Prometheus Security Group Global

Talon™ Multi-Function Security Appliance

FIPS 140-2 Cryptographic Module

Non-Proprietary Security Policy

Document: 030-00004-001

Version: 1.3

Date: 3/8/2018

REVISION HISTORY

Revision	*Date*	*Author*	*Description of Change*
1.0	08/05/2016	J. Freeze-Skret	First published version.
1.1	11/10/2016	J. Freeze-Skret	Updates per CMVP comments
1.2	2/10/2017	J. Freeze-Skret	Updates per CMVP comments
1.3	03/08/2018	J. Freeze-Skret	Updating for Non-SP 800-38F compliant changes

Table 1 – Revision History

Table of Contents

List of Tables

List of Figures

1 Introduction

The Prometheus Security Group Global Talon™ Multi-Function Security Appliance (MFSA) is a ruggedized, multi-function ultra-high security and surveillance appliance providing standards compliant, secure delivery of video, audio, sensor, control and data over an IP network. The end user can rest assured that their sensitive and critical data is reliably transported and securely delivered.

Meeting stringent Federal Information Processing Standard (FIPS) Publication140-2 Level 2 encryption and data validation standards as well as providing intrinsic physical security mechanisms at the device. Talon combines these features with secure boot, secure clock and a tamper proof enclosure capable of zeroing memory containing critical security parameters.

Talon functions either as a high definition (1080p) HD-SDI or as a standard definition NTSC/PAL video encoder which is ONVIF profiles S & G compliant. Talon delivers video at full frame rate for up to two simultaneous analog inputs or a single HD input using Motion JPEG (MJPEG) or H.264 baseline profile encoding. The device supports robust configuration parameters such as constant or variable bit rate (CBR/VBR), video profiles and multi-streaming capabilities with variable frame rates. The device provides SATA-II encrypted edge storage options for capturing, storing and playing back video and audio signals.

Talon features a high bandwidth gigabit SFP network interface, which supports communications (unicast or multicast) over existing TCP/IP backbones using category 6 cables or optional multi-mode/single mode fiber optic connections. It features a second 10/100 RJ-45 network input port allowing the device to simultaneously function as a data encryption unit by transparently passing traffic from non-secure IP devices through the encryption engine.

Talon is capable of full duplex audio support for intercom or audio surveillance applications. It offers an RS-232/422/485 serial data bus for transfer of control signaling for pan-tilt-zoom cameras as well as building automation devices. It delivers four supervised multi-state inputs, two relay control outputs and offers a wide range of operating power and temperature ranges perfectly suited for external deployments.

The Module is a combination of both hardware and firmware. The Module comes in two base hardware versions (standard definition video or high definition video), either of which meets FIPS 140-2 overall Level 2 requirements and are specified by the following product model indicator:

	Module	Module P/N	HW	FW
1	Talon Standard Definition MFSA	TAL-SD (FIPS)	v1.0	v1.0
2	Talon High Definition MFSA	TAL-HD (FIPS)	v1.0	v1.0

Table 2 – Cryptographic Module Hardware Configurations

In addition to the module P/N, the shipped package contains other accessories and options. This package is specified with nine dash-separated fields: “TAL” followed by fields A through H. The possible configuration options for each field are as follows:

A	B	C	D	E	F	G	H
Video Format	Grade	FIPS or Export	Power	Network Interface	Interface Type	Edge Storage	Size
SD NTSC/PAL	**IND** Industrial Temp	**FIPS** FIPS Validated	**CS** Customer Supplied	**COP** Copper	**RJ-45**	**NOEDGE**	**Not present**

HD HD-SDI	**COM** Commercial Temp	**EXP** Exportable	**XFMR** Included transformer	**MMF** Multi-Mode Fiber	**SX**	**EDGE**	**XXXX** Size in GB
				SMF Single Mode Fiber	**LX/LH**		
					EX		
					ZX		
					EZX		

Table 3 - Hardware Configuration Options

Note that C field will always say "FIPS", as the "EXP" variant is outside the scope of this validation. Also note that the B, D, E, and F fields do not correspond to any change in the module, as these specify the power converter (D) and SFP network interface (B, E, and F), which are outside the boundary. Fields G and H specify the presence and size of the internal hard drive, which has been excluded from the FIPS 140-2 requirements.

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated multi-function security & surveillance device. The Module is a multi-chip standalone embodiment; the physical cryptographic boundary is the entire enclosure. Internal to the module the firmware is also segmented such that security relevant features are blocked off from other firmware functionality and calling APIs are used to access the Module cryptographic functions for secure data output.

The overall level of the module is 2 and the FIPS 140-2 relevant security levels for the Module are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

Table 4 – Security Level of Security Requirements

The Module implementation is compliant with the following standards and certifications:

- TUV-SUD 60950-1 (equivalent to UL 60950-1)
    - CB Scheme IEC tested

    - OSHA Approved Factory Inspections
- CE
- FCC 47 CFR part 15 as a Class B device
- IEC-61000-4-2, Level 1
- RoHS
- ONVIF Profile S

1.1 Hardware and Physical Cryptographic Boundary

The physical forms, from all sides of the Module are depicted in Figure 1, Figure 2 and Figure 3. The front connector details are explained by Figure 4 and Figure 5 broken out by Module hardware version type (e.g. standard- SD or high definition- HD).

Figure 1 of the top enclosure depicts the physical cryptographic boundary, which is the entire product enclosure.

