OPW Fuel Management Systems, Inc.

Payment Application Data Security Standards (PA-DSS) Implementation Guide for Maintaining PCI Compliance on the FSC3000 Fuel Site Controller

PA-DSS Compliance Version 3.2
Multi-Trucking Network Package
Card Record Feature Version: 1.20j

OPW Part #: S030001

Table of Contents

1 Application 5
2 Overview 5
3 Document Use 5
3.1 PA-DSS vs. PCI DSS Compliance 6
4 Product Certification Status 6
5 Acronyms & Terms 7
6 PCI DSS and PA-DSS Reference 7
7 Implementation of PA-DSS 8
7.1 Introduction 8
1. Do not retain full magnetic stripe, card validation codes or PIN block data. 8
2. Protect stored cardholder data. 8
3. Provide secure password features. 9
4. Using two-factor authentication 9
5. Log application activity 9
6. Develop secure applications. 10
7. Protect wireless transmissions. 10
8. Test applications to address vulnerabilities. 11
9. Facilitate secure network implementation. 11
10. Cardholder data must never be stored on a server connected to the Internet. 12
11. Facilitate secure remote software updates. 12
12. Facilitate secure remote access to application. 12
13. Encrypt sensitive traffic/data over public networks. 12
14. Encrypt all non-console administrative access. 13
15. Maintain instructional & training materials for customers, resellers and integrators. 13
16. Services, protocols, components and dependencies. 13
8 Merchant's Requirements for Maintaining PCI Compliance 14
8.1 Creating and Maintaining Users 14
8.2 User Logon and Passwords 14
8.3 Third-Party Application Interfaces / Remote Access 14
8.4 OPW Device Connections 14
8.4.1 External USB Journal Key 15
8.4.2 Remote Access via Dial-in Modem 15
8.5 System Logging and Maintenance 15
8.5.1 Automatic Print and Clear of Log Data 15
8.5.2 Manual Capture of Log Data 15
8.5.3 Retention of Log Data 16
8.6 Returning System for Warranty or Repair 17
8.7 Creating a Compliant Environment when Upgrading an Existing FSC3000 17
8.7.1 FSC Installed Before Aug 1, 2008, and Does NOT Use the Ethernet Port for Remote Access 17
8.7.2 FSC Installed Before Aug 1, 2008, and USES the Ethernet Port for Remote Access 17
8.7.3 FSC Installed After Aug 1, 2008, and USES (or will use) Ethernet Port for Remote Access 18
9 FSC3000 System Installation 20
9.1 Setup 20
9.1.1 Card Processing 20
9.1.2 "System Start" command 20
9.1.3 Privileged vs. Partial Access 20
9.2 Users 20
9.2.1 "Set Admin" command 21
9.2.2 User Options 21
9.2.3 Passwords 21

9.2.4 Login Command and Administrator Access 21
9.2.5 Remote access login via Ethernet port 22
9.3 System Activation 22
9.4 Recommended Startup/Installation Process 22

1 Application

This document supports the OPW Fuel Management System's Petro Vend Fuel Controls FSC3000 Fuel Site Controller running Multi-Trucking Network Package with:

- PA-DSS Compliance Version: 3.2
- Card Record Feature Version: 1.20f (1.20e or higher, regardless of system configuration).

See Appendix D for information regarding changes and new features.

Note: Some configurations should not be used when Bankcard Payment Processing is in use. These configurations are mentioned and discussed within this document.

2 Overview

OPW Fuel Management Systems has redesigned setup/configuration control, user and data access on the FSC3000 platform, in order to provide you a PCI PA-DSS (Payment Application Data Security Standard) system that can be installed in a compliant manner. We have re-certified the Multi-Trucking application to PA-DSS 3.2 to offer a product that continues to operate in accordance with PCI PA-DSS guidelines. These guidelines are designed to assist software developers and application/equipment providers in deploying secure software platforms that provide merchants the control to comply with PCI DSS standards. With the proper use, setup and maintenance of the FSC3000 as described within this document, OPW is working to help you provide a secure environment for the processing and safety of your customer's bankcard information and privacy.

The FSC3000 is designed to be flexible and support the vast range of features requested by our customers. OPW has attempted to incorporate the required changes without directly affecting the daily operations of those customers not processing bankcards and therefore not required to comply with the requirements. However some of the procedures and control normally used to support the system have been changed. Therefore, whether you process bankcards or not, please take the time to read this document for a clear understanding of the changes employed and the steps you must follow to operate and work with the redesigned Multi-Trucking Network Package.

3 Document Use

This PA-DSS Implementation Guide contains information for proper use of the Multi-Trucking network application. OPW Fuel Management Systems does not possess the authority to state that a merchant may be deemed "PCI Compliant" if information contained within this document is followed. Each merchant is responsible for creating a PCI-compliant environment. The purpose of this guide is to provide the information needed during installation and operation of the Multi-Trucking application in a manner that will support a merchant's PCI PA-DSS compliance efforts.

Notes: Both the System Installer and the Controlling Merchant must read this document.

3.1 PA-DSS vs. PCI DSS Compliance

As an equipment vendor, our responsibility is to develop a software application to be PA-DSS Compliant. This applies to all software vendors who develop payment applications that store, process or transmits cardholder data as part of authorization or settlement. The software application itself is subject to an independent third-party audit that generates a certification report, which is then certified by the PCI Security Council. We have performed an audit and certification compliance review with an independent auditing firm to ensure our application/equipment conforms to industry best practices when handling, managing and storing payment-related information.

PCI DSS Compliance ultimately falls on you, the merchant. It's your responsibility to work with your hosting provider, use PCI-compliant server architecture with proper hardware and software configurations and access-control procedures.

Following the procedures and steps defined within this document will help you on your way to incorporate PCI DSS Compliance. It is up to you as the merchant to continue to implement and live by the rules defined to ensure you meet the requirements defined by the Payment Card Industry (PCI) Data Security Standards (DSS). The security requirements defined in the DSS apply to all members, merchants and service providers that store, process or transmit cardholder data. These requirements also apply to all system components within the payment-application environment, which is defined as any network device or application included in or connected to a network segment where cardholder data is stored, processed or transmitted.

4 Product Certification Status

The FSC3000 Multi-Trucking Network Package was evaluated by:
PSC (Payments: Security: Compliance) San Jose, CA, an independent auditing corporation.

Validated PA-DSS v1.2 compliant by the PCI Security Standards Council, Dec. 2008
Original Reference #: 09-05.00508.001
Revalidated: Jan 7, 2010 (ref#: 09-05.00508.001.aaa)
Revalidated: Jan. 2012 (ref #: 09-05.00508.001.baa) (version: 1.10c)
Revalidated: March 2013 (ref #: 09-05.00508.001.caa) (version: 1.13h)

Revalidated: PA-DSS v2.0 compliant by the PCI Security Standards Council, Nov. 2013
Reference #: 13-11.00508.002 (version 1.14b)

Revalidated: PA-DSS v2.0 compliant by the PCI Security Standards Council, Jan. 2014
Reference #: 12-11.00508.002.aaa (version 1.15b)

Revalidated: PA-DSS v3.1 compliant by the PCI Security Standards Council, Mar, 2016
Reference #: 16-11.00508.004 (version 1.17a)

Revalidated: PA-DSS v3.2 compliant by the PCI Security Standards Council, Apr, 2018
Reference #: 17-11.00508.006.aaa (version 1.19b)

Revalidated: PA-DSS v3.2 compliant by the PCI Security Standards Council, Jun, 2019
Reference #: 17-11.00508.007.aaa (version 1.20e)

Revalidated: PA-DSS v3.2 compliant by the PCI Security Standards Council, Jun, 2020
Reference #: 17-11.00508.007.aaa-cs (version 1.20i)

5 Acronyms & Terms

The follow is a list of acronyms and terms used within this document:

PA-DSS: (Payment Application Data Security Standard)

OPW: OPW Fuel Management Systems

FSC: FSC3000 Fuel Site Controller (and the Multi-Trucking software operating within).

Distributor: The equipment reseller and integrator. A qualified individual certified by OPW for the installation of the FSC3000.

Merchant: The owner/operator of the fueling location at which the FSC is installed.

User: A (case sensitive) name that has been added to the FSC, by the merchant, to allow system logon access. Users have full command line access of the system, except for network setup that is now Admin control only.

