codewerk

Cybersecurity for Rolling Stock

No
-
a square lock does not keep the attacker away

Let's focus on three use cases of the Cyber Resilience Act.

Greenfield development of components

Start from scratch
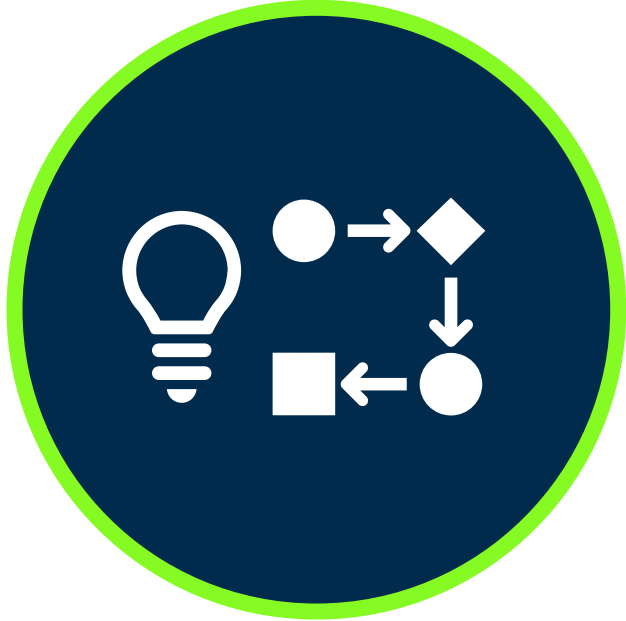
Upgrading existing components

Enhance existing systems

Railway retrofitting

Adapt legacy trains
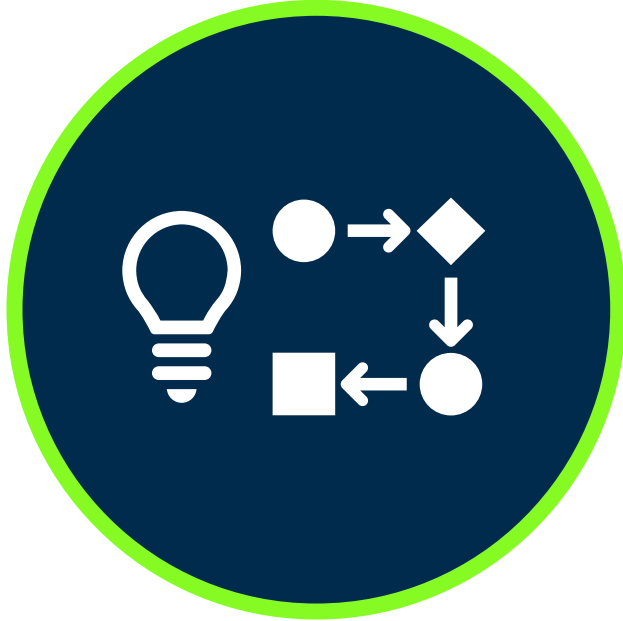
The security lifecycle in reality

