SAFETEC
AN ABS GROUP COMPANY

Railway Safety Assessment and Certification - forthcoming challenges

High Integrity Systems Symposium 2015

Bjørn Axel Gran

11/06/15

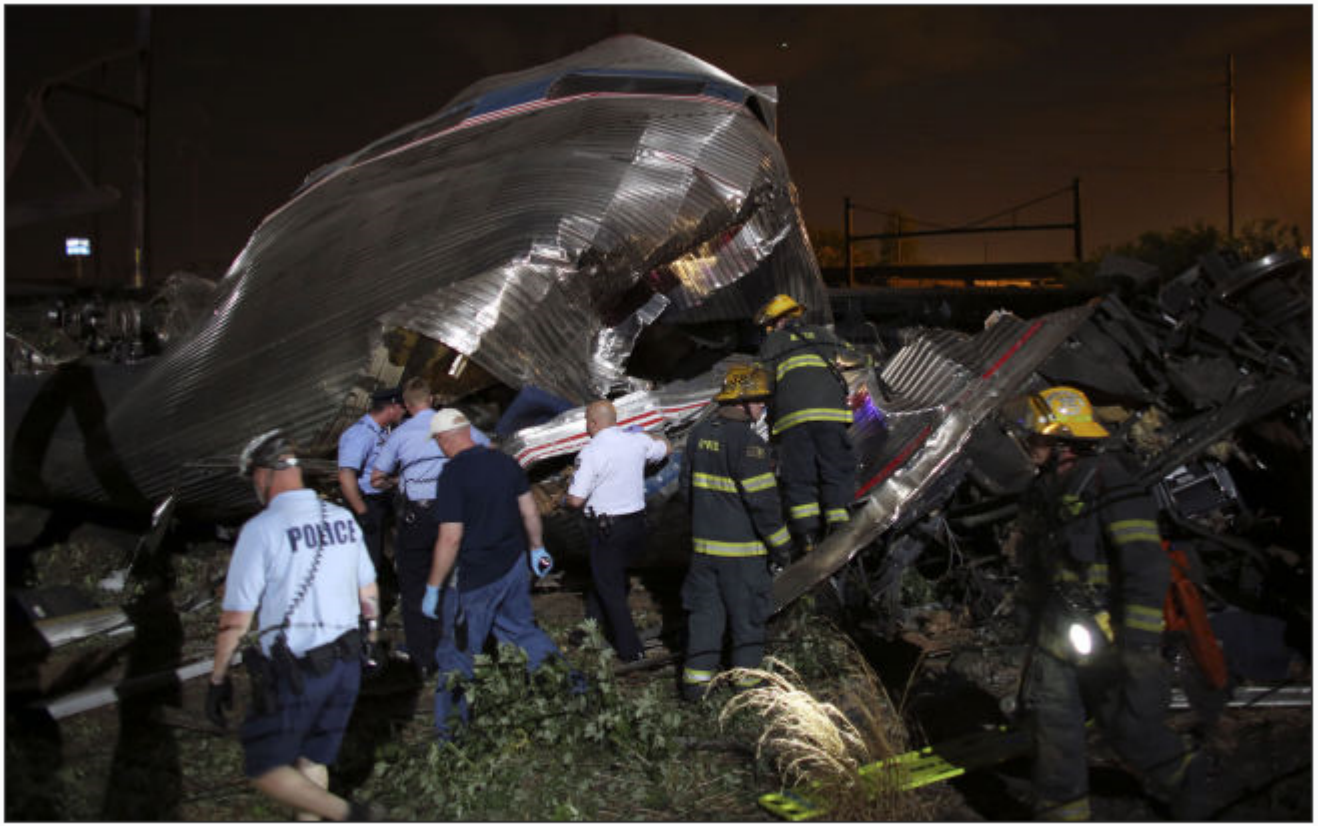
SAFETEC
AN ABS GROUP COMPANY

Content

- What is a railway system?
- What is a high integrity system in railways?
- Which work processes should I follow?
  - EN 50126, 50128 and 50129
  - The process within Signal in JBV
- A generic application?
- Challenges

