Welkom!

Ron Beij, Paul Klein en Gea Kolk

vrijdag 29 juni 2018

R.Beij@brandweerAA.nl

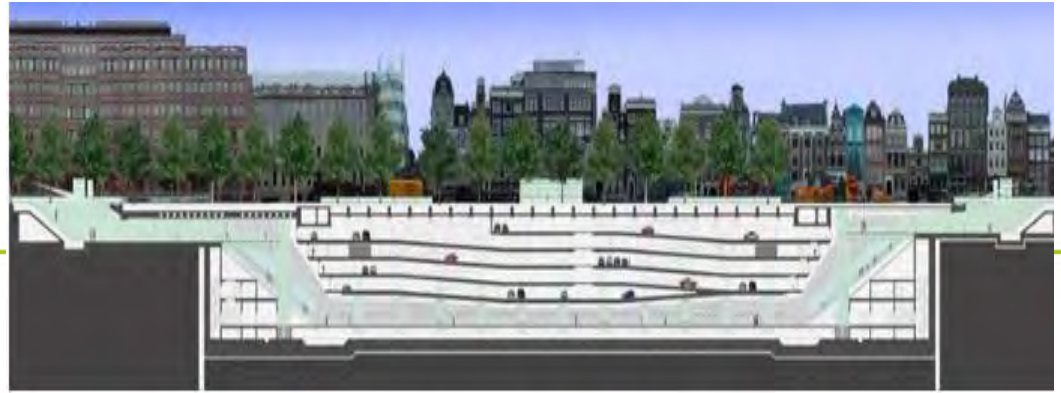
COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

Van Object- naar Systeemveiligheid

Datum

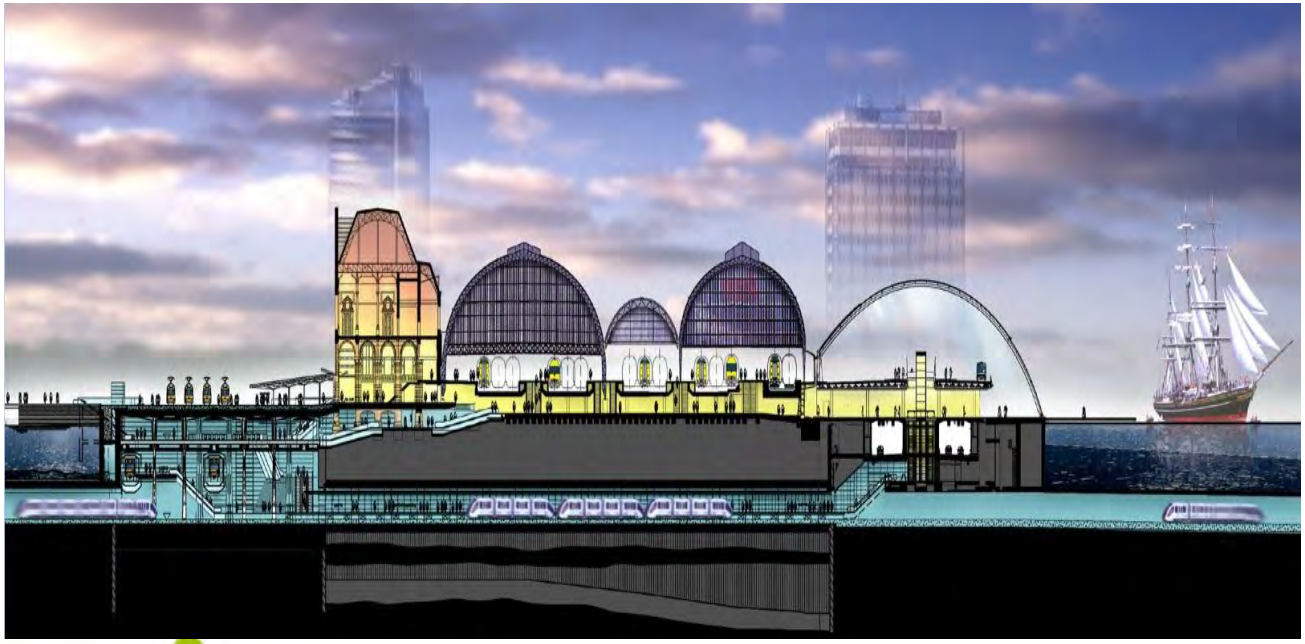
Nederlands kennis centrum voor ondergronds bouwen en ondergronds ruimtegebruik