Greenfield development of components

Start from scratch

The security lifecycle in reality

Sales promised SL3

Greenfield development of components

Start from scratch

The security lifecycle in reality

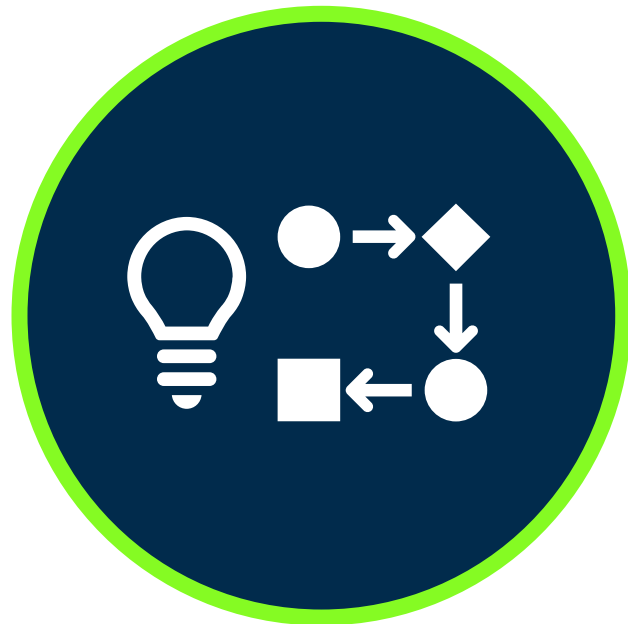**Greenfield development of components**

Start from scratch

Sales promised SL3

How security understood requirements

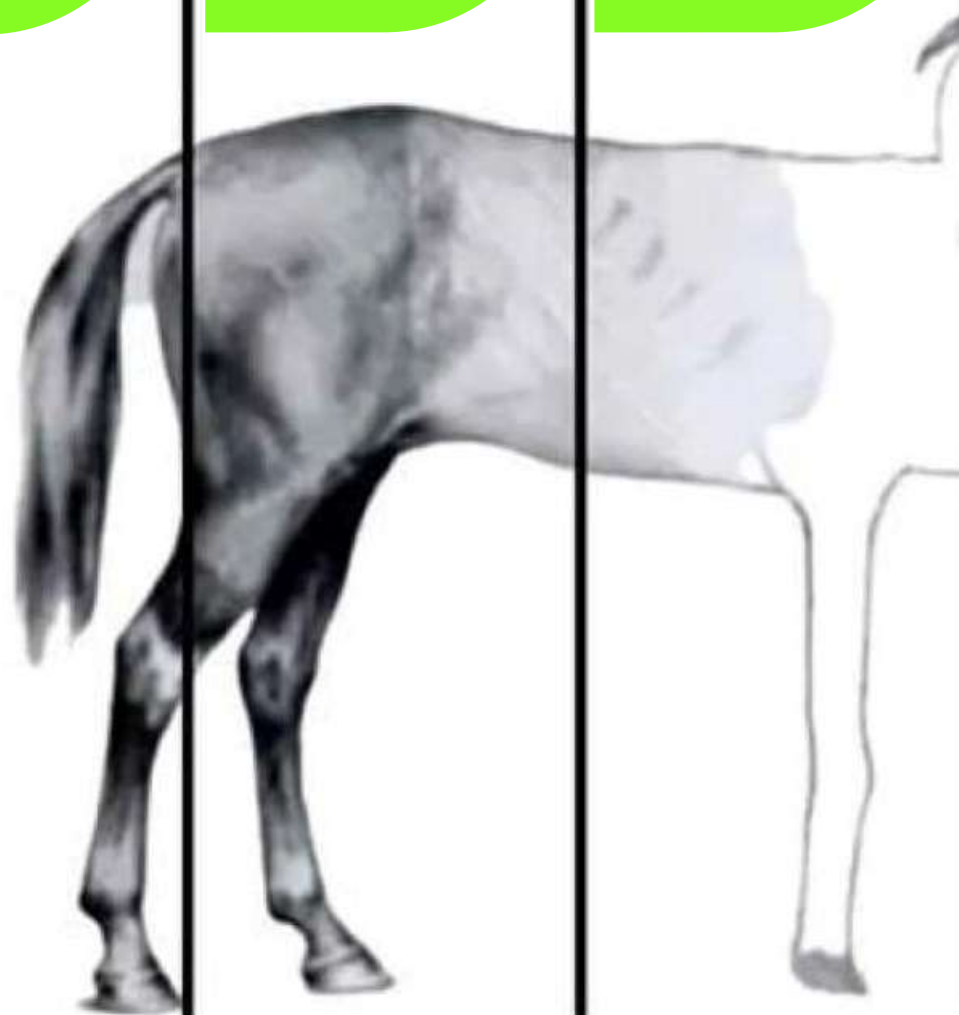# The security lifecycle in reality

Greenfield development of components

Start from scratch

Sales promised SL3

How security understood requirements

Security after budgeting

The security lifecycle in reality
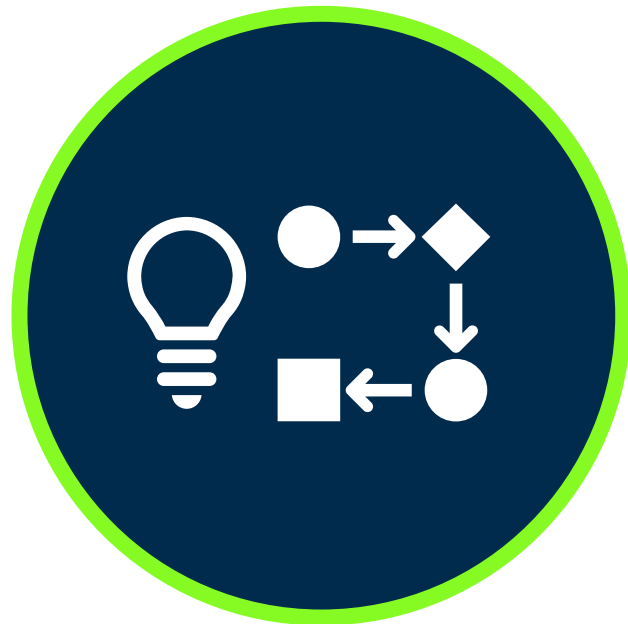
Greenfield development of components