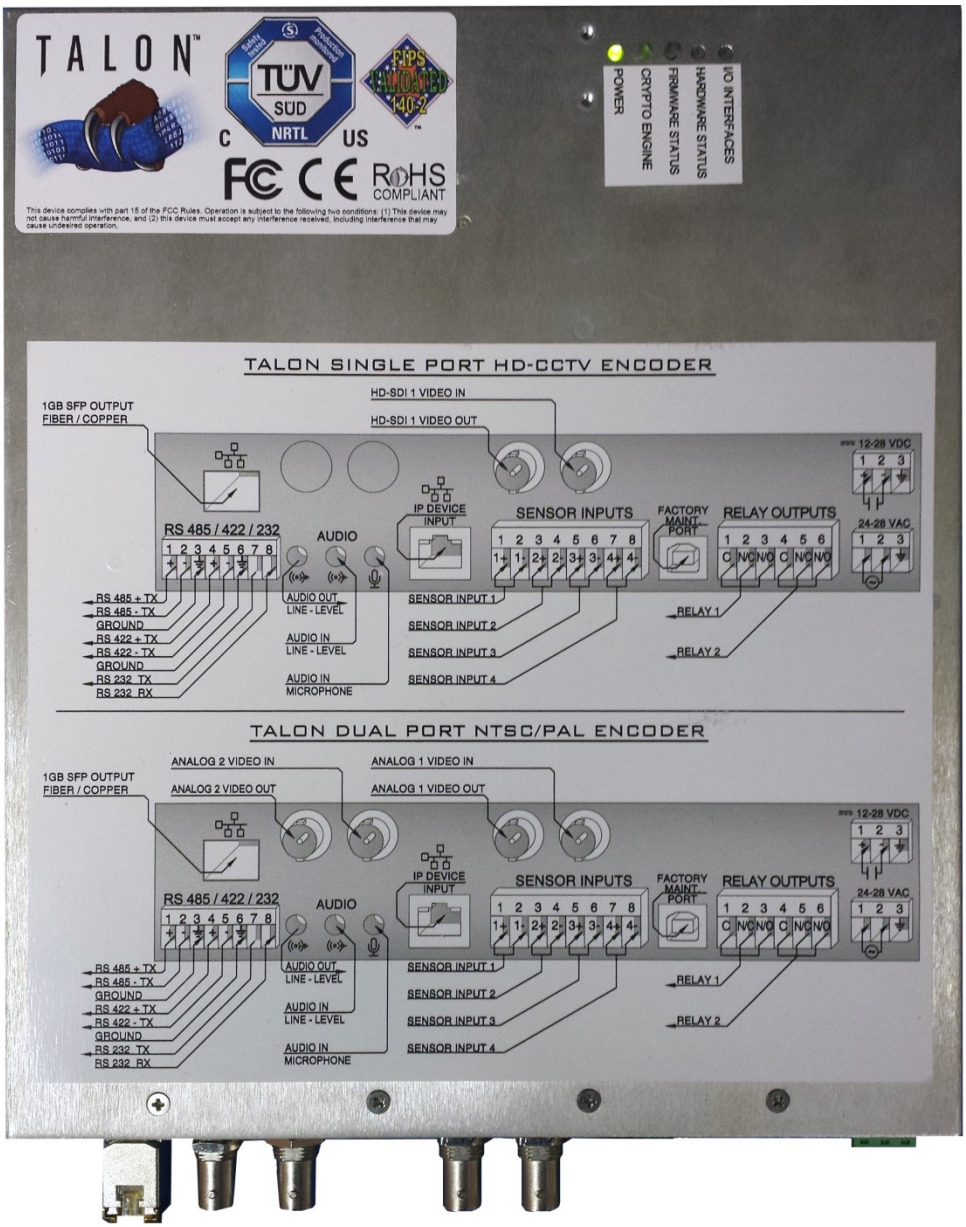

Figure 1 – Talon Analog MFSA (Top-View)

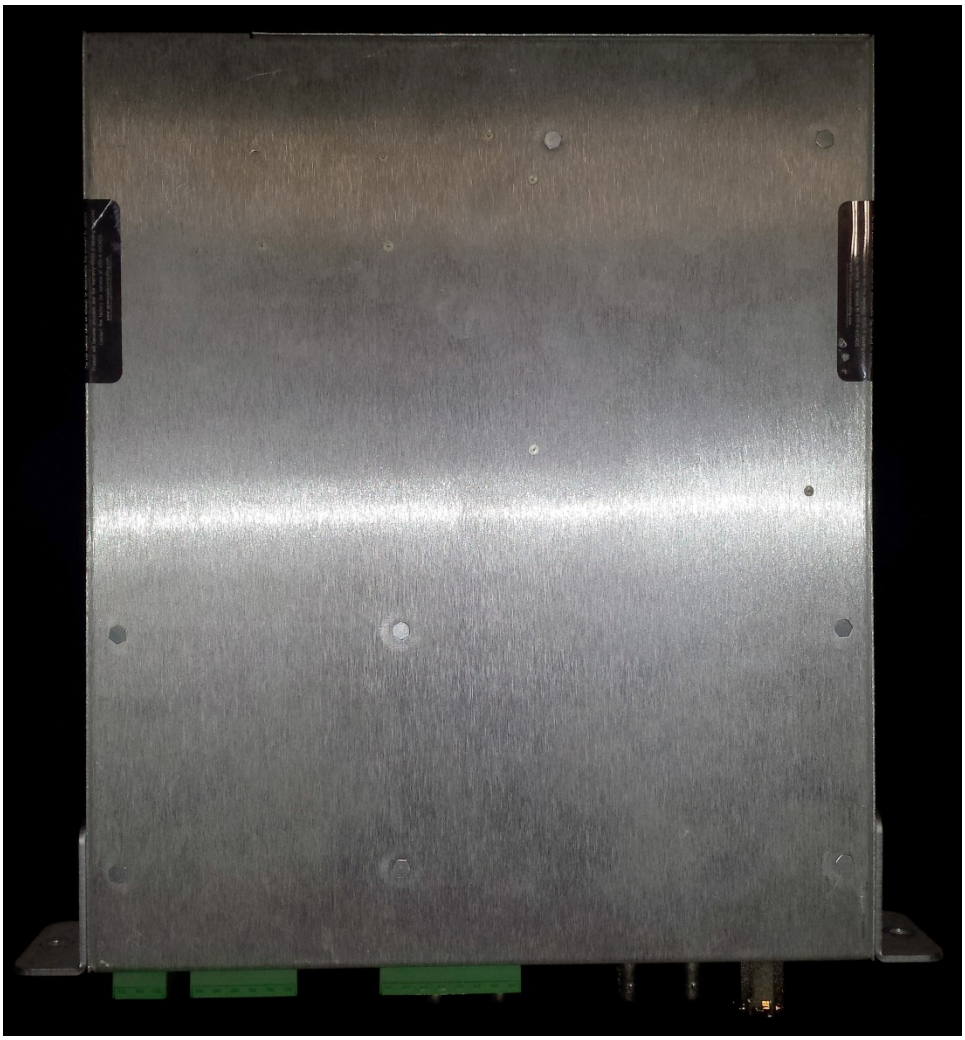

Figure 2 – Talon Analog MFSA w/ FIPS Tamper Seals (Bottom-View)

Figure 3 – Talon Analog MFSA Fan, Rear LEDs and Labeling (Rear-View)

1.1.1 Standard Definition (SD) MFSA Connectors Explained:

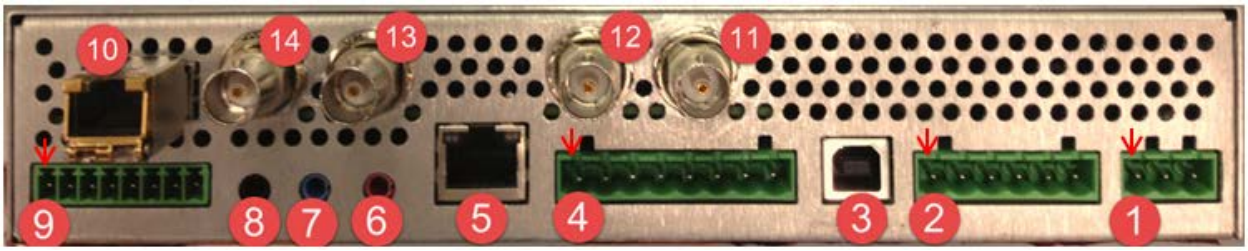

Figure 4 – Talon Standard Definition (Analog) MFSA Connector Interface (Front-View)

1. Power Input
    1. Input Power + (red arrow points to pin 1)
    2. Input Power –
    3. Input Power Ground

2. Relay Outputs

    Relay Outputs may be used to signal or control
    Resistive Load – 10A 250 VAC, 5A 30VDC

    1. Relay 1 Common (red arrow points to pin 1)
    2. Relay 1 Normally Closed
    3. Relay 1 Normally Open
    4. Relay 2 Common
    5. Relay 2 Normally Closed
    6. Relay 2 Normally Open

3. USB 2.0 – Access port for Factory Support role.

4. Switch inputs
    1. Input 1 Signal (red arrow points to pin 1)
    2. Input 1 Ground
    3. Input 2 Signal
    4. Input 2 Ground
    5. Input 3 Signal
    6. Input 3 Ground
    7. Input 4 Signal
    8. Input 4 Ground

5. Fast Ethernet – Down-line Input (RJ-45, 10/100)

6. Audio Input – Optional Microphone Level – 3.5 mm TRS
7. Audio Input – Optional Line Level – 3.5 mm TRS
8. Audio Output – Optional Line Level – 3.5 mm TRS

9. Serial Communications
    1. RS485+ (red arrow points to pin 1)
    2. RS485-
    3. Ground
    4. RS422 RX+
    5. RS422 RX-
    6. Ground
    7. RS232 TX
    8. RS232 RX

10. SFP Slot – Main GB Connection

11. Analog Video Input – Primary
12. Analog Video Output – Primary
13. Analog Video Input – Secondary
14. Analog Video Output – Secondary