De aanleiding



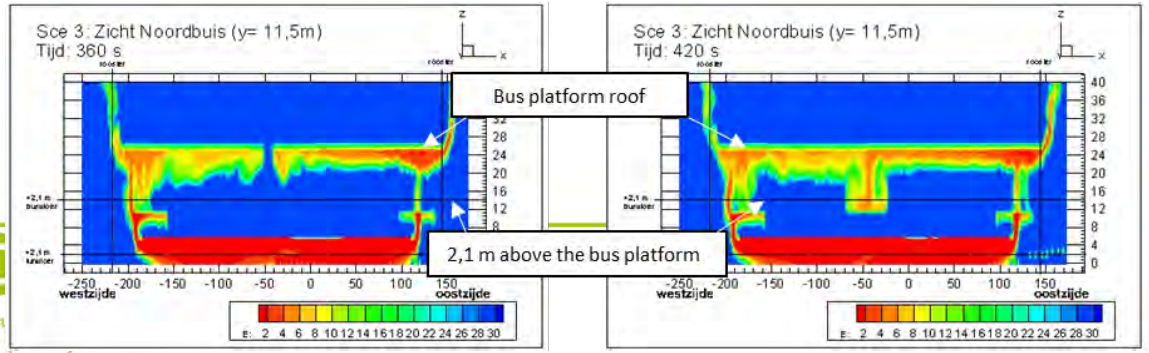
COB
Nederlands kennis centrum voor ondergronds bouwen en ondergronds ruimtegebruik

Meervoudig ruimtegebruik



COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

De Ruijtertunnel



Tunnels

- Tunnels worden vanuit een technisch perspectief ontworpen en gebouwd.
- Ze voldoen aan de wet maar worden ze daarmee ook als veilig ervaren?

Maar

- Zijn ze toekomstbestendig ontworpen ?
- Zijn ze integraal ontworpen?

Wet- en regelgeving

- **Wet en regelgeving is gestolde kennis uit het verleden.**
- **Wetten zijn sectoraal ontwikkeld en zelden op elkaar afgestemd**

En

Nieuwe risico's zitten er nog niet in!

- **Energietransitie**
- **Cybersecurity**
- **Zelfrijdende voertuigen**
- **Meervoudig ruimtegebruik**

De tunnel is onderdeel van meerdere systemen

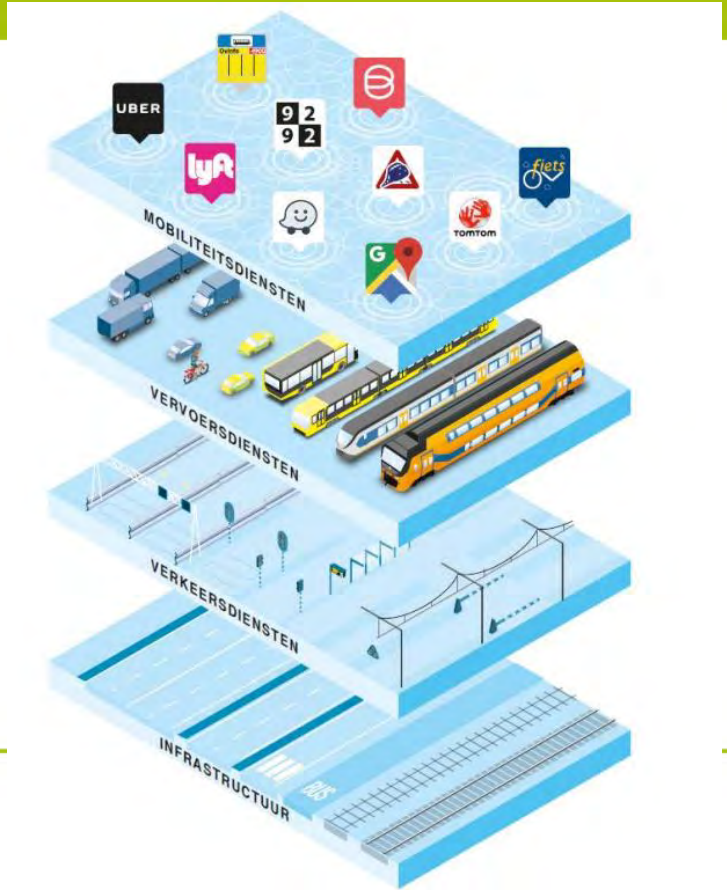
Fysiek/Geografisch

- **Een weg, een route, een netwerk**
- **Een gebouw, een stad, een (metropool) regio**
- **Meervoudig ruimtegebruik**