Start from scratch

Sales promised SL3

How security understood requirements

Security after budgeting

From a pentester's perspective
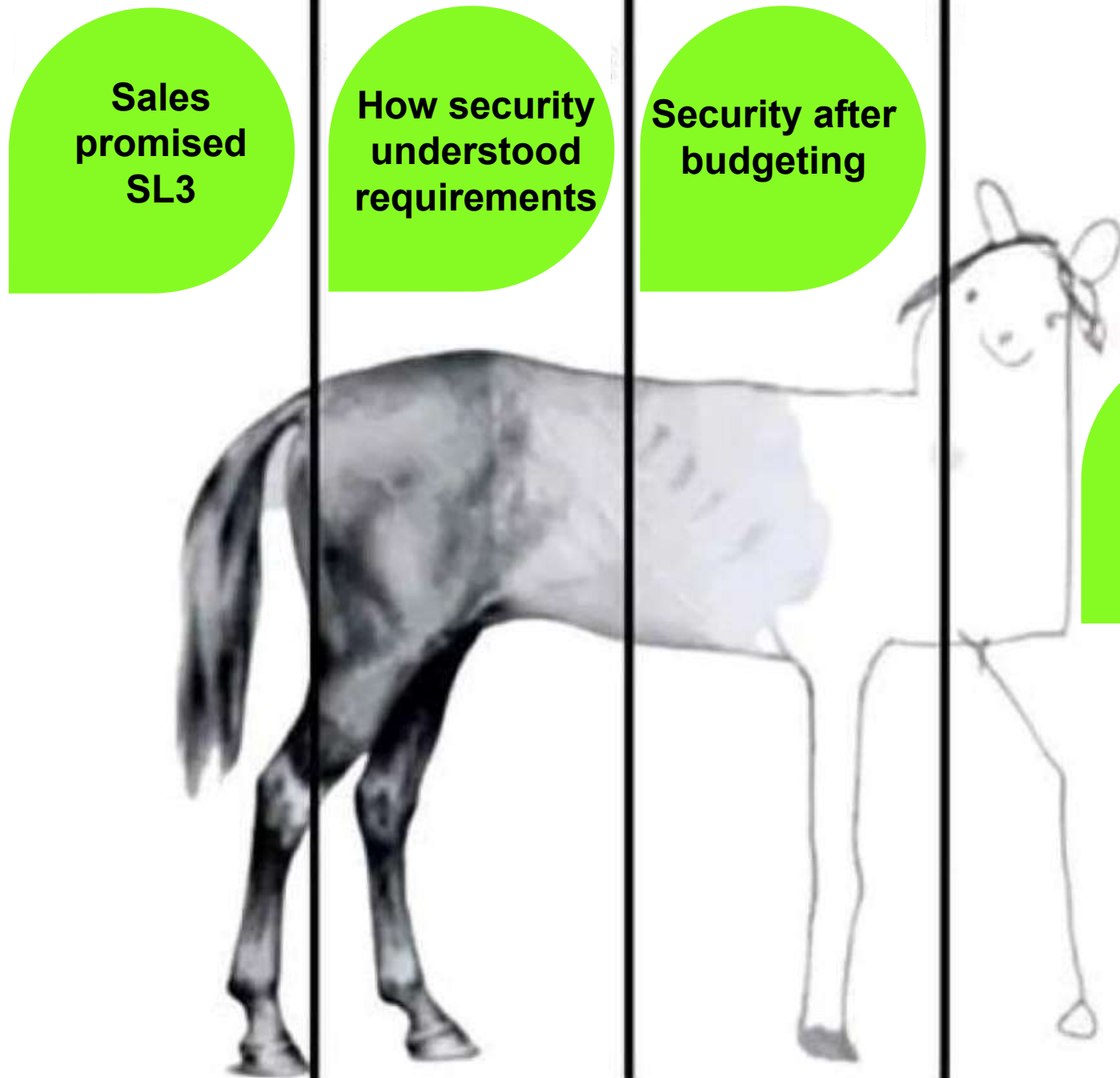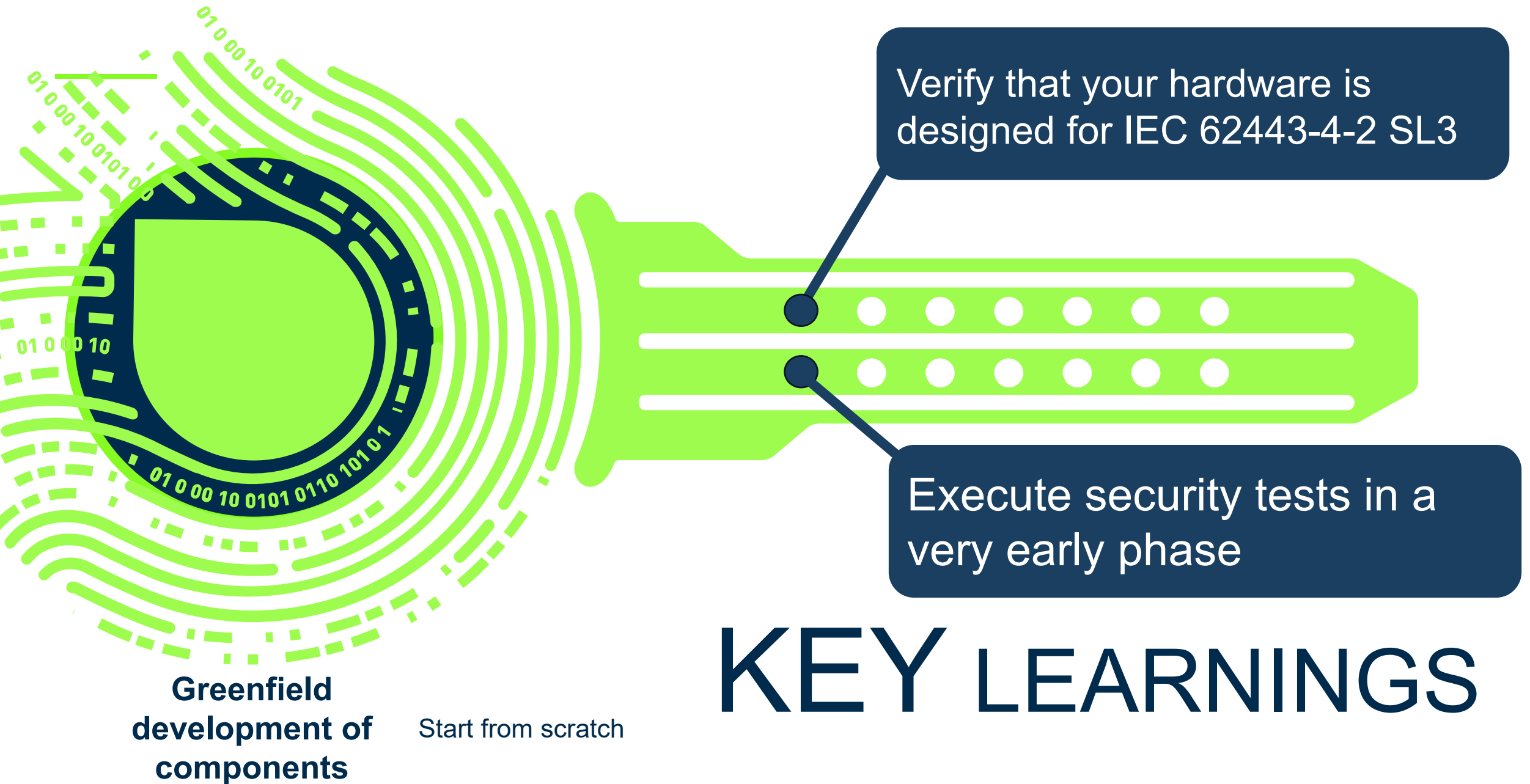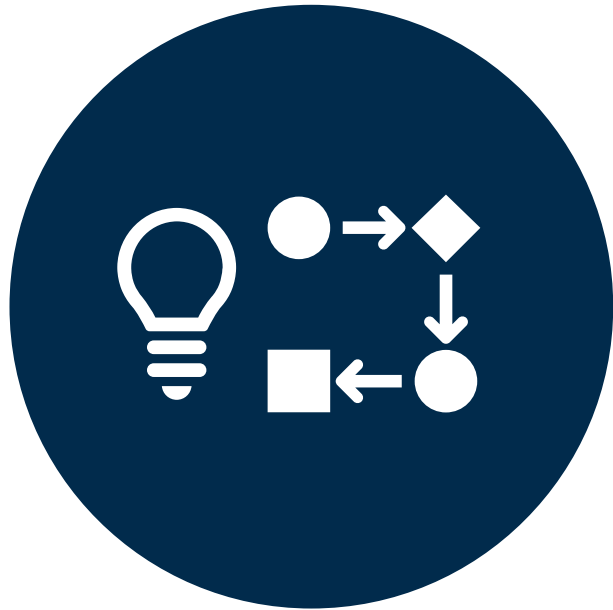
Verify that your hardware is designed for IEC 62443-4-2 SL3

