Risk

Integrated Control Systems - FMEA for Networks

Amund R. Tinderholt
Kongsberg Maritime AS

October 9-10, 2007

Return to Session Directory

KONGSBERG

Integrated control systems
FMEA for networks

Amund R Tinderholt
Kongsberg Maritime

WORLD CLASS – through people, technology and dedication

Introduction

KONGSBERG

- Integrated Control Systems are based on network technology:
  - Link between control processors and operator stations
  - Interconnect control processors
  - Connections to external administrative systems

- What do the IMCA reports tell us?
- How can we analyse the network for potential problems by using FMEA (Failure Mode and Effect Analysis)?
- What are the critical failure modes, and how can they be handled?

Overload – too many packets!

KONGSBERG

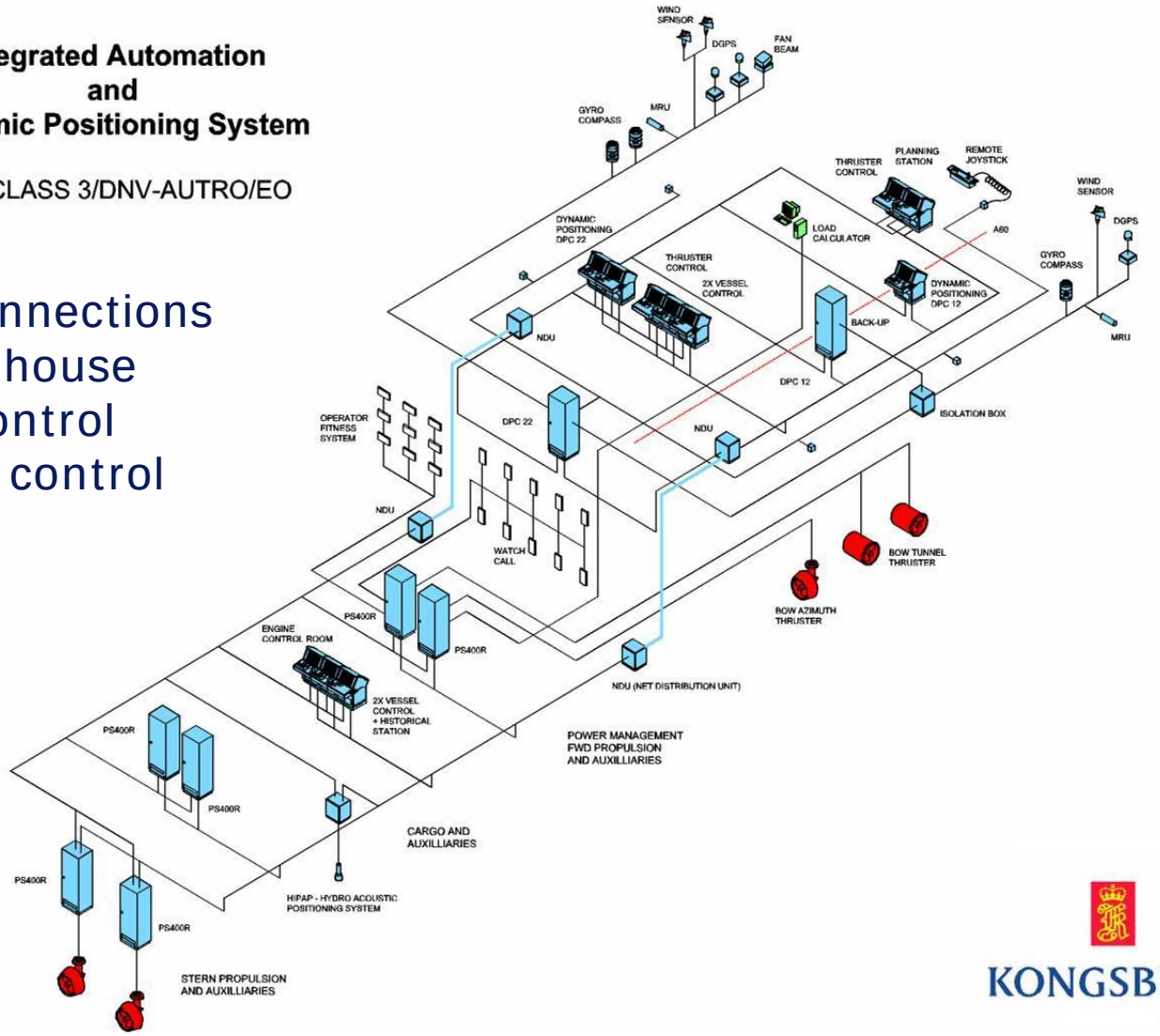
The vessel network

KONGSBERG

Integrated Automation and Dynamic Positioning System

IMO CLASS 3/DNV-AUTRO/EO

Network connections from Wheelhouse to Cargo Control and Engine control



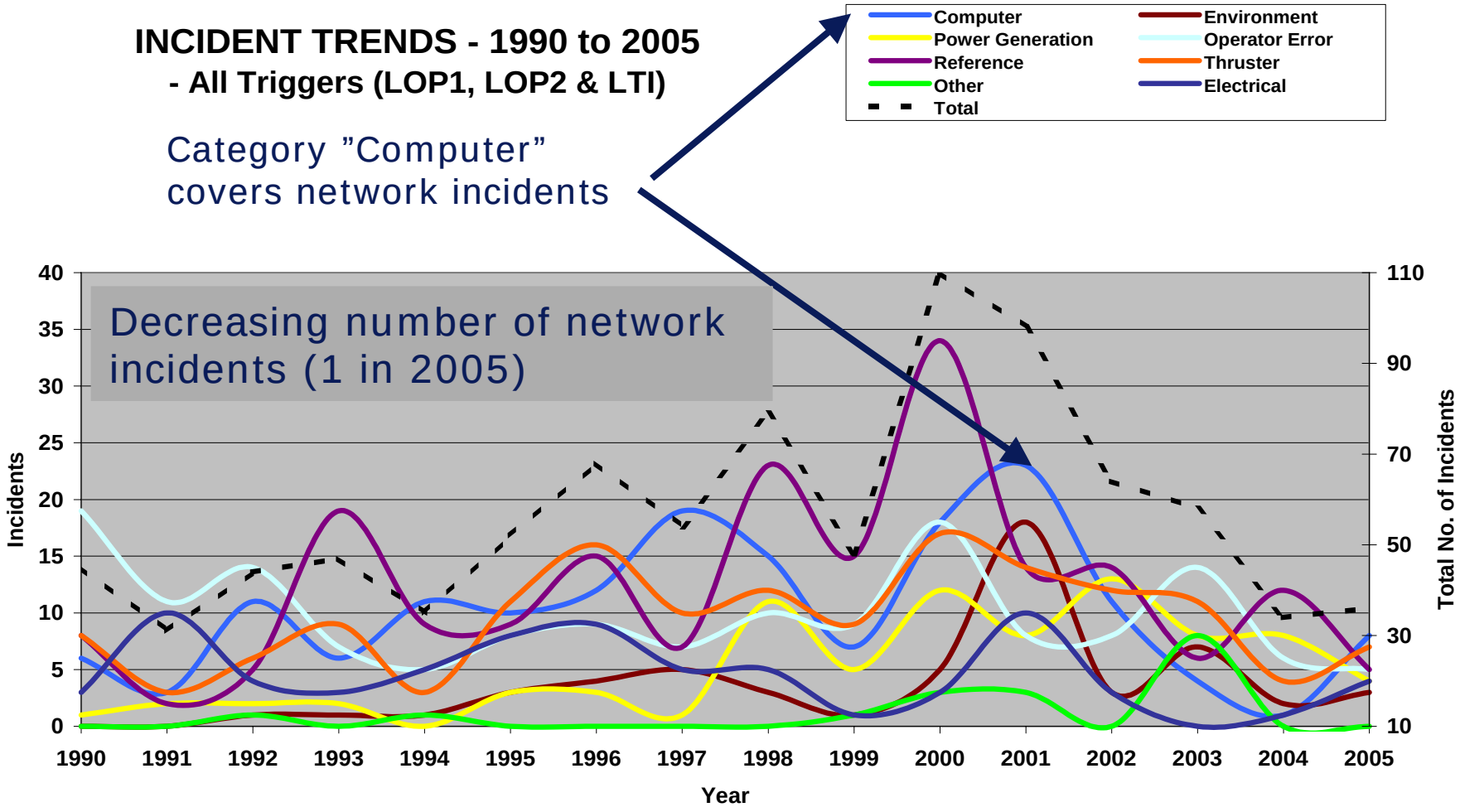
KONGSBERG

IMCA statistics

KONGSBERG

INCIDENT TRENDS - 1990 to 2005
- All Triggers (LOP1, LOP2 & LTI)

Category ”Computer” covers network incidents



Few incidents but still a critical component

KONGSBERG

- Local area networks (LAN) components have improved in stability and capacity
