# Best Practices for DanPac Express Cyber Security


This whitepaper describes best practices that will help you maintain a cyber-secure DanPac Express system.

## Table of Content



List of Figures

# 1. Introduction

Ensuring a Daniel DanPac Express system is secure from hacking attempts, viruses and other malware and security threats requires a set of best practices to be followed by everyone that interacts or has responsibility for the system. It is incumbent on the customer to determine and adhere to a security policy that best meets the needs of their specific situation.

For the purposes of this document, and in line with generally accepted terminology, “cyber-security” includes all non-physical threats to the network. This includes hacker penetration of the network, any deliberate or accidental access by an unauthorized user and the introduction of viruses, worms or other malware intended to disrupt the activities of the network or to access confidential information. To avoid unnecessary repetitions, the term “attack” will include virus, worms, malware, Trojans and other automated intrusion-enabling software, as well as manually directed attacks by persons outside the control network.

### 1.1 Defense-in-Depth

DanPac Express takes a holistic approach to security, implementing a series of layers designed to combat multiple security issues.

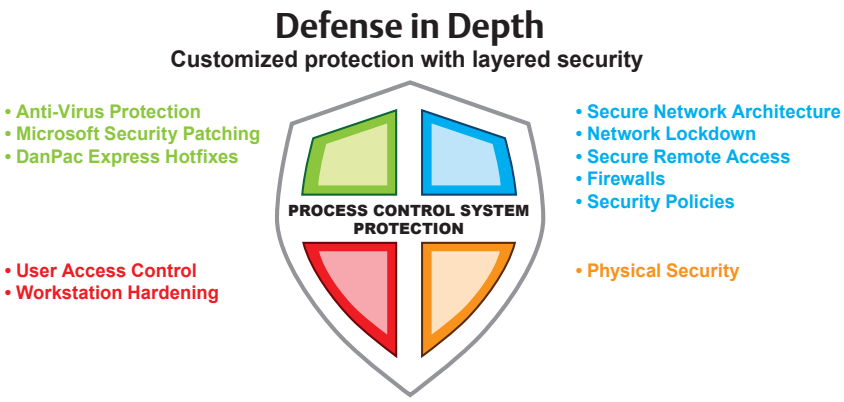


Figure 1 - Defense-in-Depth Security Strategy

It should be understood from the outset that an effective defense-in-depth strategy involves a degree of compromise on the activities performed on the system, that is, security must be balanced with usability and being fit for purpose. With this in mind, the security policy employed should document how risks are managed within the system, which threats are deemed acceptable, and which threats require mitigation.

Technology is only one tool that we can deploy in the bid to ensure security. Procedures and training also play a vital role in educating users about threats and the avoidance of those threats.

The use of this best practices document assumes that your organization has some level of security policy available to determine how and if each of these guidelines would be used in your facility.

## 2. Overall System Cyber-Security

The DanPac Express system security is based on three elements:

**Physical Access** – physical isolation of the metering control equipment in locked rooms or cabinets to prevent unauthorized access to equipment.

**User Access** – authentication and authorization, the correct implementation of user password security and role-based access to prevent unauthorized access on DanPac Express workstations within the plant and beyond.

**Network Isolation** – network isolation of the DanPac Express Metering Network from the plant LAN and any other LANs with “open access.”

## 3. System Design Practices

The DanPac Express system must be kept isolated from the plant LAN.

- All connections to the plant LAN must be made through a DanPac Express workstation.
- Network connections to the plant LAN should not be made unless absolutely necessary to run the metering, maintain the system, or for valid business reasons.
- Ensure that there are no other networks, modems or wireless connections designed into the network except for the necessary connections as previously discussed in the item above.
- Modems are not recommended. If they have to be used for remote technical support, they should be identified and made secure. They can be set to act in a call-back mode and require user password access at the modem interface once the call back is made. A manual procedure for unplugging the modem between uses is not recommended, as it leaves the system open to access if the user forgets to unplug the device.

