Safe Maritime Communication

Seminar Maritim Kommunikasjon
Trondheim, 14.02.2017

Stig Petersen, SINTEF Digital
stig.petersen@sintef.no

Contents

Functional Safety

Safe Communication

SINTEF

Functional Safety

Safety can be defined as the freedom from unacceptable risk of harm to humans, either directly or indirectly as a result of damage to property or to the environment.

Safety can be achieved through various mechanisms: physical barriers, work processes, training, monitoring and control, emergency response.

Functional safety is the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

SINTEF

Functional Safety: Example applications

- Emergency shut-down
- Safety valves
- Fire and gas detection
- Crane safe load indicator
- Machine emergency stop
- Dynamic positioning
- Anti-lock braking
- Airbags
- Railway signaling

Functional Safety: Standards

Functional safety can be achieved by adhering to safety standards:

• IEC 61508	Main (generic) standard for safety
• ISO 26262	Automotive
• ISO 13849-1	Machinery
• IEC 62061	Machines
• IEC 60601	Medical
• IEC 61511 series	Process industry
• IEC 60880 and IEC 61513	Nuclear industry
• DO 178C	Avionics
• EN 5012x series	Railway domain
• …	

Functional Safety: New domains

New domains and applications with no formal safety regulations (yet):

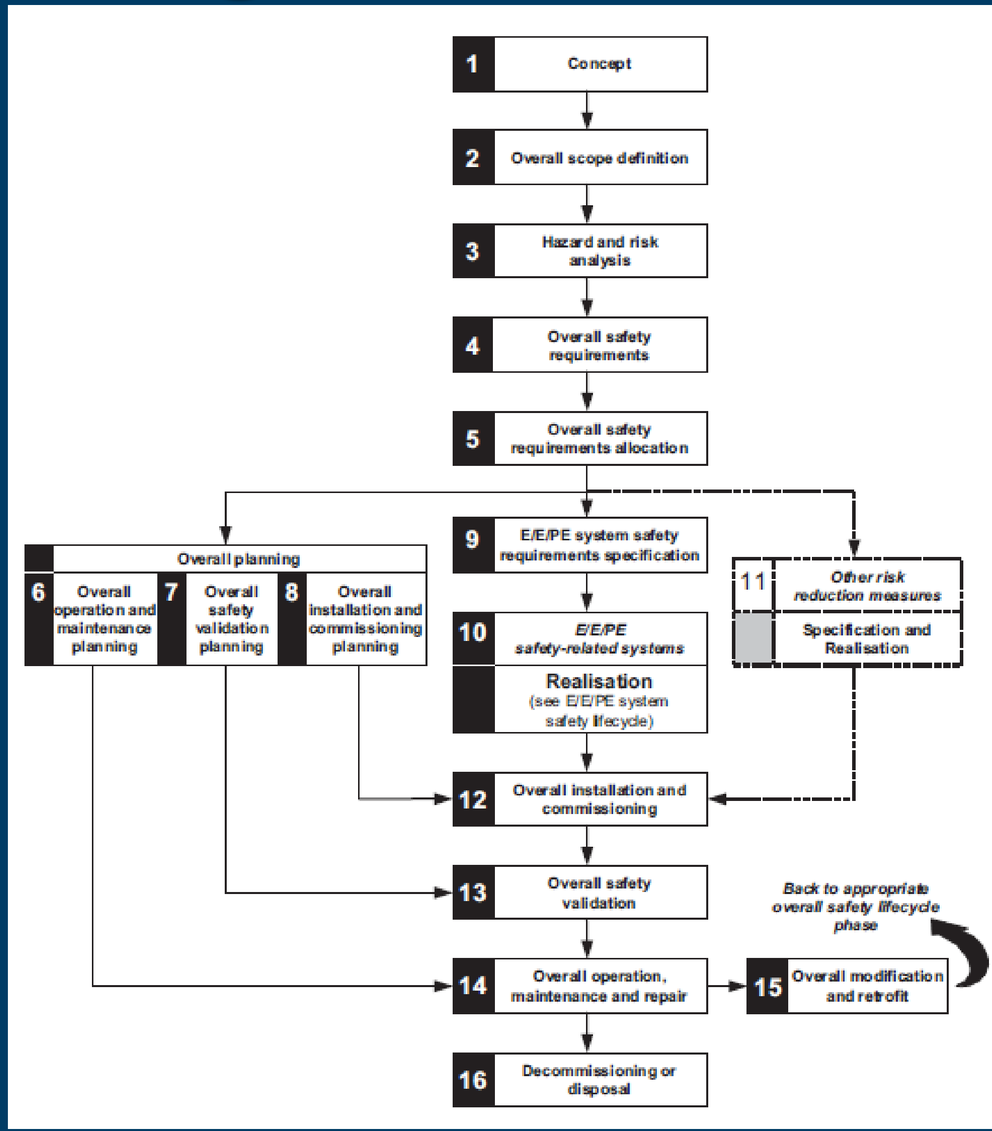
- Autonomous cars
- Drones
- Autonomous boats and ships