Execute security tests in a very early phase

KEY LEARNINGS

Greenfield development of components

Start from scratch

Let's focus on three use cases of the Cyber Resilience Act.

Greenfield development of components

Start from scratch

Upgrading existing components

Enhance existing systems

Railway retrofitting

Adapt legacy trains

Prioritised strategy based on a IEC 62443-3-2 risk assessment

Focus on evaluation criteria of IEC TS 62443-6-2

KEY LEARNINGS

Upgrading existing components

Enhance existing systems

Product development according IEC 62443-4-2 and IEC TS 62443-6-2

IEC 62443-4-2

What shall be implemented?

Network protocols require:

Confidentiality
Integrity
Authenticity

Insecure OT protocols:

CAN, MVB, WTB, TRDP, PROFINET

Is it possible to achieve 4-2 conformity with these protocols?

IEC TS 62443-6-2

How shall it be tested?

Insecure fieldbus protocols can be used if compensating countermeasures are implemented.

Let's focus on three use cases of the Cyber Resilience Act.

Greenfield development of components

Start from scratch

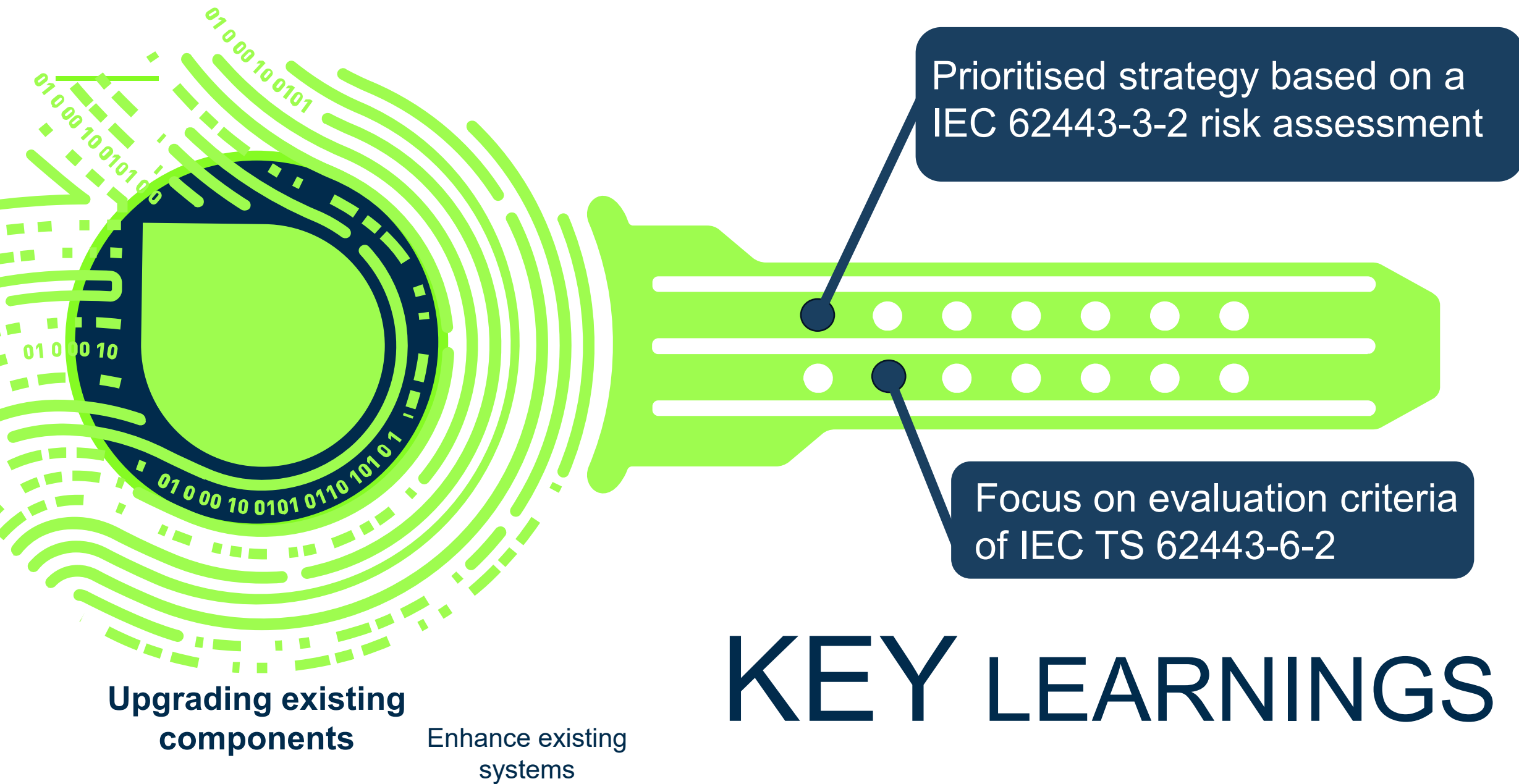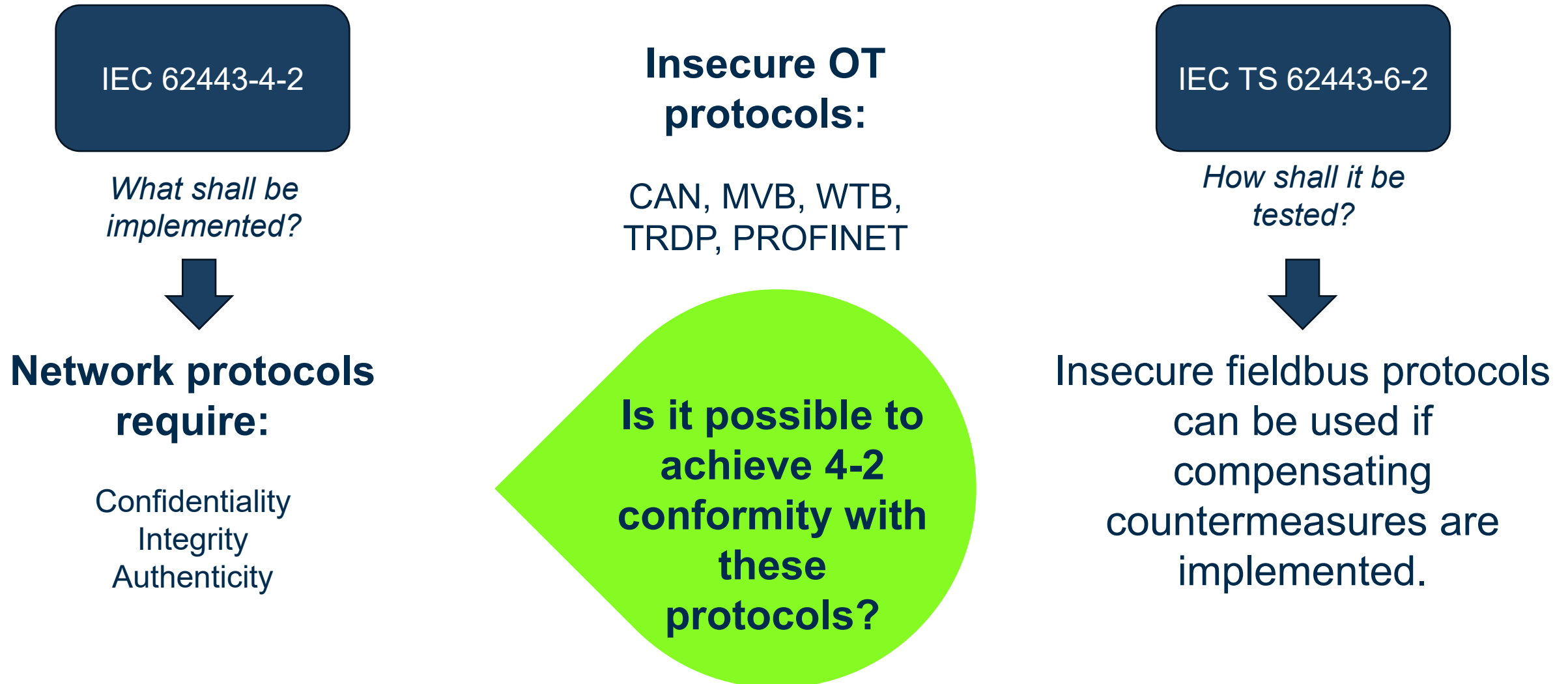**Upgrading existing products**

