



DYNAMIC POSITIONING CONFERENCE
September 16-17, 2003

DP Design and Control Systems

DP and Integrated Control Systems Networks

Nick Cranch and Doug Phillips

Global Maritime (London) and Global Maritime (Houston)

Introduction

Modern Integrated Control Systems (ICS) on Dynamically Positioned (DP) vessels often rely on Dual Networks as the medium for the data link between outstations, the control computers and operators stations. Networks have been adopted for cost benefits over hard-wired systems, for speed of data transfer and the ability to modify/add to the networks with minimum downtime/effort.

DP vessels are now so reliant on dual networks; some class societies have accepted that no direct control of propulsion is necessary, because they are seemingly confident that the networks are dual redundant. This has not however turned out to be the case, there have been a number of failures of both networks, and the DP/ICS suppliers have had to redesign their networks to make them more fault tolerant.

This paper will outline the technical aspects of networks (but not in too technical a way), and review some of the double failure incidents that have occurred and the solutions being offered by the suppliers. It will also then review the various aspects of networks they relate to DP/ICS networks in: -

- Class requirements
- Criteria of acceptability
- Automatic Monitoring
- Customer acceptance testing
- Installation, Testing and Monitoring
- Reliability, Fault tolerance, Serviceability and Availability
- Future Developments
- Failure Modes

The conclusions and recommendation drawn from this review are summarized at the end of the paper.

Background

The main reasons for adopting networks as the communication medium are: data transfer speed and much reduced cabling. The first generation of ICS used simple serial connections to transfer data from devices on the vessel to the main computers.

These serial connections were relatively slow and there were also limitations in the maximum length of cable runs. The RS-232C (and V.24) standards adopted industry wide, allowed a maximum data transfer rate of 9.6kbps for lengths not exceeding 15m. The Current Loop standards (utilizing a current signal rather than a voltage) were no faster, but allowed a greater distance between communication devices. This allowed cable lengths up to approximately 1 km. One advance was the use of RS-422/V.11 that used a double twisted-pair arrangement to reduce noise levels. This gave an increase in speed to 1Mbps for lengths up to 100m.

The introduction of high-speed networks, which are basically high-speed serial links, has allowed their use in integrated DP/ICS to become widespread.

The advantages of adopting networks over conventional parallel wiring are perceived to be both economic and technical as follows: -

Integrated Control Systems

Economic

- Reduced cabling costs
- Saving in design time
- Savings in installation
- Saving in commissioning

Technical

- Easier Maintenance
- Easier Modification
- Guaranteed response time
- Security
- Easy access to variables

The disadvantages can be considered to be: -

Economic

- more difficult cabling
- Possible loss of all or many functions
- Possible long repair time

Technical

- specialized fault finding
- longer time to repair

Network Terminology and Components

The major items that comprise a DP/ICS network and main terminology used are defined below (these are largely based on refs 1 and 2).

Network - The term ‘network’ is broad and can be used to describe many formats of distributed data communication. It tends to be called ‘data link’ in class rules.

Protocols - A protocol (in computer terms and the context of networks) is the rules that govern the transfer of data between computers. There are two main network types in use today on vessels with DP/ICS systems these are either Ethernet or one of a number of field buses (FIP, Control Net, Genius, Profibus etc).

Topography - is more normally used to describe the way of representing, on a map or chart, the physical features of a place. In computer terms it has come to mean the physical and logical configuration of a computer network.

Node – a node is a network connected device such as an operator station, DP system, PMS system, outstation, printer, logger, etc

Layers – The term layer can be used in one of two ways in the context of DP/ICS networks – at the functional level there will typically be the following ‘layers’:-

Functional Layer	Function
Information Administration Layer – or Ethernet or FIP	Used to communicate non essential information between systems – between ICS/DP and other systems
Control or Process Layer – Ethernet, FIP or Control Net	Main ICS and DP Network
Device or Remote I/O Layer – Profibus, Device Net,	Networks between equipment and outstations or between outstations
Safety Level	Direct controls that have to operate without the higher level systems e.g. Fire and Gas or Emergency Shutdown systems, manual thruster control systems