We: Throughout the sections below the term “We” is used. This term always refers to the OPW development team that created and designed the software application.

PAN: Personal Account Number (number embossed on bankcard)

SIMM: Single In-line Memory Module. The memory card inside the FSC3000 used to store the payment application and transaction information.

6 PCI DSS and PA-DSS Reference

As the merchant (and/or the equipment reseller/integrator), you should download the “Payment Card Industry, Data Security Standard: Requirements and Security Assessment Procedures” to further understand your requirements for implementing and maintaining a compliant environment under which to operate.

To learn more about PCI compliance standards visit: https://www.pcisecuritystandards.org/

7 Implementation of PA-DSS

7.1 Introduction

The OPW Fuel Management Systems FSC3000 Multi-Trucking application has been developed and tested according to the PCI PA-DSS documentation. This section covers the different sections of these documents and the actions OPW has taken to implement the requirements of each.

1. **Do not retain full magnetic stripe, card validation codes or PIN block data.**

   It is the responsibility of the application developer to ensure prohibited magnetic-stripe data is not stored or retained anywhere within the system. This implementation is designed to meet the requirements of PA-DSS from 1.1 through 1.1.5 which in turn meets your requirements of PCI DSS 3.2 through 3.2.3 where:

   - 3.2 - States sensitive authentication data should not be stored after authorization.
   - 3.2.1 – Do not store full contents of any track/magnetic-stripe data.
   - 3.2.2 – Do not store card-verification code or the 3- or 4-digit number printed on the front or back of a payment card.
   - 3.2.3 – Do not store the Personal Identification Number (PIN).

   We developed the FSC to retain magnetic-stripe data in active memory until the authorization process for fueling is complete. At that time, the memory locations used to retain that data are wiped and ready for the next card presented.

   Note: Currently the FSC does not prompt for card validation or PIN block data. No sensitive authentication data is written to transaction storage memory.

2. **Protect stored cardholder data.**

   It is the responsibility of the application developer to mask any displayed cardholder data. Storing none of the cardholder's sensitive data, including the PAN, supports this requirement. Being an embedded system, the storage of transaction data and cardholder information is not stored in a typical database but within formatted battery-backed non-volatile memory. Although this memory is not even accessible from within the system, we have chosen to support this requirement in the following manner: Upon completion of capturing the final sales data with the network host, we wipe the cardholder's expiration data from the transaction record and clear the account number portion of the PAN, except for the six-digit ISO and the last four digits. Under this process the full PAN is not even available for the Administrator to reference. This implementation allows us to comply with PCI-DSS requirements 3.3 through 3.6, which state:

   - 3.3 – Mask PAN when displayed (we only show last 4 or first 6 and last 4 digits).
   - 3.4 – Render PAN unreadable anywhere it is stored/displayed (we wipe Account portion of PAN).
   - 3.5 and 3.6 – Protect cryptographic keys and document key management (by wiping Account portion of PAN we don't use encryption to protect data).

   PCI-DSS requirement 3.1 states that cardholder data be purged after a customer-defined retention period. Based on how memory is used within the FSC, previous cardholder is purged (overwritten) each time the transaction buffer is cleared and new cards are used in the system. To ensure this process occurs in a timely manner to meet the defined retention period, the transaction buffer size should be defined to ensure that it is either cleared regularly or automatically overwritten by enabling the transaction buffer auto-wrap feature. .

   Cardholder Data, Sensitive Authentication Data or the cards PAN itself is never made available for viewing from anywhere within the FSC. Track1 is never retained and Track2 data is cleared from memory after the card authorization process is complete. As described, once the final sale is

captured to the host, the first 6-digits of the PAN is only made available to users configured for that right under the Admin setup. Based on this control, except for Users configured to see the first 6-digits of PAN, Cardholder Data is never presented by the FSC either through terminal access, printing of receipts, journal printer based reports or external FSC polling processes.

Note: see section 9.2.2 for information on how the Admin can define a user to see the first 6-digits of PAN.

3. Provide secure password features.

It is the responsibility of the application developer to ensure unique user names and complex passwords for all administrative access and access to cardholder data. We control this requirement by ensuring default factory passwords are changed before installation is complete. Due to the nature of our system and the process required to install and configure the FSC, we have designed the system to be shipped with no defined users and an inactive administrator login. Once installed and configured the administrator login (entered as: "Admin") must be activated and a password created. The factory default passwords used to access the system (even at its lowest level) must also be changed.

We recommend the following when creating users and passwords, and accessing the system:

- As stated above, forcing you to change all factory-default passwords, creating an administrator password and defining users with case-sensitive names helps us control PCI DSS requirement 8.1 and 8.2.
- For further protection of the administrator password we suggest:
  - Don't use the "Admin" login as the normal way of accessing the FSC, create regular user login for day to day use.
  - Consider creating an "Admin" password with of password length of no less than 10 characters (the longer the better) and then not using it to access the FSC except for network setup and the management of users and passwords.
- Create and maintain PCI DSS-compliant authentication access by following PCI DSS requirements 8.5.8 through 8.5.15. We have helped here by strictly enforcing requirements: 8.5.10, 8.5.11, 8.5.13, 8.5.14 and 8.5.15.

Important: Attempting to change or manipulate "out of the box" payment software installation settings that control limits, lengths or criteria of how user names and secure authentication (passwords) are accepted will result in non-compliance with PCI DSS.

4. Using two-factor authentication

PA-DSS 10.1 requires payment applications installed in an environment with remote access that it must not interfere with use of two-factor authentication technologies designed for secure remote access. The FSC3000 does not inhibit the use a two-factor authentication allowing you to meet PCI DSS standards. Two-factor authentication requires that two of three authentication methods *(see PCI DSS Requirement 8.2)* must be used for authentication. *Note: using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.* See PCI DSS requirement 8.3 for additional information.

For more information about users and passwords see: "Merchant's Requirements for Maintaining PCI Compliance" and "FSC3000 System Installation" sections below.

See Appendix C for installation diagrams in support of this requirement.

5. Log application activity

It is the responsibility of the application developer to log all user access to cardholder data. As described in topics 1 and 2 above cardholder data is not saved and therefore user access to

cardholder-sensitive data is not possible. In an effort to conform to this requirement we chose to create a logging mechanism that not only records which users view transaction information, but any changes to system access and configuration. This logged data is stored on the system in flash on FSC3000 SIMM so data is retained even if a system Cold Start is performed. Under terminal/console access only the Administrator can clear log data.

We have developed the log to meet the PCI DSS requirements defined in sections 10.1 through 10.2.7. In addition, the information logging meets the requirements defined in sections 10.3.1 through 10.3.6 by logging: username, action taken, date and time and the access point used.
For more information about managing the system log information see: "Merchant's requirements for maintaining PCI compliance" section below.

Important: Disabling the system log process in any way will result in non-compliance with PCI-DSS.

6. Develop secure applications.

It is the responsibility of OPW and all of its designers to provide a product and payment application that is developed in accordance to PCI DSS requirements. These requirements are specific to the design, control and production and testing of the product and its software. They require us to: maintain software and hardware revision control; develop applications based on industry best practices and incorporate information security throughout the development life cycle; perform application code reviews and walkthroughs to identify vulnerabilities; use separate development and test environments with the separation of responsibilities; not ship applications with test accounts for debugging information used during development and testing; provide secure update and back-out procedures; and PCI-specific testing to ensure approved implementations are maintained as updates and new releases occur.

The FSC300 Multi-Trucking network application has been developed in accordance with these procedures and we have put in place specific controls to ensure these practices are maintained for future development. These procedures and policies ensure our application meets the PCI DSS standards described is sections: 6.2, 6.4 and 6.5.

7. Protect wireless transmissions.

It is the responsibility of the implementer and Merchant to ensure that any wireless connections provided as part of the interface to the payment environment are secured according to PCI DSS requirements. The FSC3000 under normal installation conditions does not use any wireless connections as part of the interface that transmits cardholder-sensitive data. However, if it is installed within or connected to a wireless network the following rules must be followed to maintain PA-DSS requirements as defined under PA-DSS 6.1 and 6.2:

- Encryption keys must be changed from default at installation.
- Encryption keys must be changed any time anyone with knowledge of the keys:
  - Leaves the company
  - Changes positions
- Default SNMP community strings on wireless devices must be changed.
- Default passwords/passphrases on access points must be changed.
- Firmware on wireless devices must be updated to support strong encryption for:
  - Authentication
  - Transmission
- Other security-related wireless vendor defaults must be changed.
- A firewall must be installed between any wireless networks and systems that store cardholder data.

- Firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

The Merchant (including Distributor Technicians) MUST not install wireless Petro-Net modems between the FSC and Terminal Card Readers (such as the C/OPT or FIT500). Doing so would violate PCI DSS requirements and make your system non-compliant!

In addition, the Merchant should not use/install any wireless devices connected to the FSC. If you as the Merchant install a wireless device it is your responsibility to ensure the wireless connection is not available for access outside of a secure firewall. If you must use wireless technology connected to the FSC, you must ensure it is implemented in accordance with the following PCI Data Security Standards:

- 1.2.3 – Install perimeter firewalls between any wireless networks and the cardholder data environment.
- 2.1.1 – For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults such as keys and passwords.
- 4.1.1 – Ensure wireless networks transmitting cardholder data use industry best practices (for example: IEEE 802.11i) to implement strong encryption for authentication and transmission. *As of June 30, 2010 it is prohibited to use **WEP** as a security control***.**

Important: OPW accepts no responsibility for the installation of a wireless device for the purpose of remote access to the FSC. Failing to install payment applications in wireless environments according to PCI DSS requirements 1.2.3, 2.1.1 and 4.1.1 will result in non-compliance with PCIDSS.

Important: The Multi-Trucking Network Package supports the use of an internal wireless modem (WiFi). This modem provides configuration of several different security control encryption algorithms and the configuration clearly indicates which security controls are acceptable for use, under PCI-DSS 4.1.1. When a network approved for the processing of bankcards is enabled, it is the responsibility of merchant or installing distributor technician to ensure that only PCI-DSS allowed encryption is enabled for use. As indicated above, it is prohibited to use WEP as a security control.

***Note:** WPA2 encryption must be used when bankcard enabled networks are activated!*

8. Test applications to address vulnerabilities.

It is the responsibility of the application developer to ensure that payment applications are tested for security vulnerabilities according to PA-DSS requirements 6.2, while ensuring updates and patches are delivered in a secure manner. OPW performs internal regression testing before every software release to ensure PA-DSS requirements are always maintained within the system. Updates to the payment application are only available to Certified Trained Distributor Technicians via a secure login at OPW Fuel Management Systems Technician-only Web page or directly from the OPW Technical Support Group.

See Appendix B for information on how to confirm validity of software update after installing.

9. Facilitate secure network implementation.

It is the responsibility of the application developer to ensure remote access is performed securely and to ensure non-console access uses strong encryption and does not interfere with a secure network environment. All access points to the FSC, including its TCP/IP Ethernet port, interact and limit access to a terminal console interface. When making remote access connections using the FSC TCP/IP port, the FSC must be on a private LAN behind a secure firewall. You Must Not Connect the FSC to an open Internet connection. To further protect the FSC when connected to a

network via the TCP/IP port, Administrator access is not allowed. The administrator MUST always login via the direct connect terminal port or by using the dial-in modem.

When installing the FSC in a network environment it is your responsibility as the merchant to review and strictly follow PCI DSS requirements:

- 1.1 through 1.4 that relate to the installation and maintenance of a network firewall.
- 4.1 and 4.2 we help you conform to these requirements by never sending or displaying sensitive cardholder data out any FSC access point.

See Appendix C for installation diagrams in support of this requirement.

10. Cardholder data must never be stored on a server connected to the Internet.

Although the FSC never transmits cardholder-sensitive data outside of the controller, it is the merchant's responsibility to ensure that whatever server (or PC) is used to poll transaction data is not directly connected or exposed to the Internet.

Refer to PCI DSS requirement 1.3.2 for more information on limiting access to the DMZ.

11. Facilitate secure remote software updates.

It is the responsibility of OPW to provide secure software update procedures under PCI DSS. As described in number 8 above updates are available from a secure distributors' section of our Web site. Only certified OPW Distributor Technicians or OPW Technical Service Group technicians should perform software updates to the FSC. To further ensure secure updates, OPW recommends that application updates only be performed using the direct-connect serial port or the dial-in modem interface.

For more information regarding secure remote updates, refer to the PCI DSS requirement 1 for information about installing and maintaining firewall configuration to protect data along with section 12.3.9 for activation of remote access for vendors only when needed.

Refer to "FSC3000 System Installation" below for more information about creating a "Time Limited Login" for Vendor and Distributor access.

See Appendix B for information on how to confirm validity of software update after installing.

12. Facilitate secure remote access to application.

All remote access points to the FSC, whether from a modem or the Ethernet port, interact as a terminal console interface connection requiring a "Remote Connect" password and then a "Partial Access" password. Under this connection a minimal command set is allowed providing the ability to poll transaction data (containing NO bankcard or cardholder-sensitive data) and manage the internal proprietary card file. Without entering an additional login sequence (requiring a case-sensitive username and password) further access rights are not available (See: "Merchant's requirements for maintaining PCI compliance" and "FSC3000 System Installation" sections for more information about user names and passwords).

It is recommended that a dial-in modem be physically connected to a phone line only when the need for remote access is required for the purpose of polling or system management.

Important: For additional information on how to facilitate secure remote access, you must reference PCI DSS requirements 8.1 through 8.4 and 8.5.8 through 8.5.15.

See Appendix C for installation diagrams in support of this requirement.

13. Encrypt sensitive traffic/data over public networks.

Because the FSC does not retain any sensitive bankcard or cardholder data, it cannot transmit this information over a public network. The only cardholder data ever transmitted from the FSC is the

6-digit ISO (user specific) and the last 4 digits of the PAN. To further ensure the protection of sensitive data it is the merchant's responsibility to ensure the FSC is never connected to a public network (For more information regarding the transmission of the 6-digit ISO numbers refer to the "Users Options" information under the "FSC3000 System Installation" section of this guide).

Refer to PCI DSS requirements 4.1 and 4.2 for additional information regarding the encryption of transmissions across open public networks.

14. **Encrypt all non-console administrative access.**

    Although the FSC allows remote access via the Ethernet port, the interface provided under this connection type is designed to operate as a terminal console interface. However, in order to maintain PCI compliance in regards to this topic and PCI DSS requirement 2.3, administrator access is not allowed using the Ethernet port. (See: "FSC3000 System Installation" section for more information about using ether-net port for remote access).

15. **Maintain instructional & training materials for customers, resellers and integrators.**

    This Implementation Guide is designed to provide you with the instructional documentation required for maintaining a PCI-compliant environment using the FSC3000. Our resellers/distributors are trained in the installation and implementation of the FSC3000 and provided PCI compliance information in the form of this guide.

    As the merchant you should question your distributor to determine if they have been trained by OPW and explained the requirements defined within the guide, before allowing them to install the FSC3000 in your facility.

16. **Services, protocols, components and dependencies.**

    Being an embedded self-contained system with a proprietary operating system, there are no services, protocols or other components running within the system. This aligns with PCI DSS requirement 2.2.2.

8 Merchant's Requirements for Maintaining PCI Compliance

This section describes the steps and responsibilities required by the merchant in order to maintain PCI compliance with the FSC3000.

8.1 Creating and Maintaining Users

Users and unique passwords should be created before the FSC is activated for use. For more information on creating users, see the "FSC3000 System Installation" section below.

Up to 5 users with case-sensitive names can be defined for access to the system. You should not allow more than one user to access the system with the same username and password (usually referred to as group access). User names should always be deleted from the system if that person leaves your company or changes to a position that does not require access to the FSC.

Note: User names on the FSC are a maximum length of 10 characters. Because user names are case-sensitive, creating them with a combination of caps and lower-case characters adds another level of login security.

8.2 User Logon and Passwords

Users logging onto the system who have forgotten their passwords, will be locked out of the system for 30 minutes after six bad password attempts. To allow access within that time frame the administrator must logon and reset the user's password.

To maintain continued compliance, you must manage passwords using these rules:

1. Change user passwords, including remote and partial-access passwords, after 90 days.
2. The new password cannot be the same as any of the last five passwords for that user.
3. Passwords should be unique for each user.