SAFETEC

Faksimile fra V



STOR FART: Vrakdelene på stedet vitner om et voldsomt sammenstøt da hurtigtoget på vei fra Washington D.C. til New York sporet av natt til onsdag norsk tid. Nødetatene arbeider på spreng med å få oversikt. Foto: JOSEPH KACZMAREK, AP

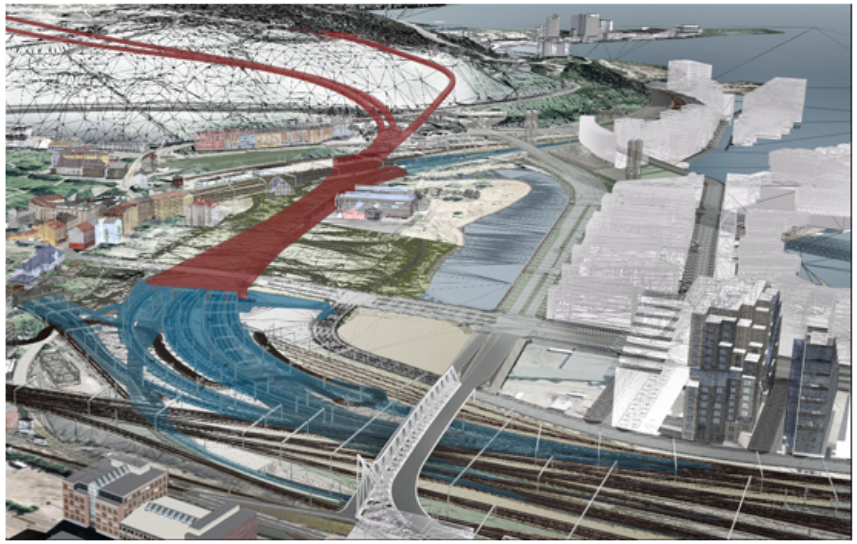
- Godsvognene kom i 140 km/t

Hadde større fart enn først antatt. Les mer

SAFETEC
AN ABS GROUP COMPANY

Railways in Norway

- The first railway in Norway came in 1854 (Eidsvoll – Oslo)
- Today it is about:
  - 4237 km tracks
  - 245 km dobbel tracks
  - 2572 bridges
  - 716 tunnels
  - 3690 crossing points
  - 337 stations



3D-illustrasjon Follobanen: Innføring Oslo S

- All depending upon high integrity systems

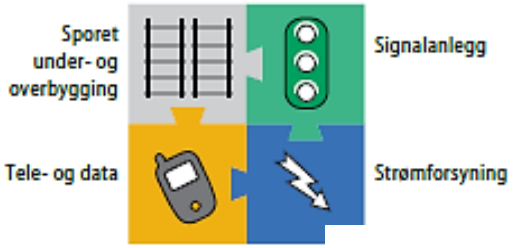
SAFETEC
AN ABS GROUP COMPANY

A railway system

Fakta

Kjørevegens fem hovedelementer:

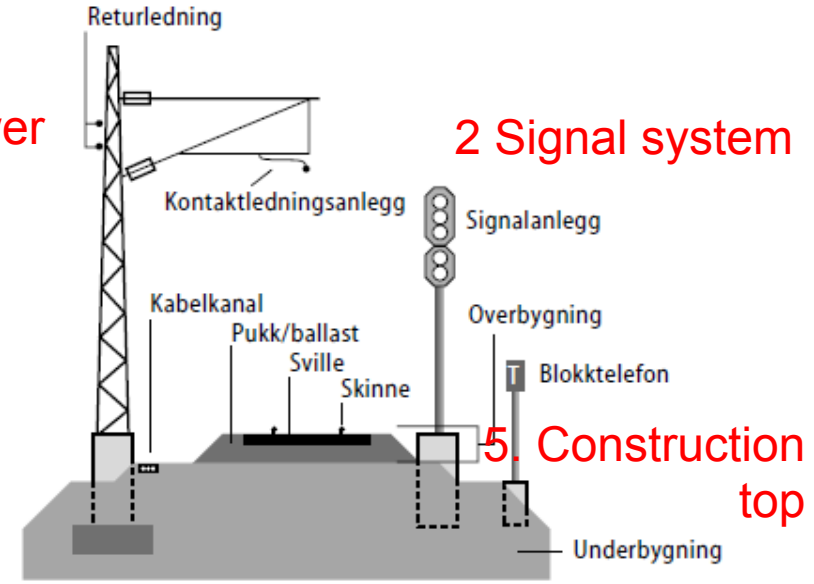
1. **Strømforsyningsanlegg:** Kontaktledningsanlegget sikrer kontinuerlig overføring av elektrisk energi til togene.
2. **Signalanlegg:** Sikrer trygg, rask og punktlig togframføring
3. **Underbygning:** Sikrer at sporet ligger stabilt
4. **Teleanlegg:** Sikrer nødvendig samband.
5. **Overbygning:** Sikrer at krav til aksellast, komfort, sikkerhet og hastighet ivaretas i togframføringen