SINTEF

Functional Safety: Life cycle management

Functional safety requirements governs the entire life cycle of a safety system, from concept and specification, through design and development, to maintenance and decommissioning.

Developing a safety system is much more complex, time consuming and costly than a similar non-safety system.



Contents

Functional Safety

Safe Communication

SINTEF

Safe communication

A communication system is considered as part of a safety system if the application involves transmission of information between different locations.

For a communication system to be safe, it must be proven and certified according to domain-specific safety standards.

- EN 50159: Railway applications
  Safety-related communication in transmission systems
- IEC 61784-3: Industrial communication networks
  Functional safety fieldbuses

EN 50159 Categories

Need not consider information security

Category 1

Systems under the control of the designer, and fixed during their lifetime.

Category 2

Systems partially unknown or not fixed, but unauthorized access can be excluded.

Must consider information security

Category 3

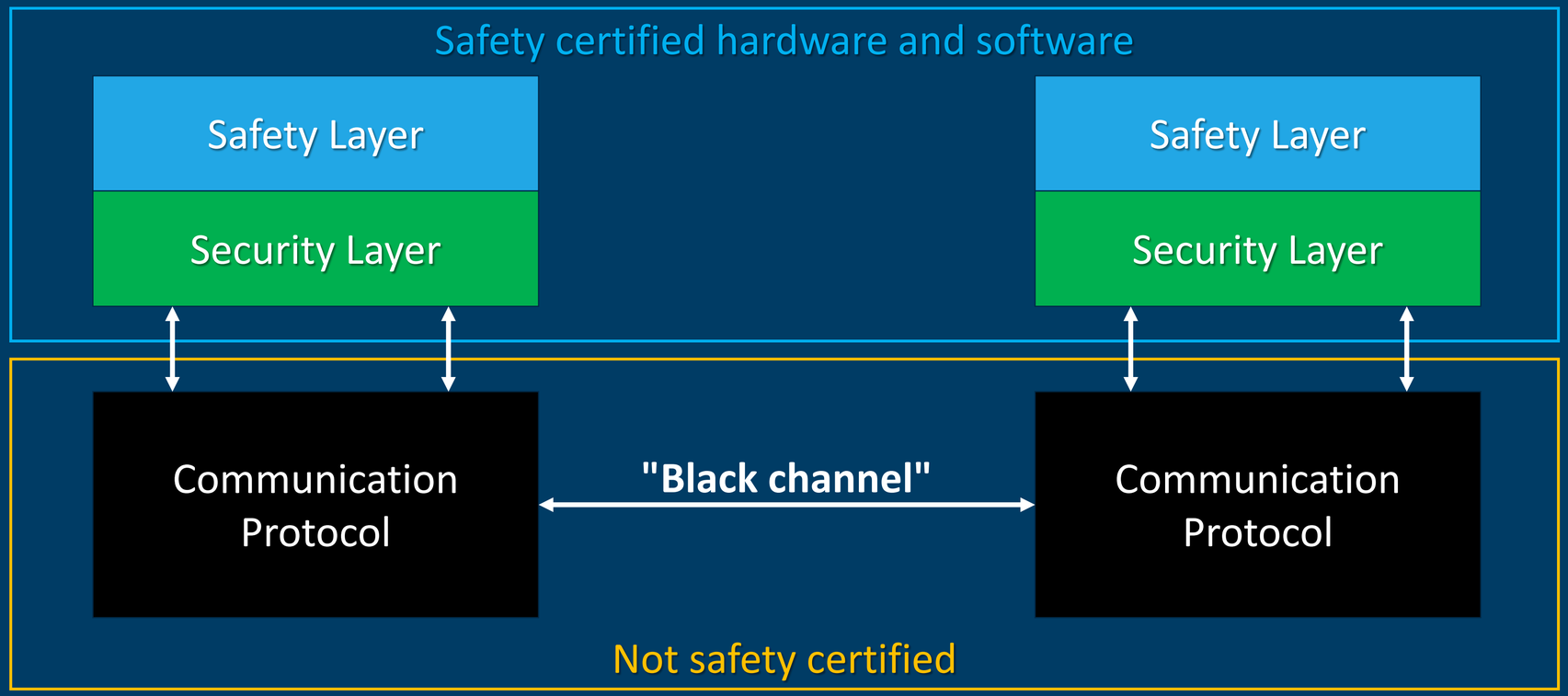
Systems which are not under the control of the designer, and unauthorized access has to be considered.