Because passwords cannot be retrieved from the system, it is IMPORTANT that you record and store the administrator password in a secure location. If you lose or forget the administrator password, you must COLD START the FSC in order to reset the administrator password.

Note: Sessions idle for more than 15 minutes are automatically logged off.

8.3 Third-Party Application Interfaces / Remote Access

OPW cannot control how third-party applications manage passwords or try to interact with the system. In order to further protect the payment system and cardholder-sensitive data, OPW has reduced the command set available to these applications. With the PA-DSS compliant release, third-party applications will only be able to poll transaction data that contains no bankcard or cardholder-sensitive data (Only the last four digits of a cardholder's PAN can ever be polled by these third-party applications) and perform card-management functions against the internal proprietary card file. Along with the limited command set, these applications are now required to access the system at the Partial Access (or Privileged) prompt. The "SH TRANS CF", Card Update, Card Restore and Card Backup commands are no longer available in non-Privileged mode.

OPW recommends you contact the vendor of any third-party application you may be using and request updates to provide secure password management or removal of password storage all together.

8.4 OPW Device Connections

When installing the FSC and its peripherals (such as: FITs, C/OPTs, FIT500s, PCMs or even UPCs), wireless modems should not be used as a connection solution for Petro-Net. Direct wiring must be used to

establish a connection between the FSC and its associated devices to ensure a PCI-compliant installation. Only the standard Internal OPW dial-in modem can be used for remote connections.

8.4.1 External USB Journal Key

When a journal printer is not desirable due to the location of the installation or the environment, an external USB key can be used in place of the journal printer. The FSC will create a transaction history log file on the USB key in the same data format that is provided to the third-party polling applications, as described above.

Where the transaction data contains no bankcard or cardholder sensitive data, only the last four-digits of a cardholder's PAN will ever be written to the file created on an external USB journal key.

8.4.2 Remote Access via Dial-in Modem

In order to maintain a higher level of security with remote access, it is recommended that internal dial-in modems be physically connected to a phone line only when the need for remote access is required for the purpose of polling or system management.

Note: External modems connected to the FSC direct connect terminal port (port 1), should not be used when processing bankcards.

8.5 System Logging and Maintenance

OPW has implemented an always-on system-logging process. This logging mechanism is designed to track events such as: user creation, password changes, logins, system resets and cold starts, users who view transaction data, and more.

Under the current implementation of this logging mechanism the data is stored in one of the flash banks located on the FSC SIMM card. Because the available space allocated to logging is fixed, the available log space could fill and therefore stop the logging the process from continuing (current tests indicate about 2,000 to 2,100 entries can be made). PCI compliance states that the merchant must retain a minimum of one year of log data. In order to help you meet this requirement, OPW has implemented an automatic log print process to the journal printer. If you're operating without an active journal printer, it is your responsibility as the merchant to capture log data manually and retain if for one year.

Note: Because the FSC3000 is an embedded system with limited storage space, the system log process is not designed to specific "Centralized Logging Mechanisms." See below for information about how to manage, collect, retain and clear log data.

8.5.1 Automatic Print and Clear of Log Data

Under the journal printer setup (SET JOURNAL) you will be prompted to automatically print log data on the first day of each month. Answering, "Yes" to this prompt will cause the system to automatically print the current log data on the first day of every month following the printing of midnight totals. Once printed, the FSC will automatically clear the log file and starts again to continuously log system activity.

8.5.2 Manual Capture of Log Data

If you do not have a journal printer installed or prefer not to auto-print the log you must manually capture and store log data to maintain your PCI compliance. To manually capture log data use the following procedure:

1. Connect to the FSC using a terminal application that provides the ability to capture text. This includes applications such as: HyperTerminal, ARTWare or Phoenix.
2. Log into the FSC using the "Admin" login ("login Admin")

3. From within the terminal application, enable text capture.
    a. Do not overwrite an existing capture file that is not more than one year old.
4. From the command prompt: “Admin>” issue the command “SHOW LOG”
5. After the log data has been completely displayed, turn off the terminal’s text-capture feature saving the capture file in a safe location that can be accessed for at least one year.
6. From the command prompt: “Admin>” issue the “SET ADMIN” command and select the “Clear Activity Log” option. This will clear the flash blank and then log an entry indicating when the clear process occurred.
7. Press “Enter” to exit the “Administrator Menu.”

8.5.3 Retention of Log Data

PCI compliance requires the retention of log data for one year, the recommended practice for retaining data is dependent on which process you follow as described approve.

If you choose to capture the System log using the manual process defined above, it is recommended that you define a Folder on your PC (typically under a documents folder made available by most OS’s) called “FSC3000 System Logs” then within that folder create sub-folders named by year. When saving the capture file as described above, name the file based on the current date, this will allow you to find the log data is a sequential order of occurrence. These folders should be stored on a machine that has limited access to only those individuals that need to review this data for a troubleshooting purpose.
A sample name of the capture file is: “My Documents\FSC3000 System Logs\2013\01212 March1.txt” where “01212” is the Site Id.

As defined in PCI DSS 10.5.3 this data should be promptly backed up to a centralized log server or media that is difficult to alter. When operating multiple locations that are processing bankcard data and you are storing that data electronically, you must develop a process that allows you to promptly push the data collected monthly to central location. This location must be controlled and secure in a way that only administrative users have access to that central location.

If you do not have a network environment that provides the ability to maintain a centralized server that can be backed up and controlled, then you need to consider the use of media that is difficult to alter. Such as promptly recording the monthly log data to a DVD and storing that media in a secure location that non-administrative users have access to.

When printing the System Log, you need to determine a location where all monthly printed copies can be stored. These printouts should be stored in a secure location only accessible to employees who need access to this data for the purpose of troubleshooting problems. If you manage multiple sites you must build a process in which the printed copies properly forwarded to a central location where printouts of all logs can be secured and controlled. Example of centralized printout control process; Scan month printed logs into a computer at the local site converting them to TIFFs or PDFs. Immediately copied scan doc files to secure folder on central server. Delete scan docs from local machine. Secure original printouts in offsite secure location for Administrator access only.

8.6 Returning System for Warranty or Repair

As the merchant you are responsible to ensure that no sensitive bankcard or cardholder data is allowed to leave your facility. Therefore, if you need to return the FSC to OPW or your local distributor and bankcard transactions have been processed, the transaction storage memory must be wiped.

Follow these steps to ensure transaction memory is cleared.

1. Disconnect power to the FSC and remove the cover.
2. Locate the battery on the SIMM card and place a piece of paper between the battery and its hold clip.
3. Allow this paper to remain in position for minimum of four minutes. This will allow the battery's backed-up memory to decay, removing any sensitive data from the system.
4. Remove the paper and reattached FSC cover (or allow to remain to conserve battery life).
5. The FSC is now safe to release to OPW or your distributor.

Note: This procedure can also be used before upgrading your site from previous versions of FSC software not certified as PCI-complaint. This provides compliance for the PA-DSS requirement 1.1.4: "Delete sensitive authentication data stored by previous application versions"

Note: the process defined here conforms with the NIST SP-800-88 specification for how to "Clear/Purge" Dynamic Random Access Memory (DRAM).

8.7 Creating a Compliant Environment when Upgrading an Existing FSC3000

If you currently own a FSC3000 Fuel Site Controller and you are preparing to upgrade to a PCI-certified compliant version of software several steps may be required to ensure the existing FSC is used in a manner that meets compliance. Reference the topics below that apply to you and follow the define steps.

Note: If this is a new site installation you can skip this section.

8.7.1 FSC Installed Before Aug 1, 2008, and Does NOT Use the Ethernet Port for Remote Access

If you installed your FSC prior to this date then you have FSC board revision "B." You can upgrade your application software and continue using the FSC as you do today. However, if you ever connect an Ethernet cable to provide TCP/IP access to the system, you MUST then follow the next topic.

8.7.2 FSC Installed Before Aug 1, 2008, and USES the Ethernet Port for Remote Access

If you installed your FSC prior to this date then you have FSC board revision "B." Using the Ethernet port on this version FSC, as it is today, does not allow you to operate in a compliant environment. You must therefore choose one of the processes below to ensure compliance.

Note: If you need assistance with any of the processes defined here, please contact the OPW Technical Service Group for support to ensure the process is completed successfully.

Process 1: Return the FSC and upgrade to a new controller directly from OPW Fuel Management Systems.