Sociaal/economisch

Politiek/bestuurlijk

Raad voor de Leefomgeving 2018



COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

Infrastructuur

- Is niet integraal ontworpen maar stapsgewijs gegroeid.
- Is niet primair ontworpen met veiligheid als doelstelling.
- Na verloop van tijd veranderen het gebruik en de gebruiker
- Verschillende modaliteiten raken steeds vaker vervlochten.
- Infra is daardoor onderling afhankelijk geworden

Overzien we het geheel nog wel?

COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

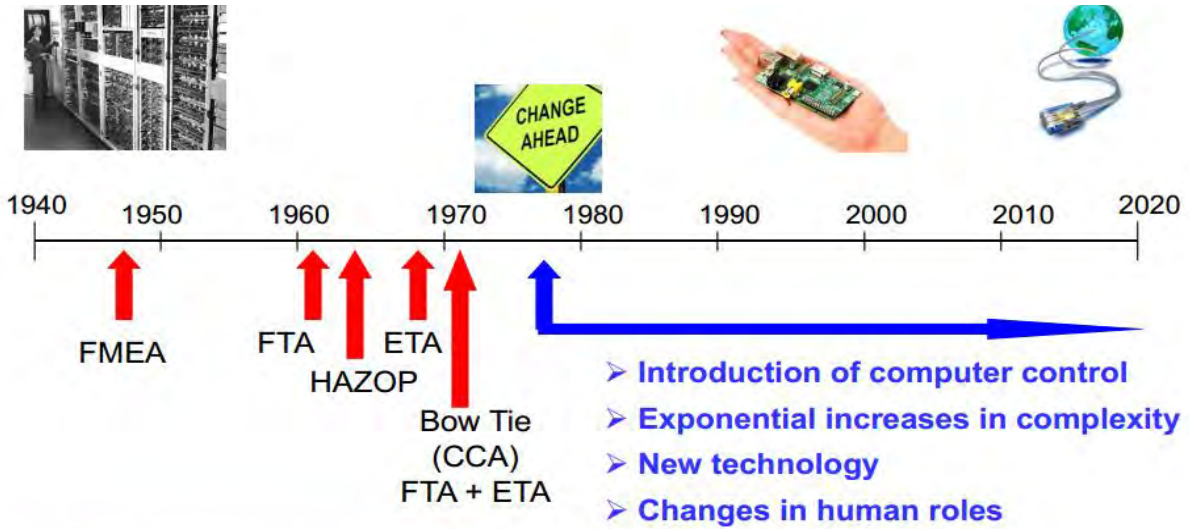
De Trucendoos

- Theorieën
  - Systeemtheorie
  - Complexity theorie
  - Chaostheorie
  - Speltheorie
- Analyses
  - Actoren
  - MKBA
  - Monte-Carlo
  - Real options

De Trucendoos

- Modelering
  - System enginering
  - System dynamics
  - Agent based modelling
  - Discrete event simulations
  - Gaming
- Standaardisering
  - Interoperabiliteit
  - Interconnectiviteit
  - Functionele eisen
  - Prestatie eisen

Onze instrumenten zijn echter al 50-60 jaar oud. En onze technologie is enorm verandert!



Nancy Levenson, 2018

Van Ontwerp vanuit

- De Techniek
  - Hardware
  - Software
- De Mens
  - Gebruiker
  - Burger/omwonende
- De socio-technische Interactie

- Het Governance model
  - Wet- en regelgeving
  - Politiek
  - Ambtelijk opdrachtgever
  - Management

Leefwerelden

Ingenieurs	Managers	Politici
Design proces V-model	Control proces Jaarrapportage	Politiek proces Coalities
Gedefinieerde onzekerheden Je weet wat je niet weet	Prestatie onzekerheden KPI	Scopeonzekerheden
Beste oplossing	Geaccepteerde oplossing	Onderhandelde oplossing
Hard tools Calculaties, Simulaties, Modellen	Mixed tools Project en Proces management	Soft tools Draagvlak, image

COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

Naar Ontwerp vanuit

Een maatschappelijke opgave

- **Duurzaamheid**
- **Mobiliteit as a Service (MAAS)**
- **Risico reductie ?**
- **???**

Hoe krijgen we hier grip op?

