SIITS

United Nations Round Table on Protection of transport infrastructure at the stages of design, construction, and operation - Geneva - 7 September 2022

Security aspects designing, constructing and operating inland transport infrastructure

PREPARED.

Anne-Kari Valdal, SIITS and Proactima September 2022

Contents

- Brief introduction

- Questions addressed

1. Why is it important for Governments and other stakeholders to be aware of security risks in their transport infrastructure construction projects?

2. What security risks (or vulnerabilities) may occur in transport infrastructure projects at the stages of design, construction and operation?

3. How can involved stakeholders detect, prevent, and (address) security risks?

4. What can governments do to improve protection of the inland transport infrastructure from security threats?

SIITS

Proactima and SIITS

Proactima «A more secure and sustainable society»

- *SIITS – manging new vulnerabilities and risk in future intelligent transport systems*
- *Consortium with partners from regulating authorities, research/university, technology, insurance, law, investments a.s.o.*
- *Proactima – project responsible/owner*
- *Focusing on understanding possible future transport scenarios – identifying new threats and vulnerabilities – developing awareness, methods and tools to address and control risk*

Statens vegvesen
SJT Norwegian Railway Authority
DISRUPTIVE ENGINEERING
ITS Norway
SINTEF
Tryg
University of Stavanger
inSpire invest
ARVE FØYEN
CIKLUM

SIITS

With funding from
The Research Council of Norway

Focus

Security

Value

Vulnerability

Asset

Threat

Risk

SIITS

Transport and mobility of the future

- *Digital superpowers, secure, effective, green and sustainable*

Anything to worry about?

We have a parallel development in the entire transport sector and among the various actors. Everyone makes technology choices that set the terms for the transport and mobility of the future - but without us having control over the system they are put together in, as a whole

Collected text from animations on previous slide

We have a parallel development in the entire transport sector and among the various actors. Everyone makes technology choices that set the terms for the transport and mobility of the future - but without us having control over the system they are put together in, as a whole

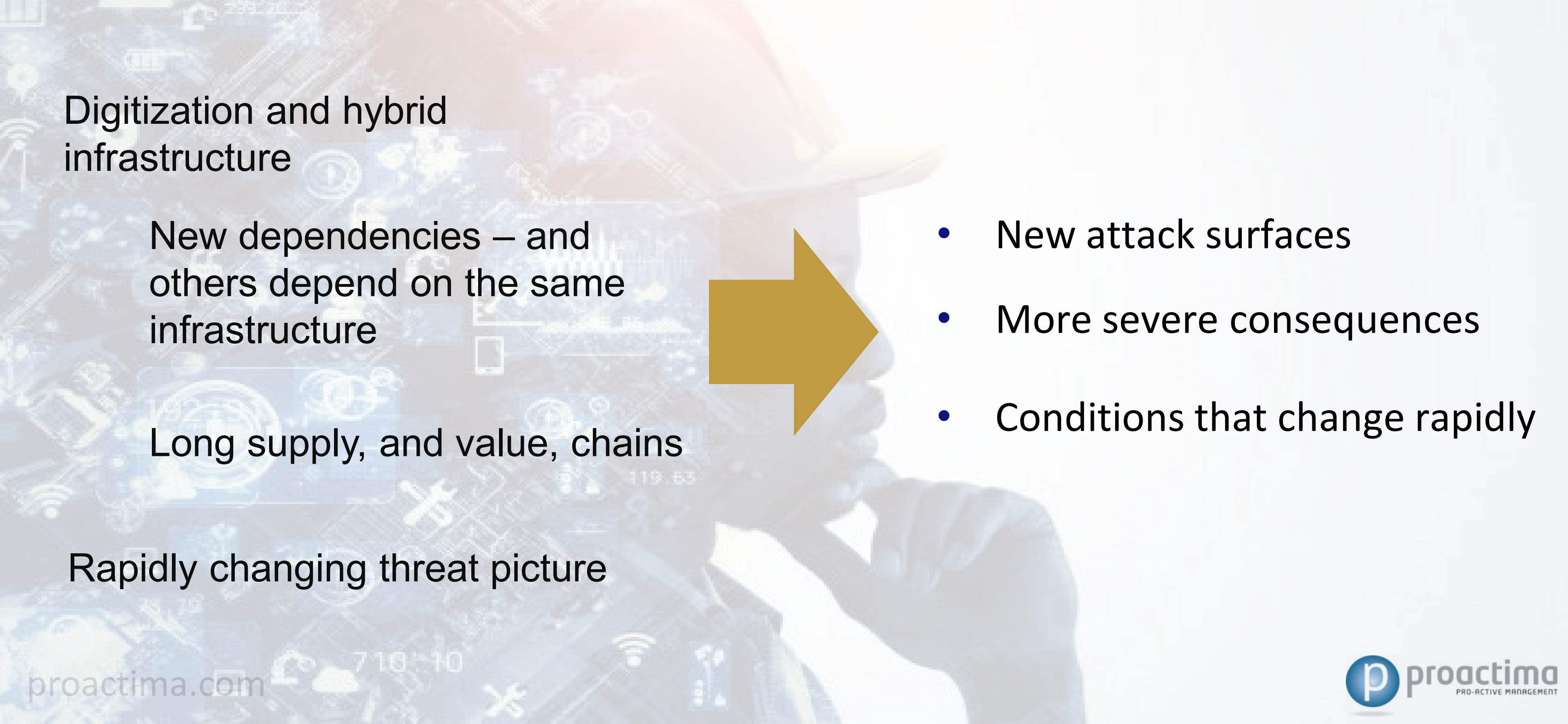
Technology, components and subsystems are connected in large, complex structures characterized by dependencies, long digital value chains and many stakeholders - with different interests. The transport systems have more and new dependencies, and other parts of the society depends on the transport systems