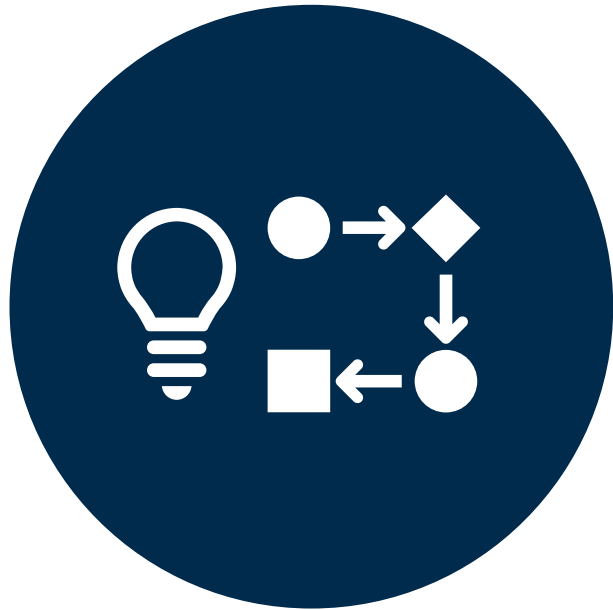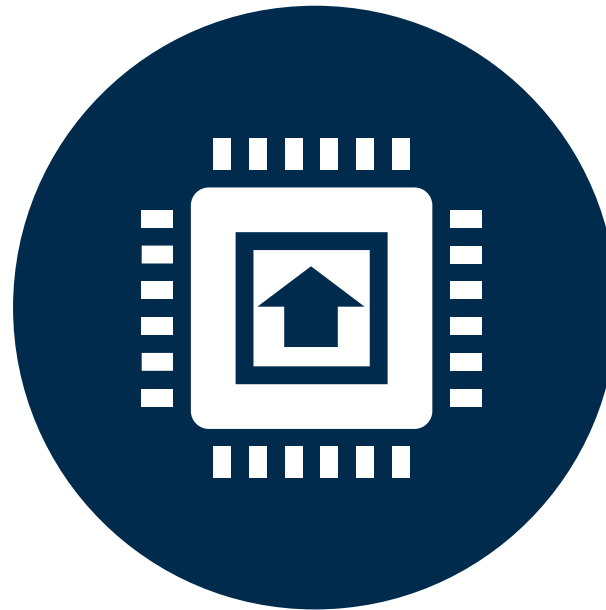Enhance existing systems