Integrated Control Systems

The lower level of layers (protocol stack) is actually in each item that is connected to the DP/ICS Network. In this case they can be considered as

Application Layer	the software in the system that require to send and receive certain data
Data Layer	this works between the application layer and the physical layer and performs the transfer of data to and from each
Physical Layer	the physical way the devices communicate with each other by the transmitting of frames over the networks

It is interesting to note that the application layer may be different for each node connected to the network. But the data layer will need to be the same or similar in each node (software or firmware). Thus every node is susceptible to systematic failures. These are where a certain set of conditions arises that has not been designed for and results in all data layers and therefore nodes failing to communicate with the application. However as industrialized standards are used the data layer can be well proven.

Frames – Framing provides a controlled method of transmitting bits across the physical medium. Frames have a specific structure depending on the protocol in use. A block of bits is framed with a header and check sum is appended so that the frame can be checked for corruption. If a frame is corrupted or lost only that frame need be resent rather than the entire set of data.

Broadcast – just like a TV broadcast, the transmitted frames are heard by all nodes. But nodes receive only the frames that are addressed to them, like a TV set, it is only tuned to a particular channel to just receive the information it needs.

Multicast – is a way of efficiently transmitting information to a select number of nodes.

Point-to-Point – a point-to-point connection is a dedicated communication link between two nodes.

Back Bone – the connection between two star networks.

Collision Domain – this is a set of network nodes that share the same transmission medium and contend for access to it. Ethernet Networks have a collision domain whereas Fieldbus does not. The access that nodes get on a field bus network is controlled by one of the nodes being a bus arbiter.

Repeater – a repeater extends the distance of a network by amplifying and retiming signals. A repeater corrects for attenuation problems that occur when a network extends over a long distance. A repeater does not physically segment a network.

Hub – a hub is basically a repeater with multiple ports. It allows the network to operate in a star topography.

Bridge – a bridge divides a network in two separate collision domains while maintaining the broadcast domain,

Switch – a switch is a programmable multi port bridge that can temporarily bridge any port to any other port and therefore connect the nodes connected to those ports. Unlike a hub a switch, if configured, can forward frames from one port to the required destination port – not

Integrated Control Systems

all other ports. This reduces traffic on the rest of the network since frames are only traveling between the end nodes that are sending and receiving, rather than all nodes as in the broadcast domain.

Bandwidth – is the carrying capacity of a communications channel. It is helpful to think of a communication system like a pipe or hose; the size of the pipe or hose is analogous to the bandwidth and the flow to the data rate.

Twisted pair cable – The cable consists of copper-core wires surrounded by an insulator. The two wires are twisted together to provide protection from interference. Further protection from interference is provided by screening the insulator with a foil screen that can be earthed at one end – shielded twisted pair (STP). Traditional 10 megabit networks use two pairs, one for transmit and one for to receive. 100 Megabit and Gigabit uses four pairs to transmit and receive simultaneously. Twisted pairs tend to be used for the ‘copper’ part of star networks.

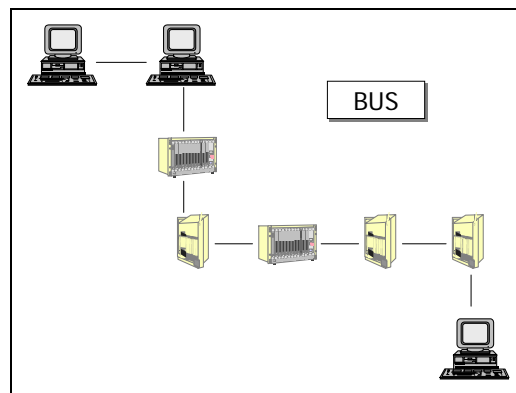
Coaxial Cable – This cable consists of a single copper core surrounded by an insulator, a combination shield and ground wire and an outer protective jacket. Coaxial cables tend to be used for the ‘copper’ part of bus and ring networks.

Fiber-Optic – This cable consists of a center glass core through which light waves propagate. This core is surrounded by a glass cladding, which reflects the inner light of the core back into the core. A thick plastic outer jacket surrounds this assembly along with special fibers for added strength. The advantage of using fiber optic is the increased bandwidth and immunity from interference. The disadvantages are the cost and complication of its installation.

