Dynamic
Positioning
Committee
Marine Technology Society

DYNAMIC POSITIONING CONFERENCE
October 11-12, 2016

CYBERSECURITY

Network Storms and Other Communication Systems Failure Modes

Ahmed Hamody
Independent

DYNAMIC POSITIONING CONFERENCE
October 11-12, 2016
Cybersecurity SESSION

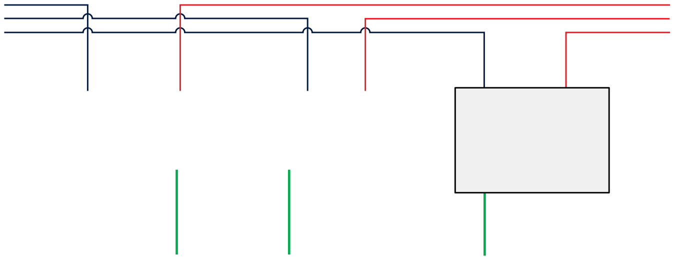
Network Storms and Other Communication System Failure Modes

By Ahmed Hamody
Independent

Agenda

- What is the architecture of DP Ethernet Network?
- What is the failure mode of Network storm (Cyber Storm) ?
- How serious the Network storm (Cyber Storm) is?
- What are the potential causes of Network Storm (Cyber Storm)?
- What is the effect of Network storm (Cyber Storm) ?
- How the network can be protected against Network Storm?
- How the Network should be tested?
- Serial Network Architecture, Failure Cause, Effect and Protection
- Conclusion – Q&A

What is the architecture of DP Ethernet Network?



What is the failure mode of Network storm (Cyber Storm) ?

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 both communication networks become unusable to exchange the important data for the system operation.

How serious is the Network storm (Cyber Storm) ?

- This issue is classified as network serious Cyber threat to any network
- The Department of Homeland Security (DHS) is carrying out a regular exercise (every two years) called exercise “Cyber Storm”.
- 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)

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

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

(3) Sophos, Threatsaurus The A-Z of computer and data security threats, 2013

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

What are the potential causes of Network Storm (Cyber Storm)?

The potential causes are:

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

Inherited design issue

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.

What is the effect of Network storm (Cyber Storm) ?

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 storm 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.

How the network can be protected 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.

Continued..

How the network can be protected against Network Storm?

- 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.

Continued..

How the network can be protected against Network Storm?

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.

How the Network should be tested?

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.

Continued..

How the Network should be tested?

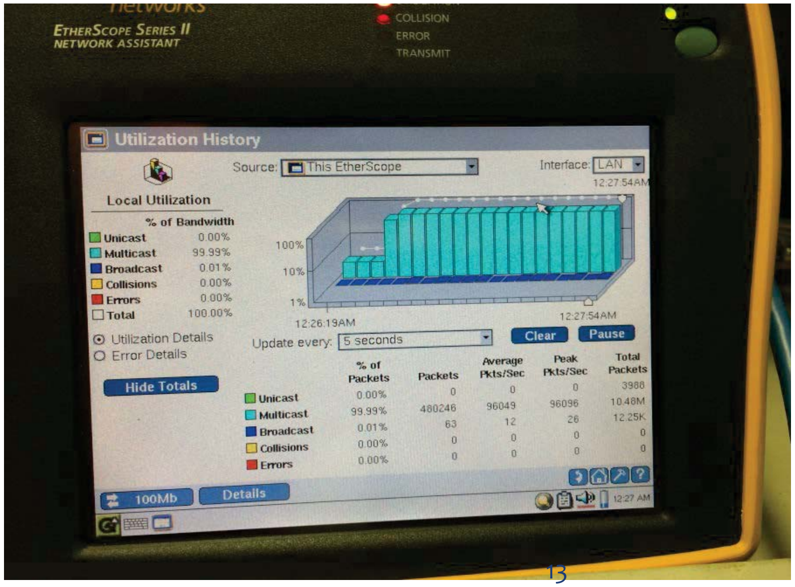
It is important to carry out the network storm on both networks at the same time. This might appear as two failures simultaneously, however, the root cause of such scenario is a single failure affecting one node with multiple effects.

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.

Continued..

How the Network should be tested?