Wireless communication is always considered a Category 3 system.

SINTEF

EN 50159 End-to-End Architecture

EN 50159 introduces application level end-to-end safety and security:



SINTEF

EN 50159 End-to-End Architecture

Observations about the end-to-end safety architecture:

The application is assumed to have a fail-safe mechanism.
E.g. process shutdown, emergency brake, safe-to-shore, …

The performance of the communication protocol is not considered.
The fail-safe mechanism may trigger often or seldom depending on Quality of Service.

A safe application may be "useless" due to frequent fail-to-safe events.
E.g. due to poor wireless communication performance.

SINTEF

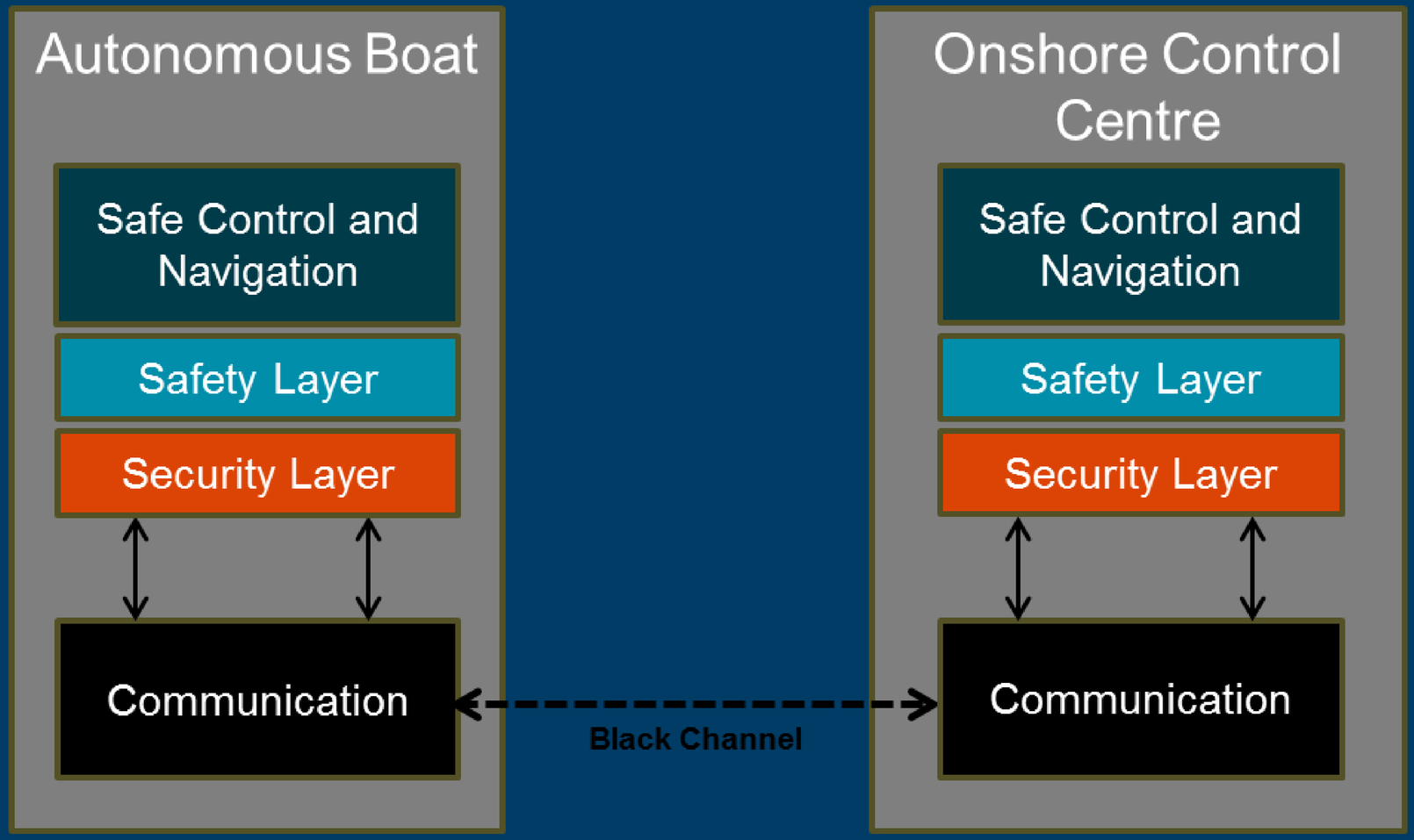
Safe maritime communication

For autonomous and remotely operated ships to be acceptable for commercial use, they must be at least as safe as conventional vessels in similar service.

It is expected that future regulations will require control and navigation systems for autonomous ships to be certified according to functional safety requirements.

A communication solution supporting an autonomous operation will thus be considered as an integral part of the safety system, and require safety certification.

Safe maritime communication



SINTEF

Summary

Autonomous ships will have to adhere to (future) safety regulations in order to be as safe as conventional vessels.

