Dynamic Positioning Committee
Marine Technology Society

DYNAMIC POSITIONING CONFERENCE
October 11-12, 2016

Cybersecurity SESSION

Network Storms and Other Communication System Failure Modes

By Ahmed Hamody

Independent

Abstract

DP class rules require that vessel and DP control networks are redundant and not subject to a common cause of failure. Despite this, there have been high profile DP incidents associated with total loss of communication to all thrusters.

Although there are two main data highways, all the network nodes (Field Stations or Operator Stations) connect to both networks and represent common points between the two redundant DP groups. Although these networks are usually able to tolerate benign failures such as wire breaks and power supply failures, experience confirms that more aggressive failure modes have the potential to cause total communications failure in some cases. One such failure mode is the Cyber (Network) Storm on Ethernet based systems but other type of failures and other types of transmission hardware have had suffered similar failures.

Although protective functions are provided in some designs, experience from DP incidents and DP trials results suggests such measures can be defeated.

Class rules on the subject of redundant communications are fairly limited and there is little detailed guidance on the design and testing of such systems which is specific to DP.

This paper provides:

- A discussion on the design of fault tolerant data communications
- Guidance on the failure modes to which such systems are susceptible
- The protective functions employed to address those failure modes
- The type of testing that should be carried out to prove system performance and correct operation of protective functions
- The monitoring and alarms required to indicate when communications systems are no longer fully fault tolerant

Experience and information on these issues have been gathered from the DP community but also from other industries which have similar requirements for redundancy and fault tolerance in communications networks.

Abbreviation / Definition

AO	Analogue Output
DI	Digital Input
DGPS	Differential Global Positioning System
DP	Dynamic Positioning
DPC	Dynamic Positioning Controller
DO	Digital Output
FMEA	Failure Mode and Effect Analysis
FO	Fibre Optic
GUI	Graphical User Interface
HMI	Human Machine Interface
IACMS	Integrated Automation Control And Monitoring System
IP	Internet Protocol
I/O	Input/Output
LAN	Local Area Network
NIC	Network Interface Card
NSU	Network Switch Unit
OS	Operator Station
PLC	Programme Logic Controller
Profibus-DP	Profibus Decentralised Peripherals
PRS	Position Reference System
STP	Spanning Tree protocol
TCP	Transmission Control Protocol
UPS	uninterruptible Power Supply

Introduction

Ethernet Network Architecture

As required by the DP class rules the IACMS/DP Ethernet communication networks are redundant and they are independent arms, where each network arm has its own communication lines (cables) and Network Switch Units (NSU).

As shown in Figure - 1, the network comprises:

1. Operator Station: It is the user interface unit, which runs GUI-HMI application, for the user to monitor and control the system.
2. Programmable Logic Control: It is industrialised real-time computer system, it monitors the reading acquired from field (via serial line and discrete/analogue Inputs), and –based on its programme- it takes control action/s in coordination with other parts of the system.
3. Network Switch Unit: computer networking device that connects numerous nodes (PLC/OS) forming a mesh of nodes. The main function of the switches is directing data packets traffic around the network nodes. In addition, some network switches have more advanced configurable functions and management features. There are different network topologies. For IACMS/DP systems, a combination of star and line topologies is used.

In certain DP vessels (DP-3) the location of the NSU, network cable routing and the distribution and location of NSU's power supply (UPS) are designed carefully while the failure definition is extended to include the risk of fire and flood.

In IACMS/DP systems to achieve redundancy of data communication network, the exchanged data on both arms are identical, i.e. each node (PLC/OS) sends the same information to the relevant recipient(s) via both arms at the same time.

By this design, it gives the control system high availability communication means and certain level of fault tolerance. But, can it tolerate more severe failure, this is discussed in further in later part of the study.