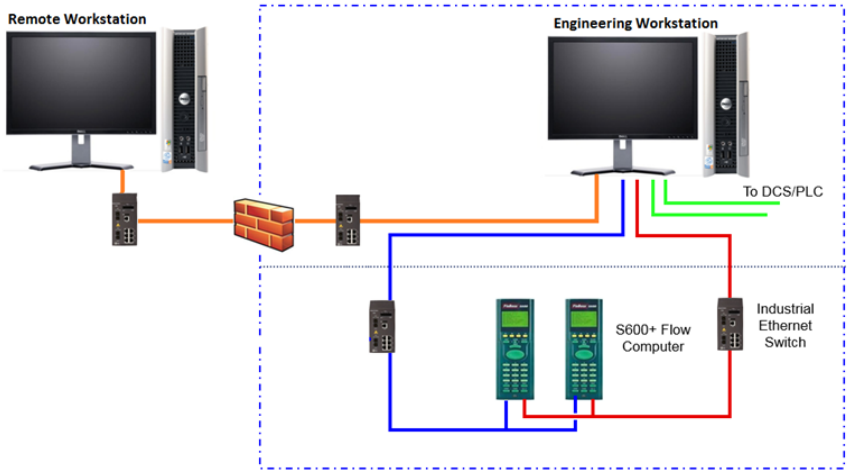


Figure 2 - System Design

## 4. System Configuration and Integration Practices

Organizations involved in the configuration and integration of a DanPac Express system have a responsibility to maintain a secure environment for the DanPac Express system. Viruses, worms and malware can attack a system from any network connection. It is possible to “stealth” install unwanted and undesirable software at any time. Maintaining a secure system is important even during system integration. This section of best practices is specific to managing a system while it is in the integration process, regardless of the location where actual tasks are being done.

When a PC is received from Dell® and prior to any external network connections being made, the following should be done:

- The latest supported security patches from Microsoft® should be installed.
- The latest supported anti-virus program and the latest anti-virus signature files should be installed.
- The anti-virus program and anti-virus signatures must be kept up-to-date at all times.

E-mail programs must never be run on any DanPac Express workstation or any computer directly connected to the DanPac Express LAN at any time.

During DanPac Express installation, all default user passwords should be changed to prevent unauthorized users from accessing the system. Only the personnel actually engineering the system should know the passwords for that specific system. Accounts should be set up consistent with the duties of each user. Administrator privileges should be reserved for only the very few

individuals who will be responsible for these tasks – in general, users who are performing engineering tasks.

The DanPac Express system should never be connected to any network unless it is properly protected with a correctly configured firewall. The firewall should specifically block any/all port 80 traffic (Internet) and any port that could be used for e-mail traffic. All ports should be blocked in both directions except for those needed for the applications on the DanPac Express network.

Each person doing configuration work on the DanPac Express system should have a unique account (user-specific name and password), enabling user activities to be properly controlled.

All user accounts not required for commissioning and startup should be deleted from the DanPac Express system before the system is shipped to the customer. After startup is complete, all non-customer accounts should be deleted. To ensure only authorized customer accounts remain on the system after implementation, the customer administrator should change the admin password and delete any vendor accounts.

At this time, if a vendor account is required, the user should set up this account, but it is strongly suggested that these accounts be given limited capabilities and disabled until actually needed. These vendor accounts should be enabled only for the time required for the vendor to provide the necessary service and then disabled again following service.

General business laptop or desktop computers should never be used as DanPac Express workstations, nor should they ever be connected into the DanPac Express system. Data should be moved between general purpose laptops and desktops by the use of USB thumb drives or CDs. All portable media must be scanned for viruses prior to insertion into a DanPac Express workstation.

If a virus-infected computer is discovered during integration, an anti-virus program may not completely remove the virus. Since other undetectable malicious programs may have also been installed, it is a best practice that computers that become infected should have the hard drive reformatted and the system completely reinstalled. This procedure is performed to ensure no traces of the infection remain and to remove any undetected malware.

The intention of these practices is to ensure that the customer receives the most cyber-protected, cyber-secure system possible.

# 5. DanPac Express Security Best Practices: Overview

Basic system security for a DanPac Express system is relatively easy to implement and monitor:

**Physical Security**

- Computers and network devices should be mounted in secure cabinets.
- Control and equipment rooms should be secure.
- Open, logged-on workstations should not be left unattended.

**Anti-Virus Security**

- Install and maintain anti-virus software.
- Disable access to any floppy and CD/DVD drives.
- Disable access to unused USB ports, especially those on the front panel (this may require physically disconnecting the ports within the computer).

**Password Security**

- Maintain user lists, adding required users only and deleting users that are no longer immediately required.
- Never share user names and passwords.
- Change all default passwords immediately upon system install.

**Network Security**

- All plant LAN connections to the DanPac Express system must be made through a workstation.
- Routers and firewalls should be used to isolate plant LAN connections.
- Any network ports that are not required by the metering system should be blocked.
- All users should have their own user name and password.
- User access must only be given to those who absolutely require it.
- Data users should be kept off the metering system through the use of data transfer mechanisms.
- Dual firewalls from different vendors can be used for optimum protection.