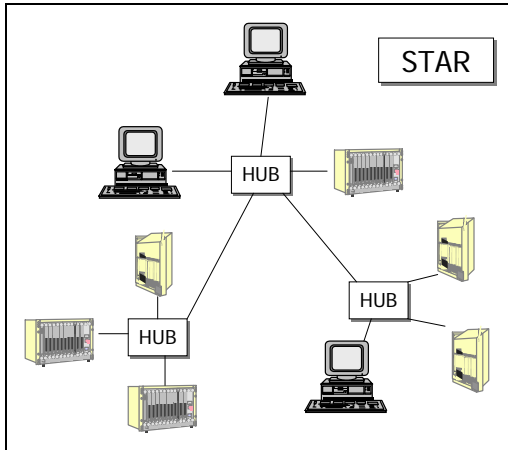
Network Topology

The architectural type of a DP or ICS network, its topology, can be BUS, STAR or RING (plus variations on these themes), generally depending on the age of the system with STAR or RING being the preferred for most DP/ICS DP class 3 installations. Bus is more often used for DP class 2 installations.

- A BUS format will have all nodes on the network in one long chain with repeaters at each connection and a termination at the end of the chain. All devices connected on the network will be via drop cables connected at repeaters/hubs.

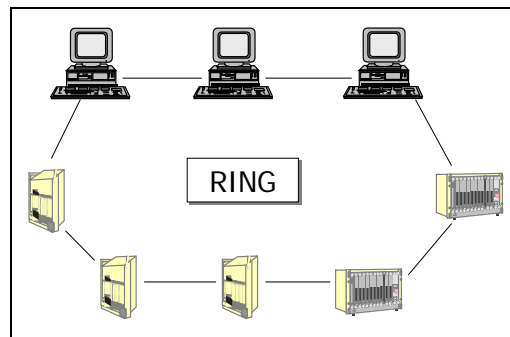


Integrated Control Systems



- A STAR format will be centered on a main hub where spurs will run off to further hubs/repeaters where drop cables are connected to the devices. The STAR format allows for individual failures without complete network loss as a section of the network can be disconnected without affecting the remainder.

- A RING format is simply a complete loop version of a BUS network incorporating all devices and control computers on the network. Connections to control computers can be via drop cables or within the RING. Again there is the possibility of a failure forming a break in the chain. However by using the RING communications can be continued because the break reduces the ring to a bus and that is still operational.



For ICS and DP networks to meet class 2 redundant networks are necessary, and to meet class 3 the redundant networks are run in separate cable runs and the equipment is housed in separate A60 compartments so that no compartment failure through fire and flood can cause both networks to fail. The topography chosen for each class is different for different supplier – some chose a star for class 3 and a bus for class 2. While others use a star for class 2 and a ring for class 3. Some mix the ICS and DP on one networks, others keep them separate.

Ethernet

Ethernet is one network protocol of choice for one major DP/ICS supplier. It utilizes the industry standards emanating from the US federal government. The operating system adopted by the suppliers is now Microsoft's Windows NT4 Workstation that is based heavily around the Ethernet format and TCP/IP (Transmission Control Protocol/Internet Protocol) protocol stack.

The format for Ethernet is defined as Carrier Sense Multiple Access/Collision Detection (CSMA/CD), where the nodes attached (multiple access) listen to the network (carrier sense) before transmitting, and if in use wait. Collision Detection (CD) is used so that when more than one device transmits on a clear channel and a collision occurs a time delay is applied to ensure the re-transmit does not result in a further collision.

Speed and reliability of communications can be significantly improved by introducing hubs and switches.

Ethernet speed can be 10 or 100 Mbits/sec. A new Giga bit (1000 Mbits/sec) version is also now available. These speeds are faster than those described below for Field Bus but overall performance may not be that different as there is a larger overhead of software and time

Integrated Control Systems

delays due to collisions. But this depends on the topology and configuration. Use of full duplex for instance eliminates collisions.