1.1.2 High Definition (HD) MFSA Connectors Explained:

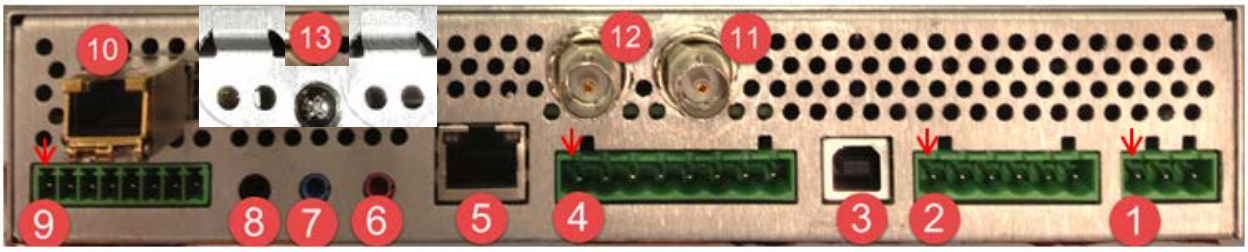

Figure 5 – Talon High Definition (Digital) MFSA Connector Interface (Front-View)

1. Power Input
    1. Input Power + (red arrow points to pin 1)
    2. Input Power –
    3. Input Power Ground

2. Relay Outputs

    Relay Outputs may be used to signal or control
    Resistive Load – 10A 250 VAC, 5A 30VDC

    1. Relay 1 Common (red arrow points to pin 1)
    2. Relay 1 Normally Closed
    3. Relay 1 Normally Open
    4. Relay 2 Common
    5. Relay 2 Normally Closed
    6. Relay 2 Normally Open

3. USB 2.0– Access port for Factory Support role.

4. Switch inputs
    1. Input 1 Signal (red arrow points to pin 1)
    2. Input 1 Ground
    3. Input 2 Signal
    4. Input 2 Ground
    5. Input 3 Signal
    6. Input 3 Ground
    7. Input 4 Signal
    8. Input 4 Ground

5. Down-line Input (RJ-45, 10/100 Fast Ethernet)

6. Audio Input – Optional Microphone Level – 3.5 mm TRS
7. Audio Input – Optional Line Level – 3.5 mm TRS
8. Audio Output – Optional Line Level – 3.5 mm TRS

9. Serial Communications
    1. RS485+ (red arrow points to pin 1)

2. RS485-
3. Ground
4. RS422 RX+
5. RS422 RX-
6. Ground
7. RS232 TX
8. RS232 RX

10. SFP Slot – Main GB Connection

11. Digital Video Output – Primary
12. Digital Video Input – Primary

13. Blank Plate – Covers Unused Secondary Video Port

1.1.3 Physical Ports & Interfaces

Physical Interface	Interface Description	Interface Type
BNC connector	Analog or Digital Video	Data in
BNC connector	RAW Video Loop back	Data out
3.5 mm TRS stereo jack (black)	Audio Line OUT	Data out
3.5 mm TRS stereo jack (blue)	Audio Line IN	Data in
3.5 mm TRS stereo jack (pink)	Audio MIC IN	Data in
SFP Module	Gigabit Ethernet	Data in / Data out / Control In / Status Out
RJ-45	Fast Ethernet	Data in / Data out
USB 2.0 type B serial port	Access port for Factory Support role	Data in / Data out / Control In / Status Out
Phoenix contact – 6 pin	Relay contact outputs	Data out
Phoenix contact – 8 pin	Sensor contact inputs	Data in
Phoenix contact – 8 pin	Multi-format serial port	Data in/ Data out
Phoenix contact – 3 pin	DC Power	Power
LEDs	Front and Rear	Status Out
Tamper Monitoring	Provides tamper mitigation	Control In

Table 5 – Physical Ports and Interfaces

1.1.4 Logical to Physical Interface Mapping & Function

FIPS 140-2 Logical Interface	Module Physical Interface	Information Type
Data Input	RJ-45, audio IN ports, signaling and video interfaces, SFP Module, 8-pin Phoenix contacts, Factory Maintenance Port (USB)	User management interface (configuration commands), Various types of IP data, various audio signals, various video signals, various types of IP data, various types of sensor, relays and serial data
Control Input	Tamper Monitoring	Internal to module, monitors cryptographic boundary for intrusion attempts and responds with zeroization when detected
Data Output	RJ-45, audio OUT ports, signaling and video interfaces, 8-pin and 6-pin Phoenix contacts, Factory Maintenance Port (USB)	Various types of IP data, various audio signals, various video signals, various types of sensor, relays and serial data, various types of console command & response data
Data Output	SFP Module	Cipher text data output (AES/HTTPS)
Control Input	Factory Maintenance Port (USB), SFP Module	Plain text control input (configuration commands), Ciphertext (HTTPS)
Status Output	LEDs, Factory Maintenance Port (USB), SFP Module	Visual status output, plain text status output (locally accessed logs), cipher text status output (remotely accessed logs)
Power	Power Input	N/A

Table 6 – Logical Interface to Physical Interface Mapping

1.1.5 Talon MFSA Visual Status Indicators (LEDs)

The Talon has five multi-color visual status LEDs and their meanings are explained here:

LED NAME	STATE	MEANING
POWER + ALL OTHERS	GREEN + RED	CRITICAL TAMPER RESPONSE HAS OCCURRED
POWER	OFF	NO POWER
POWER	GREEN	POWER APPLIED
HARDWARE STATUS	OFF	NO POWER
HARDWARE STATUS	GREEN	SELF TESTS PASSED, HARDWARE OPERATING NORMALLY
HARDWARE STATUS	RED	HARDWARE FAILURE
HARDWARE STATUS	AMBER	INITIALIZING
FIRMWARE STATUS	OFF	NO POWER
FIRMWARE STATUS	GREEN	SELF TESTS PASSED, FIRMWARE OPERATING NORMALLY
FIRMWARE STATUS	RED	FIRMWARE INTEGRITY CHECK FAILURE

LED NAME	STATE	MEANING
FIRMWARE STATUS	AMBER	INITIALIZING
CRYPTO ENGINE	OFF	NO POWER
CRYPTO ENGINE	GREEN	SELF TESTS PASSED, CRYPTO ENGINE PROPERLY INITIALIZED
CRYPTO ENGINE	RED	SELF TESTS FAILED, CRYPTO ENGINE FAILURE
CRYPTO ENGINE	AMBER	INITIALIZING
I/O INTERFACES	OFF	NO POWER
I/O INTERFACES	GREEN	SELF TESTS PASSED, PIC MCU OPERATING NORMALLY
I/O INTERFACES	RED	SELF TESTS FAILED, MCU NOT OPERATING NORMALLY
I/O INTERFACES	AMBER	INITIALIZING

Table 7 – Talon MFSA LED Indicators

Figure 6 – Talon MFSA LED Indicator for Tamper Response

1.2 Firmware and Cryptographic Functionality

The Talon MFSA is divided into four main functional areas as shown in Figure 7 which depicts the module's logical arrangement. While the entire Talon is within the boundary, its cryptographic functionality (algorithms, key handling, etc.) has been specifically segmented from the rest of the product functions to form a logical sub-boundary and is shown in the dotted **RED** area labeled ***SECURITY MODULE***.