# 6. DanPac Express Security Details

### 6.1 Securing a Stand-Alone DanPac Express System

Even when a system is isolated and not connected to other communications systems, there are security risks that must be considered. Securing physical access and local user access to the system becomes the primary security action.

To maintain a secure environment for a stand-alone DanPac Express System, it is critical to:

- Disable access to email programs or web browsers.
- Maintain passwords.
- Disable CD and DVD drives.
- Disable USB ports.
- Secure CPUs in locked cabinets where possible.

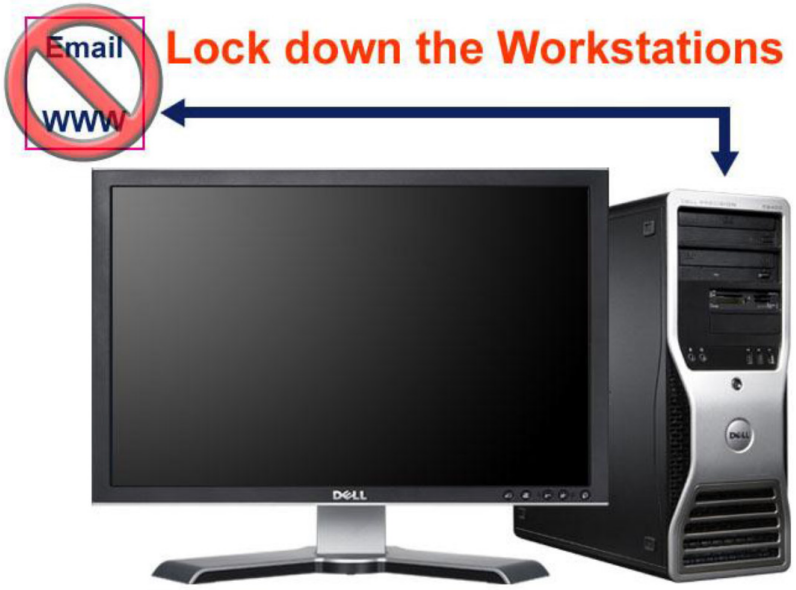


Figure 3 - Securing a Stand-Alone Workstation

The first-level and primary system security is based on limiting physical access to the DanPac Express workstations and network equipment. Access to the control room or local equipment rooms where workstations are available should also be controlled, especially in terms of access to the metering control system workstations.

Operators should always log off and not leave workstations with open access while a control room is unattended. Workstations should always be locked while they are unattended.

On remote located workstations, operating procedures should dictate that operators log out or lock consoles when not in use. At a minimum, consoles should be set up for the screen to automatically lock after a very short time of inactivity: no more than a two-minute delay is recommended.

Any computers or other smart devices connected to the DanPac Express network for maintenance purposes should have processes in place to ensure that the devices are certified free of virus and malware before they are connected.

In addition, authorization should be required for plant personnel and visitors to carry laptop computers or other portable devices with network connections (including Ethernet wireless access) into the process plant. Unauthorized access can be made and systems can be infected with malware from network connections made to non-secure portable equipment.

To aid plant personnel in identifying and reporting unauthorized devices, it is recommended that any authorized devices be painted a conspicuous color or labelled in some visible manner to ensure unauthorized equipment is easily identifiable.

To protect against connection of unauthorized wireless access points to the system, areas where network equipment is installed should be periodically scanned for wireless signals, using inexpensive wireless signal monitoring devices.

If laptops are used as DanPac Express workstations (laptops are not recommended nor are they supported by Emerson as part of a DanPac Express solution):

- They should be dedicated for metering control functions and never connected to an “open” LAN.
- To maintain system isolation, laptops that are also used as general purpose business computers (with Internet and email access) should never be used as DanPac Express workstations directly connected to the metering LAN.

## 7. User Access and Password Security

After physical access security, the next level of securing the DanPac Express system is to control user access via a password protection scheme. DanPac Express password access is multi-level and role based.

Passwords must be properly maintained to prevent unauthorized users from gaining access to the system. Steps to ensure the system is protected against unauthorized access include:

- Default passwords must be reset.
- Proper roles must be assigned to each user.
- User access must be carefully maintained.
- Users who no longer need access must be removed.
- Users without significant business reasons should not be given access.
- A system access and password policy should be in place and enforced.
- Generic or shared user names and passwords should not be used.