4. Tele and ICT

1. Power

2 Signal system



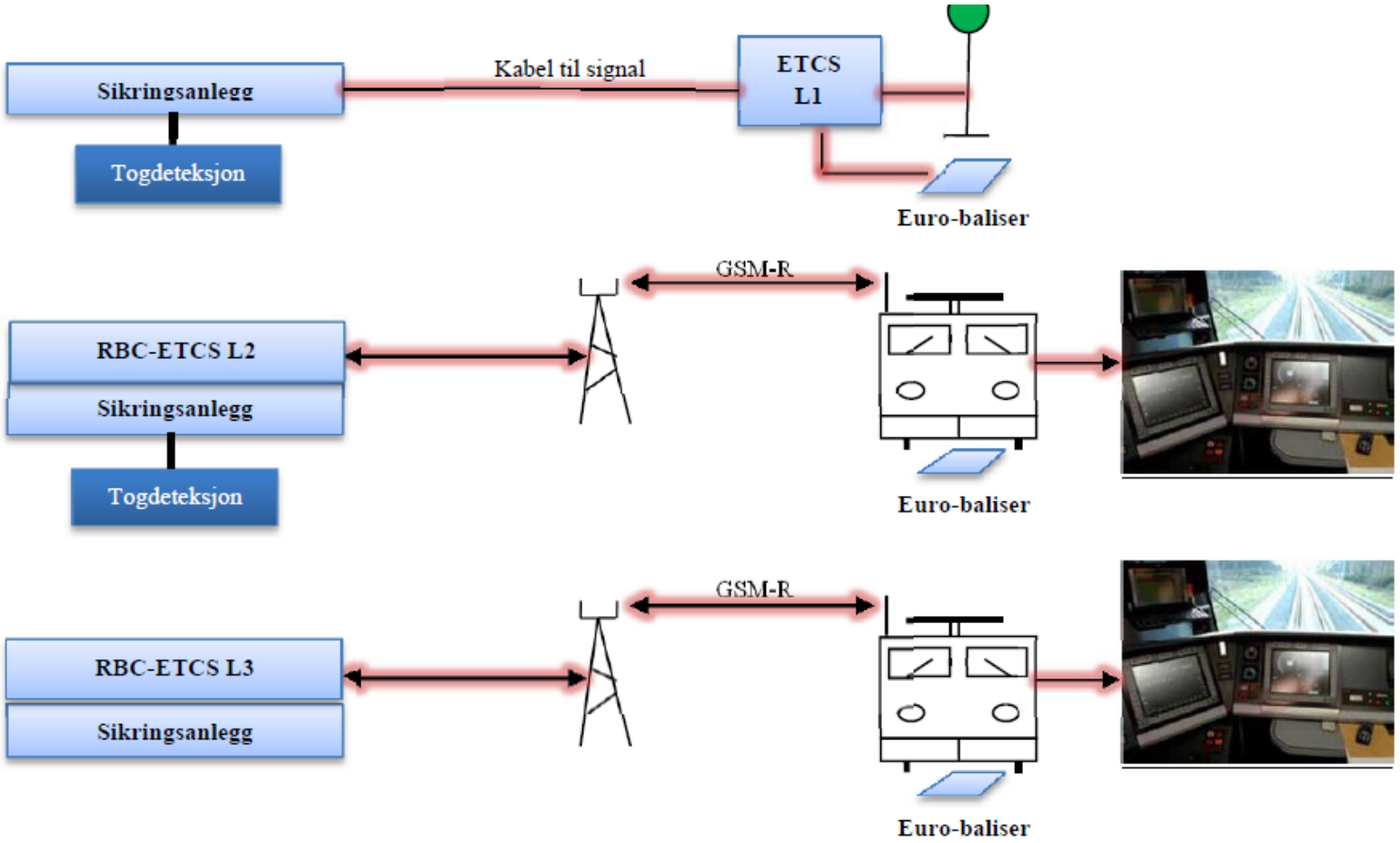
5. Construction top

3. Construction base

Cost new builds:
50% construction base
