Infinity® Acute Care System™ monitoring system

Workstation security in a networked architecture

Introduction
The benefits of networked medical devices for healthcare facilities are compelling. However, the use of such technologies can raise concerns about security and threats from malicious software. Dräger takes these concerns very seriously and has prepared this document to help network security managers, IT directors and users understand the fundamental security concept behind the Infinity® Acute Care System™.

At Dräger, we consider security to be a process rather than a product-based solution. This document describes how protecting a patient monitor differs from protecting a general purpose computer. It outlines measures that Dräger has in place to protect the system and offers recommendations to the healthcare facilities to further secure its network.

Infinity Acute Care System monitoring: a networked system
The Infinity Acute Care System monitoring system is an innovative two-screen solution that opens the door to a new dimension of mobility, adaptability and configurability. It enables you to monitor vital signs and therapy, control alarms, review Web-based diagnostic images, access patient records, and scale up functionality based on patient acuity level. By integrating vital signs data, clinical applications and the hospital network, the Infinity Acute Care System monitoring solution delivers comprehensive clinical information to the point of care.

Open systems vs. embedded systems
To understand the security concept behind the Infinity Acute Care System monitoring solution, it is important to clarify the differences between a general-purpose computer, such as an office laptop or any kind of personal computer, and a patient monitor. Although it has some general-purpose computer-like functionality, the Infinity Acute Care System monitoring solution is built to meet different requirements. Thus it has a different approach to these functionalities and holds different measures to protect the system.

The Infinity Acute Care System consists of a hand-held Infinity M540 vital signs monitor integrated with a Dräger Infinity Medical Cockpit™. The M540 is the vital signs engine that monitors the patient at the bedside and on transport; the Medical Cockpit displays monitored information together with networked clinical data at the bedside.
To illustrate this difference, a general-purpose computer can be described as an open system. It is designed to be flexible and provides open access to its operating system (OS) to accommodate frequent software installations and alterations to meet a wide range of end-user needs. General-purpose computers usually have a limited lifetime of just a few years.

In contrast, a patient monitor can be described as a closed or embedded system. A closed system, such as a patient monitor, is designed to perform a specific, dedicated function over its lifetime. Closed systems prohibit open access to the OS to accommodate frequent software installations and alterations. Patient monitors are expected to run continuously for years and are intended to recover by themselves if an error occurs.

The Infinity Acute Care System monitoring solution utilizes Microsoft® Windows XP embedded as its OS. This gives Dräger, as the designer and manufacturer of such embedded or closed systems, the opportunity to optimize the system towards its intended use to increase the reliability, performance and security of the system. To accomplish this goal, Dräger carefully selected the components used by the system and removed or disabled unneeded components to reduce the risk of illicit access or intrusion, as malicious software targets specific flaws in software or operating system code. Additionally, the Infinity Acute Care System monitoring solution is thoroughly tested in this original state. This state is preserved, or hardened, to achieve its original purpose at all times.

**Protection from malware**

Information integration and network connectivity offer significant benefits to the hospital – such as the ability to bring patient information to the point of care and remotely access vital signs information in near-real-time. However, the use of such technologies can raise concerns about security and the threats from malicious software. Feared by users and IT professionals alike, malicious software, nicknamed "malware," comes in a variety of forms.

Protecting the Infinity Acute Care System from malware is primarily the responsibility of the healthcare facility.

**IACS and antivirus software**

Antivirus software is often a standard requirement for networked devices in hospitals that may implement the Infinity Acute Care System monitoring solution. If updated regularly and maintained correctly, antivirus software packages counter most virus threats. However, antivirus software applications are reactive solutions. As such, they depend on timely updates of patterns or signatures in order to be effective against recently identified attacks. This means that zero-day attacks are not addressed. As a result, antivirus software is not effective. It provides a false sense of security and places an additional burden on management to track which devices may have out-of-date signatures or definitions.
While offering significant benefits for general purpose computers that are directly connected to the Internet, antivirus software is insufficient and has undesired side effects for embedded systems. Antivirus software was designed for an enterprise environment that has end users or administrative users in the security loop. Often, this isn’t a good process. A real-world example would be an airport parking self-service payment kiosk that is locked up with a security alert waiting for a confirmation from an end user – which isn’t possible because there are no input devices other than one button. In the medical environment, a more serious example would be antivirus software running on a medical device, popping up at inopportune times with security alert messages containing medically sensitive terms such as “virus”, “infection”, and “abort”. In cases such as this, antivirus software cures are sometimes worse than the disease.