Field Bus

Field Bus is the network protocol of choice for two of the major ICS and DP suppliers. A field bus is a network that has been designed for use in an industrial control environment. Those used in DP/ICS applications are the European open architecture - Field Interface Protocol (FIP), and the Rockwell Automation's proprietary commercial off the shelf system - Control Net.

FIP can operate at 0.3, 1 or 2.5 Mbits/sec but is used at 1 Mbits/sec for DP/ICS and Control Net at 5 Mbits/sec. The major difference between these and Ethernet is that they are deterministic. That is to say that, unlike Ethernet, the network has a guaranteed update time for all key parameters being transmitted on the network. They also have routines in place to allow for the transmission of variables and messages that only need to be exchanged periodically without any tight time requirements.

Ethernet can have guaranteed update rates when the network is suitably organized and when in addition full duplex is used for the backbone. Ethernet systems also often at process level use some form of fieldbus.

FIP can be considered as having three types of transmission:-

Cyclic	always on time
Events	when they occur
Messages	transferred when required, down loads, set ups, up load of diagnostics.

An Ethernet based system can have quite similar transmissions. But cyclic "on time" requirements are achieved by organization of the functions in the system (same controller, units connected to same process/field net to the controller, segmentation of network through switch setup etc.). This also applies to the statement "transmission of variables and messages that only need to be exchanged periodically without any tight time requirements", which with Ethernet is more of an application function than a characteristic of the network.

Class Requirements

Prior to the advent of dual networks classification societies required that alarm, control and safety systems be kept independent and separate. The philosophy was based on the principle that if a control system was inoperative then the alarm would work (and vice versa), and as a back up to both the safety system would act and make the plant safe. Therefore many early ICSs had a system for alarms and a separate one for control, with possibly some supervisory computer presiding over the two of them. The DP was totally separate. The safety system was directly acting on the plant. However, with the advent of dual networks and redundant processors in the critical process stations class societies have accepted this redundancy in lieu of the traditional redundancy achieved by the split of alarm, control and safety philosophy. Thus many vessels are now totally reliant upon the performance of a dual network, which if both networks fail control will be lost.

For example current ABS rules for Computerized Systems (part 4, chapter 9, section 6.) states the following:-

3.11 System Independence

Control, monitoring and safety systems are to be arranged such that a single failure or malfunction of the computer equipment will not affect more than one of these system functions. This is to be achieved by dedicated equipment for each of these functions within a single system, or by the provision of redundancy, or by other suitable means considered not less effective.

5.5 Data Communication

5.5.1 Data Link

The data link (data highway) is to be continuously monitored to detect failures on the link itself and data communication failure on nodes. Any abnormal condition detected is to be alarmed at the centralized control station and on the navigation bridge. Safeguards are to be provided to prevent unacceptable data transmission delays (overloading of network). Alarm is to be activated prior to a critical data overload condition.

5.5.2 Duplicated Data Link

When the same data link is used for two or more essential functions (e.g. propulsion control and generator control), this link is to be duplicated, and each is to be routed as far apart from the other as practical. The duplicate link is for standby purpose only and not to be used to reduce traffic in the online link.

Duplicated data link is to be arranged so that upon the failure of the on-line link, the standby link is automatically connected to the system. Switching between duplicated links is not to disturb data communication or continuous functioning of the system. The failure of one link is to be alarmed at the centralized control station and on the navigation bridge.

5.5.3 Connection Failure

A complete failure in connectivity between component systems and the data highway is not to affect individual functionality of the component systems.

Current DNV rules for Dynamic Positioning Systems (Part 6, Chapter 7, section 2) state

C 500 Arrangement and layout of data communication links

501 When two or more thrusters and their manual controls are using the same data communication link, this link is to be arranged with redundancy in technical design.

502 When the DP-control system uses a data communication link, this link is to be separate from the communication link(s) for manual control.

503 The communication link for the DP-control system is to be arranged with redundancy in technical design for **AUTR** and **AUTRO**.

504 For **AUTR** no failure mode, as specified in B301, and for **AUTRO**, as specified in 302, are not to have an effect on the functionality of both networks.

Where AUTR is equivalent to ABS Class 2 and AUTRO equivalent to ABS Class 3.

