



DYNAMIC POSITIONING CONFERENCE
October 9-10, 2007

Risk

**Integrated Control Systems -
FMEA for Networks**

Amund R. Tinderholt
Kongsberg Maritime, AS

Integrated Control Systems FMEA for Networks

Introduction

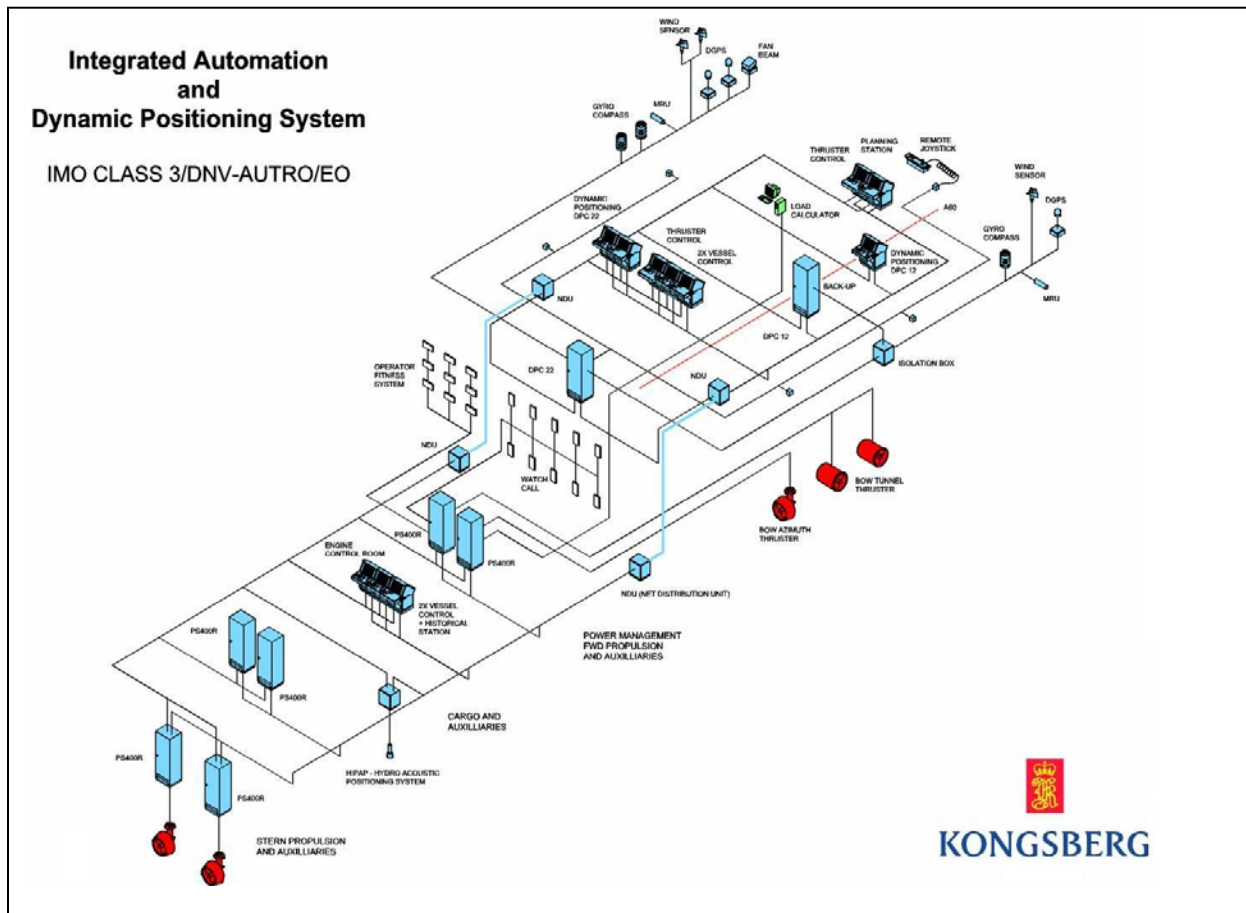
Integrated Control Systems today are based on network technology. Local Area Networks (LAN) are used to collect data from the ship equipment into control processors, interconnect control processors and to link the control processors to operator stations or other equipment.

The same approach is used for connections to the surrounding administrative systems.

This presentation focuses on Ethernet as medium for the network communication between control processors and between control processors and operator stations.