Process 2: Disable Ethernet Web interface. This process should only be used if you don't expect to connect any external devices to the FSC requiring the possible change to your

system's connection point baud rates *(if you expect to add external devices follow process 1)*:

1. Access the Web interface (available from any browser) for the Ethernet controller. This can be done by entering the IP address of the FSC into the address bar of your browser or by selecting the "Open Web interface" option using the Digi Device Discovery tool (provided on the ARTWare installation CD).
    a. If a login screen is presented the username is "root" and the password is: "dbps"
2. Under the "Configuration" menu on the left, click on the "Network" link.
3. From the Network Configuration screen (at the bottom) select the "Network Services Settings" link.
4. Under this section disable (or uncheck) the following options: a) "Enable Telnet Server" b) "Enable Web Server" and "Enable Remote Login."
    a. Click the "Apply" button. Your browser should now display an error indicating the page cannot be found. You are now ready to operate in a compliant environment.

8.7.3 FSC Installed After Aug 1, 2008, and USES (or will use) Ethernet Port for Remote Access

Before continuing with this process, remove the cover of the FSC and determine the board revision you have. The revision letter of the board can be found on the front edge directly beneath the right side of the display, to the left of a white square. If the board revision is "B" you can follow process 1 or 2 above. If the board revision is "C" follow the steps below. When complete and the software has been upgraded you will be able to switch port baud rates as needed.

1. Access the Web interface (available from any browser) for the Ethernet controller. This can be done by entering the IP address of the FSC into the address bar of your browser or selecting the "Open Web interface" option using the Digi Device Discovery tool (provided on the ARTWare installation CD).
    a. If a login screen is presented the username is "root" and the password is: "dbps"

    OR

    b. If your browser displays an error indicating the page cannot be found, then your system was configured as needed from the factory and you can proceed with the software upgrade. Skip the remaining steps.
2. Under "Configuration" menu on the left, click on the "Serial Ports" link. When the "Serial Port Configuration" screen is displayed click the "Port 1" link.
3. Scroll to the bottom of the page and click on the "Advanced Serial Settings" link.
4. Under the section "Serial Settings" locate the checkbox option "Enable RCI over Serial (DSR)" and check the checkbox (You Must See This Box Checked!). Scroll down and click the "Apply" button.
    a. After the screen refreshes, ensure a message at the top reads: "Changes have been saved successfully." Double check that this is checked before proceeding to step 5.
5. Using ARTWare, update the FSC to the latest version of PCI-complaint software.

6. After cold start/reset you should see this message displayed at the CAP port; “LAN Device Configured.” If not, repeat step 1 above. You should see the condition under 1.b.
    a. If NOT please contact OPW Tech Support for further troubleshooting.

9 FSC3000 System Installation

9.1 Setup

Setup of the FSC hasn't changed, but availability of the command-line interface has been altered to reduce user access once the system has been activated ("Started") for the processing of cards. These changes and how they affect system use are explained throughout this section (FSC3000 System Installation).

Note: Distributors unfamiliar with the new setup and configuration of this software version should contact OPW's Technical Service Group for assistance.

9.1.1 Card Processing

The FSC will not process any cards without the system being activated for use. Your distributor will be able to install and configure the system as needed, but the processing of any cards (including PCF-defined and Private Fleet) is not allowed until the factory default passwords (Remote Access, Partial Access (previously known as "Privileged") and the Administrator password are changed and the "System Start" command is issued.

9.1.2 "System Start" command

Requirements of PA-DSS compliance forced the creation of new commands designed to strengthen security and user access to the system. The "System Start" command, which is only available after the factory default passwords have been changed, causes two main actions to occur. One activates the system to allow the processing of cards and the other changes the availability of system configuration commands. Once the system has been "Started" all command-line setup is disabled, unless logged in as one of five merchant-definable users or the administrator. Once started, the system cannot be stopped and configuration commands (including some "Show") are available only when logged onto the system.

9.1.3 Privileged vs. Partial Access

Historically, OPW FSCs allowed for two levels of access: "Show" and "Privileged." Privileged access allowed for complete control of the system while "Show" only allowed a user to see information but never alter it. The "Show" access mode has been eliminated completely and "Privileged" mode is now dependent on system activation. Before system activation "Privileged" mode operates as it always has, but once activated this access level changes to "Partial Access" mode. Partial access mode provides the ability to see system settings with limited ability to "Set" daily system functions. Some of these daily commands include: "Set Fueltype" for pricing changes, "Set Pump On" for manual activation of a pump and "Install Pump X" so individual pumps can be placed back in service due to activation of the Pump Sentry feature.

***Note**: The "Show Trans" command is only available to logged-in users.*

9.2 Users

To provide a stronger level of security, individual user logon access has been added to further support PCI compliance. You are able to create up to five individual user names for system login. Each user name is case-sensitive, must be at least 5 characters in length and can be assigned its own password. In addition to these five users, a factory-defined username of "Admin" has also been added to the system. This administrative user has been specifically designed for the purpose of managing users and password and clearing the system activity log, it cannot be deleted. When defining users OPW recommends the creation of a user with a unique password that can be used to provide access to your distributor's technician or OPW's Technical Service Group. This password can then be assigned as needed to operate for a limited number of days (See below for more information about creating users).

9.2.1 "Set Admin" command

This command allows you to define up five individual users of the system. They can be created and deleted or have their passwords changed whenever the system administrator desires. This command is also used to initially change the factory default passwords for the Remote and Privileged (Partial Access) logins, along with managing the administrator password. It is available for use under the Privileged login until the administrative password is defined. Once set, this command is ONLY available under the "Admin" login. This now provides the administrator exclusive access for the management of system users.

9.2.2 User Options

When creating users, two configurable options are available; one defines how card numbers are displayed for bankcards when viewing transactions and the other is a "Limited Logon" option that allows you to define a limited number of days for which logon can occur. The card number option allows you to say whether a user can view just the last four digits of a card number or the 6-digit ISO along with the last four digits (displayed as: 123456xxxxxx4321). The limited logon option is useful for a technician login (as recommended above), or someone who needs brief access to test or troubleshoot the system. Each time the password for a "Limited Logon" user is set, the administrator can define how many days (up to 15) this user is allowed to access the system. Once the number of defined days is passed, that user's logon is no longer valid until the password is reset.

9.2.3 Passwords

Coupled with the addition of individual user access, password creation and management has been modified to: 1. Ensure all passwords are uniquely encrypted on each FSC using a SHA1 hashing algorithm, 2. Remove the ability to decode a password by the OPW Tech Service Group, 3. Disable system functionality until factory default passwords have been changed. In the case of the FSC, this means that no cards can be processed without changing the factory default values and 4. Require strong password-creation rules. OPW has instituted the follow rules for password creation:

- Must be a minimum of 8 characters in length, with a max length of 20.
- Each password must contain at least:
  - 1 capital (or upper-case) letter
  - 1 lower-case letter
  - 1 numeric digit
- Special characters (those available on a standard keyboard) are allowed but not required.

Important: Whenever the administrator password is changed, you must record this information and store it in a safe place. If you lose or forget the administrator password you must "Cold Start" the system to regain access to the "Set Admin" command.

9.2.4 Login Command and Administrator Access

Once users are defined, they must login using the "Login <username>" command. As stated above user names are case-sensitive. If when created, the administrator entered "Tech1" as the username, an entry of "login tech1" will not be valid.

Once the administrator password is set the "login Admin" command must be used to gain administrative access. This controlled access allows and is restricted to:

- "SET ADMIN" command, to manage users and clear system log.
- Use of the "SET NETWORK" and "SET FLEET" commands
- All available system configuration commands.

- Disabled access via the Ethernet port. *"Admin" users must login using direct connect or dial-in modem.*

Note: If a user (including the "Admin") enters an incorrect password six times in a row, that account will be suspended from use for 30 minutes.

9.2.5 Remote access login via Ethernet port

As stated above, remote access is not allowed for the Administrator ("Admin") using Ethernet access. If remote access is be used as the primary connection point, via the Ethernet port, it is important to ensure at least one additional user is created.

9.3 System Activation

Once setup is complete, the factory-default passwords have been changed (using the "Set Admin" command) and the desired users have been created, issuing the "System Start" command will allow the processing of cards and restricts use under Privileged mode.

