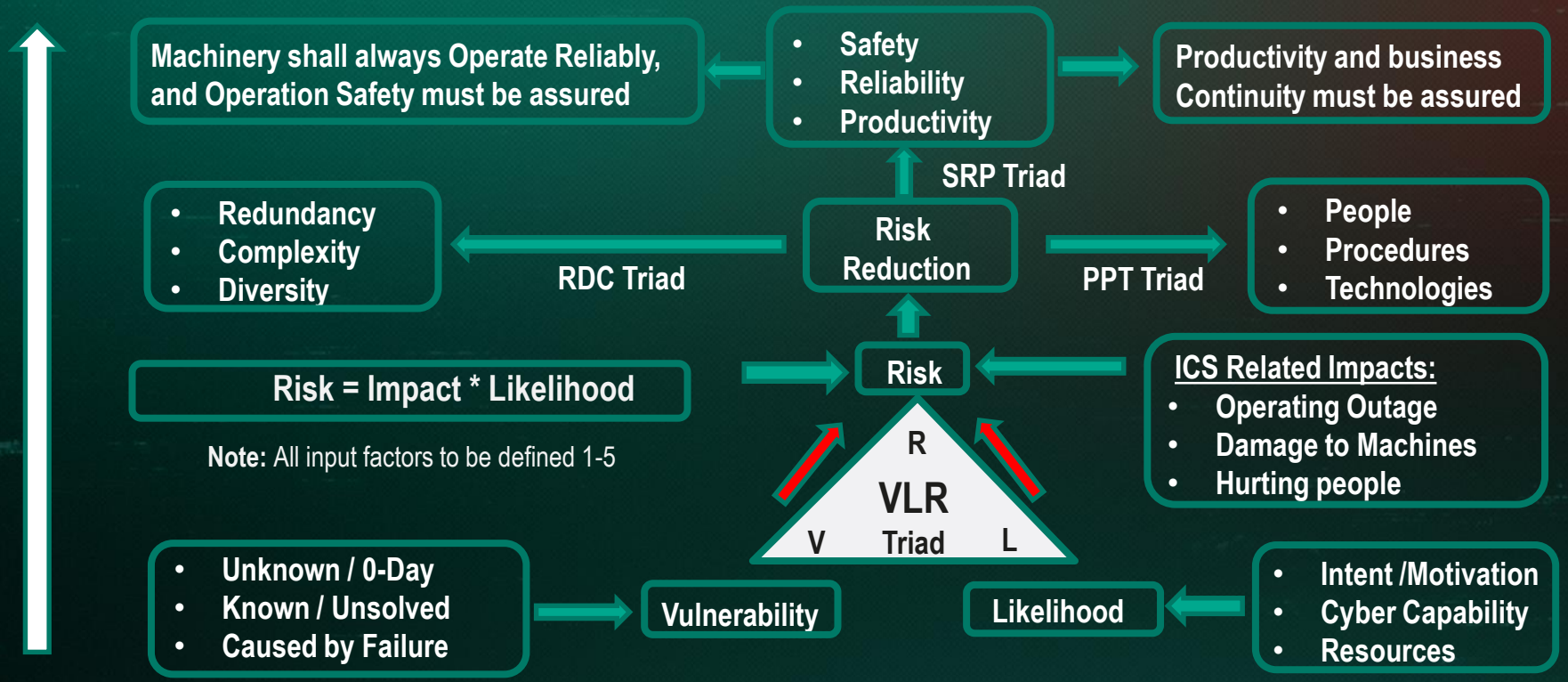
kaspersky

Selecting solutions for Risk Reduction

- **Reducing the Risk through the PPT Triad**
  - P-People: Must be trained and knowledgeable to protect the system
  - P- Procedures/Policies: Must be written, accessible and enforced
  - T- Technologies: Upgrades to be planned and budget to be allocated

- **Reducing the Risk through the RDC Triad**
  - R- Redundancy: Deployed to prevent operation outage during failure
  - D- Diversity: Use of defense mechanism from different vendors
  - C-Complexity: System must not be simple, making the attack complex

Summary of the presented Method



Kaspersky Industrial Cybersecurity Conference

Thank you!

Daniel Ehrenreich

Consultant and Lecturer ICS Cyber Security

SCCE

Daniel@scce.co.il

kaspersky