The system's properties, vulnerabilities and risks are not a sum of the parts. We do not fully understand where we become vulnerable, what kind of events or actions that can cause the systems to fail. The threat picture is changing

Regulations, responsibilities and ownership have not been clarified or adapted to this development, or to the integrated transport systems of the future - nationally or internationally

What could be the potential consequences of incidents when everything is connected? How do we stop threats?

Why is it important to be aware of security risks in transport infrastructure construction projects?



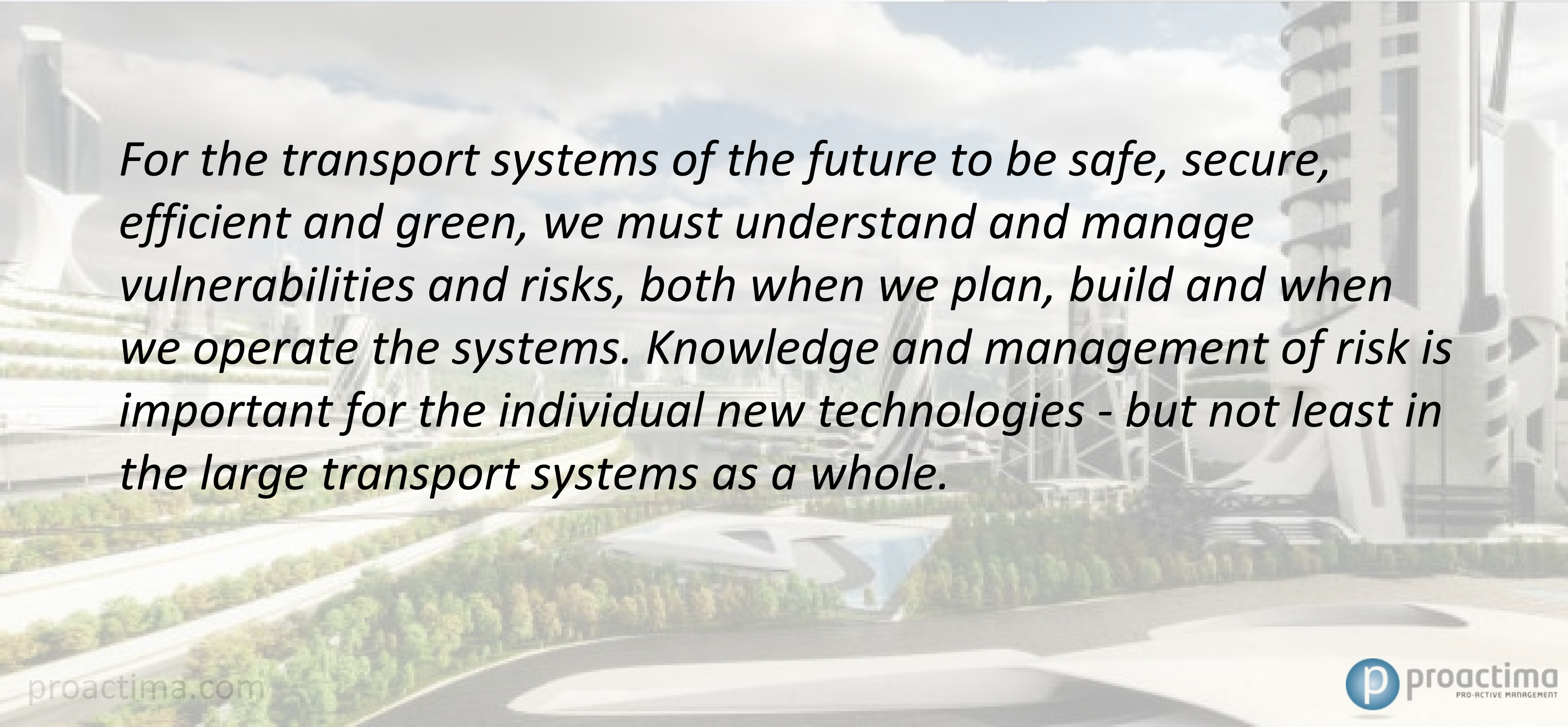
Digitization and hybrid infrastructure

New dependencies – and others depend on the same infrastructure

Long supply, and value, chains

Rapidly changing threat picture

- New attack surfaces
- More severe consequences
- Conditions that change rapidly



For the transport systems of the future to be safe, secure, efficient and green, we must understand and manage vulnerabilities and risks, both when we plan, build and when we operate the systems. Knowledge and management of risk is important for the individual new technologies - but not least in the large transport systems as a whole.

Examples of how security risks (or vulnerabilities) may occur through design, construction and operation

The lack of a common thread from design to operation

- design does not take into account practical operation, and the system is not operated as assumed during design

Plan and design

- Lack of awareness and knowledge
  - not taking into account threats, assets, vulnerabilities, needs for control
- Designing for today – not tomorrow
  - Not resilient to changing threats, technology, climate and requirements
- Designed in a "vacuum", not as part of the whole system
  - Lack of communication, understanding and knowledge
  - Unaware of designed vulnerabilities
- Not protecting the design
  - Either built in vulnerabilities – og just leaking knowledge that can be exploited later

Construction

- Not built as designed
  - Knowledge and lifespan
- Lack of supply chain control
- Information security
  - Access, availability – who builds?

Operation

- Used in different environments and connected to other systems (efficiency)
- Operative measures not according to plan/design
- System changes without updating barriers
- Sharing data – optimization versus security?
- Maintenance, remote control

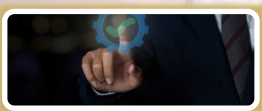
How can involved stakeholders detect, prevent, and address security risks?