9.4 Recommended Startup/Installation Process

Because of the PA-DSS enforcement, OPW recommends the following setup steps to ensure the simplest installation process of the FSC3000.

1. As explained above, login to "Privileged" mode and issue the "SET DATE" and "SET TIME" commands. Because the system log is active on cold start, the date and time should always be set first to ensure the correct timestamp is logged to all further commands.
2. Install and configure the system as needed to ensure terminals are configured and running. Pumps should be installed and operational (using the "SET PUMP ON" command to test pump installation). Network configuration information should be entered for each network enabled.
3. If attached, configure the office journal printer to automatically print the system log on the first of every month.
4. Issue the "Set Admin" command. Change the factory default passwords for Remote and Partial access. Create an administrator password (be sure to record and store the administrator password).
5. Create additional users for access to the system.
6. Issue the "System Start" command. Cards can now be processed and fueling can occur.

Appendix A – Loyalty Prompt (and tiered accounts)

This appendix is specific to merchants who purchase bankcard networks with the Loyalty Card Prompt Feature enabled on the FSC3000 Fuel Control System. The loyalty card feature is designed to allow merchants to ability to track a fueling transaction to a specific customer in lieu of having access to the bankcard PAN. With the use of this feature an increased level of risk exists through the possibility of malicious individuals attempting to compromise the system for the purpose of obtaining sensitive cardholder data. By following the recommendations described below and those outlined in the PCI DSS requirements, you as the merchant, can protect yourself from unscrupulous individuals attempting to compromise fuel transaction data.

PCI DSS Requirement 7: Restrict access to cardholder data by business need-to-know

> 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.
>
> 7.2 Establish an access control system for systems components with multiple users that restricts access based on that user's need to know.

Based on Requirement 7, limited access by using unique logins for each user on FSC is only part of the control you as the merchant needs to consider. Limiting access to the individual components of the fuel control system is just as important. These components include the fuel island terminals such as the FIT500, C/OPT and the K800 Hybrid. Although these terminals do not retain any sensitive cardholder data they are the mechanism for which bankcard data passes through to the fuel control system. Therefore limiting access to your fuel island terminals is just as important as limiting access to the FSC itself.

As the merchant you should not only control who has login access to the FSC, but also who has access to these terminals. Whether your terminals display bitmap images or plain text, regular review and monitoring of the messages displayed are what you as the merchant authorize for use. If you are unsure of what messages are acceptable for use at your terminals contact a PCI Council-approved assessor for approval of the messages displayed at your fueling location(s).

Through implementation of the loyalty card prompting feature OPW has developed its support to provide limited control for implementing the use of this purchasable feature. This control, although limited, provides you the merchant the ability to define the message displayed at the terminal. With this ability to customize the displayed message, whether it is a bitmap or text, you as the merchant become responsible for the integrity of the message/prompt displayed for the loyalty card prompt. By design the loyalty card prompt can only be presented if a bankcard host is enabled and the loyalty card prompt feature is purchased. The prompt can then be enabled through configuration of the bankcard host. The prompt, from a cold start of the system, will display the message "Enter Loyalty # (zero to skip):" and must only be modified by the Administrator (a similar prompt of this type is used for Tiered Accounts). As described above, when this prompt used in conjunction with a FIT500 terminal and is configured to display a merchant-designed bitmap, you as the merchant must implement a process to ensure the display message is reviewed and monitored on a regular basis, confirming you fuel control system remains in compliance with PCI DSS requirements.

The information presented above will help you as the merchant remain compliant and protect the sensitive cardholder data of your customer. For additional information regarding the security and protection of cardholder sensitive data when using the loyalty card feature, contact OPW Technical Support for assistance in answering any additional concerns not addressed within this document.

Appendix B – Ensuring Valid Software Updates

Along with following the rules documented throughout this guide, use the following process ensure you have obtained and installed the latest version of Multi-Trucking software on your FSC3000.

The feature tracking version number is defined as: "X.xxl" where the leading digit ('X') represents the application specific version. It is the next incremental application number available for the specific product line in which it is used. Once assigned the leading digit never changes. The digits following the decimal point ("xx") are the system memory map control digits (00-99). This value changes when the internal memory map of the application changes, indicating a System Cold Start must occur when moving to a higher value digit. This value can increment forever as needed by the developers. The letter character ('l') indicates a change to the application without the need for additional memory. This indicates that an update can occur without the need for a system Cold Start.
For example, in the version number 1.15b, the "1" denotes that it is Multi-Trucking Network Package. The "15" denotes that it users memory map 15, so if you are upgrading from 1.14 it would require a system cold start. The "b" is the minor feature letter. You could, for instance upgrade from 1.15b to 1.15d without having to cold start the device, but an upgrade to 1.16a would require one.

To stay compliant, make sure your version is the same version **or greater** than the one listed on the PCI web site.
Check the secondary boot loader version to make sure it is version 1.02c or higher. Using the Show Sys or Show Version commands, it will be listed as "Loader2". If it isn't, obtain a copy of the latest FSC3000 Multi-Trucking firmware from OPW at: http://www.opwglobal.com/TechSupport/OtherSoftwareDownloads.aspx

You should always validate that the application checksum is correct before allowing the system to continue the processing of bankcard data. Starting in version 1.17a, updates are digitally signed to make them tamper-proof. The following procedure has been simplified accordingly.

Note: this is written with the assumption that you are an OPW certified distributor technician, or you as the merchant, have been trained by your certified distributor.

1) Obtain a copy of the latest FSC3000 Multi-Trucking firmware from OPW at: http://www.opwglobal.com/TechSupport/OtherSoftwareDownloads.aspx
   a. Download: FSC3K_1_XXx.zip - OPW Part#: S030001
   b. A copy of ARTWare is also required for downloading the firmware to the FSC3000.
2) Record the "Application Checksum" shown for the downloaded version.
3) It is no longer necessary to open the FSC3k_xxxxx.abs file to verify the checksum. If you are used to doing this, be aware that it is now on the first line of the file, the numbers on the second line are part of the digital signature.
4) Open the ARTWare application and connect to the site. For the most secure connection during download connect to the FSC3000 using either the direct connect CAP port (1) or the internal modem.
   a. Once connected and logged in, select "Upgrade" from the "Online" menu and select the downloaded FSC3k_xxxx.abs file.
5) After the download is complete and the FSC restarts reconnect and login using ARTWare and open a terminal window from the "Online" menu.
6) In the terminal window at the command prompt issue the "SH FLAGS" command. The following information will scroll by and the FSC will then calculate checksums for each of the Flash Banks available on the FSC3000 SIMM.

```
  FSC3000: PA-DSS Certified Version: 2.0
  Card Record Features Version #:  1.14b - SIMM Serial #: 123456
  FPGA:        2.0
  Loader:      1.01A  Jun 30,2005
  Loader2:     1.02A

       SIMM SERIAL #: 123456
MAX CARDS:                        64000
MAX TRANS:                        1000
       :
TIERED DISCOUNTS:                disabled
TIERED ACCOUNTS:                 disabled
MAX # OF DTCs:                    0

  EXECUTING OUT OF FLASH

  FLASH ADDRESS BLOCKS:

  0:100000-17FFFF (155D) Main App      8:500000-57FFFF (BLNK)
  1:180000-1FFFFF (FAB3) [1010]        9:580000-5FFFFF (BLNK)
  2:200000-27FFFF (155D) Prod Ship    10:600000-67FFFF (xxxx) PCI Cert
  3:280000-2FFFFF (FAB3)              11:680000-6FFFFF (xxxx)
  4:300000-37FFFF (xxxx)              12:700000-77FFFF (xxxx) Log Buffer
  5:380000-3FFFFF (xxxx)              13:780000-7FFFFF (BLNK) Sys Params
  6:400000-47FFFF (????) DPC Exec     14:800000-87FFFF (6845) Boot Ldr
  7:480000-4FFFFF (A168) USB Boot     15:880000-8FFFFF (xxxx) FactoryUse

                    16:900000-97FFFF (B189) RAM
```

7) First confirm that the "`App feature ver:`" information shown matches the first line of information in the downloaded ABS file. If this information is not same, retry the download process or contact OPW Tech Support.