Motivated by reported DP incidents with relation to networks, the presentation shows how FMEA procedures can be used to analyse a dual network system and highlight the important issues of reliability by:

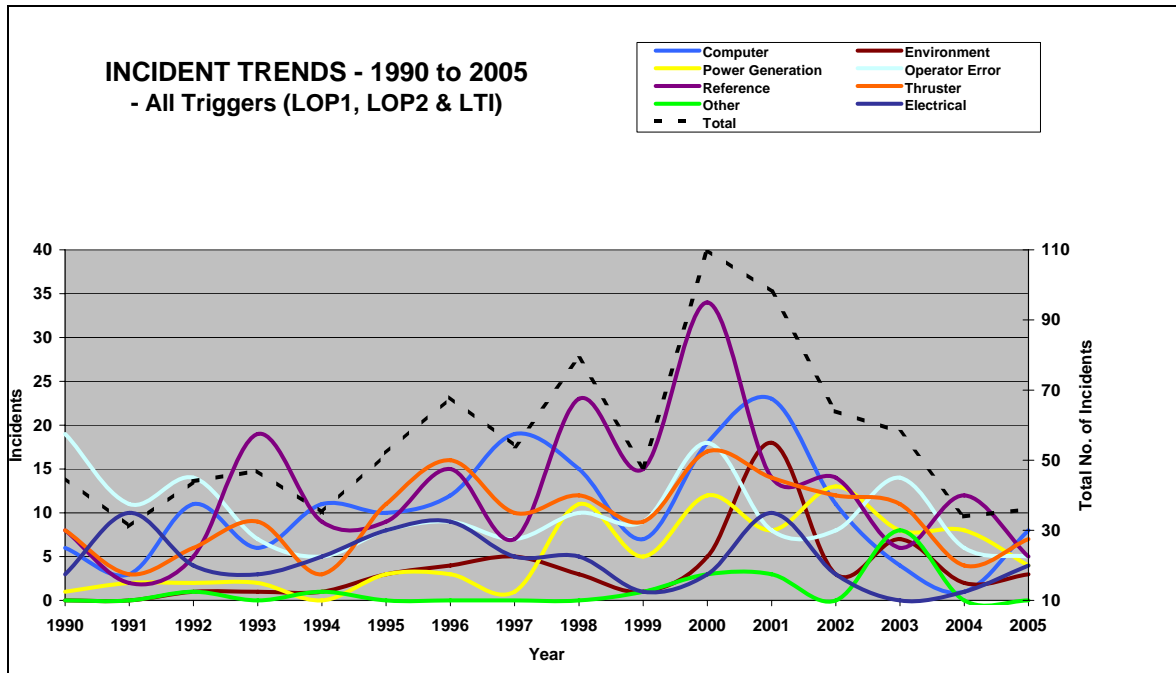
- Identifying potential failures.
- Analysing effects regarding safe process states and safe operator control/communication.
- Summarising current requirements from Class certification societies.



Typical integrated system, showing network and related components

Incident reports related to networks

The IMCA reports for the years 2001-2006 show a decreasing number of incidents related to “Computer” and “DP Control System” categories. The 2005 report shows only 1 out of total 36 incidents related to network, and this incident is classified as “Lost Time Incident”. As it can be seen from the figure copied from the IMCA report (ref. 1), the category “Computer” shows a remarkable decrease from earlier levels. Network related incidents are included in this group.



IMCA diagram showing incident trends

However, in increasing complex systems there will always be a worry regarding the quality, stability and load in the LAN. There are experiences from network in the office where strange things happens. The network technology today is driven as much by the consumer market as by the industrial market. One may also ask what extra measures are used to ensure the stability of networks in the critical applications like the DP and automation systems. Although the network appears as a stable component, the consequences of network failures may be serious.

One way to highlight the potentially weak points in a system is to apply a Failure Mode and Effect Analysis (FMEA). This method is normally applied as part of the delivery for major systems. However, the focus is then primarily on the operational aspects of the DP system, not to analyse the network traffic in particular.

The network is often assumed to be a stable underlying component in the system, although e.g. the DNV rules states that a separate FMEA shall be done for the communication networks and links.

The FMEA method

The purpose of the analysis is to give a description of different failure modes of the equipment referred to their functional objectives, and to detect possible critical points in the system at block level. The analysis is performed in two major steps:

- 1) Preliminary Safety Analysis (PSA) and (if relevant):
- 2) Failure Mode and Effect Analysis (FMEA)

PSA is an initiating, systematic walkthrough of the subsystems at network component level in order to identify if there are critical failure modes present with respect to the system level.

If no critical failure modes are detected on component level, further analysis of the block is not performed.

If critical failure modes/points are detected, these have to be notified in the PSA table (see example below), for further investigation in the FMEA table.

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

PSA table example

The failure modes found to be critical in the PSA walkthrough shall be further analysed in the FMEA table.