Multicast Network storm



Utilization History

Source: This EtherScope

Interface: LAN

Local Utilization

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

● Utilization Details
○ Error Details

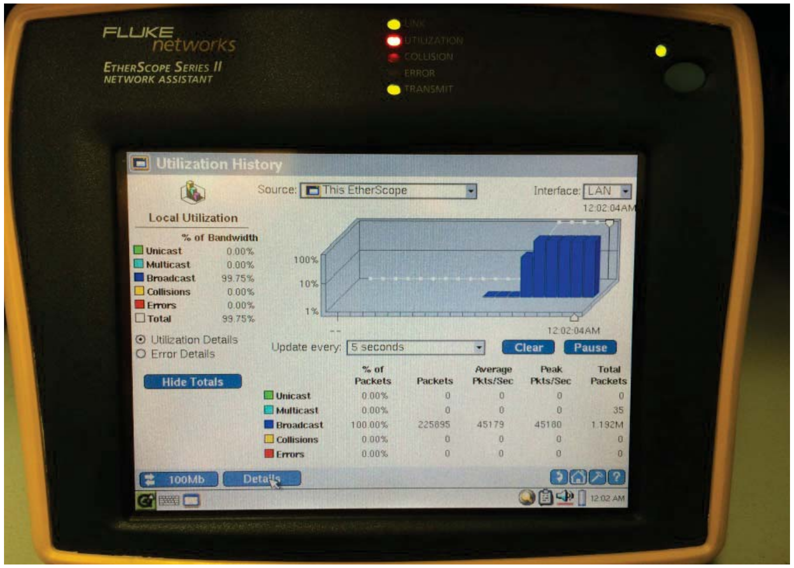
Update every: 5 seconds

	% 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

Continued..

How the Network should be tested?

Broadcast Network Storm



Utilization History

Source: This EtherScope

Interface: LAN

Local Utilization

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

● Utilization Details
○ Error Details

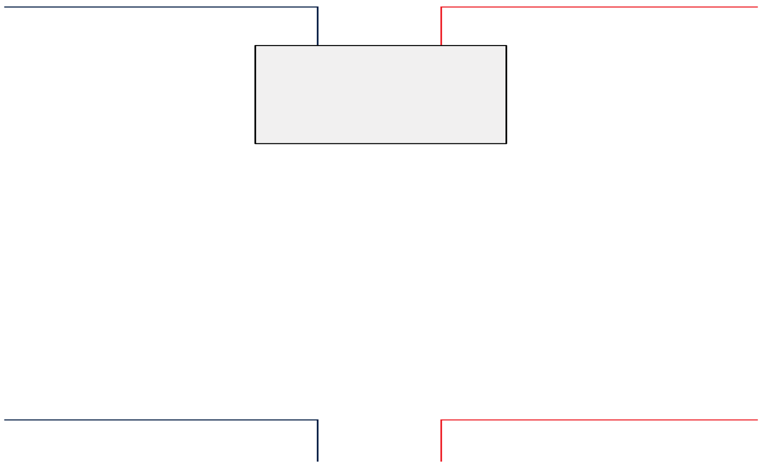
Update every: 5 seconds

	% 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

Continued..

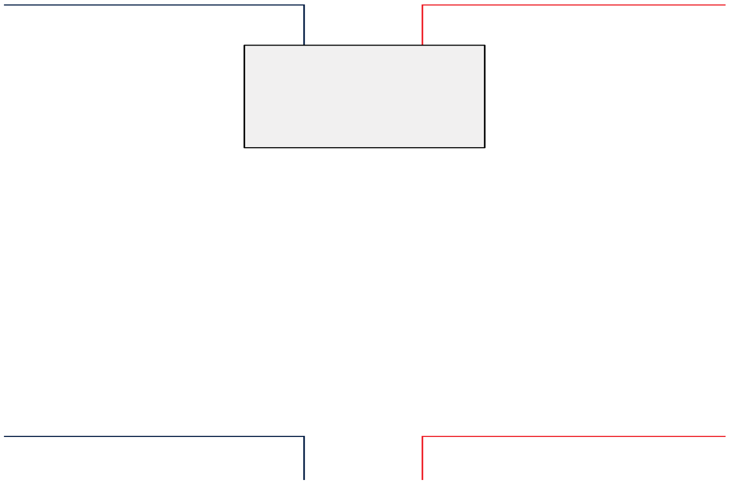
Serial Network Architecture, Failure Cause, Effect and Protection

DP Class rules require certain number of position reference systems and sensors feeding the DP Controller (DPC),



Serial Network Architecture, Failure Cause, Effect and Protection

In other cases, the serial communication lines are also used for communicating with thrusters control units for monitoring and controlling the thrusters.



Continued..

Serial Network Architecture, Failure Cause, Effect and Protection

- 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.

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.

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.

The issue is known, let us fix it rather than live with it.

Thanks for you attention

Q&A

Network Storms and Other Communication System Failure Modes

By Ahmed Hamody
Independent