- But: LANs are well known from the office, and problems occur ….
- And: LAN problems in integrated systems can be very serious

- LAN is only one component in the total system, but needs attention
- Finding the critical points with FMEA and further verification of system behavior is one solution

The FMEA method

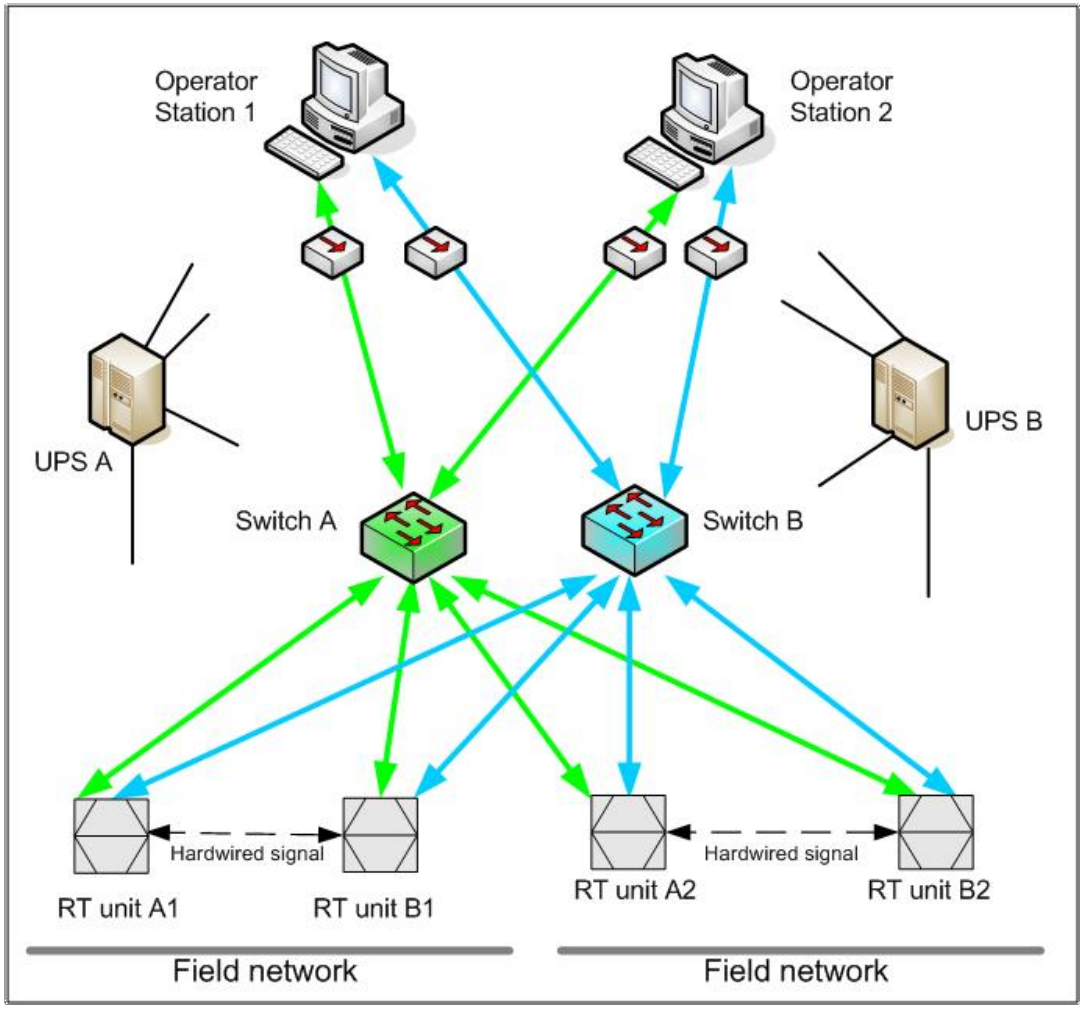
- Purpose:
  - Give a description of different failure modes of the equipment referred to their functional objectives
  - Detect possible critical points in the system at block level.
- The analysis is performed in two major steps:
  Preliminary Safety Analysis (PSA)