Network Incidents

Despite the class societies requirements and acceptance of dual networks/data links and in particular when not direct manual controls have not been required, there have been a number of dual network failures. Ten have been reported and or presented to IMCA. These are given in outline below:-

Incident 1. Failures on one network, taken offline, remaining net fails through overload of errors. The system was using older technology with a specialist cable that required greater maintenance than it was receiving.

Incident 2. Loss of both networks simultaneously due to poor design and installation. One outstation had a single connection to another system, which produced corrupted data onto both networks. Poor design in ESD chain and NO/NC relays resulted in the shut down of all engines and thrusters.

Incident 3. Loss of both networks simultaneously due to poor design and installation. One outstation had a single connection to another system, which produced corrupted data onto both networks. Poor design in ESD chain and NO/NC relays resulted in the shut down of all engines and thrusters.

Incident 4. Loss of both networks simultaneously due to jabber from an optical-copper converter. System design was flawed as the redundancy occurred in the rings only and loss of this device (optical-copper converter) caused both networks to receive faulty messages and overload/shutdown.

Incident 5. Loss of both networks simultaneously due to jabber from an optical-copper converter. System design was flawed as the redundancy occurred in the rings only and loss of this device (optical-copper converter) caused both networks to receive faulty messages and overload/shutdown.

Incident 6. Faulty hub in dual networks caused both networks to receive faulty messages and processors of servers ran at 100% causing timeouts and shutdowns. Fault eventually identified as faulty hardware.

Incident 7. Failure occurred in transit but this is an integrated system so all thruster commands travel over network. No hardwired thruster controls. This was a failure to do with 24VDC earths, which caused the control interface to try and switch networks, but both sets of controllers went down, similar to another incident. Captain required tug assistance.

Incident 8. Failure occurred in transit but this is an integrated system so all thruster commands travel over network. No hardwire thruster controls. Networks overload; causing the controllers to hang up as they were continually dealing with the information being sent to them, they could not deal with the amount of information.

Incident 9. Faults on B network causing it to fail. Traced to faulty hub. Vessel lost position when Net A failed when net B was being upgraded.

Incident 10. On computer gives a 'run time exceeds limits', then 'send mail error' and warning 'net waypoint input error'. DP freezes up. Cause was an incident failure.

These incidents have been kept anonymous but what can be pointed out that these ten incidents are split 50:50 between two different DP/ICS suppliers. Seven of them were on drill vessels, two on support vessels and one on an FPSO. As can be seen from the text some were the same fault but on another DP/ICS but generally a sister vessel.

Although the networks were designed with the intent of dual redundancy these examples clearly show that there is a possibility that both networks can fail. The hardware, software and architecture of each are after all identical.

In the examples it can be seen that an error or failure produced on one of the redundant networks can in some circumstances/installations lead to catastrophic events and a dual

Integrated Control Systems

network failure. The majority of these failures were due to some form of ‘jamming’ of both networks from a common single device.

The causes of dual network failures can be difficult to work out. The manifestation of the problem leads to numerous alarms, information and facts on which the solution might be based come from the observations of untrained crew. The initial problem is trying to unravel the information available to begin to look in the right direction. This can be a long and protracted process yielding little or no results until the correct piece of information has been isolated and there is evidence still in place to back-up or confirm suspicions.

The DP/ICS suppliers have worked to remove these failure modes and avoid them in new systems designs, many of which occurred as ‘infant mortalities.’ Their solutions included doubling up the networks, adding switches in place of hubs and introducing addressing and data checking.

In some cases network components has been identified as the cause, and have been replaced by components from other vendors with better technology. Plus the error modes identified have been added to the acceptance test for the network.

Criteria of acceptability for DP and ICS Networks

One supplier’s criteria of acceptability that seems to be a reasonable set for an Ethernet network used for control are:-

- No network alarms
- No network errors
- Minor loss of messages
- Hub based – 25 to 30% utilization of 10 mbits/sec
- Switch based – 20% utilization of 10mbits/sec
- Update time of key parameters – per application
- No latency in switching between networks

A field bus can accept higher utilization than this as they are deterministic and therefore does not need so much spare time to allow for collisions, dropped frames etc. A figure of 50 to 70% would be considered reasonable. By comparison an office IT network would be run at 80% utilization. The update time for key parameters in a Fieldbus should be a fixed number. That for Ethernet is more difficult to decide and may require having a tolerance, as it is not deterministic.