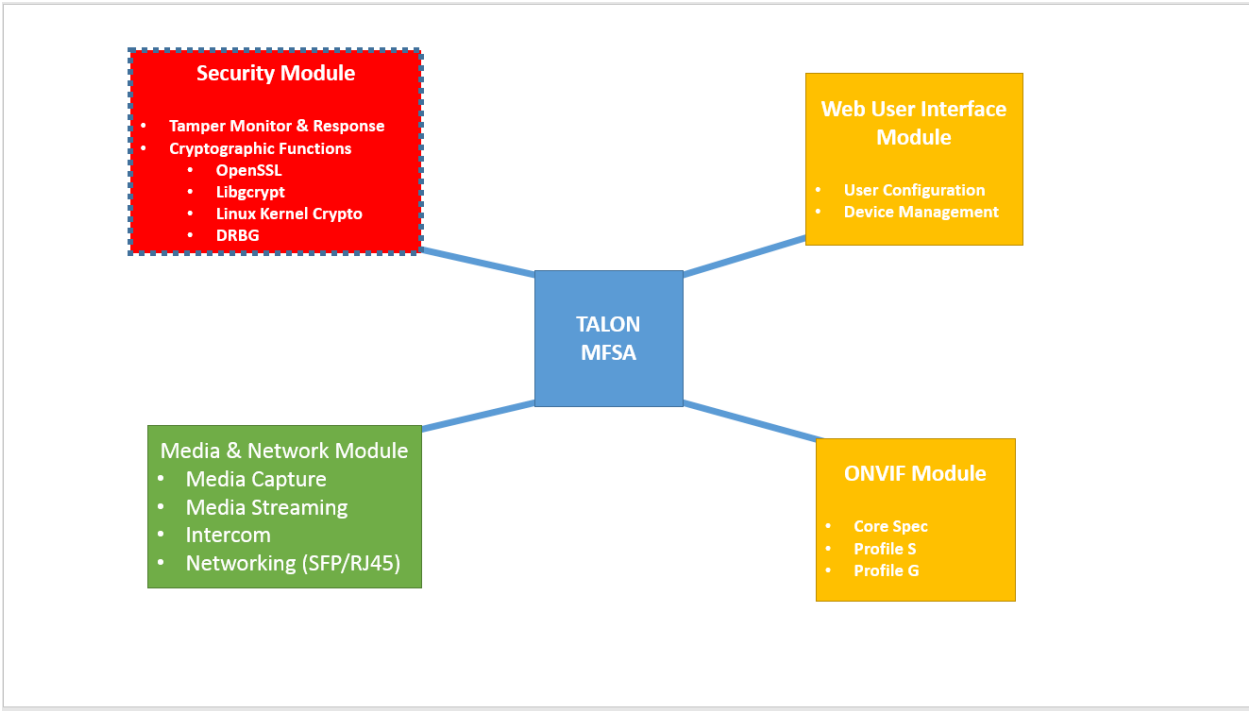

Figure 7 – Talon MFSA Logical Block Diagram

The Security Module handles all cryptographic functions of the product. It is responsible for initialization of the cryptographic module and enforcement of the product's tamper response mechanism. It is comprised of multiple firmware modules; other components of the Talon module that need to encrypt or decrypt data do so through internal API calls to the security module.

The Media & Network Module handles the low level hardware interfaces and drivers for using the physical ports and interfaces on the device. It also provides the media streaming, networking and intercom features of the product.

The Web User Interface Module handles all user configuration and device management functions. It allows for configuration of the media and network module, it represents the configuration and status of the device to the user.

The ONVIF (Open Network Video Interface Forum) Module handles all configuration and communication relating to compliance with the core specification as well as Profiles S (media streaming and control) and Profile G (stored media and retrieval).

1.3 Mode of Operation

The Talon MFSA is designed to only operate in an Approved mode of operation. The product is ordered as either a FIPS or NON-FIPS version of the product. When the product leaves the factory it is configured for one or the other mode and cannot be modified.

To verify that a module is in the Approved (i.e., FIPS) mode of operation and functioning normally (e.g., not in an error state), check the following indicators.

1) The model field label and firmware version should match one of the models specified in Tables 2 and 3; in particular the fourth field should always read FIPS as shown in the highlighted image below

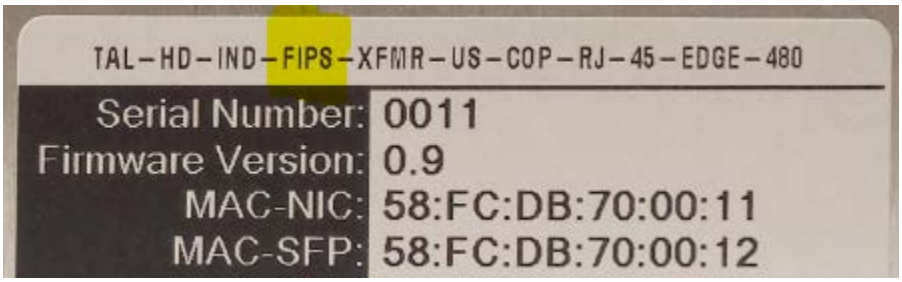

Figure 8 – Talon MFSA Product Labeling with Model Field

2) The tamper evident seals should not show ANY evidence of tamper
   a) Reference document # 030-00004-013 for visual inspection procedures
   b) This information is also available in section 5.1.1.
3) The "CRYPTO ENGINE" LED status indicator should be green
   a) Reference Table 6 & Figure 6 in this document for states and explanation
   b) Reference document # 030-00004-013 for operational procedures & required configuration steps
4) The Security Status Menu in the Web User interface should show FIPS running mode
   a) Reference document # 030-00004-013 for how to access and read this menu

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the table(s) below. This table sorts algorithms by the three algorithm implementations in use on the Talon MFSA which are Libgcrypt, Disk Encryption, and OpenSSL.

Algorithm	Description	Cert #
Libgcrypt		
DRBG	[SP 800-90A] Functions: HMAC DRBG using SHA-256 (no reseed) Security Strength: 256 bits	1135
HMAC	[FIPS 198-1] Functions: Generation (for HMAC DRBG and password hashing) SHA sizes: SHA-256 (for DRBG), SHA-512 (for pw hashing)	2550
SHA	[FIPS 180-4] Functions: HMAC SHA sizes: SHA-256, SHA-512	3235
Disk Encryption		
XTS-AES mode	[FIPS 197, SP 800-38E] Functions: Encryption, Decryption Key sizes: 256 bits (Note that XTS-AES mode is used only for storage of data on disk.)	3926
OpenSSL		
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: CBC Key sizes: 128, 256 bits	3924
DRBG	[SP 800-90A] Functions: CTR DRBG using AES-256 Security Strength: 256 bits	1134
HMAC	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1, SHA-256	2549
KDF (TLS)	[SP 800-135] Functions: TLS v1.0/1.1 KDF (Note that TLS v1.1 is not implemented; the KDF is the same for TLSv1.0 and TLSv1.1.)	780 (CVL)

Algorithm	Description	Cert #
KTS	[SP 800-38F §3.1] Function: Key Wrap, Key Unwrap Variant 1: AES-128-CBC and HMAC/SHA-1 Variant 2: AES-256-CBC and HMAC/SHA-1 Variant 3: Triple-DES TCBC (3-key) and HMAC/SHA-1	3924 (AES) 2153 (TDES) 2549 (HMAC)
RSA	[FIPS 186-4, ANSI X9.31-1998, and PKCS #1 v2.1 (PSS and PKCS1.5)] Functions: ANSI X9.31 Signature Verification, PKCS #1 V1.5 Signature Generation Key sizes: 2048 with SHA-256 (verify only), 3072 with SHA-256 (generate only)	2004
SHA	[FIPS 180-4] Functions: Signature Generation, Signature Verification, HMAC SHA sizes: SHA-1 (HMAC only), SHA-256	3234
Triple-DES (TDES)	[SP 800-67] Functions: Encryption, Decryption Modes: TCBC Key sizes: 3-key	2153

Table 8 – Approved and CAVP Validated Cryptographic Functions

2.1 Non-Approved but allowed Cryptographic Functions

The following table outlines the non-approved but allowed cryptographic functions.