A group of different measures have to be in place to mitigate the risk of malware intrusion since antivirus software is not suitable for embedded environments such as patient monitors. To this end, Dräger has designed a layered, in-depth defense strategy and implemented security measures that provide more complete protection to the Infinity Acute Care System monitoring solution and minimize the risk of potential vulnerability.

Maintaining System Priorities
First and foremost, the Infinity Acute Care System monitoring solution is a patient monitor. Measures have been implemented to ensure that priority is given to the actual vital-signs monitoring of the patient and prevent the vital-signs data from being preempted. As a result, malicious code introduced by a malware intruder would not be able to continue to execute code under privileged rights for an extended period of time. A computer hardware timing device called a “watchdog timer” triggers a system reset if the main program neglects to regularly service the watchdog due to some fault condition such as a hang up. The intention is to bring the system back from the hung state into normal operation by resetting the Medical Cockpit. The patient continues to be monitored by the Infinity M540 patient monitor and the patient’s vital signs will be visible on the device.

Firewall Security
Because the Infinity Acute Care System monitoring solution is a networked medical device, it uses a software firewall as a security mechanism for preventing intrusion and damage caused by network-based services. Firewalls only allow a defined set of services running on open ports to access the network. Instead of counting on virus scanners to defensively monitor and detect new viruses, the firewall can block unauthorized services and prevent the machine from being infected in the first place. The key to understanding the usefulness of firewalls as virus and intrusion prevention tools is that firewalls operate at multiple layers. Unlike antivirus software, which needs to be updated with new virus definitions, firewalls can prevent all access to unused services or protected internal IP addresses. Client-based firewalls protect an individual machine in the same way that a network firewall protects the entire network. A firewall protects the machine from
Unauthorized access by other compromised or malicious machines within the medical network.

Routing Between Network Cards
The Infinity Acute Care System monitoring solution participates as an active Transport Control Protocol/Internet Protocol (TCP/IP) member on the network. To prevent hospital network traffic from routing through the workstation to the monitoring Local Area Network (LAN), the Infinity Acute Care System monitoring solution has multiple network interface cards (NICs). Dräger disabled inter-NIC routing so that no traffic can traverse the two networks on the medical-grade workstation.

Running an Integrated Web Browser
The Web browser is a common system entry point for malware. Users download infected files and programs or access sites that may have ActiveX controls embedded with malicious code. To minimize the risks associated with the use of an integrated Web browser, Dräger has made several modifications and restrictions on the browser interface:

- All standard browser menus are removed to prevent the configuration restrictions from being modified by the user.
- The right-click functionality is removed. This functionality in the browser window typically provides access to changing browser properties and downloading of links/files and is a security risk.
- The navigation options are limited to a list of approved URLs that are entered through a password-protected service interface at the time of configuration.

Every site added through the password-protected Windows interface is considered a "trusted site." Trusted sites are given ability to download files and fonts, and download and run signed ActiveX controls, as well as unsigned ActiveX controls following a security prompt confirmation. However, there is still a risk that users may be able to navigate to an unsafe website through a link on a trusted site. Thus, customized restrictions are in place on non-trusted sites, including:

- Downloading and execution of unsigned and unsafe ActiveX controls are disabled.
- File download is disabled.
- Access to data sources across the domain is disabled.
- Privacy settings are configured to block “cookies” that use personally identifiable information without consent, as well as any third-party cookies that do not have a compact privacy policy.

