



# Some Security Aspects in Safety Related Systems

Odd Nordland  
SINTEF ICT  
Trondheim  
Norway

[odd.nordland@sintef.no](mailto:odd.nordland@sintef.no)



# Introduction

- A (very) brief introduction to SINTEF
- “Security is not my table”
- Dependency on computer systems
- Example 1: ERTMS
- Example 2: Interlocking systems
- Example 3: Power station
- “Security IS your table!”

# SINTEF

## ■ Largest independent R&D organisation in Scandinavia

### ■ Located in Trondheim (HQ) and Oslo

- offices in Stavanger, Bergen, Ålesund, Tromsø, Hirtshals (DK), Skopje (MK), Houston (TX), Rio (BR) ...

### ■ 7 divisions

- Information and Communication Technology
- Technology and Society
- Health
- Oil and Energy
- Materials and chemistry
- Marine
- Building technology





# “Security is not my table”

- Safety engineers tend to regard security as outside the scope of their task
  - a safety system cannot protect against sabotage, burglary, vandalism
  - human behaviour (malicious or benevolent) is too unpredictable
    - “You cannot make a system fool-proof, because the fools are so ingenious”
  - heavy reliance on e.g. access control, fences etc.
    - the safety system must be protected, not be protecting



# Dependency on computer systems

- Modern safety systems are increasingly based on computers and electronic systems
  - ERTMS: radio based traffic management system
  - Interlocking systems: distributed computers with intense communication
  - Power stations: turbines controlled by software
- Interfering with radio communications can have serious safety related consequences
- Software maintenance (upgrades) can go wrong
- Hacking into safe software can make it unsafe

# Example 1: ERTMS

## ■ European Rail Traffic Management System

(see <http://www.ertms.com>)

- ETCS (European Train Control System) to transmit speed information to driver and monitor his compliance
- GSM-R for exchanging voice and data information between traffic control and train
- Ultimately (“Level 3”) movement authorities by radio
- Falsified radio telegrams can indicate
  - too high speed limit to train driver
  - lower train speed to traffic control
  - illegal authority to move
- Is GSM-R encryption enough?

# Example 2: Interlocking Systems

- Current railway signalling systems (“pre-ERTMS”)
  - Distributed computers communicating with each other and trains
  - Software includes track layout, topology, traffic rules etc.
    - Needs to be updatable
  - Updates uploaded from technician’s terminal (laptop with CD)
    - Falsified update can wreak havoc
  - Protection through access control to computer room
    - No hardware based handshake (e.g. dongles)
    - No authority checking once the software is being updated
    - Neither of the above is specified as a requirement ...

# Example 3: Power station

- Turbines are controlled by software
  - often remotely
- Hacking into the software can result in physical destruction of the turbine
  - demonstrated by U.S. Department of Homeland Security!  
(see <http://www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCText>)
    - Up to 60 % of power supply can be lost for months
    - Catastrophic consequences for the economy
    - Catastrophic consequences for society
- From a safety point of view,  
a dead turbine is a safe turbine!



# “Security IS your table!”

- Security breaches can have serious safety consequences
- Current protection mechanisms are not good enough
  - Terrorists have money and advanced technical resources
  - They come from the inside
    - they can access internal information such as
      - communication protocols
      - encryption methods
      - authorisation procedures
  - Safety requirements specifications do not include security aspects
- **BUT THEY SHOULD!**