Title: **Network Storms and Other Communication System Failure Modes**

Author: **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.