

The **Cyber Hardened** Advantage For Your Transmissions

The **Cyber Hardened IBUC** version takes the Block Upconverters to the next level:

- Prevents Cyber Attacks and malicious activity.
- End-to-End Embedded Encryption, Authentication, and Privacy.
- User Interface Enforcing Cyber Safety measures and best practices.
- Strong passwords are supported and required. No user is allowed to have a weak password.

Cyber Hardened Features

- » **SSHv2 (Secure Shell):** A cryptographic network protocol offering command line management interface by securing and encrypting the connection.
- » **SNMPv3 Interface:** An interface providing privacy, authentication, & access control. This enables flexible multi-level security management control & secret-key authentication that assures end to end message transmission delivery will not be altered or replayed.
- » **HTTPS:** Safe access to webpages using HTTPS (Secured HTTP) with encrypted connections.
- » **XSS Protection:** Protecting your system from Cross-Site Scripting Attacks.
- » **Secure Firmware Upgrades.**

Applications

The **Cyber Hardened Core IBUCs** are full-featured Intelligent Block Upconverters embedded with the highest Cyber Security Standards in the SATCOM industry. Their layers of encryption and authentication protocols solve the security issues related to any typical Ethernet device.

Our units are designed for long lifetime performance in demanding environments and remote terminal performance optimization. As a result, the Cyber Hardened IBUCs are perfect solutions for mobile defense terminals operating in demanding environments, ground stations, commercial use, and any other applications with safe transmissions requirements.

C-Band | X-Band | Ku-Band | Ka-Band **Cyber Hardened Core IBUCs**

The new high-end **Cyber Security** feature for your IBUCs



New
Transmit
Redundant
System Tx 1:1

New
Receive
Redundant
System Tx 1:1

Multi-Orbit
and
Multicarrier
Application

GaN
or
GaAs
Tech

3
Year
Warranty

THE ULTIMATE MANAGEMENT & CONTROL

- » 70+ User Configurable Thresholds & Alarms «
- » Local Web Interface & NMS-Friendly SNMPv3 «
- » Embedded Web Pages for Universal Web Browser Access «
- » Performance Trend Analysis Tools Entries & Statistical logs «
- » Upgraded Statistics and Event Log with 1,000 Sensor Readings «

The **Cyber Hardened Core IBUC** versions have embedded new high-end Cyber Security features, from hardware to software, including a new controller board and the new firmware.

Frequency Ranges Available

C-Band, X-Band, Ku-Band, and Ka-Band The Cyber Hardened IBUCs are available in all our frequency Bands.

Management Interface / Monitor & Control

Ethernet via RJ45 Connector

- » Command Line Interface SSH v2 and Serial Port (Baud rate: 115200 bits/s)
- » Web HTTPS (Secured HTTP with encrypted connections)
- » SNMP v3 with USM and VACM

Accounts

- Users** 20 users by default
- Lock out** 3 consecutive failed attempts
- Unlock period** 15 minutes
- Levels**

Two Account Levels	Functionality
- Administrator	Full reading & editing
- Operator	Read-only

Passwords

- Customizable for each user** The default password works for the first login only. After that, the system forces the password change.
- Strength**

Minimum Requirements:

 - 15 Characters
 - 1 Upper Case Character
 - 1 Lower Case Character
 - 1 Special Character (Examples: *%&@_ - ^ " \$ = +)
 - 1 Number
- Change History Password Change** 10 Level
At account Setup
Customizable minimum number of days for password change.

Encryption Algorithm

- AES** Key size of 192+ bits
- RSA** Key Size of 2048

Hashing Algorithm

- SHA2** Hash size of 256

Security Protocols

- TLS** v1.2
- SSH** v2
- SNMP** v3 with USM and VACM

Restoration

- Configuration** Text File

Web Server

- Protocol** HTTPS
- Security** TLS v1.2
- Port** 443
- HTTP security header** Enabled
- XSS Protection** Enabled
(Cross Site Scripting)

Login Sessions

- Max Limit of Concurrent Sessions (SSH and Web)** 5
- Number of failed attempts to disconnect** 3
- Idle Timeout (SSH and Serial)** 15 minutes
- Incomplete or Abandoned Timeout** 60 seconds
- Login Banner (SSH, Web and Serial)** Enabled
- Last Login Message** Date, time and port/IP Address of access.
- Failed Login message** Number of failed attempts.

Firewall

- Type** Linux based nftables
- Blocks** All ports except: SSH (22), SNMP (161, 162), HTTPS (443) and Firmware Upgrade (8080).

Time

- Configuration** Two NTP Servers Providing Redundancy or Manual
- Timezone** Configurable

Customizable Specifications

For additional and customized specs, contact us using the contact info below.

Monitor & Control - For Standard units and Cyber Hardened IBUCs

Item / Feature	Standard IBUC Versions	Cyber Hardened IBUC Versions	Via
Ethernet	HTTP (No Data Encryption Implemented)	HTTPS (Encrypted Connections Implemented)	RJ45 Connector
	Telnet	SSHv2	
	SNMPv2c	SNMPv3 with USM and VACM	
RS232	✓	✓	
RS485	✓	✗*	MS-Type Connector
Handheld Terminal	✓	✗*	
FSK	✓	✗*	Multiplexed on TX IFL
XSS Protection (Cross Site Scripting)	✗	✓	RJ45 Connector
Two NTP Servers Providing Redundancy	✗	✓	
FIPS 140-2 NIST compatible	✗	✓	NIST Standard

* **Cyber Hardened IBUC** units do not support HTTP, RS485, Handheld Terminal, and FSK to enhance Cyber Security.

Note: This Datasheet refers exclusively to the cyber security features involved in the **Cyber Hardened IBUC** units. Please refer to the other IBUCs' datasheets for further technical information regarding RF specs, including their particular Frequency Ranges, Input signals, Connectors, Gain, RF Output, Output Power (both Linear and Saturated), Power Supply, SSB Phase Noise, Operational temperature, and further details.