Automatic monitoring

On-line monitoring of the networks is generally provided on the operator stations with alarms raised for errors. Due to the complication of networks on board troubleshooting may be difficult with untrained crew and the only course available for the crew is to contact the supplier for support. With the advent of remote diagnostics more can now be done before having to mobilize a service engineer from the suppliers.

There are alarms generated that are carefully chosen and, to trained crew and engineers within the suppliers' organization, they can provide a great deal of information. Alarms are typically provided for a total network failure.

Statistics on network performance are logged and recorded by the DP/ICS and this information is available to the operator.

Customer Acceptance Testing

The area of benchmarking or base lining the performance of a network is difficult and differs greatly as to the technology employed and the ICS/DP supplier. So it is hard for a customer to decide if a network is performing correctly. The criteria of acceptability similar to those already described and agreed with the DP/ICS supplier above should be used as a basis for the CAT.

Once the criteria have been met the normal or expected performance can be recorded and defined and subsequently used to check the network performance in the future.

On board installation, testing and monitoring

It has already been mentioned that the initial cabling installation is key to the reliability of the DP/ICS network. The requirements for cables and their installation; should be defined in detail by the DP/ICS supplier (ref 3). They should cover

Cable Types – for twisted pair, co-ax and fiber

Cable Handling – particularly fiber that must be hand pulled not machine pulled, they should not be twisted or bent more than the minimum-bending radius (typically 55 mm)

Routing – separation of redundant networks and equipment

Segregation – distances from High Voltage cables, RF equipment, variable frequency drives etc. These do not apply to fiber optic cable.

Protection – in harsh environments, use of conduit etc (especially for fiber)

Terminations – special requirements and tools

Connectors – to be used and special tools

Screening – screen earth requirements

Reliability, Fault Tolerance, Serviceability and Availability

The RAS (reliability, availability and serviceability) of the dual network is clearly of great importance because of the serious potential consequences of a dual network failure.

A reliable fault tolerant network keeps the availability as high as possible by maximizing the MTBF; and by its serviceability minimizes the MTTR. Availability of networks can be defined as being within a certain Availability Class (ref 1) as follows.

Availability Class	Availability Measurement	Annual Downtime
Two Nines	99%	3.7 days
Three Nines	99.9%	8.8 hours
Four Nines	99.99%	53 minutes
Five Nines	99.999%	5.3 minutes
Six Nines	99.9999%	32 seconds

One published figure for a dual failure of both DP/ICS networks is a MTBF of 53.84 years. To achieve a 'six nines' rating the MTTR would need to be 28.7 hours (99.999% of 53.84 years), for 'four nines' nearly two days. If a dual network failure requires call out of an engineer, possibly from Europe, this whole process could easily take up to a week and would give it a class between 'three' and 'four' nines.

Network fault management is the ability on board to be able to locate faults, determine their causes and make corrections. This requires fault tolerant hardware and fault tolerant procedures. These can be achieved by the following

Fault Tolerant Hardware and installation

- Careful specification, monitoring, checking and verification of the network cabling to DP/ICS supplier's requirements.
- Use of environmental tested equipment
- Continuous monitoring and collection of performance statistics
- Setting of threshold conditions that can warn the operators of conditions that may be an indication of a potential failure
- Redundant Components – e.g. power supplies
- Both networks are used and monitored continuously and changeover is transparent

Procedures, personnel and equipment

- Holding test equipment on board such as a network or protocol analyzer and knowing how to use it
- Holding a suitable inventory of spares
- Remote Diagnostics accessible by the DP/ICS supplier
- Monitor network periodically – on DP check list
- Test network annually or every mobilization
- Maintain and inspect network as part of the vessel's planned maintenance
- Provide procedures that an unskilled user can follow if necessary
- Ensure proper documentation of all systems.
- Include in the DP Operations Manual what is to be done in the event of network problems.