25% construction top
10% power
10% signal
5% tele and iCT

SAFETEC
AN ABS GROUP COMPANY

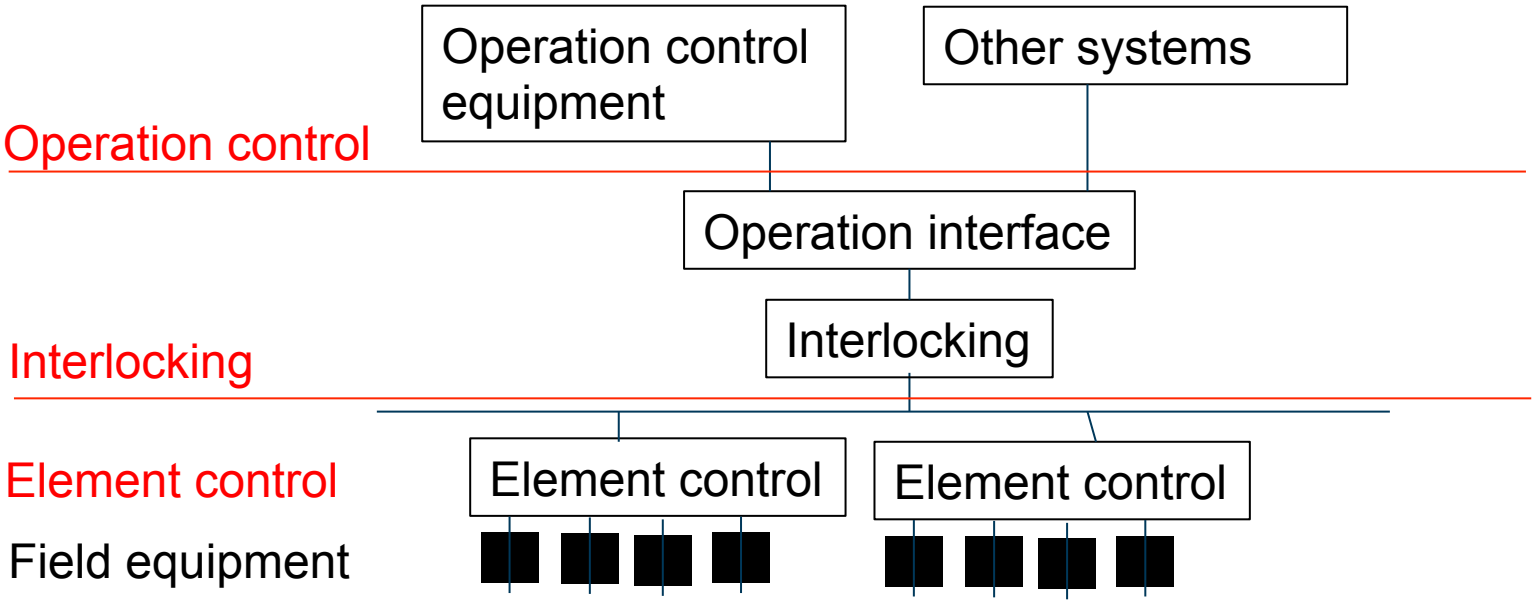
European Rail Traffic Management System (ERTMS)



