MPS
Malware Protection System

Malware Protection System form KONGSBERG is designed to protect all kinds of control systems. Malware can cause serious damage to and downtime for vessels, and updated malware protection is vital to ensure safe and efficient operations. With Malware Protection System, KONGSBERG has redefined control system malware protection.

Customer benefits

- No negative impact on critical control systems equipment
- No risk for false positives
- Always updated antivirus protection
- Improves overall system safety
- Reduces risk for system downtime

Key Functions

- USB protection, securing Operator Stations from external media threats. USB devices are scanned in the Malware Protection server unit. If the device is clean, an encrypted signature is written to the device, allowing it to access Operator Stations.

- MPS can operate in low-bandwidth / high latency environment. Malware signature files are downloaded to one server only, in a redundant or multi-server installation signature files will be distributed from the central server.
- Supports redundant setup
- Notifications when malware is detected. The system supports notification via SNMP, syslog, e-mail etc. allowing for both active and passive monitoring of malware notifications. Integration with Remote Diagnostic, MPS enables KONGSBERG to support closely if malware is detected.

- Portable scan engine enables always updated malware scanning and cleaning capability on Operator Stations and other windows computers (not restricted to KM computers)

Hardware

MPS can be installed on a variety of HW platforms. On larger installations the typical setup will be one or a redundant pair of net centric, high-performance network scanner(s) and several smaller touch-panel based USB scanners installed at strategic points on the vessel.
For smaller installations the easy mounted touch-panel model will be sufficient.

Applications

- Engine Room, protecting power management system
- Bridge, protecting DP and Navigation systems
- Control Room, protecting IAS and Safety systems
- IT Room, protecting vessel IT systems (e-mail etc.)
- Onshore Office, protecting vessel server networks
- Supports up to 10 Gb/s networks

- High availability solution: MPS high availability solution enables organizations to survive system or application failures with no discernible interruption to business-critical applications. MPS supports different levels of fail-over options for high-availability networks.
- Enhanced Security: Thousands of malicious files are using network protocols to get deeper into your network. With MPS, for the first time, you are able to prevent spreading on frequently used network protocols like RPC, Windows file sharing protocols in addition to the traditional internet protocols.

- Prevention: When the MPS appliance detects a malicious file in transfer on your network, it can actively terminate the file transfer and it blocks the specific network path to prevent other users or systems from accessing the same file.
- Transparency: MPS operates on Layer 2 in the network and is transparent to the IP traffic. No IP re-configuration of your network is needed, just add an address for the administration interface and MPS is instantly protecting your network.

- Backward compatible: Can easily be installed in existing systems. No need for any changes in the control system other than the installation of the USB driver.*

- Can protect any installation: Will provide protection even to stand-alone systems without network connectivity via the USB protection.*

USB driver can be installed on Windows XP SP2 and newer versions.

MPS Touch screen

MP8200 Desktop server

HP Proliant DL320 server

372299 / Rev. C / June 2013