Algorithm	Description
OpenSSL	
Non-SP 800-56A Compliant DH	[IG D.8] Diffie-Hellman 3072-bit (key agreement; key establishment methodology provides 128 bits of encryption strength)
MD5 within TLS	[SP800-135]
NDRNG	Ring-oscillator-based NDRNG within the i.MX6Q processor provides the CTR_DRBG with entropy. This entropy is sufficient for the module's strongest randomly generated keys. (DH-3072, which has 128 bits of strength).
Non-SP 800-56B Compliant RSA Key Transport (Encapsulation)	[IG D.9] RSA 3072-bit (key wrapping; key establishment methodology provides 128 bits of encryption strength)

Table 9 – Non-Approved but Allowed Cryptographic Functions

2.2 FIPS Mode Allowed Protocols

The following table identifies the protocols that are allowed in FIPS operating mode.

Protocol	Description
TLS v1.0	[IG D.8 and SP 800-135] Cipher Suites: TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
EAP-TLS	[IG D.9] Cipher Suites: TLS_RSA_WITH_AES_128_CBC_SHA

Table 10 – Protocols Allowed in FIPS Mode

The above protocols have not been reviewed or tested by the CAVP or CMVP.

Note that all instances of RSA and DHE are 3072 bits, providing 128 bits of encryption strength. If used, the Triple-DES cipher suite reduces the strength of keys loaded over TLS to 112 bits of encryption strength.

2.3 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 3.3.

CSP	Description / Usage
ENCRYPTED CSP KEY STORE	
MCU Master Key	AES-256 with 32-byte master key; Used to setup encrypted key store for all CSPs (AES Key Wrap). Uses OpenSSL library for encryption.
CONSOLE CLI ACCESS	
Factory Support Password	HMAC-SHA-512 encrypted password stored in cipher text; Used for login of the Factory Support role.
802.1X EAP-TLS	
EAP-TLS Master Secret	Master Secret; Generated during the session.
EAP-TLS Private Key	RSA 3072 length; Establishes EAP-TLS connections.
EAP-TLS Session Authentication Key	HMAC-SHA-1 key; Used for EAP-TLS session authentication.
EAP-TLS Session Encryption Key	AES128;

CSP	Description / Usage
	Used for session encryption.
HTTPS TLS	
HTTPS/TLS Master Secret	Master Secret; Generated during the session.
HTTPS/TLS Private Keys	RSA 3072 length; Establishes HTTPS connections.
HTTPS/TLS Session Authentication Key	HMAC-SHA-1 key; Used for HTTPS/TLS session authentication (including KTS).
HTTPS/TLS Session Encryption Key	AES128/256/Triple-DES triple key; Used for session encryption (including KTS).
OPEN-VPN	
TLS Master Secret	Master Secret. Generated during the session.
TLS Session Authentication Key	HMAC-SHA-1 key; Used for TLS session authentication.
TLS Session Encryption Key	AES128/256/Triple-DES triple key; Used for session encryption.
Server Private Key	RSA key 3072 length; Used for TLS and to communicate with VPN clients.
Diffie Hellman Private Key	DH key 3072 length; Used with TLS sessions for perfect forward secrecy.
OPEN-SSL	
CTR_DRBG Seed	Seed for NIST SP-800-90A DRBG with 256-bit AES
CTR_DRBG State	State variables (V and Key) for NIST SP-800-90A DRBG with 256-bit AES
User and CO Passwords	Pre-calculated HMAC-SHA-1 digests; Used for Crypto Officer and User role authentication.
LIBGCRYPT	
AES Key	AES256-XTS; Mode for data encryption and decryption. Serves hard drive encryption service
DRBG State	Internal HMAC DRBG state. Used at factory to generate AES-XTS keys.
DM-CRYPT	

CSP	Description / Usage
Libgcrypt DRBG Seed	2048 bytes of random data used to seed the HMAC DRBG which in turn generates the XTS key pair. Used to encrypt/decrypt data on optional HDD.

Table 11 – Critical Security Parameters (CSPs)

2.4 Public Keys

Key	Description / Usage
OpenVPN CA Certificate	RSA Length 3072; Used to establish VPN tunnel connections.
OpenVPN Server Certificate	RSA Length 3072; Used to establish VPN tunnel connections.
OpenVPN DH Parameters	Pre-generated Diffie Hellman 3072 parameters and ephemeral public key used by OpenVPN. Diffie-Hellman Parameters are used for perfect forward secrecy in TLS session keys once tunnel is established.
EAP-TLS Certificates	RSA Length 3072; Used to establish EAP-TLS connections.
HTTPS TLS Certificates	RSA Length 3072; Used to establish TLS connections.
Firmware Load Public Key	RSA Public Key 2048; Used to verify firmware integrity when updating to new firmware versions is attempted.

Table 12 – Public Keys

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports three distinct operator roles, User, Cryptographic Officer (CO), and Factory Support. The cryptographic module enforces the separation of roles using three distinct user interfaces each with their own authentication. The module interfaces separate out the services that are available to each operator role. Internal cryptographic functions (e.g. self-tests, key management, API calls and algorithm selections) are handled by the module firmware and are not controlled by any role. The cryptographic officer role can only configure security relevant parameters which feed into the firmware, such as uploading of certificates, setting passwords and configuring interfaces.

The purpose of the Factory Support role is to allow the USB2.0 Factory Maintenance Port to be used for advanced troubleshooting of fielded product with the Factory involved. This role is the only user that can log in via the CLI port and the role is a limited user with access only to necessary troubleshooting commands required for factory support (no CSP access). Note that, despite the name of the port, this is not a Maintenance role. The Crypto Officer and User roles cannot log in to the port.

Table 13 – Roles Description lists all operator roles supported by the module. The Module does not support a maintenance role and/or bypass capability. The Module supports concurrent operators by allowing User and CO operators to be logged into the web user interfaces at the same time, and by allowing Factory Support to also be logged in concurrently over the CLI interface. The authentication information is cleared by termination of the session. Termination of the session occurs at log out, or, for Web users, can also be timed out based on two minutes of inactivity in the interface. When an inactive session is terminated the operator is required to log back in to the module before any other actions can be taken. When a user logs in to the module the password entry is obscured. In the back end storage, the user password information is stored in hashed form and uses HMAC-SHA-1 (Web UI) or HMAC-SHA-512 (Serial CLI) for authentication verification by comparing the user presented data for the log in attempt to the stored hash value.

All authentication data is stored in RAM which is wiped out as part of either the shutdown or reboot functions. If the user executes a “clean” shutdown this happens prior to removal of power or reboot, however if a "dirty" shutdown occurs (e.g. power is removed during run time) then it happens when the board is initializing and prior to accepting any authentication attempts.

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer – This role has access to all administrative features and services of the module.	**Identity-based, Single Factor**	Username, Password, Identifying information
User (U)	User – This role has access to limited administrative features and services of the module. This role has no access to security relevant features.	**Identity-based, Single Factor**	Username, Password, Identifying information

Role ID	Role Description	Authentication Type	Authentication Data
Factory Support (F)	This role has access to limited user features and services of the module. This role has no access to security relevant features. This role has access to log in to the external USB 2.0 console CLI.	**Identity-based, Single Factor**	Username, Password, Identifying information

Table 13 – Roles Description

3.2 Authentication Methods

Single Factor Authentication

The module supports single factor authentication combining a username and password. The user's ID and enrolled information is used as the identification for identity-based authentication. The password is 8-30 characters long. Log in attempts to the module are tracked in the system logs for failures or success.