SAFETEC
AN ABS GROUP COMPANY

The sw in a High Integrity System

- System software
- Interlocking software
  - Generic functions
  - Specific functions related to infrastructure
- Location specific software
  - Developed specific for each delivery



SAFETEC
AN ABS GROUP COMPANY

Important procesess

- EN 50126: Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) [EN 50126:1999]
- EN 50128: Railway applications – Communication, signalling and processing systems – Software for railway control and protections systems [EN 50128:2011]
- EN 50129: Railway applications – Communication, signalling, and protection systems – safety related electronic systems for signalling [EN 50129:2003]
- FOR-2014-10-27-1344 Forskrift om en felles sikkerhetsmetode for risikoevaluering og –vurdering. (based upon (EU) nr. 402/2013).
- Technical Specifications for Interoperability (TSIs) (ERA)
- Work process for Signal («Signaltjenesters arbeidsprosess») (NAP).
  - Build on the basis of EN 50126, 50128 and EN 50129

SAFETEC
AN ABS GROUP COMPANY

EN 50126, 50128 and 50129

EN 50126: The life cycle – phases & tasks – apply for all high integrity railway systems – independent if they are containing signals or programmable logic

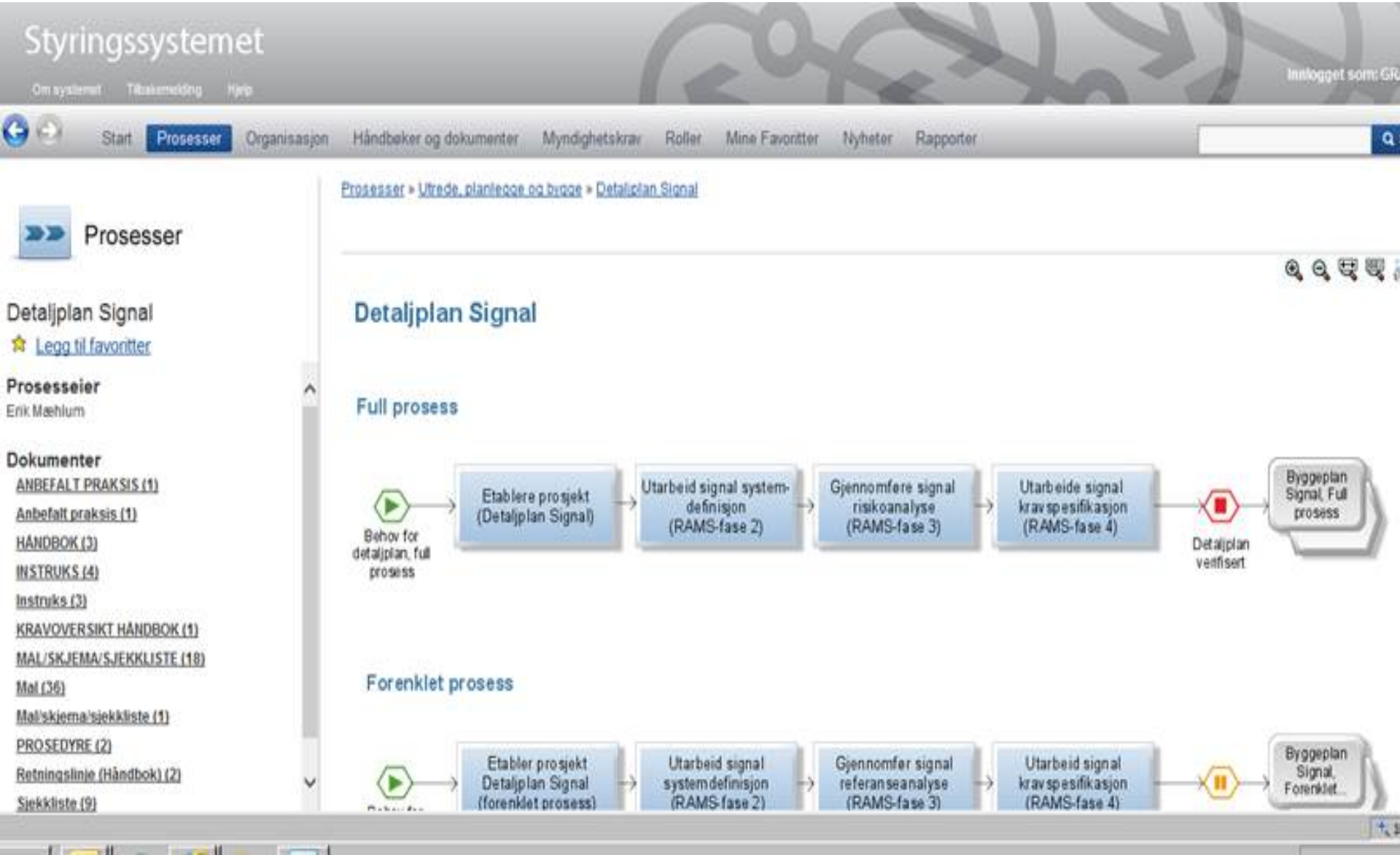
EN 50128: The life cycle to be applied when the application includes sw