Failure Modes of ICS and DP Networks

The IEC on Failure Modes and Effect Analysis (ref 5) provides the following generic failure modes. Those ticked are considered to be relevant to DP/ICS networks and a suggested failure mode is given.

Generic Failure Modes	✓	Related to Networks
❖ Structural Failure (rupture)	✓	failed fiber optic cable
❖ Physical (binding or jamming)	✓	kinked fiber optic cable
❖ Vibration	✓	poor connections
❖ Fail to remain (in position)		
❖ Fails to open		
❖ Fails to close		
❖ Fails open		
❖ Fails closed		
❖ Internal leakage		
❖ External Leakage		
❖ Fails out of tolerance (high)	✓	messages too long
❖ Fails out of tolerance (low)	✓	network response too slow
❖ Inadvertent operation	✓	changeover to other network
❖ Intermittent operation	✓	poor connection
❖ Erratic operation	✓	high jamming traffic
❖ Erroneous indication	✓	frame scrambled or interference
❖ False actuation		
❖ Fails to stop		
❖ Fails to start		
❖ Fails to switch	✓	switch failure – node to node
❖ Premature operation	✓	sends frame at wrong time
❖ Delayed operation	✓	delayed response from node
❖ Erroneous input (increased)	✓	frame received too long
❖ Erroneous input (decreased)	✓	frame received too short
❖ Erroneous output (increased)	✓	frame transmitted too long
❖ Erroneous output (decreased)	✓	frame transmitted too short
❖ Loss of input	✓	no frames received
❖ Loss of output	✓	no frames transmitted
❖ Shorted (electrical)	✓	cable failure - short
❖ Open (electrical)	✓	cable failure - open
❖ Leakage (electrical)		
❖ Other unique failure conditions applicable to the system characteristics, requirements and operational constraints.	✓	frames misaddressed
	✓	data displaced
	✓	non operational network faulty
	✓	latency in network switching

Future Developments

In the light of their recent experience and developments in technology, the main DP/ICS suppliers are each considering developing their networks, ideas on the drawing board at the time of writing are:-

- Replacing hubs with switches
- Use of new traffic protocols

Integrated Control Systems

- Have totally separate redundant networks for the thruster control system
- Put a Bridge between DP and ICS networks
- Moving to ring topography from a bus topography.

Conclusions and Recommendations

As an owner or potential owner, user or maintainer of a DP/ICS network the following summarizes the main recommendations and conclusions that can be drawn from this paper:-

- Be aware that the operation of the dual network can be essential to the vessel's safety
- Be aware that each network of a dual network DP/ICS can fail simultaneously
- Install the network properly to the recommendations of the DP/ICS supplier
- Get the suppliers criteria of acceptability and test to it
- Review suppliers FMEA of the network for the failure modes identified
- Decide the baseline performance of the network
- Validate the cabling and test the network's performance on board
- Monitor performance and statistics on board as part of regular watch keeping, field arrival/mobilization trials. Check against the bench mark performance
- Test network failure modes annually
- Check physical condition connections on a regular basis as part of the vessels planned maintenance
- Train maintenance personnel
- Plan for disaster recovery and have simple instructions available for non technical personnel
- Review level of spares and test equipment and compare to the cost of down time
- Consider remote diagnostics
- If the potential of loss of both networks is serious and there are no direct controls of thrusters available; consider direct controls

References

1. Encyclopedia of Networking and Telecommunications – Tom Sheldon
2. Webster's Pocket Computer Dictionary
3. Installation Manual – SDP/SVC/SSS network
4. Nick Cranch – article accepted for Offshore Engineer magazine
5. Analysis techniques for system reliability – Procedure for the failure modes and effects analysis (FMEA). CEI/IEC 812:1985

Acknowledgements

The authors would like to thank the following DP/ICS supplier and individuals for their assistance with this paper. The paper though must be regarded as the authors' personal view and its contents are not approved by these DP/ICS suppliers.

Kongsberg Simrad	Amund Tinderholt
Nautronix	Glen Rozak
Alstom	Bruce Kauffman