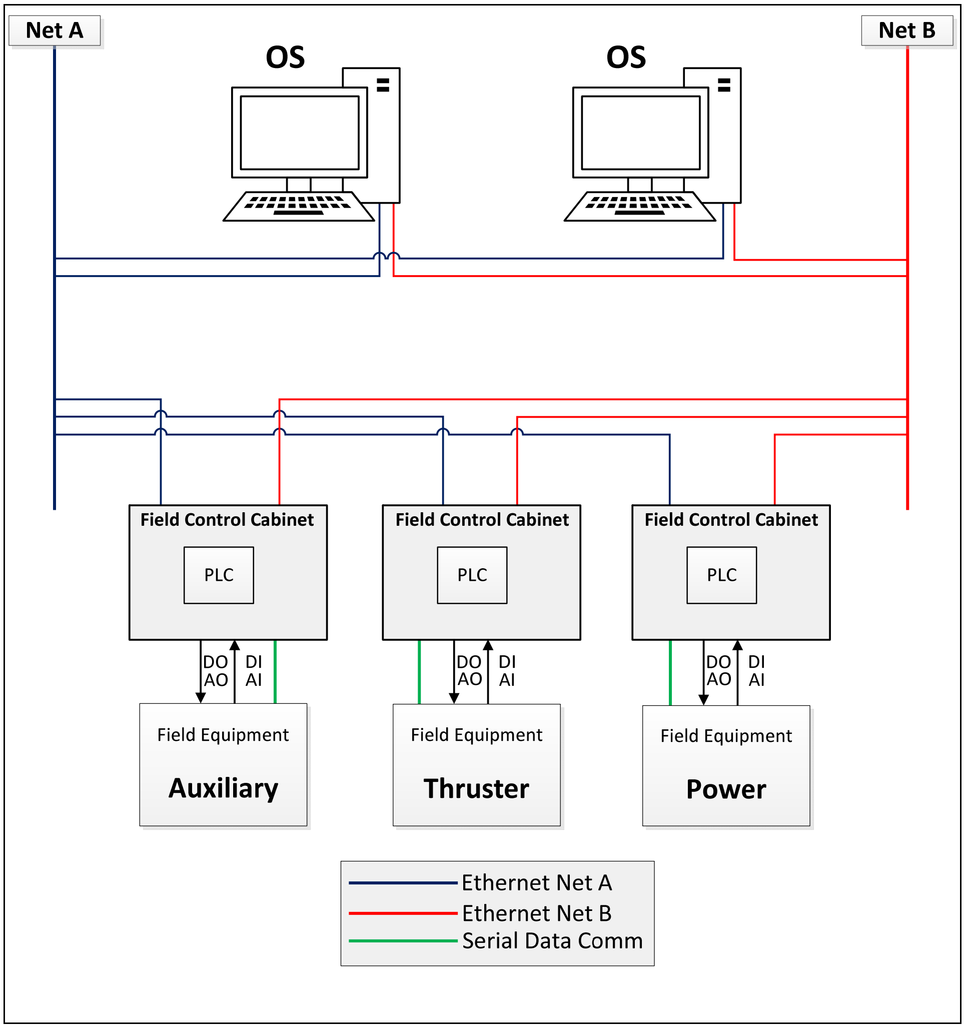


Figure - 1 IACMS Network Topology

Network Strom (Cyber Storm) Failure Mode

The failure mode of so-called "Network Storm" or "Cyber Storm" is an identified network issue across the industrialised automation industry.

The communication traffic of Ethernet has three types: Unicast (a message is sent from one network node to another node), Multicast (a message is sent from one network node to multiple nodes) and Broadcast (one network node sends a message to all other network nodes).

The "Network/Cyber Storm" occurs when a node broadcasts excessive amount of messages in uncontrollable way, resulting large volume of data saturating the network capacity, and subsequently the communication networks becomes unusable to exchange the important data for the system operation.

The immediate effects of this failure will be:

1. Loss of communication among system nodes.
2. Major consumption of processor computation resources.

This issue is classified as network serious Cyber threat to any network. Therefore, authorities, operators and manufacturers took extensive measures to prevent it and rectify it once occurred.

Therefore, due to the criticality and severity of this failure, the Department of Homeland Security (DHS) is carrying out a regular exercise (every two years) called exercise "Cyber Storm", which is the most extensive and administratively organised of its kind. The exercise results and finding is published to public. 2016's exercise 115 participants involved in the exercise, including government agencies at the federal, state and local levels, along with international agencies and corporations.[2]

Network Storm (Cyber Storm) Potential Causes

There are several causes originate this malfunction, these causes can be categorised as:

1- Software failure
2- Hardware failure
3- Human Error
4- Inherited design issue
5- Network Configuration Error

The software failure could occur at different levels, application level, Operating System level or low level component firmware. Depending on the failure nature, the end effect would be irrepressible cyber storm. More hazardously when the root cause of this failure is not software bug or glitch, instead it is caused by a Malware. As this Malware is designed to perform extended damage.