## 8. Virus Prevention and Detection

As a best practice, Emerson Process Management recommends that, at a minimum, anti-virus software be installed on any workstation connected to an outside LAN. For additional protection, anti-virus software should be installed on every workstation on the metering network. Once installed, it is essential that virus definition files be kept up to date, and there are a number of ways of ensuring the system is protected by the latest versions. Contact your local Emerson Process Management representative to discuss the options.

## 9. Approved Software for DanPac Express Workstations

Security can also be impacted by the installation of non-approved software on a DanPac Express workstation. Non-approved software in this case is any software that has not been approved to be installed on the workstations by the customer's DanPac Express system administrator.

## 10. Securing a Connected DanPac Express System

Once the user makes a network connection to an outside system, additional aspects of security must be considered. These security procedures are in addition to those mentioned above in the section "Securing a Stand-alone DanPac Express System."

All network connections between a DanPac Express system and a plant or other outside LAN must be made through a DanPac Express workstation protected by a router/firewall. Direct connections between an outside LAN and DanPac Express network hubs or switches are not permitted or supported. See the next section, "Protecting the Network Interface to a DanPac Express System" for details on this connection.

DanPac Express connections use specific ports for communications, and all other ports not used for DanPac Express applications should be closed or disabled to prevent connections through other open ports. In the event other ports are required for customer-installed software, then only those ports should be allowed to be open.

All connections to DanPac Express applications require some level of user authentication. Because only specific persons with permissions to connect will be allowed access to the system, the setup of the firewall/router should be made to allow only those specific individuals or computers to connect to the system. This setup can easily be tightened down to prevent unauthorized access because the DanPac Express connections should not be set up for general access.

Most companies or sites have some sort of password policy and, at a minimum, this should be followed for control system users as well. Emerson recommends a strong password policy be adopted to prevent easy cracking of passwords. Password changing should also follow corporate guidelines or be set up on a 90-day rotation. Default passwords should not be used and must be changed during implementation of the system.

It is important that the DanPac Express system administrator keep control of the user setup for DanPac Express users. They should know who and why a person is granted access. Access should be tightly controlled and users who no longer need access (such as contractors who are used only during initial implementation or employees who change responsibilities or leave the company) should be removed immediately.

Under no circumstances should a DanPac Express workstation run an e-mail application or make a general-purpose, open-use connection to the Internet.

## 11. Protecting the Network Interface to a DanPac Express System

At a minimum, the connection between a workstation node on a DanPac Express metering LAN and an external LAN (regardless of whether or not DanPac Express is installed on the node) must be protected by a router/ firewall device. The firewall should be set up as required to allow only specific users to access the system and to block access through any ports not specifically needed to support the DanPac Express connections to the outside LAN.

Maintaining access through a workstation creates an interface called a demilitarized zone (DMZ) which creates a buffer zone between the DanPac Express metering LAN and the external LAN. In this configuration, the workstation acts as a “neutral zone” between the control network and the plant network. It prevents plant users from getting direct access to the devices on the control network. Isolating the network from the plant LAN greatly reduces the opportunities for unauthorized access from outside the plant or from users of the plant LAN who should not be accessing the control network.

Note that when using a firewall, change management procedures to prevent unauthorized or improper changes that would compromise security of proper data flow should be developed and followed.

## 12. Data Access vs. System Access

Most remote users require only data access to view metering data or to help with process troubleshooting. It is not necessary to provide these users with access to the actual metering control system workstations because access to data is sufficient for their requirements.

Metering data access can be provided by a number of data hand-off mechanisms onto a data server. The DanPac Express system provides the metering data to these servers on a real-time or on an as-needed basis. This measure ensures plant LAN users who only need data access never connect to a node on the control system.

## 13. Summary

Performing a system risk assessment and then implementing the appropriate security practices outlined in this whitepaper will allow the user to provide adequate and cost-effective security for the DanPac Express metering control system.

**Emerson Process Management**

Daniel Measurement and Control, Inc.
North America / Latin America:
Headquarters
USA - Houston, Texas
T +1.713.467.6000
USA Toll Free 1.888.FLOW.001

Europe: Stirling, Scotland, UK
T +44.1786.433400
Middle East, Africa: Dubai, UAE
T +971.4.811.8100
Asia Pacific: Singapore
T +65.6777.8211

**www.Daniel.com**

Scan with your smart phone for more information



DANIEL™

EMERSON.
Process Management