Probability	Justification
Single Factor Authentication provides a false acceptance rate of 1 in 2.18 x 10^{14}, which is less than 1 in 1,000,000.	Password is enforced at a minimum of 8 alphanumeric characters so it is 1 in (26*2+10)^8, which is less than 1 in 1,000,000.
Single Factor Authentication provides a false acceptance rate of 1 in 1.09 x 10^{13} within a one-minute time span, which is less than 1 in 100,000.	The module implements purposeful time delay of 3 seconds after 1 failed attempt, giving a maximum of 20 attempts per minute. Probability of false authentication in 1 minute is 20 in (26*2+10)^8, which is less than 1 in 100,000.
The total number of failed log in attempts in five minutes cannot exceed 30.	To provide additional security the number of successive failed log ins in a five-minute period is tracked. When this value exceeds 30 the module responds with zeroization of runtime CSPs (stored as plaintext in RAM) for the session, halts operation and requires a power cycle to restore operation. This zeroization does not destroy the master key so requires successful authentication to occur post reboot.

Table 14 – Authentication Description & Strength

3.3 Services

All services implemented by the Module are listed in the table below. The Module supports concurrent operators by allowing each operator to be logged into the web user interface at the same time, yet the module provides for this by making each log in its own independent session and it separates the privileges as shown in the table below.

Service	Description	CO	U	F
WEB UI (general)	The system provides a distinct web user interface for each role, both protected by TLS.	X	X	
	Inputs: UI navigation commands			
	Outputs: UI pages			
WEB-UI Status→ All sub menus	Shows overall status of the module services and functions. This uses no CSPs.	X	X	
	Inputs: UI navigation commands			
	Outputs: Module status, services, functions			
WEB-UI System	Allows configuration of module host name and time parameters. This uses no CSPs.	X	X	
	Inputs: New host name & time parameters			
	Outputs: Confirmation or rejection of new parameters			
WEB-UI System → Administration	Allows configuration of user level password.		X	
	Inputs: New password			
	Outputs: Confirmation or rejection of new password			
WEB-UI System → Scheduled Tasks	Allows configuration of tasks attached to timers. This uses no CSPs.	X		
	Inputs: Timer configuration information			
	Outputs: Confirmation or rejection of configuration			
WEB-UI Services	Allows miniDLNA media sharing service to be configured. This uses no CSPs.	X	X	
	Inputs: miniDLNA config information			
	Outputs: Confirmation or rejection of configuration			
WEB-UI Network	Allows networking parameters and interfaces to be configured and basic diagnostics to be performed. This uses no CSPs.	X	X	
	Inputs: Network configuration information			
	Outputs: Confirmation or rejection of configuration			
WEB-UI Network → Firewall	Allows system firewall to be configured. This uses no CSPs, but controls routing of data over the secure VPN tunnel.	X		

Service	Description	CO	U	F
	Inputs: Firewall configuration information			
	Outputs: Confirmation or rejection of configuration			
WEB-UI Talon → Camera, GPIO, Audio, Virtual Serial, Edge Storage, User Manual, Scene Authentication	Allows hardware (non-security relevant) features of the module to be configured. These all use no CSPs.	X	X	
	Inputs: Hardware configuration information			
	Outputs: Confirmation or rejection of configuration			
WEB-UI Talon → Security	Allows all security relevant features of module to be configured.	X		
	Inputs: Security functionality configuration			
	Outputs: Confirmation or rejection of configuration			
WEB-UI Talon → Backup System & Upgrade System	Allows unit backup and restore functions as well as signed firmware upgrades.	X		
	Inputs: New firmware image (optional)			
	Outputs: Backup image; or FW load confirmation/rejection			
WEB-UI Talon → Poweroff / Reboot	Allows the module to be halted for power removal or rebooted. This uses no CSPs.	X		
	Inputs: Poweroff command			
	Outputs: None			
WEB-UI Talon → Log out	Allows the authenticated session to be logged out. Applies individually to the logged on user and closes the session. This uses no CSPs.	X	X	
	Inputs: Logoff command			
	Outputs: Logout confirmation			
Serial Console	Allows the factory user to enter the Linux console shell locally. Note: The factory user can log in but has only limited user rights (e.g. no root access, CSP access aside from own password, or firmware loading) and the Crypto Officer or User cannot log in.			X
	Inputs: Console commands			
	Outputs: Console command responses			

Table 15 – Authenticated Services (CO,U & F)

3.3.1 Unauthenticated Services

The module offers very few unauthenticated services. These are captured in the following table.

Service	Description
Module Reset (Self-test)	Reset of the Module by removal of external power.
Login	Authenticates the operator and establishes secure channel.
Show Status	External LEDs (rear or top) which indicate the status of one or more device interfaces.
Tamper Monitoring	The module continuously monitors for intrusion events and will zeroize even if nobody is logged in whenever a critical tamper state is detected.
RTSP	This service applies username/password with digest authentication as an additional layer of security to restrict access to device audio and video data. This uses no CSPs and is not treated as operator authentication. Inputs: Authentication data Outputs: Authentication confirmation or rejection
ONVIF	This allows remote configuration and device management for non-security relevant video and audio features of the device. This uses no CSPs and is not treated as operator authentication. Inputs: Configuration information Outputs: Confirmation or rejection of configuration
Internal API calls	Internal features and function calls that have no external user configurability or access.
Decommission	Decommission the module, inducing zeroization. (See Section 8.1.2 for details.)

Table 16 – Unauthenticated Services

3.3.2 CSP Access Rights

Table 17 – CSP Access Rights within Services defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.

- X = NONE
- Z = Zeroize: The module zeroizes the CSP.

Service	CSPs											
	MCU Master Key	Factory Support Password	HTTPS/TLS Master Secret, Session Authentication Key and Session Encryption Key	HTTPS/TLS Private Key	802.1X EAP-TLS Master Secret, Session Authentication Key and Session Encryption Key	802.1X EAP-TLS Private Key	OpenVPN Session CSPs, Master Secret, DH Private Key	OpenVPN Server Private Key	OpenSSL CTR_DRBG CSPs	User and CO Passwords	Libgcrypt AES Key	Libgcrypt DRBG Seed, State
Internal API calls	E	X	G, E	E	G, E	E	G, E	E	E	E	G, E	E
Login	X	E, W	X	X	X	X	X	X	X	E, W	X	X
WEB UI (general)	X	X	E	E	E	E	X	X	X	X	X	X
WEB-UI System →Administration	X	X	X	X	X	X	X	X	X	E, W	X	X
WEB-UI Talon → Security	X	X	X	W	X	W	X	W	X	X	X	X
WEB-UI Talon → Backup System & Upgrade System	X	R, W	X	R, W	X	R, W	X	R, W	X	X	R, W	X
Serial Console	X	W	X	X	X	X	X	X	X	X	X	X
Tamper Monitoring	X	X	Z	X	Z	X	Z	X	Z	X	X	Z
Decommission	Z	X	Z	X	Z	X	Z	X	Z	X	X	Z

Table 17 – CSP Access Rights within Services

Note 1: Services not listed in the table above do not access any CSPs.

Note 2: The keys not zeroized by the Tamper Monitoring service are protected by the MCU Master Key and rendered unrecoverable upon Master Key zeroization.

4 Self-tests

Each time the Module is powered up, it fetches the MCU Master Key from the MCU. If this fails, the module cannot decrypt the CSP key store and executes tamper response. The module also tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. If any of these fail, the Module enters Critical Error State and will attempt to reboot itself to start the entire sequence over. If successful, the Module verifies the integrity of the firmware image. If this fails, the Module enters Critical Error State and will attempt to reboot itself to start the entire sequence over. Critical Error State reboots are tracked and if three unsuccessful attempts occur the board will stop trying and halt with tamper response indication set. If the AES-XTS fails, the error happens in the kernel and will induce the Emergency Halt State.

Self–tests are available on demand by power cycling the module or initiating a module reboot from the user interface.

Each of the individual software libraries in use by the module are already FIPS validated in their own right and the Module implements self-tests in accordance with their documented APIs or the self-test are self-contained within the library (e.g. library won't work unless self-test passes).