- Applies 4 SIL-levels
  - Detailed guidelines on activities, methods, tools, competence, documentation, traceability, etc.
  - Identifies 10 roles to be filled
  - Selection of techniques and measures

EN50129: pinpoints the importance of independence between roles

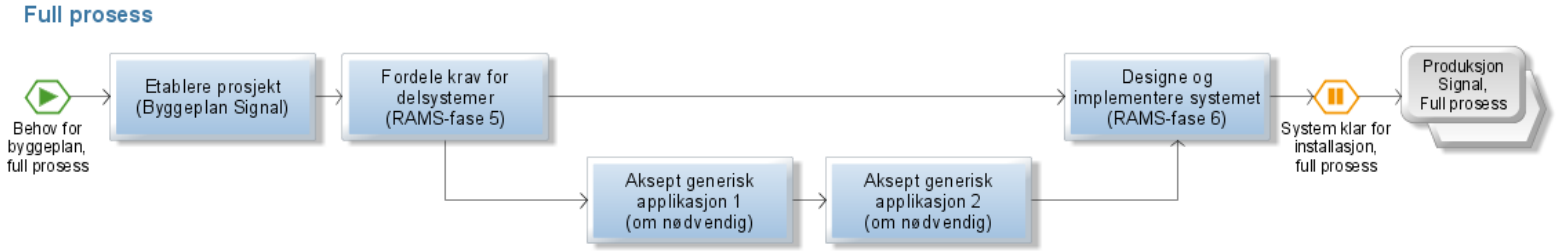
SAFETEC
AN ABS GROUP COMPANY

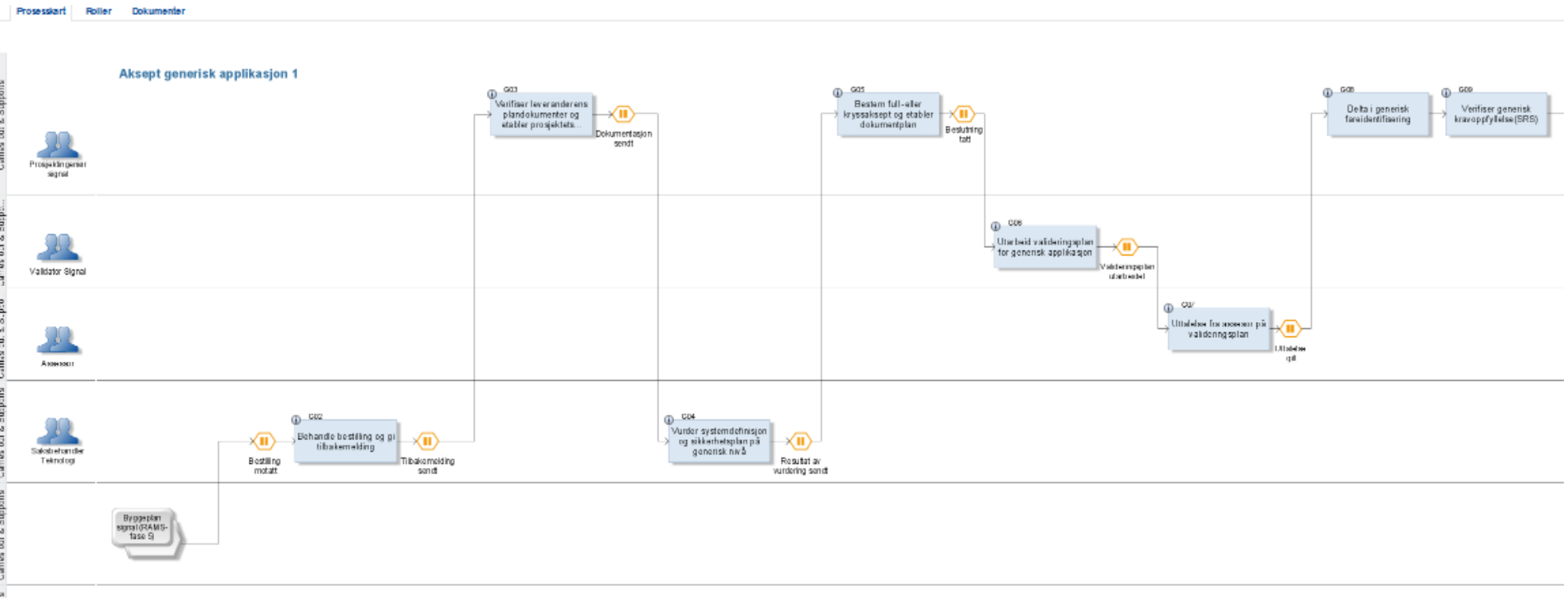
UPB – Detailed plan Signal



SAFETEC
AN ABS GROUP COMPANY

UPB Signal – Plan for Build





SAFETEC
AN ABS GROUP COMPANY

Some techniques

- Defensive programming
- Failure detection and diagnosis
- Self detection in code
- Modularisation
- Diversity
- Redundancy
- One approach is also to apply formal verification
  - See research by Terje Sivertsen, JBV
  - Applied HALDEN (Halden Algebraic Language and Design ENvironment) Prover and HALDEN ASL (Algebraic Specification Language) on the NSB-94-ssytemt at Heggedal station

SAFETEC
AN ABS GROUP COMPANY

Some challenges

- Each activity requires specific competence
  - Is the competence available?
- Most applications are provided by a supplier
  - How to transfer the knowledge from supplier to developer and operator?
- All systems have an interface to other systems
  - How to assure knowledge about neighbour (old) systems?
  - How to assure interoperability?
- Each activity requires a control, and each phase a validation and verification
  - How to maintain indolence in persons?
  - How to have access to competent assessors?

SAFETEC
AN ABS GROUP COMPANY

A bigger challenge?

Jernbaneverket

Handlingsprogram 2014–2023

13. februar 2014

Nasjonal transportplan 2018 – 2027

Publisert 07.10.2014 i Nyheter

Need 100 new engineers (+ 66%)?

Need 100 new validators (+ 33%)?

SAFETEC
AN ABS GROUP COMPANY

The new challenge

Thank you, Bjørn Axel

- Your conversation on the train made you an obvious target
- Your password was easy to guess
- Your e-mails showed us your critical contacts
- Your local files provided us with the design
- It was an easy task to hack the railway application

SAFETEC
AN ABS GROUP COMPANY

Thank you

Bjørn Axel Gran
R&D Manager Safetec
bjorn.axel.gran@safetec.no
+47 90 95 52 95

Bjørn Axel Gran
Professor II, IPK, NTNU
bjorn.a.gran@ntnu.no
+47 90 95 52 95