1. Hard skills. Nieuwe instrumenten

STAMP?

System Theoretic Accident Management and Process.

- Menselijk gedrag
- Software

Hoe krijgen we hier grip op?

1. **Hard skills. Nieuwe instrumenten**
2. **Resilience**

   Kwetsbaarheden accepteren en de gevolgen beperken?

COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

Hoe krijgen we hier grip op?

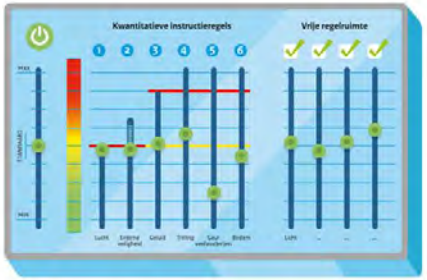
1. **Hard skills.** Nieuwe instrumenten
2. **Resilience.** Kwetsbaarheden accepteren
3. **Soft skills.**

Andere manier van met elkaar omgaan?

Hoe krijgen we hier grip op?

1. **Hard skills.** Nieuwe instrumenten
2. **Resilience.** Kwetsbaarheden accepteren
3. **Soft skills.** Omgangsvormen
4. **Wetgeving die achterloopt**

Omgevingswet met een ander sturingsmodel?



COB
Nederlands kennis centrum voor ondergronds bouwen en ondergronds ruimtegebruik

Aan de slag met de Omgevingswet

Hoe krijgen we hier grip op?

1. **Hard skills.** Nieuwe instrumenten
2. **Resilience.** Kwetsbaarheden accepteren
3. **Soft skills.** Omgangsvormen
4. **Wetgeving die achterloopt.** Governance

Kansen!

- De Omgevingswet kan een instrument en een tijdsframe zijn! 2021
  - Infrastructuur komt daarna
- Van Infrastructuurfonds naar Mobiliteitsfonds!

Wat gaan we doen?

- Voorbeelden verzamelen waar we aan de wet voldoen maar toch geen goed gevoel bij hebben. 2018
- Voorbeelden analyseren. Waar ligt het aan? 2019
- Waar willen we staan in 2025?
- Oplossingen bedenken, toetsen en implementeren

Wie hebben we al in de projectgroep?

- Een burgemeester
- Een metrotunnelbeheerder
- Een wegtunnelbeheerder
- Een metro-, tram-, busvervoerder
- Een lector
- Een veiligheidsbeambte
- Een consultant
- Een brandweerman

Wie doet er mee?

Integrale systeemveiligheid - methode

Gea Kolk, Movares

Veiligheid van een systeem <> de som van veiligheden van de subsystemen

- => integraliteit door samenwerking
- => integraliteit ondersteunt door methoden en aanpak (inzicht)

Bekende methoden:

- Decompositie, beoordeling per onderdeel; interactie ontbreekt

STAMP staat voor

System-Theoretic Accident Model and Processes

- Ontwikkeld door prof. Nancy Leveson (MIT)
- Op basis van Systeemtheorie: regelkringen met feedback
- **“Accident = control problem, not a failure”**

STAMP

STAMP is familie van methoden:

STPA voor safety engineering (het **vooraf** bepalen welke gevaarlijke situaties (hazards) kunnen optreden)

CAST voor incidentonderzoek (CAST) **(achteraf** onderzoeken hoe een ongeval heeft kunnen gebeuren); o.a. gebruikt door Onderzoeksraad**.**

STAMP

STAMP is gebaseerd op 3 basisconcepten:

1.Safety constraints

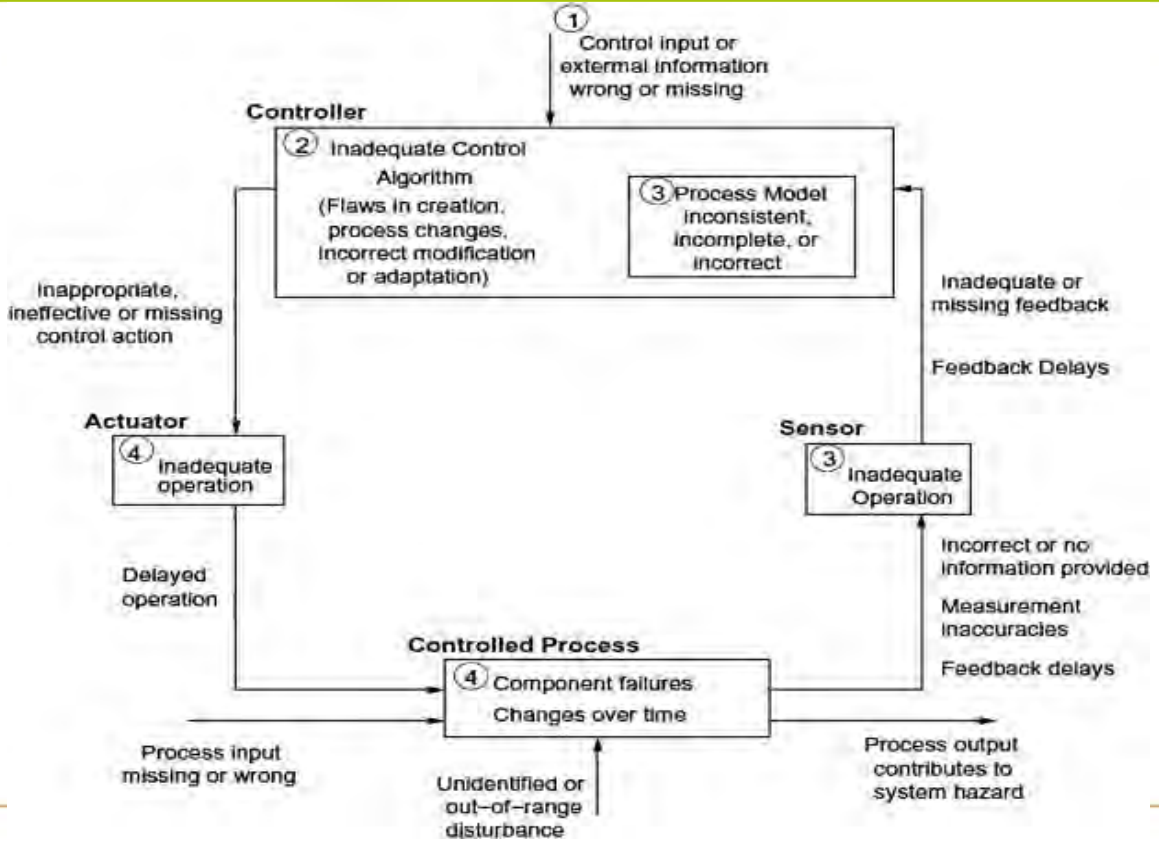
2.Safety control structure

3.Procesmodellen

Dynamisch evenwicht d.m.v. terugkoppeling (feedback control loops). Aanpassing aan omgeving en aan interne veranderingen.

STAMP/STPA

Regelkring met mogelijke afwijkingen



STAMP/STPA

Claims over STAMP zijn o.a.:

- Er worden meer oorzaken / scenario's gevonden dan met traditionele methodes
- Ontwerpfouten, sociale en organisatorische factoren
- Geen **WYLFIWYF** (What You Look For Is What You Find)
- Sneller dan traditionele methodes met minder inspanning

STAMP

STPA:

- Beschrijf accidents, hazards en safety constraints.
- Beschrijf safety control structure volgens STAMP.
- Stap 1: bepaal de “unsafe control actions”
- Stap 2: bepaal hoe iedere “unsafe control action” kan worden voorkomen
  a) Identificeer scenario’s.
  b) Bepaal hoe gedurende de tijd “controls” kunnen afnemen.

STAMP

STPA voorbeeld

STPA: Hazard: A system state or set of conditions that together with a worst-case set of environmental conditions, will lead to an accident (loss).