On power up or reset, the Module performs all self-tests described in Table 18 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the Critical Error state.

Test Target	Description
OpenSSL Self-Tests	Provides KATs for each algorithm implemented. Encrypt and decrypt tests. Provides DRBG self-test. Provides Software Integrity test using KAT, HMAC-SHA256. **AES:** encryption and decryption with 128-bit key **Triple-DES:** encryption and decryption with three keys **RSA:** sign and verify KATs **HMAC:** HMAC-SHA1, SHA-256 **DRBG**: CTR_DRBG, AES 256 with and without derivation
Libgcrypt Self-Tests	Provides KATs for each algorithm implemented. Provides Software Integrity test against the binary. **HMAC:** SHA-256, SHA-512 **DRBG:** HMAC 256
Hard Drive Self-Test	**AES-XTS:** encryption and decryption with 512 key size (AES 256 x2)
Firmware Integrity	**HMAC**: HMAC-SHA-256 verification of firmware image. (HMAC key is not a CSP)

Table 18 – Power Up Self-tests

The module performs the following additional conditional self-tests during operation as shown in Table 19 – Conditional Self-tests.

Test Target	Description
DRBG	DRBG Continuous Test performed when a random value is requested from the CTR DRBG. (The same test is implemented for the HMAC DRBG, however this DRBG is not used after the module leaves manufacturing.) Entropy input to OpenSSL tested with the same test. (OpenSSL's CTR DRBG is the only DRBG in use in the field, so this tests all outputs from the NDRNG.)
NDRNG	NDRNG Continuous Test is performed whenever the CTR DRBG is seeded. (The NDRNG is used only to seed the CTR DRBG.)
Firmware Load	RSA 2048 signature verification performed when firmware is loaded.
DRBG Health Checks	Performed conditionally per SP 800-90A Section 11.3.

Table 19 – Conditional Self-tests

The module also performs the following critical function tests.

Test Target	Description
MCU Master Key Retrieval (power up)	Verification of no power off tamper or previous power on tamper states and successful communications with tamper monitoring before decrypting and unpacking CSPs for device initialization.
Electronic Key Entry	Electronic Key Entry Test is performed whenever a key, certificate or security parameter is uploaded to the device via the user interface. The key entry test validates the size of the file and the type of file against what the user has uploaded.

Table 20 – Critical Function Self-tests

5 Physical Security Policy

The Module provides FIPS140-2 Level 2 compliance for secure data transmission and cryptography. In order to maintain the security that the device provides, the crypto officer (or other cognizant administrator) must ensure the following steps are taken:

Upon receipt of the device and prior to secure operation, the device should be visually inspected to determine if the device is ready to operate securely. There are two items that require visual inspection: the first are the tamper evident seals (two) and the second is the Cryptography Engine light emitting diode (LED) indicator. These are discussed below, along with other physical security procedures.

5.1.1 Tamper Evident Seals Inspection

Each device has a unique serial number applied to the tamper evident labels, which will look similar to this:

Figure 9 – Talon Tamper Evident Seal

When the device is first received these labels should be visually inspected to ensure that there is no evidence of tampering. The serial number from the device tamper label should be recorded and stored in a safe area. In the future, upon whatever interval is required by internal processes, the device should be re-inspected for evidence of tamper and the original numbers should be compared to recorded ones from future inspections to ensure no differences exist.

To inspect the seals, the device should be with power off and the operator should view both seals from all angles to read the serial number and determine that no evidence of tamper exists.

The two tamper evident seals are placed on the sides of the device in the following locations noted in the figure below:

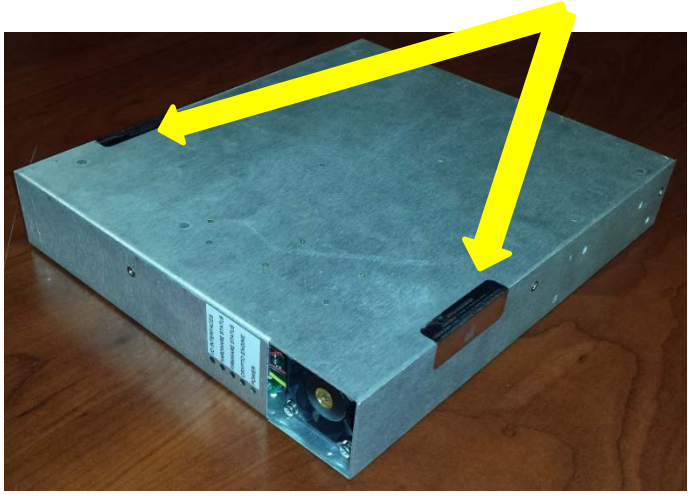

Figure 10 – Talon Tamper Evident Seals Applied

Examples of tampered product seals are shown in the figures below:

Figure 11 – Tampered Product Seal #1

Figure 12 – Tampered Product Seal #2

Figure 13 – Tampered Product Seal #3

If the seals appear tampered on either side (top/bottom) or appear like they have been removed and re-applied, the device should be taken out of service until the CO can log in and ascertain the ongoing security of the device and rotate any critical security parameters.

5.1.2 Cryptographic Engine Light Emitting Diode (LED) Inspection

To inspect the Cryptography Engine LED, the device should have power applied. The LED can be viewed from either the top or rear of the module.

The following figure depicts both viewing orientations. The proper LED to inspect is labeled 'Crypto Engine'.

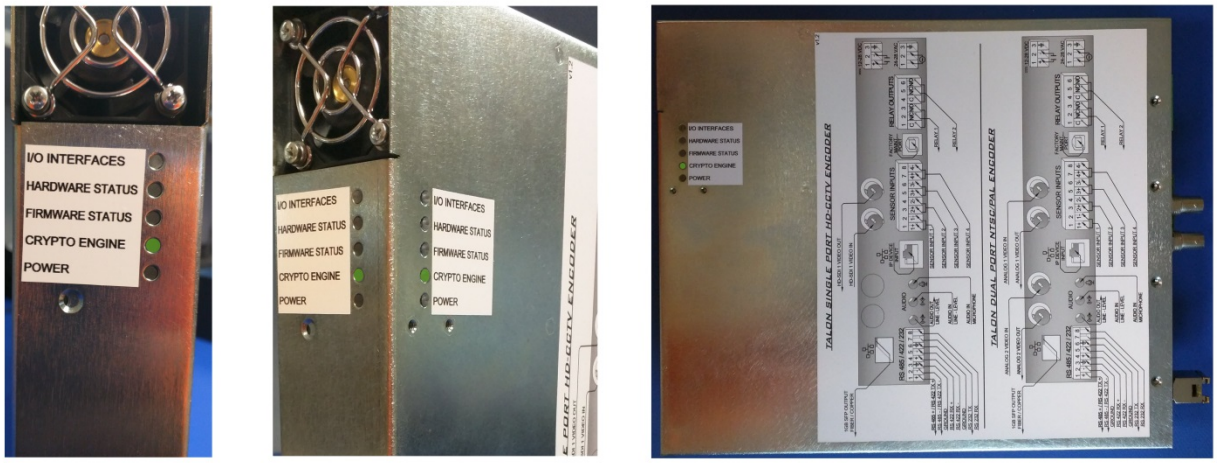

Figure 14 - Cryptography Engine LED Indicators

The operator should see a green LED. This indicates that the board has not detected any external intrusions and that the Cryptography Engine has successfully completed all of the built in power on self-tests (POST) and the unit is initialized and ready to securely transmit data. If the LED indicator for the cryptography engine is ANY other color, verification of the cryptography functions has been unsuccessful or the device's secure perimeter has been violated. In either of these cases, the device should be taken out of service and returned to the factory for inspection and re-initialization.