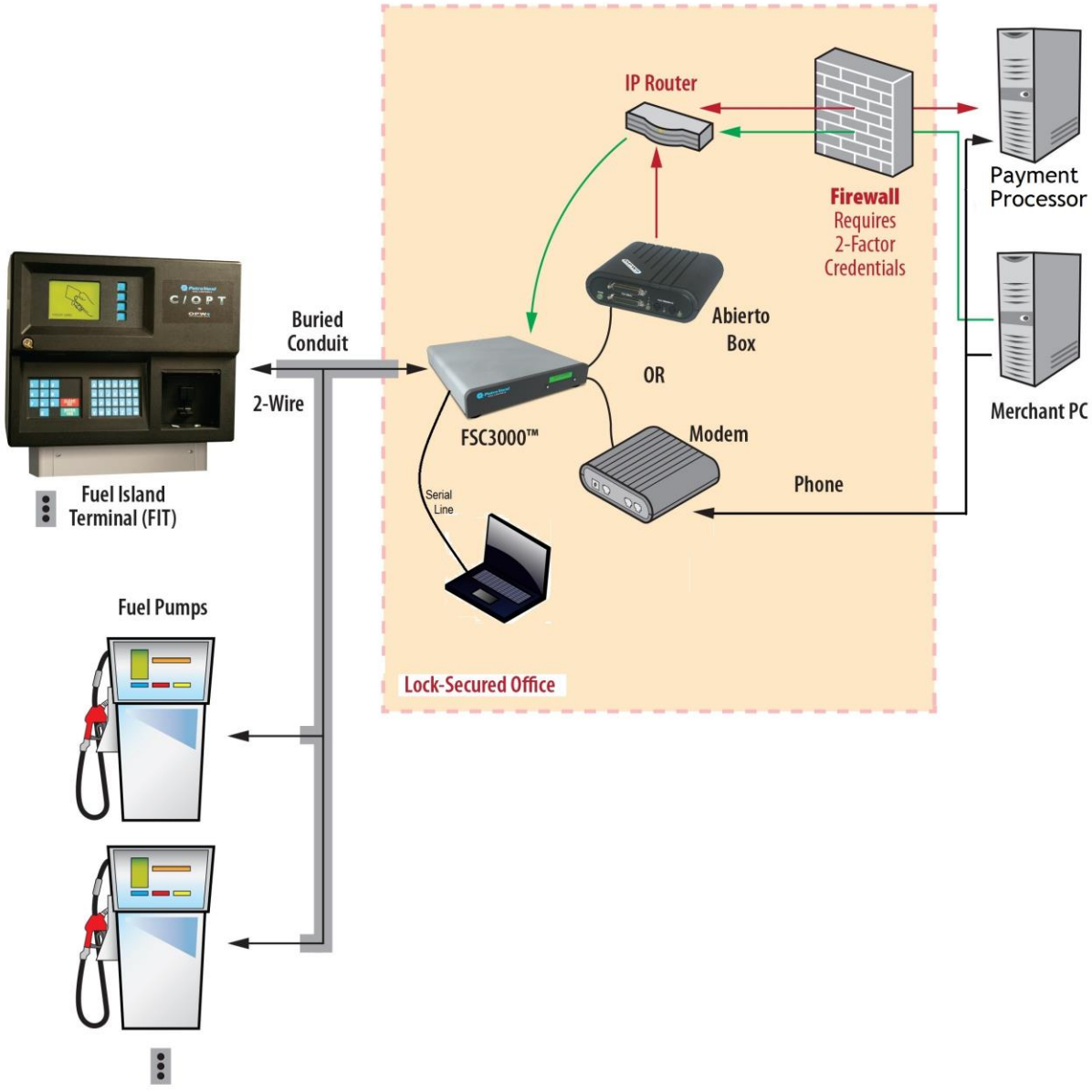
8) Reference the information shown in flash address block "1:180000-1FFFFF" after the flash block checksum *(shown as: (FAB3))* there is second set of characters in square brackets; '[xxxx]' *(shown as: [1010])* this is the string that must match the checksum recorded from the Web Site when you downloaded the update.

   Important: If the checksum information does not match, even though the App Feature Version confirmed above does, contact OPW Technical Support. Do not continue to process bankcard transactions until OPW Technical Support can validate the mismatched information.

Appendix C – System Connection Diagram

The diagrams below show the different forms of possible connections for the installation of an FSC3000 running a Multi-Trucking network version of software. The different areas of concerns related to these diagrams are discussed within this guide.

FSC3000™ MULTI-TRUCKING
PART #: S030001



Typical configuration of a standard FSC3000 using either an Abierto Serial-to-TCP/IP convertor for secure connection to host or a standard analog modem dialing out to the network host. Per PCI DSS 8.3 requirements two-factor authentication is required for accessing the firewall protected network.

Appendix D – Version revisions

Card Record Feature Version:

1.20j - Removed need for DFS Purchase Flag, always available for use.

Updated support for EFSLCC (TCH) Fleet Network to allow the routing of FleetOne, WEX Crossroads Cards, plus two additional MC Fleet ISOs. Note: FleetOne will still route to FleetOne host if configured as such.

Fixed the wrong reporting of FMGC expiration dates under CFN Fleet Network.

Added TCH network configuration option, in support of direct IP connection via Systech box.

1.20i - Added support for DFS Cloud solution, allowing a site status packet to be sent.

Removed printing of Price & Total from CFN host processed recipts.

1.20h – Added the ability to update Network prompts to load French messages when selected.

Added support to process WEX card to Atio-Net host.

Changed card recognition for NBS Fuel-Net, due to miss programming of track2 data.

Fixed COPT French keyboard issue.

Fixed an issue where the Pump 1 DTC would ask the driver to pay inside rather than issue receipt.

1.20g – Renamed Ultramar host to “Parkland”

Added routing of T-Chek card to Parkland host.

1.20f – Added Watchcard for Quarles

Added CFN Legacy support for FleetCor and FleetCor proxy to NBS.

Added the ability for the KTTH card to route to KardTech.

Fixed an issue where the IAT sometimes wouldn’t turn on for under a gallon on electronic pumps.

1.20e – Fixed some issues with the soon-to-be released Inside Authorization Terminal (IAT):

- The IAT task occasionally locked up from bad communications to device.
- .The receipt header and footer wouldn’t change when the FSC’s did.
- Added support for a different pump icon when buffer full.
- Added additional support for preset values.

Fixed not being able to set zero timeouts for pump handle, first pulse, and missing pulse.

Fixed a condition in AVI where driver\vehicle tags could lose odometer value.

Added to AVI: If the VID has engine hours, but not odometer, engine hours go into the odom field for reasonability.

1.20b – Added the following features for OTI:

- Single Tag transactions may be started from the FIT with odometer and pump entry.
- Added support for custom tag, attendant tag, and dual tag.
- Added support for tag time-outs to pause/resume fueling.

Added support for Indoor Authorization Terminal (IAT).

Added PV Systems support for Enterprise and Enterprise Plus bundles.

Added option for Comdata POS to NOT automatically prompt for Refer.

Added support for VIT commands for older ARTWare versions.

System start now prompts for date and time if the date is still on the default year.

If a second SIMM is installed at cold start, diagnostics automatically begins logging to the second SIMM until configured otherwise.

Added references to PV200 in set/show FIT.

"DISCONNECT TIMEOUT" for termination code Q, changed to "FSC STOPPED PUMP" to reduce confusion.

Intevacon, Atio, and Company Card can no longer be configured to process offline.

Fixed an issue where BUYPASS would record zero-quantity fleet cards as FAILED captures.

Fixed receipt Low Paper being treated as if Paper Out.

Fixed the first character missing in prompts after cold start or Format Display Default.

Fixed an issue where SET PUMP ON would occasionally not activate the pump.

1.19b – Added support for Fleetcor to process to their new Hermes host.

- Added support for multiple network downloaded prompts for CFN network.
- Added support remove the Pride controller from service.

Added support for OTI non-intervention hardware.

Added support for Kardall IPN to process Fleet1 and WEX cards.

Improved capture process to Buypass network to handle poor connectivity.

Added State of PA Training screens (single screen changed per Fire Marshal request).

Added support for future DPC diagnostic logging.

Changed default for reprompting to off.

Updated Visa Fleet & MC Fleet embedded prompting for newer formats.

Receipt prompt at the pump will follow configurable prompt timeout.