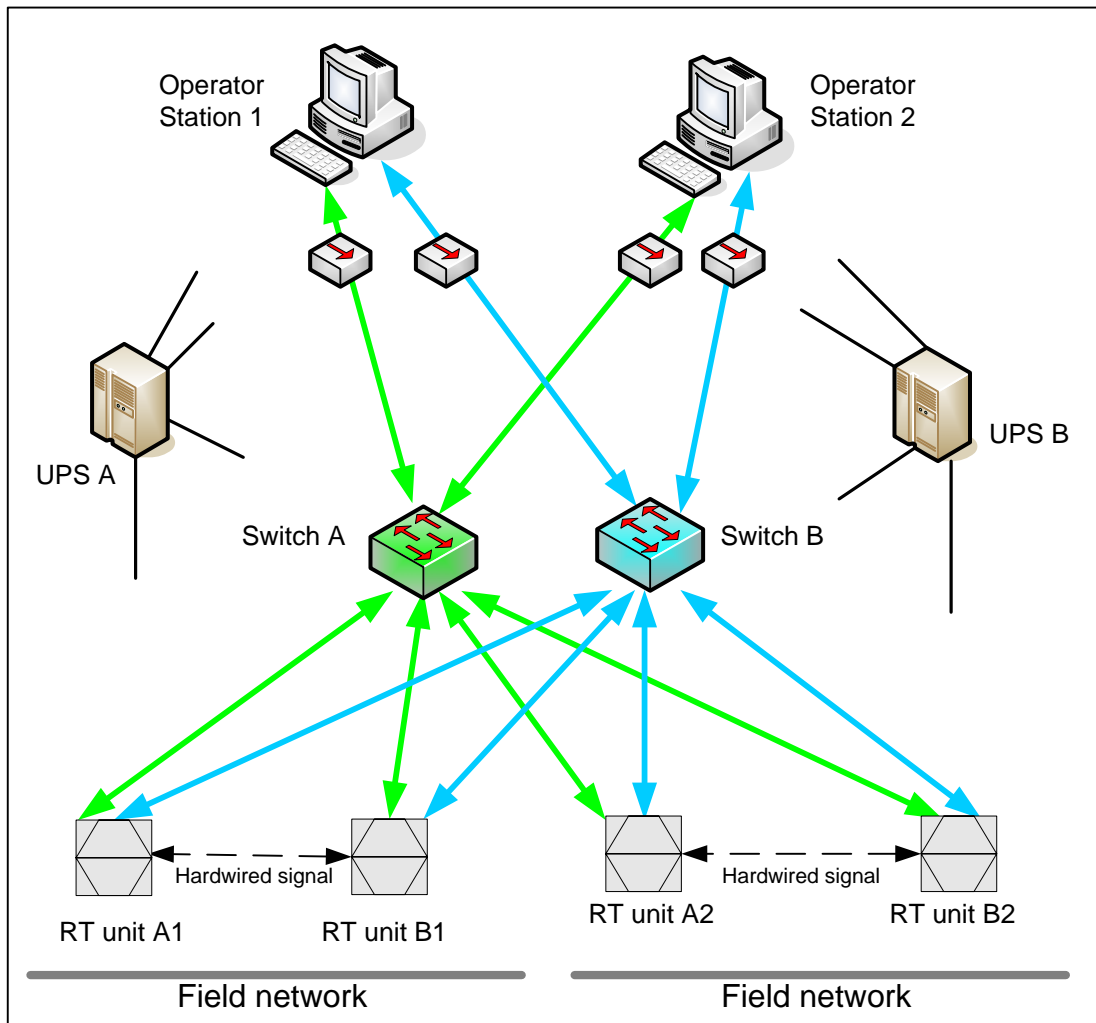
A description of each physically and functionally independent item and the associated failure modes with their failure causes and failure mechanisms related to normal operation is presented.

A description of the subsequent effect from each failure mode locally and of the primary function is given wherever it has been possible to predict. The FMEA is based on a standard form, one table per item:

<i>Item/ Comp. ident.</i>	<i>Func- tion</i>	<i>Mode of oper- ation</i>	<i>Failure mode</i>	<i>Failure cause(s)</i>	<i>Detection method</i>	<i>Failure effect locally (or other)</i>	<i>Failure Effect on Primary (DP) Functions</i>	<i>Compensating provisions</i>
-----------------------------------	-----------------------	------------------------------------	-------------------------	-----------------------------	-----------------------------	--	---	------------------------------------

FMEA table example

The FMEA test case



FMEA case study setup

In this simplified setup a lot of precautions against interrupted service due to single failures are built in:

- Operator Stations are duplicated.
- Real Time units are duplicated (A and B/Redundant pair).
- Dual network in all units.
- Power segregation (UPS) for network and other critical components.
- Administrative communication from Operator Stations on separate network (not shown, not part of the analysis)

Prerequisites for FMEA analysis

In a presentation on the DP conference 2003 (ref. 3), a number of possible failure modes were listed. Some of these were related to installation problems, other to bad design of the network. This study focuses on problems related to communication problems when the initial configuration is tested and found ok. The failure modes are therefore limited by assuming a set of conditions as prerequisites for the study:

- System in normal operation
- No faults present (all components relevant for the analysis ok)
- The control system software in the computers is not been analysed. It is assumed that after the system is tuned up and tested, no errors will arise from the computer software itself.
- Hardware components are discussed down to real-time controller level represented by failure modes which in each case is considered being relevant and sufficient for the item in question with respect to critical effect on primary functions.
- FMEA for field data communication, e.g. Modbus, Profibus is not included.
- Only functions / items that are considered to have influence on vital functions are analysed, hence peripheral equipment like printers, data logging equipment etc. are not analysed. However, erroneous network behavior due to such items is discussed.
- The operation mode considered for the systems is with relevant UPS power supplies to the operator stations, process stations and the network components available.
- Failure modes caused by external environments like: lightning, fire, flooding, complete physical destruction of compartments etc. are not fully examined.
- Only single errors are generally considered, a few possible common cause of failures have been included.
- LAN bandwidths up to 100 Mbits/s are considered, e.g. the LAN topology is based on units which negotiate speed up to 100 Mbits/s, full or half duplex. However, connections between switches with 1 Gbits/s are allowed.
- Only items/units with 2 process networks are considered. Items with only one network (laptop test equipment, etc.) are considered as not critical items.
- Anti Virus solution, either on the external links or within the Operator stations is supposed to be activated.

Components and failure modes

The components studied in the FMEA are:

1. Operator stations	MS Windows type computers, 3 network interfaces
2. Media converters	HW units that convert between copper (twisted pair/STP) and fibre. May be separate units or embedded in switches.
3. Network switches	Managed or non-managed units with automatic adaptation to speed, duplex mode etc.
4. Real Time controllers (RT units)	All control functions for safety, control and monitoring are located in the controllers. Control functions may be duplicated in an A/B pair, where one unit is the active controller and the other is ready to take over depending on specified conditions.

The network is based on standard TCP/IP protocols (ICMP, UDP, TCP). Thus all other traffic will be neglected by the components.

Message addressing considered is broadcast, multicast and unicast/singlecast

Failure modes considered are:

1. Power failure
2. Loss of data on one network interface (i/f)
3. Loss of data on both network i/f
4. Transmit erroneous data on one network i/f
5. Transmit erroneous data on both network i/f
6. Transmit overload on one network i/f
7. Transmit overload on both network i/f
8. Receive overload on one network i/f
9. Receive overload on both network i/f

The failure mode “Erroneous data” may be due to error in one or more of the fields in the protocol. For the following analysis, it is assumed that such packets are discarded at either the application layer, the IP protocol level or by the software driver.