Some examples of Malwares caused network storm are:

1. Conficker(3) worm: has created media storm across the world affecting millions of computers including government, business and home computers.
2. Stuxnet(4): it was highly sophisticated malware. Its target was Siemens industrial control and monitor system.

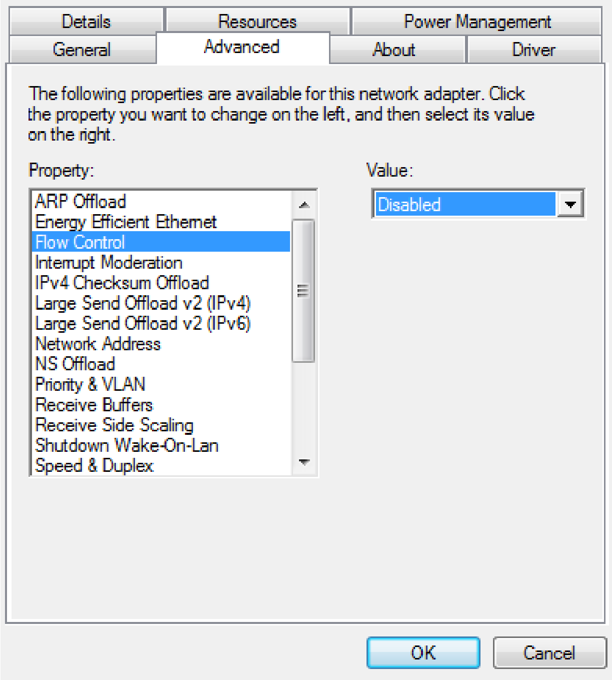
The hardware failure is due to either cable connector defect this causes intermittent disconnection, or circuitry flaw.

The human error occurs by connecting loop back Ethernet cable from a port to another on the same network switch. STP protocol should prevent the storm from occurring, however, it works only if the switch is configured to enable this feature.

DP class rules require that vessel and DP control networks are redundant to provide higher availability of communication means. However, this design inherently creates common points (network nodes) between the two redundant groups. As, all the network nodes (field control cabinet and operator stations PC) are connected to both networks.

The network configuration error includes wide range of settings. These settings determine the network's reaction against a fault, and are applied for the network nodes and NSUs.

In a case, where OS suffers from operating system failure, which could be due to hard-drive fault or operating system halt, the NIC revert to self- management using its firmware and setting, therefore if "Flow Control" property is enabled, as shown in Figure - 2 this could lead to sending uncontrollable data packets. This example shows a combination of causes, where operating system fault penetrated through configuration error and subsequently causing the Cyber storm.



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property: Flow Control

Value: Disabled

Figure - 2 NIC Flow Control Configuration

Network Strom (Cyber Storm) failure effect

In DP industry domain, although protective functions are provides, it has been see high profile DP incidents associated with total loss of communication to all thrusters, which means these measures can be defeated.

In O&G industry, from experience, the effect which has been seen –due to a Cyber Strom triggered by a Malware- a total loss of communication between onshore base station and offshore control units, and subsequently, operation shutdown and avoidable down time.

Protection against Network Storm

To make the DP Ethernet Network fault against such severe failure, all the causes –mentioned above- should be addressed correctly.

A particular attention should be paid to address the commonality between the two redundancy groups. The most effective way to address this issue is by configuring the NSUs to control the data traffic and restrict it once needed.
In such configuration, each network switch's port restricts the amount of allowed data to be transferred through it. As each port represents the connection point of a node (Field Control PLC/Operator Station) to the network, therefore, the maximum amount of transmitted data is known therefore no excess above this limit should be allowed. Once the data amount exceeds the allocated limit, this will be seen as abnormal data transmission from a node and subsequently the affected node will be blocked. Nevertheless, the impact will be a loss of communication with a node, on the other side the whole network will be operational normally.

The philosophy of this protection technique is that, the network data traffic are controlled and protected by the NSU, and it is the base of regulating the traffic.

Road Traffic Light analogy describes this network protection technique. As at road intersection, the traffic light system regulates the flow of traffic in safe and controllable manner, instead of relying on a driver to assess the traffic ahead and determine whether to cross or wait.
If the road is occupied by illegitimate traffic (Cyber storm), this prevents the needed information -for operation- from being transferred then used for monitor and control.