Fixed an issue where FITs occasionally reset on pump user timeouts.

Fixed an issue where hidden prompts didn't work as expected on K800 and System2 terminals.

1.17f – Fixed an issue where a fake, mostly blank, transaction was occasionally created.

Fixed an issue where a pump could be reserved indefinitely if the FIT reserving it reset.

1.17e – Added minor security enhancements.

Added support to improve host communications over TCP/IP where the IP channel does not emulate dial-up modem.

1.17c – Added support for NBS FuelNet. This feature requires the purchase of an option flag to activate.

Enhanced receipt counter to continue to count receipts after paper low warning is received from the printer. As before, the FSC does not increment the counter when it receives a jam or paper out alarm.

Added FleetOne support for 2-digit DEF product codes.

Added protection to avoid upstream tcp/ip issues with CFN and NBS hosts

Added enhanced security to immediately clear host packet data as soon as the line gets hung up.

Raised dollar limit for daily allocations for proprietary cards from $2,000 to $2,000,000.

Added pump communication error detection and correction for zero quantity terminations after flow has been detected.

1.17b – Fixed an issue in 1.17a affecting some receipts.

Enhanced to accept the CFN cobranded card while offline.

1.17a – Added support for FleetOne 2-digit DEF product codes.

Added Quarles Product Restriction Codes for CNG & LPG.

Fixed an issue where manual bypass transactions were being recorded multiple times.

Added an auto-restart feature to the diagnostic log while adding forensic information to track the source of the corruption.

Improved the timing of Dual host dialing for authorizations and captures.

Accommodated a ComdataPOS host issue by sending captures individually.

Fixed an issue where the last character from the network receipt would occasionally get dropped. Some receipts, for instance, ended in "Thank Yo"

Added resending of pump configuration after any PetroNet interruption to protect pumps against brown-outs.

Enhanced FSC's interaction with ARTWare to allow online limits of greater than $100, as well as correctly accept all Micronode, AVS, and training screen configurations.

If you purchased a second SIMM, set transaction buffer size now assumes you want maximum transactions, rather than prompting you for how many you want.

For PCI 3.1, added digitally signed software updates (requires Secondary Boot Loader 1.02c or higher).

For PCI 3.1, added the storage of the last five passwords for each user. Password history is now automatically checked when changing passwords. Additionally, passwords may now be as long as 20 characters long. User names now require a minimum of five characters.

For PCI 3.1, added the following events to the system log: any access to the fleet table, Install/Remove Program commands, and any failed Admin password revalidations.

The following commands were moved to more appropriate access levels:

- Install/Remove PCT Position will be allowed from the P> prompt.
- Set Site requires a user log in.
- Administrator level commands (Set Admin, Set Fleet, Set Network) will revalidation the admin password as well as verify that the remote (TCP/IP) port isn't the access method.
- Once the system is live, ARTWare users need to be logged in locally as Admin to change network phone numbers.

Added numerous internal security improvements dealing with memory usage and encryption.

1.16b – Added Refer Prompt support for ComdataPOS host allowing prompt to occur based on diesel product selected.

Added a separate column in the Fuel Type table specific to the TCH host.

Added additional diagnostic logging to support enhanced error trapping conditions.

Added support to show 8 hose totals for UPC's under the "SHOW PCT TOTALS" command.

Added ISO support to present a Buypass Liability acceptance in regards to the processing of Visa/MC $1 requirements.

Finalized support for the new EFS LLC MasterCard Fleet card routing to TCH host.

Fixed condition between FSC and ARTWare where setup of Comdata ComChek card processing to CFN did not get enabled on the FSC.

Fix reported problem that when processing transactions on the 2nd SIMM with a full buffer, that a search of transactions with certain conditions would temporary halt Petro-NET communications causing some FITs/COPTs to go offline.

Condition was corrected that caused the ComdataPOS host to send a second authorization request packet after the condition was dropped caused an extended "Processing Please Wait" message for the user.

Corrected a clear transaction condition that had the potential to create transaction queue synchronization, resulting in a possible loss of fueling data.

Corrected problem where Growmark Fast Stop was no longer processing correctly.

Fixed condition where some Wright Express card did not process correctly to Paymentech host due to prompting identifier mismatch.

Fixed reported problem where the "Pump Activation Error" count was incrementing excessively

Fixed reported problem where Pacific-Pride Advantage cards where dispensing more than the host approved limit.

Fixed reported problem where FleetOne cards reported the wrong hose when UPC's are in use.

1.15d – Resolved BuyPass® PDL download errors.

Enhanced features during processing and clearing transactions.

Enhanced the "Set Network" Fleet Table to prevent data corruption if a network is added or removed after the site is already in operation.

Enhanced the ComdataPOS network to properly support the trip number prompt.

Enhanced Comdata host communication to resolve network communication errors.

Enhanced diagnostic data logging includes transaction information. Resolved issue with SH COM

– Initialization Error.

Resolved issue with continuous port header being displaced with mode connection.

Enabled security feature to hide Alpha-Numeric prompts.

Added support to match UPC product codes with Gilbarco pump codes.

1.15b – Added support for the new Pacific Pride Advantage card. NOTE: Only available with the Pacific Pride network option.

Added support for the Micro-node IP converter. This device is required when accepting Sinclair cards on the First Data Buypass network.

Added support for the First Data Buypass network to be processed via the Dual/Secondary host port. NOTE: The Dual Host option must be purchased.

Enhanced the diagnostic to capture Petro-Net communication.

Resolved a possible cold-start condition when polling transactions containing the “P” prompt.

Resolved a port locking issue when using dual networks.

Resolved possible misconfiguration by disabling the ability to preserve fleet table data when adding or deleting table entries.

Resolved a condition that incorrectly caused a “Pump In-Use” message to appear.

Resolved a minor authorization issue regarding Comdata fleet cards and Comadata MasterCard.

Resolved an issue with the Atlantic time-zone display.

Added Tiered Account support for the First Data Buypass network.

Host number added to Pacific Pride receipts.

Zero quantity authorizations from the host are now treated as declined authorizations.

Added Date, Time and Software version to the header of the Host Monitor.

Added additional fraud protection to the First Data Buypass network.

Added a separate product code column for TCH (EFS LLC).

Modified some default Fuel Man Gas Card fuel codes to align with Pacific Pride fuel codes.

Proprietary cards with allocations are now flagged to prevent concurrent fueling.

1.15a – Added support for ComdataPOS (retail) host to provide host based prompting.

Added enhanced support for Pacific-Pride to provide customers a migration path from the obsoleted Smartlock device.

Added enhanced diagnostics to record customer specific interaction at the terminal and host authorization messaging.

1.14k – Change fixed pump prompt timeouts to use the configurable host prompt timeouts. This change was made after numerous customer requests.

1.14j – Per a customer request, the max limit used for $1 authorization is configurable under the NBS Bank host. This change does not affect the $75 rule unless NBS agrees to support this feature. The customer must directly contact NBS for support of this feature.

1.14i – Fixed a problem with Buypass transactions were being prematurely set to a captured state that stop the final sale transaction from being captured to the host.

1.14h – In support of the DTC product the hose prompt selection was changed to a single digit entry.

Change was made to ARTWare protocol allowing Phoenix SQL to support a new price change feature.

Protection was added to ensure bankcard cardholder data was not exposed when no networks were enabled in the system.

1.14f – Added support so Comdata ComCheck can process into CFN host for card authorization.

1.14e – A problem was found during beta testing of DTC product, where a DTC generated time-out error, the stopped the capture of host transactions.

Added change for NBS Bank host to provide additional prompting on Visa/MC purchase cards. Prompts are collected after authorization and sent to host on transaction capture.

1.14d – Buypass dial-out phone numbers where locked down to protect user from mis-configuration.

1.14c – Changes made in support of CRIND/CAT terminal support, allowing users to select grade by lifting hose and selecting grade.

A DTC option flag was added to control use of additional hardware purchased for use with CRIND/CAT's.

In support of IP Convertor box FSC allows host port configuration of 9600.

To protect cardholder data, all RAM is zeroed on a Cold Start.

1.14b -- corrected issue found when processing FM/GC cards to Chase Paymentech host that stopped allocation of fuel.

1.14a -- added support for Buypass host (host certified Aug. 2013)

1.13h -- previously certified PA-DSS 1.2