Communication to and from autonomous ships will be a part of the total safety function along with control and navigation systems.

A safe communication protocol is a prerequisite for remotely operated and autonomous ships.

Technology for a better society

Safe Cooperating Cyber-Physical Systems

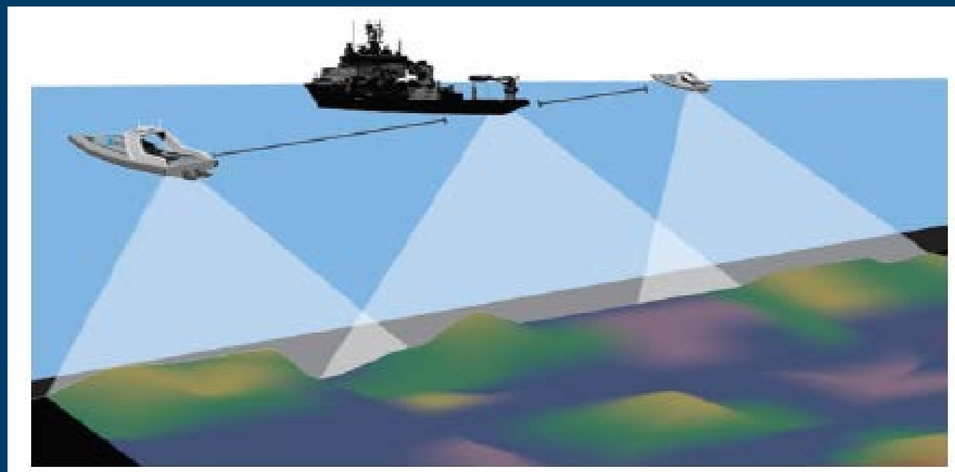
H2020 ECSEL Project, 2016 – 2019
DNV GL, Maritime Robotics, SINTEF Digital and 20+ other European partners.

Background

New cooperating systems, e.g. autonomous cars and boats, require new certification mechanisms in addition to safe wireless communication protocols.

Main Objectives

- Certification of cooperative safety functions
- Development of safe wireless communication.
- Norway: Cooperative bathymetry with boat platoons



Safe Communication for Autonomous Ships

RCN MAROFF Project, 2017 – 2020
Kongsberg Maritime, SINTEF Digital and SINTEF Ocean

Background

Before autonomous ships can be successfully launched, it is imperative that they are capable of **safe operation**, with freedom from unacceptable risk of harm to humans, property or to the environment.

Main Objectives

- Specification of a generic safe communication protocol for autonomous ships
- Implementation of a prototype safe communication protocol for a specific communication solution