In addition to physically restricting users by disabling functions, the healthcare facility should also educate its users and establish policies and procedures to help maintain a secure environment. However, access to the Internet should be severely restricted for all servers and bedside devices.
Enhanced Write Filter (EWF)

The main focus of the Infinity Acute Care System monitoring solution security strategy is on taking a proactive approach and creating a network and workstation environment that averts the intrusion of any malicious software. However, Dräger takes additional measures to protect the Infinity Acute Care System monitoring solution and its surrounding network in the unlikely event that malicious software intrudes into the system. Instead of relying on antivirus software, which is unsuitable for an embedded system, the Infinity Acute Care System monitoring solution utilizes the EWF component — which is typical for Microsoft Windows XP embedded systems — to protect the system from being unintentionally or maliciously overwritten during operation.

Very simply, EWF protects the system from undesired flash memory writes (flash memory is where the operating system and functional software components reside). It does this by sending the writes to another media or “overlay” as it is called, which could be either a partition on the RAM or the hard disk. In effect, the partition looks read-writable, but the original files are not touched or changed since the writes are sent elsewhere. The intercepted flash writes stored in the overlay are available as long as the system remains active, but will be lost when the system is rebooted or shut down.

In combination with the aforementioned watchdog, a reset of the Medical Cockpit is triggered if the primary processes are corrupted. The patient continues to be monitored by the Infinity M540 patient monitor and vital signs will be visible on the device. In the case of some fault condition, any malware that is temporarily on the overlay will be eradicated once the Cockpit reboots. Hence, EWF offers protection from viruses or any other kind of malware tampering with the protected partition of the system, thereby addressing concerns that the healthcare facility may have regarding networked medical devices.

Dräger recommendations

Securely design and manage the network infrastructure

The healthcare facility must play an active role as careful planning is the key for successfully protecting the network. Early involvement of all contributing parties allows designing a network that follows the IT security guideline of the individual healthcare facility and meets the requirements of the Infinity Acute Care System.

As discussed above, a general purpose computer requires different protection measures compared to the Infinity Acute Care System. To meet these requirements on a network level, Dräger recommends that the healthcare facility implement amongst others the following measures when integrating the Infinity Acute Care System monitoring solution into the hospital network:

- The hospital network should be segmented into different Virtual Local Area Networks (VLANs) to reflect different security requirements for different domains. Strictly define and implement a firewall policy for traffic flow between these VLANs. The goal is to control the traffic that goes between the Infinity Acute Care System
VLAN and other networked applications used by the staff, such as computers on wheels or Voice over IP telephones.

- Network managers should set up a complex, customized acceptable use policy (AUP). The AUP is a set of rules applied by the owner/manager of the network that restrict the ways in which the network site or system may be used to allow authorized network use and prevent all other access. For example, the AUP addresses issues such as personal use of the Internet and prohibits access to Internet sites that have inappropriate content. It may also limit guest access for patients and visitors to the Internet so that they have no access to the hospital’s network.
- For IT workstations, it should be clearly defined who is allowed to access the network and how. Passwords, tokens or other certificates for users are viable options for preventing unrestricted access and should be considered.
- A security gateway appliance is an additional measure that can be used to protect medical-grade workstations and the integrity of the hospital information system. These devices analyze network traffic up to the application layer and can detect application viruses such as email viruses or html attacks. A security appliance runs on its own hardware and as such does not interfere with the primary processes of the medical device. Furthermore, a single security appliance can provide consistent virus protection for multiple end devices and is easy to install and upgrade. This eliminates the need for multiple point products and can lower total cost of ownership.

None of these components on its own can fully protect a health care facility’s network. However, by adding comprehensive layers of protection, the healthcare facility can help ensure network and workstation security. In the rare case that all protection measures fail to prevent malware intrusion, well defined automated alarming and notification protocols can also help IT departments react faster and more efficiently if network system is affected.

**Conclusion**

To counter the serious security threats from malicious software, Dräger takes a multi-layer approach to providing workstation security for the Infinity Acute Care System monitoring system. This starts with a workstation that is designed with security in mind and includes the implementation of all measures that are appropriate for embedded monitoring systems. Specifically, we apply appropriate modifications and restrictions and utilize special security features that Microsoft Windows XP embedded offers. We also encourage the healthcare facility to play an active role to ensure the highest possible workstation security in a networked environment.

For more information, please contact your local Dräger representative.