ITEM DESCRIPTION			*FAILURE DESCRIPTION*			*ADDITIONAL INFO*	
Unit/ Module	*Function*	*Redundancy (Y/N)*	*Failure mode*	*Failure detection*	*Failure consequence*	*Compensating measures*	*Detailed FMEA (Y/N)*

- And if relevant: Failure Mode and Effect Analysis (FMEA):

Item/ Comp.ident	*Function*	*Mode of operation*	*Failure mode*	*Failure cause(s)*	*Detection method*	*Failure effect locally (or other)*	*Failure Effect On Primary (DP) Functions*	*Compensating provisions*

The FMEA test case



- Duplicated Operator Stations
- Duplicated Real Time units
- Dual network in all units.
- Power segregation (UPS)
- Adm. communication on separate network (not shown)

Prerequisites for network FMEA I

KONGSBERG

- FMEA done for system in normal operation.
- No faults present in relevant components.
- Analysis of the control system software is not included.
- Hardware components are discussed down to real-time controller
- Field data comm. is not included.
- Peripheral equipment like printers, data logging equipment etc. are not analysed.
- The operation mode considered is with relevant UPS power.

Prerequisites for network FMEA II

KONGSBERG

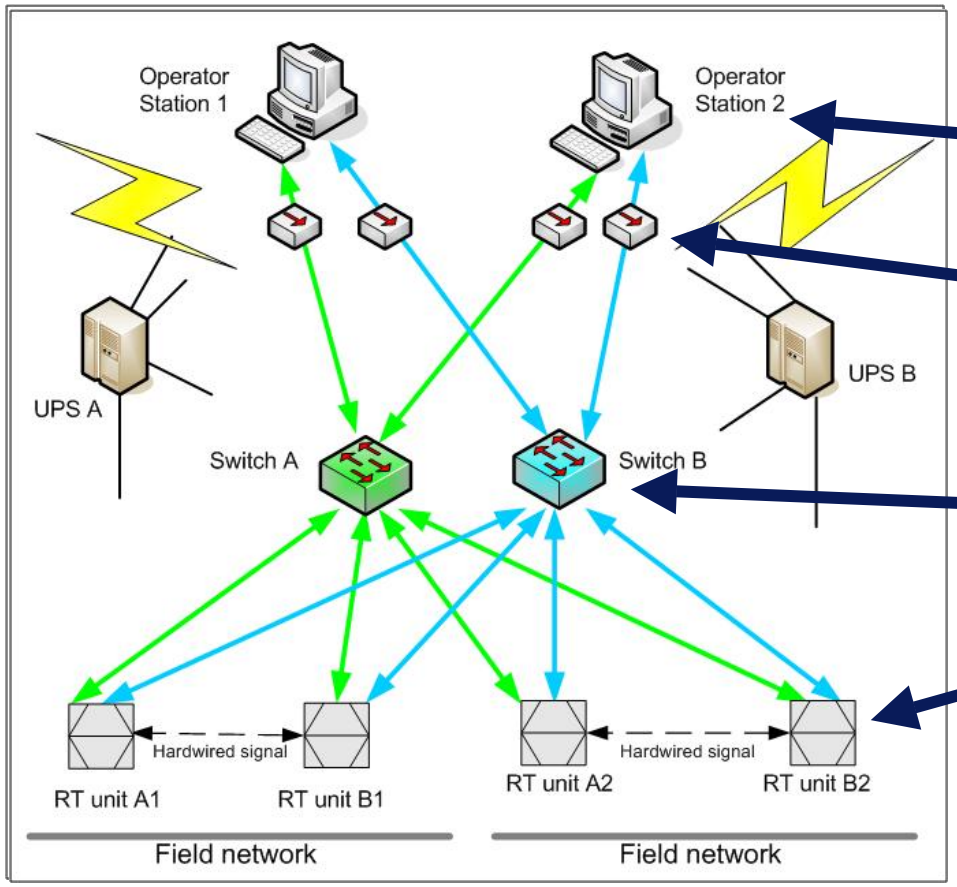
- Failure modes caused by external environments like lightning, fire, flooding are not fully considered.
- Only single errors are generally considered.
- LAN bandwidths up to 100 Mbits/s are considered:
  LAN topology is based on units which negotiate speed up to 100 Mbits/s, full or half duplex. However, connections between network switches with 1 Gbits/s are allowed.
- Only items/units with 2 process networks are considered.
- Anti Virus solution, either on the external links or within the Operator stations is supposed to be activated.