In addition to the engineering approach to tackle this issue, there are also other measures to be undertaken such as:

1. The DP rules outlines the top-level design requirement, however, this level of design aspects are not greatly discussed. Developing the Class rule to accompany the advancements is important to fill the current gap and to proactively address the potential cyber threat.
2. This development of the rules will provide the foundation to develop testing procedure and collect quantified results. It also will be the criteria for approval of specialised measurement equipment and utilities.
3. Include this test as part of the regular sea trials for technical assurance measures.

Network Strom Tests

The network (Cyber) storm can be tested by either using a software utility or hardware equipment, which is capable to generate data packet.

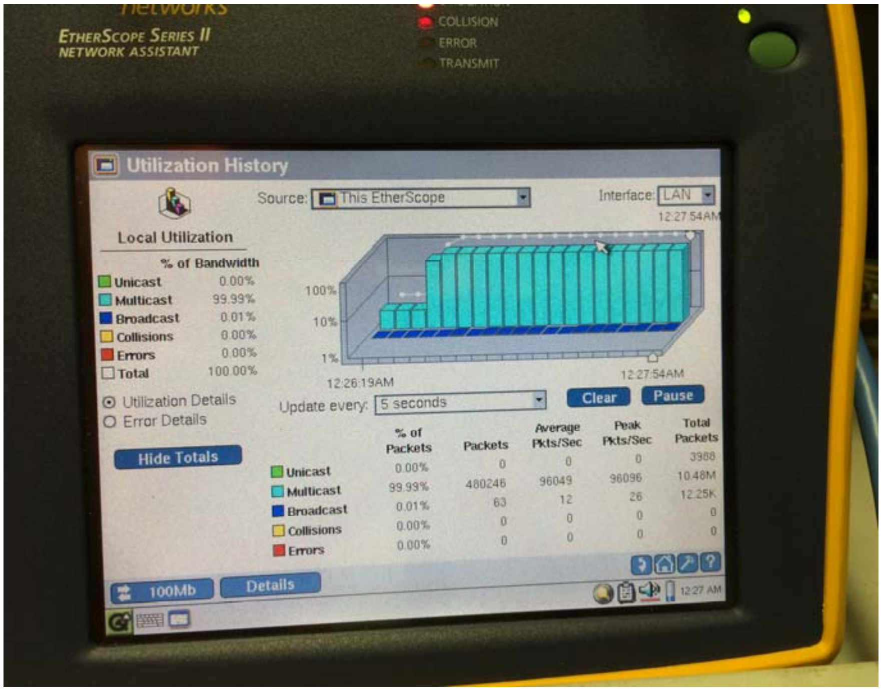
There are two aspects to be taken into consideration with testing tool:

1. Testing Tool: The used Software utility or hardware kit should be tested and approved for the purpose of the test. Moreover, to tool appropriate for the system that is being tested.
2. The amount of data that is being injected to simulate the storm must be the amount of the bandwidth. The nodes' nominal usage of the total bandwidth is small fraction, under normal circumstances, therefore if the total injected data is less that the total capacity, then there will be a space for the operational data to be exchanged, therefore the objective of the test is not achieved.

As detailed previously, despite the DP/IACMS Ethernet network are redundant; however all the network nodes (Field Control PLC and Operator Station) are considered as common point of failure, thus upon a severe failure affecting one node could lead to storm both network arms at the same. Subsequently, it is important to carry out the network storm on both networks at the same time.
This might appear as two failures simultaneously, however, the root cause of such scenario is a single failure affecting one node with multiple effects.

The test could also be associated with the use of network monitoring device or software. The advantage of using monitoring tool, is to verify to storm details and quantify the storm level.

As shown in Figure – 3, this test was carried out to simulate multicast storm.