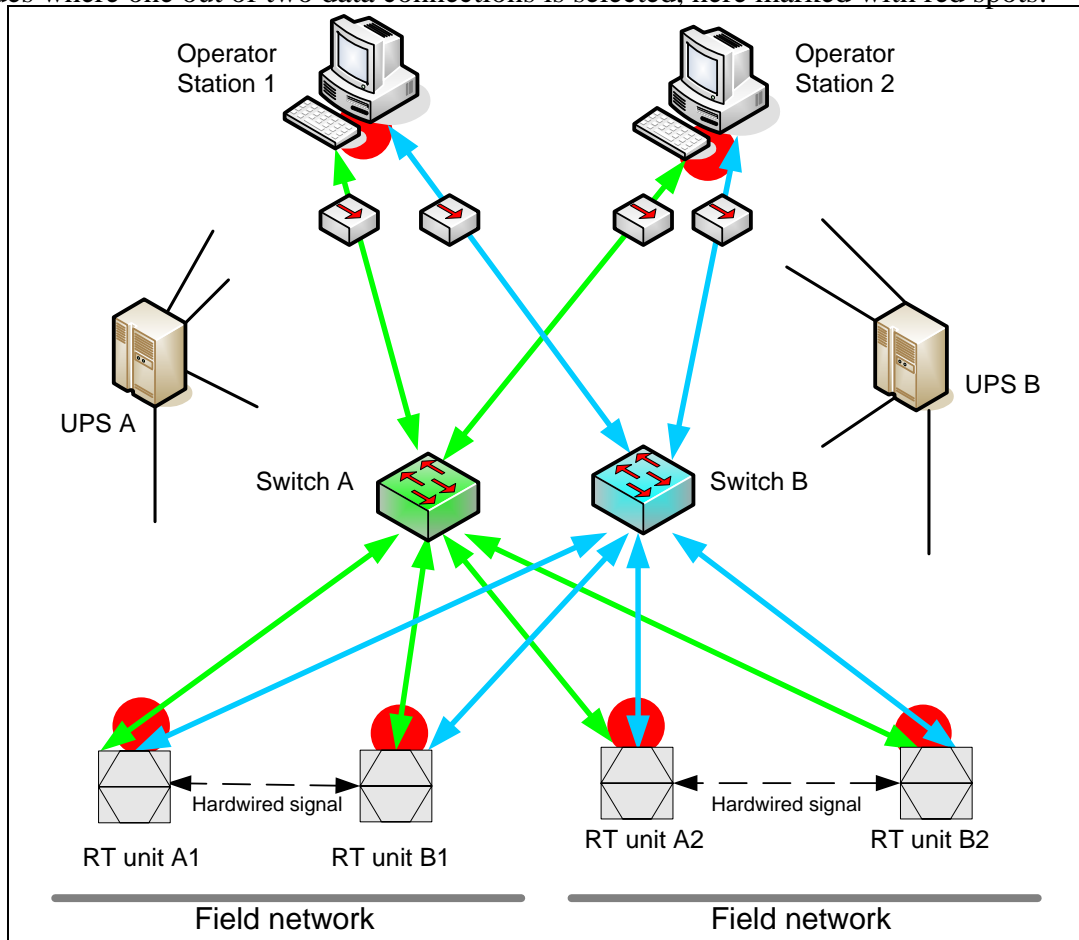
The failure mode “Network overload” may consist of packets with a single destination (unicast), multiple destination (multicast) or messages to all units (broadcast). Denial of service is a common term for this.

For these failure modes, it is important to verify the failure effect on the system components through a varied set of tests.

PSA and FMEA results

The PSA and FMEA tables are extensive and not shown as part of this paper.

The PSA shows that a detailed FMEA analysis is required to analyse single and double errors for the nodes where one out of two data connections is selected, here marked with red spots:



FMEA case study, critical points

Component	Failure mode	Problem description
Operator station	Erroneous data receive on both networks	No data received on networks (double error)
Operator station	Data transmit overload on both networks	Can make the station inoperable and jam the network.
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 and jam one network.
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 network	Will stop the RT unit.

Measures taken to avoid the problems can be:

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.
Excessive load protect	Specific limits set on RT units, disable network interface if required.
Message throttle	Limit amount of messages sent from Operator Stations
Message consistency	Only messages with legal application types are accepted.
Failsafe settings	Failsafe settings will apply if RT unit is stopped.

With these measures, the behavior of the inspected components will be:

Component	Failure mode	Reaction
Operator station	Erroneous data receive on both networks	No data received. Other Operator Station in other network segment works.
Operator station	Data transmit overload on one or both networks	Throttle the output to avoid network overload.
Operator station	Data receive overload on 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	RT unit shall go to Failsafe condition or increase real time control priorities.
RT unit	Transmit overload on one network	Shall be caught by a Watchdog and stop the unit.

Summary

Measures can be taken to prevent denial of operation in an automation network by:

- Ensure correct installation of network
- Only use qualified and approved network components. Consider use of a mix of components from different manufacturers.
- Check network normal operation parameters.
- Analyse weak points through FMEA.
- Avoid messages types that typically cause network storm.
- Implement methods to avoid excessive load.
- Analyse effects of changes in configuration by new FMEA.
- On-line reporting of network communication problems

The Classification societies require documentation regarding topology, FMEA, capacity and cable routing for communication networks. (ref. 2) Thus a specific walkthrough as described here is a necessary task to do.

Although the IMCA reports at present show little problems related to networks, the network is a part of the installed system that must be examined carefully and given attention during the operation lifecycle.

The demand for more functions and more equipment connected to network is increasing. Thus a detailed knowledge of the network parameters is required to avoid potential incidents related to network communication.

References

1. Station Keeping Incidents Reported for 2005, Draft May 2007, IMCA M XXX
2. Rules for classification of Ships/High speed, Light craft and Naval surface craft, Part 6, ch. 5: Integrated Computer systems, Det Norske Veritas (DNV)
3. DP and Integrated Control Systems Networks, Nick Cranch & Doug Phillips/Global Maritime