Failure modes considered

KONGSBERG

- Power failure
- Loss of data:
  - on one network interface (i/f)
  - on both network i/f
- Transmit erroneous data:
  - on one network i/f
  - on both network i/f
- Transmit overload:
  - on one network i/f
  - on both network i/f
- Receive overload:
  - on one network i/f
  - on both network i/f

Components studied



Operator stations

Media converters

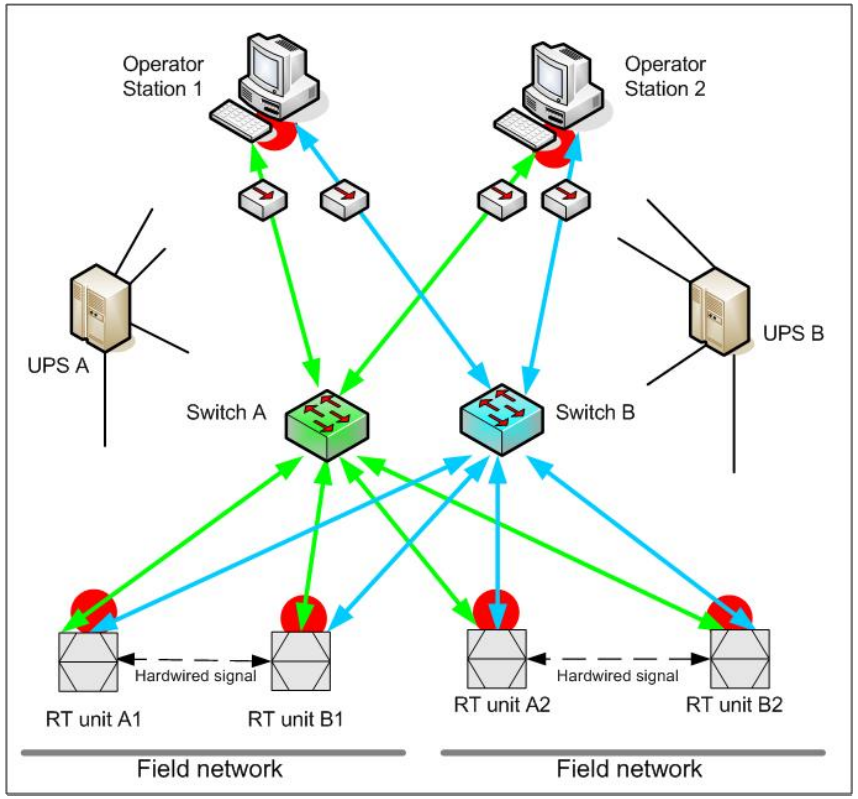
Network switches

Real Time controllers (RT units)

Test load applied:

FMEA results

PSA and FMEA tables is not shown here.