Utilization History

Source: This EtherScope

Interface: LAN

12:27:54AM

Local Utilization

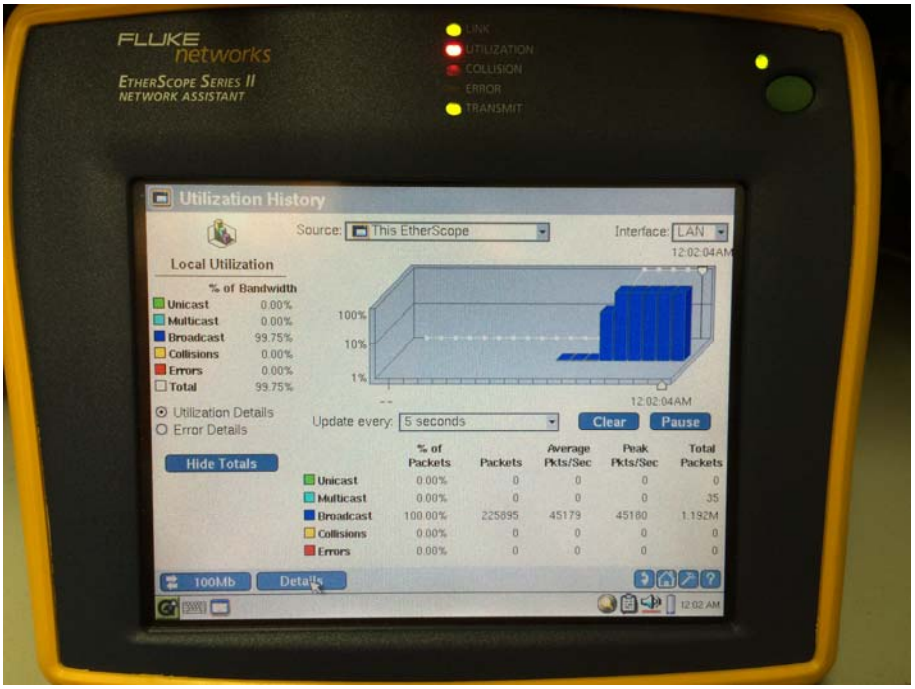
	% of Bandwidth
🟩 Unicast	0.00%
🟦 Multicast	99.99%
🟦 Broadcast	0.01%
🟨 Collisions	0.00%
🟥 Errors	0.00%
□ Total	100.00%

Update every: 5 seconds

	% of Packets	Packets	Average Pkts/Sec	Peak Pkts/Sec	Total Packets
🟩 Unicast	0.00%	0	0	0	3988
🟦 Multicast	99.99%	480246	96049	96096	10.48M
🟦 Broadcast	0.01%	63	12	26	12.25K
🟨 Collisions	0.00%	0	0	0	0
🟥 Errors	0.00%	0	0	0	0

Figure - 3 Multicast Network Strom

As shown in Figure – 4, this test was carried out to simulate broadcast storm.



Utilization History

Source: This EtherScope

Interface: LAN

12:02:04AM

Local Utilization

	% of Bandwidth
🟩 Unicast	0.00%
🟦 Multicast	0.00%
🟦 Broadcast	99.75%
🟨 Collisions	0.00%
🟥 Errors	0.00%
□ Total	99.75%

Update every: 5 seconds

	% of Packets	Packets	Average Pkts/Sec	Peak Pkts/Sec	Total Packets
🟩 Unicast	0.00%	0	0	0	0
🟦 Multicast	0.00%	0	0	0	35
🟦 Broadcast	100.00%	225895	45179	45180	1.192M
🟨 Collisions	0.00%	0	0	0	0
🟥 Errors	0.00%	0	0	0	0

Figure - 4 Broadcast Network Strom

Serial Network Architecture, Failure Cause and Effect

The most common serial data communication network topologies are either: point-to-point (peer-to-peer) or star configuration, where there is one master communicating to numerous devices.
This makes the serial network confined and less vulnerable to certain cyber threats.

DP Class rules require certain number of position reference systems and sensors feeding the DP Controller (DPC), as shown in Figure - 5, this is achieved by connecting each device to all DPCs simultaneously, either directly or indirectly via data splitter or optical convertor. Many of these sensors are sending the readings and measurements via serial data communication lines to the controller. There are different designs for the hardware connection configuration, where NMEA 0183 is the most common communication protocol.
In other cases as shown in Figure - 6, the serial communication lines are also used for communicating with thrusters control units for monitoring and controlling the thrusters.

For both cases above, the serial network forms star topology, in which the DP Control PLCs are the common point for all thrusters' control PLCs.
The serial communication, however, is exposed to hardware failure, this could lead the affected component or device to a state of storming serial bus; as a result the DP control PLC will be no longer able to communicate with all thrusters.

The resolution of this issue can accomplished by either separation of serial channels, therefore upon a failure of one channel there will be no wider effect to all channels, or facilitate advanced serial modules these are capable to block the affected port.