**Railway retrofitting**

Adapt legacy trains

Railway retrofitting

Adapt legacy trains

» *Why invest in cybersecurity for older trains?*

They've been operating safely for decades! «

Flat network architecture with direct connection to the operator

Railway retrofitting

Adapt legacy trains

Segment the network

Add a security gateway

Add an intrusion detection system
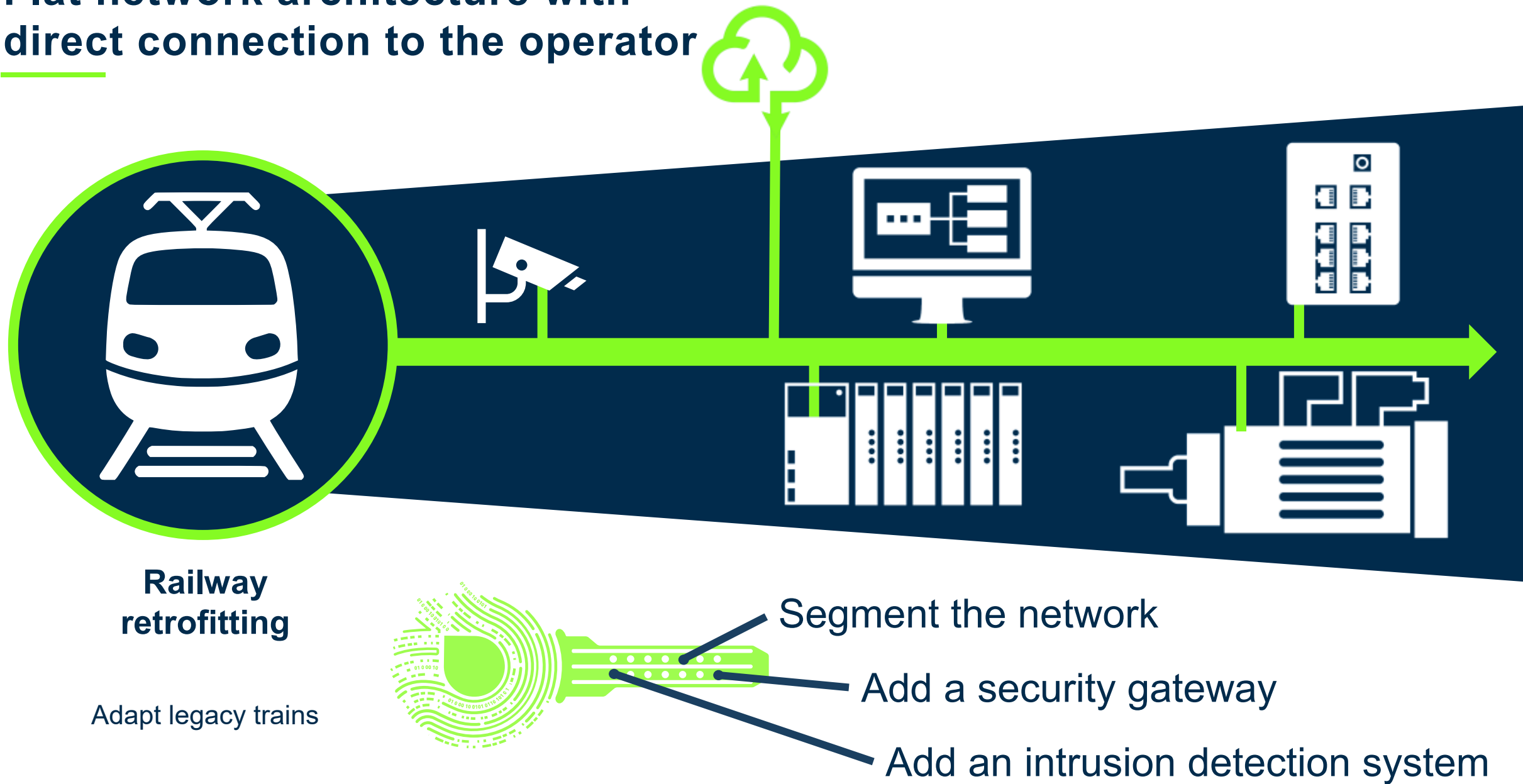
Measures in retrofitting projects

Technical measures

- Network Segmentation

- Security Gateway

- Greatly improves security,
  but must be closely coordinated

Organizational measures

- Physical Access Control

- Intrusion Detection Systems

- Less intrusive changes,
  but require new processes

No
-
a square
lock does
not keep
the
attacker
away

codewerk

Timon Eßlinger

Codewerk GmbH
Siemensallee 75
76187 Karlsruhe

timon.esslinger@codewerk.de

www.codewerk.de

Q&A