Comp.	Failure mode	Problem description
Operator station	Erroneous data receive on both networks	Station not showing data. No data received on networks. (double error)
Operator station	Data transmit overload on both networks	Can make the station inoperable and jam the network. (double error)
Operator station	Data receive overload on both networks	Can make the station inoperable. (double error)
Operator station	Data receive overload on one network	Can make the station inoperable.
RT unit	Receive overload on one network	Can slow down or stop the control functions.
RT unit	Receive overload on both networks	Can slow down or stop the control functions (double error)
RT unit	Transmit overload on one or both network	Will stop the RT unit.

Measures that can be taken

KONGSBERG

Measure	Description
Bandwidth limitation	Bandwidth limitation on switches will reduce the effect of a network storm.
Limit message types	Avoid message types that can cause overall Storms, e.g. Broadcast messages.
Excessive Load protect	RT units: Specific limits set, disable network interface if required. Op. Station: CPU capacity must be is sufficient.
Message throttle	Limit amount of messages sent from Operator Stations
Message consistency	Only messages with legal application types to be accepted. (extended protocol check)
Failsafe settings	Failsafe settings will apply if RT unit is stopped.

Component/system behavior with measures taken

KONGSBERG

Component	Failure mode	Reaction
Operator station	Erroneous data receive on both networks	No data received. Other Operator Station in other network segment OK.
Operator station	Data transmit overload on one or both networks	Throttle the output to avoid network overload.
Operator station	Data receive overload on one or both networks	Switch limitations activated. Continue normal operation.
RT unit	Receive overload on one network	Overloaded network shall be switched off. Continue normal operation on one network.
RT unit	Receive overload on both networks	Increase real time control priorities or go to Failsafe condition.
RT unit	Transmit overload on one or both networks	Shall be catched by a Watchdog and go to Failsafe.

Summary I

KONGSBERG

Some measures that can be taken to prevent problems in an integrated system network:

1. Ensure correct installation and topology doc. of network.
2. Only use qualified and approved network components.
3. Consider use of a mix of components from different manufacturers.
4. Check network normal operation parameters.
5. On-line reporting of network communication problems.
6. Analyse and test weak points through FMEA, take precautions (as specified).
7. Analyse (and test if required) effects of changes in configuration by new FMEA.

Summary II

KONGSBERG

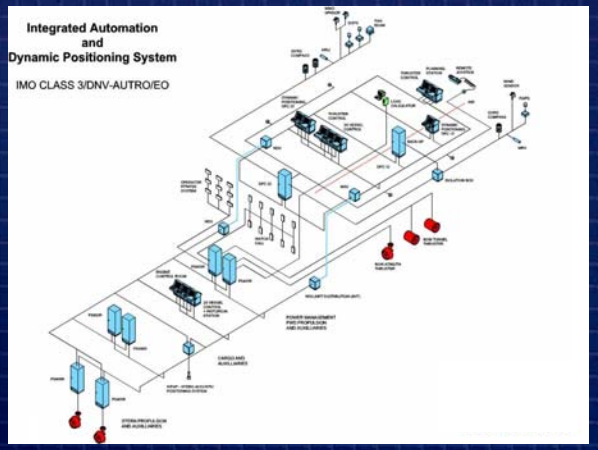
Classification societies require documentation for communication networks:

- Topology
- FMEA
- Capacity
- Cable routing

FMEA:
Experience and implementation!

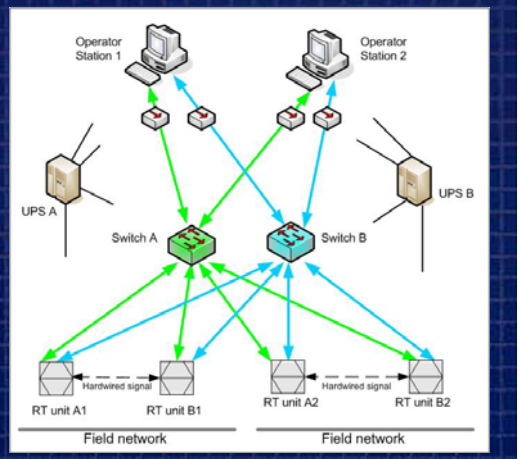
KONGSBERG

Integrated control systems
FMEA for networks



Amund R Tinderholt
Kongsberg Maritime

The end



WORLD CLASS – through people, technology and dedication

Return to Session Directory