De tijdelijke snelheidsbeperking is niet in ERTMS aangebracht waardoor de ERTMS-trein rijdt met een snelheid die hoger is dan de toestand van de infra toelaat

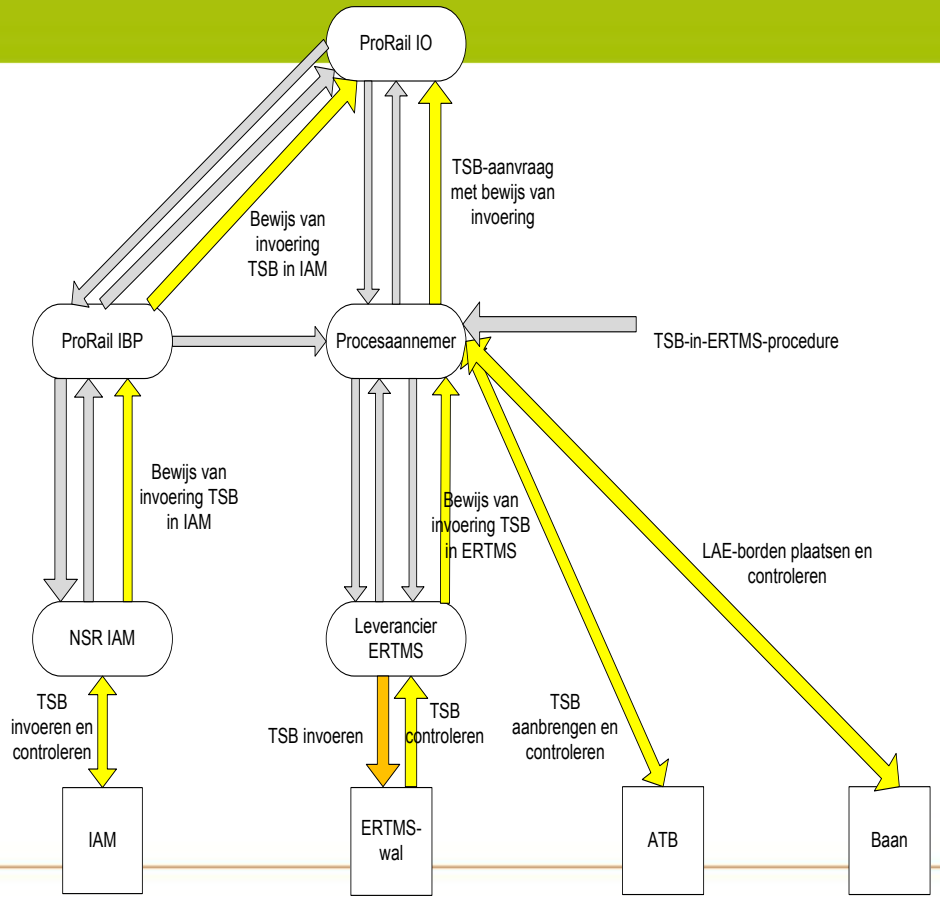
STPA: Accident: An undesired and unplanned event that results in a loss, including a loss of human life or human injury, property damage, environmental pollution, mission loss, financial loss, etc.

Ontsporing van de ERTMS-trein door te hoge snelheid met als mogelijk gevolg dode of gewonde reizigers, schade aan infra en materieel.

STAMP

STPA voorbeeld

Control structure



STAMP

Conclusies:

- Bij de vergelijking met de originele HAZAN blijkt dat we met STPA **meer achterliggende oorzaken** boven water krijgen (meer scenario's) en ook **enkele oorzaken die in de originele HAZAN ontbreken**.
- STPA lijkt een geschikte aanvullende methode voor hazardidentificatie. STPA ondersteunt de safety engineer door de controle structuur in kaart te brengen. STPA lijkt daarom met name geschikt voor **hazardidentificatie in complexe situaties waarin meerdere partijen samen moeten werken** om de veiligheid te garanderen.

STAMP

Conclusies (vervolg):

- STPA vraagt van de safety engineer zogenaamde **safety constraints** op te stellen. Door STPA in een vroeg stadium toe te passen kunnen deze safety constraints worden meegenomen als safety requirements voor het **systeemontwerp**. STPA ondersteunt bovendien meerdere niveaus van controle structuren waarin ook meerdere niveaus van safety constraints/requirements mogelijk zijn.
- Het opstellen van safety constraints is te beschouwen als een **eerste stap richting formele bewijsvoering** van de correctheid van een systeemontwerp.
- STPA is niet geschikt voor kwantificering van hazards.

Vragen? Gea.Kolk@movares.nl