Seek information and competence regarding threats, risks and measures – as well as risk management education

Adopt holistic risk management that includes security aspects – starting from planning and design

- Involve relevant stakeholders

Focus on resilience (long term investment)- build in security

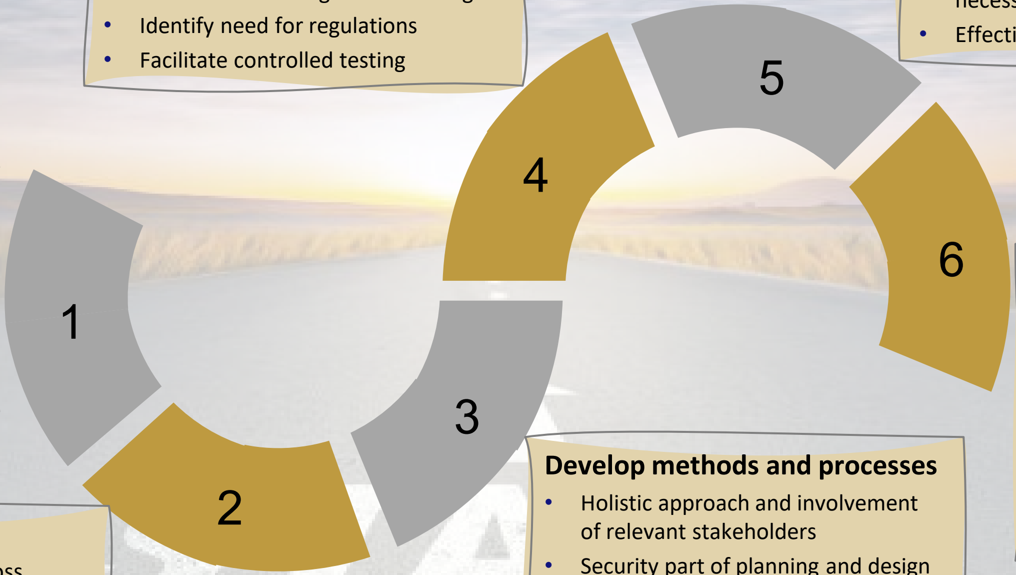


Require and implement existing standards (both technical and management) – internationally

Manage information security in projects (from planning and design and throughout construction and operation)

Establish and participate in industrial cooperation – share experience and best practice

What can governments do to improve protection?



Raise awareness

- Politically and with authorities
- Information to all actors
- Threat assessments

Facilitate cooperation

- Cooperation within and across sectors
- Cooperation across borders
- Understanding, share experiences

Develop methods and processes

- Holistic approach and involvement of relevant stakeholders
- Security part of planning and design
- State security, societal security included

Support and engage in R&D projects and activities

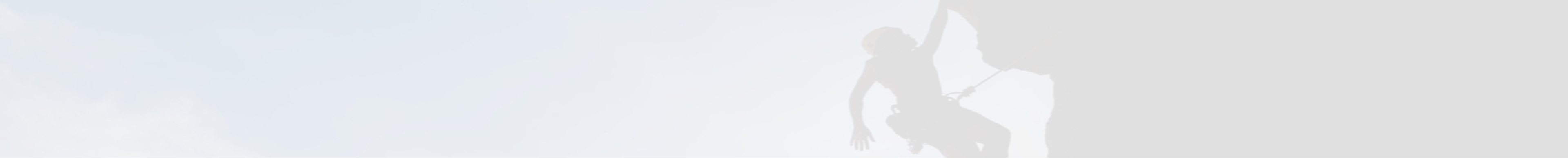
- Gain understanding and knowledge
- Identify need for regulations
- Facilitate controlled testing

Regulate and control

- Require and follow up on existing standards
- Develop new/revised standards sector independent
- Balance need for certainty and control with necessary uncertainty to explore new innovation
- Effective authority control

Educate

- Government and authorities
- Establish relevant educational opportunities
  - Threat and security
  - Complex systems and technology
  - Risk management and analytical methods



proactima.com

Prepared.

Feel free to contact Anne-Kari at anne-kari.valdal@proactima.com

and to have a look at our project website www.siits.no