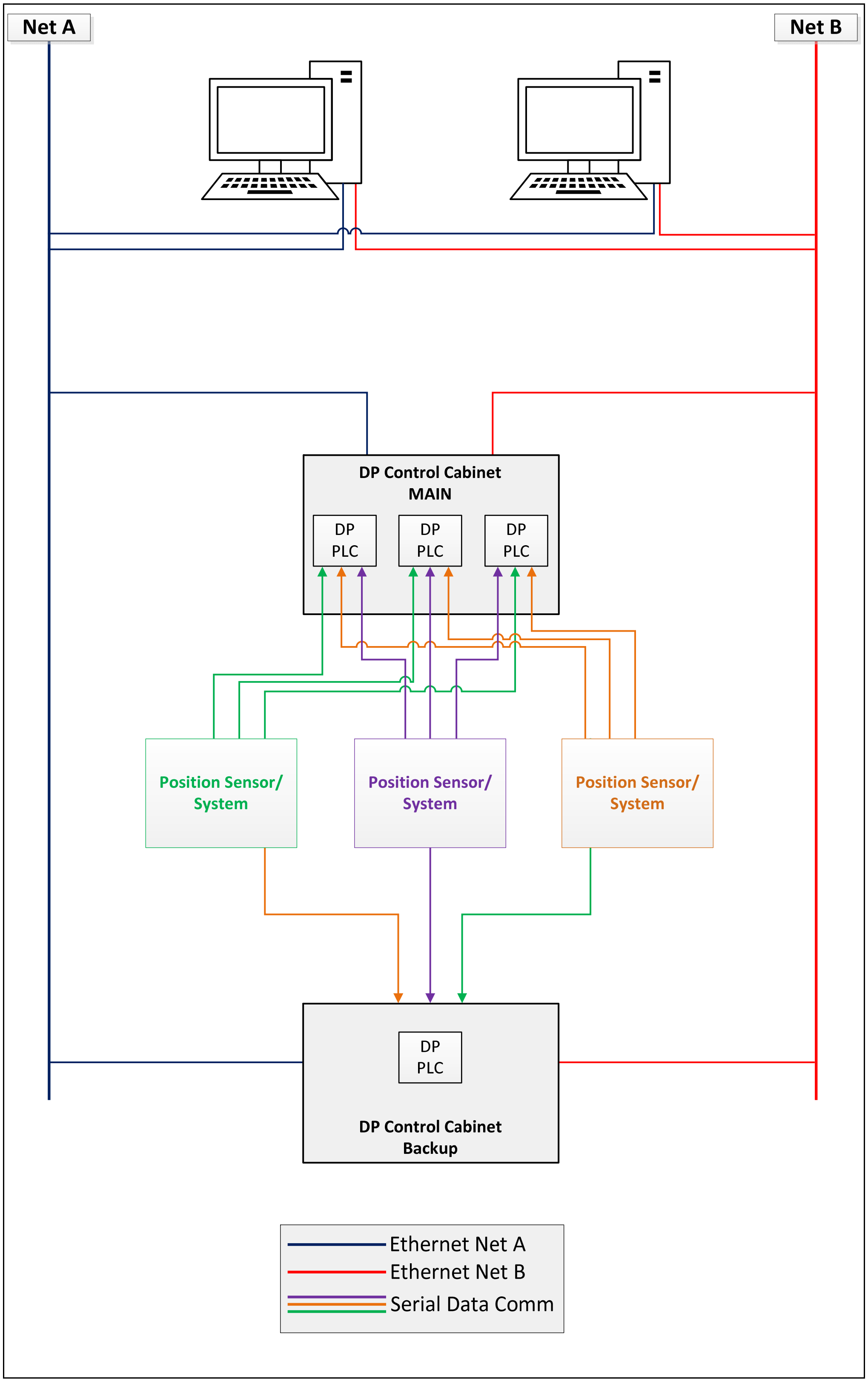


Figure - 5 **DP System (Position Reference) Serial Communication Topology**

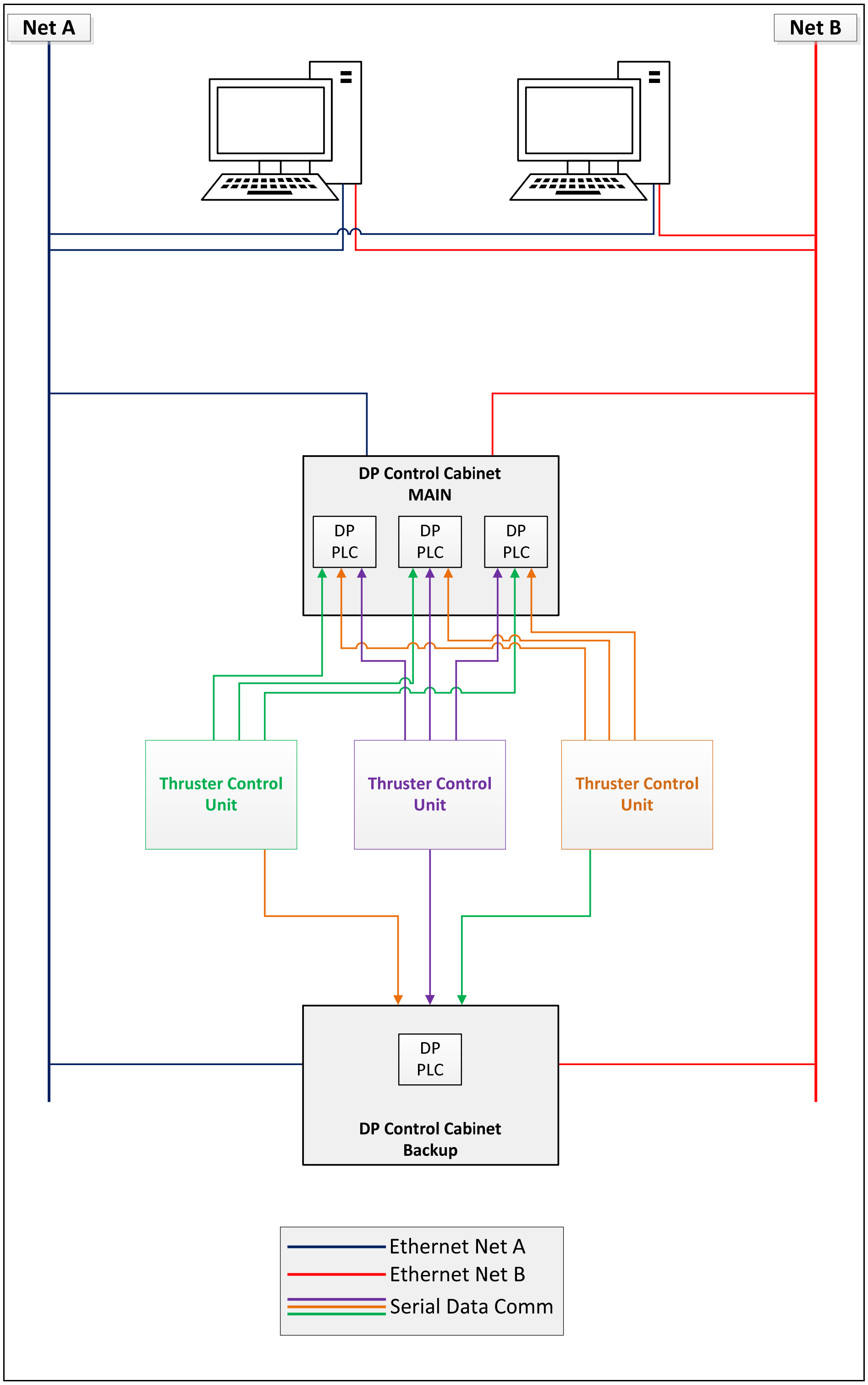


Figure - 6 DP System (Thrusters) Serial Communication Topology

Conclusion

From the above discussion, it can be concluded that the cyber security is developing challenge threatening the industry, which should be addressed proactively and properly.

Particular

Enhancing the DP Class rules to accompany the increasing cyber threat is only the starting point, then complemented by additional measures.

From experience, particular attention should be paid to address design and configuration aspects.

Acknowledgements

I would like to express my acknowledgement to DNVGL-ND DP Department who has supported the idea of this paper, during my work as part of the team.

I would also like to extend my acknowledgment to the operator (Transocean) and system manufacturer (Kongsberg and GE Converteam) for the efforts they have exerted to facilitate the available capacity to carry out the test.

References

(1) http://www.schneider-electric.co.uk/documents/solutions/process-automation/open-connectivity/Broadcast%20Storm%20Mitigation%20on%20Ethernet%20Networks.PDF

(2) https://www.dhs.gov/cyber-storm

(3) Sophos, Threatsaurus The A-Z of computer and data security threats, 2013, https://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf?la=en

(4) https://www.enisa.europa.eu/news/enisa-news/stuxnet-analysis

(5) European Network and Information Security Agency, ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR, November 2011