5.1.3 Routine Inspection and Test

It is recommended that periodic physical inspections of the device, tamper evident seals, and status indicators occur. Furthermore, operational and functional tests of the device should also be performed in accordance with time intervals defined by local policies, processes, and procedures applicable to the environment where the device is being operated.

5.1.4 Battery

The Module is equipped with an internal non-rechargeable battery that allows the device's physical security features to operate while there is no external power being supplied to the device. The amount of time left on the battery can be monitored from the Module web interface in the **B**attery menu. Additionally, there is an icon to the right of the header menus that displays the current battery status. When the battery life is at an acceptable level the icon will be green and read BATTERY HEALTHY. When the battery drops below the thresholds discussed below, the icon turns red and reads OUT OF BATTERY.

Warning! If the Talon's battery is allowed to run down, the device can no longer monitor its intrinsic security features during power off situations. Once this occurs, the Module undergoes zeroization and must be returned to the factory for re-initialization.

The battery's current status should be checked on a monthly basis—or more often if so desired—and the lifetime days remaining logged. When the battery days remaining falls to 7 days or less OR if the battery lifetime days remaining reaches 70 days or less, the Module logs will show constant alerts and a notification banner will be displayed on the Module web interface. Once this occurs, the operator should contact support so that factory maintenance can be performed on the device to ensure continued secure operations. Should the battery completely die the device will treat this as a critical tamper situation since the intrinsic security features can no longer be monitored in power off situations and it will execute tamper response.

It is also possible that a Talon's battery could be completely discharged if too much time passes between its initialization at the factory and when it is deployed on site. Deployment should take place within 30 days once a Talon is shipped from Open Roads or the device should be connected to external power to prevent complete battery discharge.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	3 months	Refer to section 5.1.1
Device Battery	1 month	Refer to User Guide

Table 21 – Physical Security Inspection Guidelines

5.1.5 Components Quality

The module is produced with either commercial or industrial grade components capable of meeting a minimum of commercial specifications for power, temperature, reliability, shock and vibration.

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

While not meeting Level 3 physical security, the module does provide tamper response functionality within its shielded secure area. Attempts to remove the cover from this area will trigger the mechanism, which zeroizes the MCU Master Key.

8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The module provides three distinct operator roles: User, Cryptographic Officer, and Factory Support.
2. The module provides identity-based authentication.
3. The module clears previous authentications on power cycle. (All session-based authentication data is stored in volatile memory.)
4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
5. The operator is capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output is inhibited during power-up self-tests, module zeroization, and error states. Data output is logically disconnected from processes performing key generation, conditional self-tests, and individual key zeroization.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The module uses an SP-800-90A DRBG, which does not use the seed / seed-key input format.
10. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
11. The module does support concurrent operators.
12. The module does not support a maintenance interface or role.
13. The module does not support bypass capabilities.
14. The module does not support manual key upload for security relevant features. The module does support electronic key entry through the web user interface.
15. The module uses external audio/video devices for entry of audio/video data. The module does not have any external input/output devices used for entry/output of other data (e.g., key loaders).
16. The module has no CSP feedback to operators.
17. The module enters plaintext CSPs only during the initial HTTP key loading; this must be performed over a direct physical connection (i.e., Manual Distribution of keys). The module does not output plaintext CSPs.
18. The module does not output intermediate key values.
19. The module does not have user serviceable internal components and is bordered by a strong tamper resistant enclosure capable of zeroization of CSPs.

8.1 This section documents the security rules imposed by the vendor.

1. The module does not support the update of the logical serial number or vendor ID.

2. If the module remains inactive in any valid role for a maximum period of 2 minutes, the module automatically logs out the operator.
3. After thirty consecutive unsuccessful password validation attempts have occurred within a five-minute period, the module shall enforce a run time zeroization of CSPs for that session in order to add further time delays and interruption of service to a would be attacker's attempt. This state requires a hard power reset, re-initialization and then returns to authentication input.

8.1.1 Configuration Requirements to Maintain Security of Module

The internal cryptographic implementation of the product is not externally configurable or controllable by the operator and therefore none of these configuration options affect the Module's validated status.

However, the Module does implement multiple different security relevant features which use this validated cryptography. Not all features are required for every operational environment. The Crypto Officer only needs to configure those security items relevant to the use of the Module in their operational environment. The CO should refer to the Module User Guide for detailed instructions on how to accomplish these tasks.

Table 20 documents the security relevant features of the Module, their default state and whether they are **MANDATORY** or *RECOMMENDED* to maintain the Module security.

Test Target	Description
Configure User Access	The Module comes with published and well known default user accounts and passwords. It is **MANDATORY** for the CO to change the passwords and/or account names to maintain the security of the Module.
Configure TLS Interface	The Module comes with default certificates and keys to establish and use the TLS based web user interface. It is *RECOMMENDED* that the CO establish keys and certificates to enhance the security of the default Module.
Configure 802.1X Interface	The Module does not come with default certificates and keys to establish and use the 802.1X interface. It is **MANDATORY** that the CO establishes keys and certificates to operate this feature of the Module, IF 802.1X is part of the intended operational environment of the product.
Configure VPN Interface	The Module does not come with a default configuration for the VPN interface. It is **MANDATORY** that the CO establishes keys and certificates to operate this feature of the Module, IF the VPN is part of the intended operational environment of the product.
Configure IP tables with VPN Interface	The Module comes with a default configuration for IP tables and routing of network traffic. It is **MANDATORY** that the CO configures the IP tables of the Module, IF the VPN is part of the intended operational environment.

Table 22 – Module Configuration Requirements

8.1.2 Decommissioning the Unit via Procedural Zeroization

When the module has reached end of service life or if the Cryptographic Officer (or other cognizant security official) wishes to decommission the unit the following steps must be taken in order to perform this function.

NOTE: This procedure MUST be executed while the operator is in control of the module and physically present to observe that the method has completed successfully.

1) Remove the outer tamper evident seals with a flat edged tool, for example an X-ACTO knife. Ensure that tamper evidence is left behind like is shown in figures: Figure 11, Figure 12and Figure 13
2) Ensure that the unit has power and that all LEDs are green.
3) Remove all of the outer screws (9) with a Philips head screwdriver
4) Lift the module cover upwards ensuring separation of the two pieces of the cover make physical separation.
5) Observe that all LED indicators go to solid red indicating a tamper condition has occurred as shown in Figure 6.
6) Power off the unit.
7) Re-apply power to the unit and ensure that it boots up to a state where all LED indicators are RED as shown in Figure 6.
8) Decommissioning via procedural zeroization is completed.

9 References and Definitions

The following standards are referred to in this Security Policy.

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[SP-800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[IEC 60950-1]	Information Technology Equipment – Safety - :2005 (Second Edition) + Am 1:2009 + Am 2:2013; CB Scheme
[FCC 47 CFR part 15 Class B]	Federal Communications Comission, Title 47 Code of Federal Regulations, Radio Frequency Devices
[IEC-61000-4-2, Level 1]	International Electrotechnical Comission, ESD
[ONVIF Profiles S & G]	Open Network Video Interface Forum, Profile S for video streaming, Profile G for edge storage and retrieval
[CE]	Conformité Européene, European Union
[RoHS]	Restriction of Hazardous Substances

Table 23 – References

Acronym	Definition
CAVP	Cryptographic Algorithm Validation Program
CBR/VBR	Constant or Variable Bit Rate
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standards
HD	High Definition
HD-SDI	High definition serial digital interface
KAT	Known Answer Test
MFSA	Multi-Function Security Appliance
NTSC/PAL	National Television System Committee/Phase Alternating Line
ONVIF	Open Network Video Interface Forum
P/N	Part Number
SD	Standard Definition

Table 24 **– Acronyms and Definitions**