TERRASAT Communications, Inc
Engineered to Endure.

315 Digitial Drive Morgan Hill, CA 95037
+1 (408) 782-5911
Sales@TerrasatInc.com
www.TerrasatInc.com

Tightening Cybersecurity in SatCom Ground Terminals with Cyber Hardeneded IBUCs

2021 White Paper

Spring 2021

Abstract

LEADING THE WAY FOR CYBERSECURITY BLOCK UPCONVERTERS

With cybersecurity threats spreading throughout industries worldwide, it is up to the leaders in the satcom supply line of ground terminal equipment to address and integrate cybersecurity protocols and advancements to safeguard critical communications. With seemingly many options available in Block UpConverters, only Terrasat Communications' new Cyber Hardened Intelligent IBUCs meet the requirements for optimized cybersecurity enhancements while maintaining their well-known reliability and superior performance. The purpose of this white paper is to educate the benefits cybersecurity and integrating Terrasat's enhanced Cyber Hardened IBUCs with ground satcom terminals as well as provide an example of a successful installation in partnership with Airbus Space and Defence division.

"....many BUCs on the market could be successfully "hacked" in a few minutes. The new cyber hardened IBUCs will effectively implement security management control & assures that end to end message transmission delivery will not be altered."

MIKE GOLD, REGIONAL VP, AMERICAS & ISRAEL REGION

HOW CYBERSECURITY BECAME A STRATEGIC PRIORITY FOR SATCOM INDUSTRIES WORLDWIDE

Today, cybersecurity remains a hot topic and driving force of transformation in satellite communications with many industries facing sophisticated attackers motivated by money from industrial espionage and ransomware attacks. The most notable example, Operation Cloud Hopper, was a wake-up call for telecom service providers.[1] Launched in 2017, a cyberespionage group attacked managed service providers through their telecom service to divert targeted corporate assets and high value data. The attackers infiltrated the cloud-based systems of the managed telecom and technology providers and then hopped into the targeted client systems. The telecom system was the weakest link, and the attackers exploited the service providers. Operation Cloud Hopper has shaken up the industries by demonstrating the cost of improper security with damage to critical assets.

Commercial industries are not the only segments facing uncertainty within the evolving world. Military and government sectors are also frequently targeted by nefarious actors. According to a recent Chatham House study, US and NATO command and control systems are open to compromise because of vulnerabilities in the satellite systems carrying mission-critical data.[2] Cyberattacks on satellites are said to have the potential to wreak havoc on strategic weapons systems and undermine deterrence by creating uncertainty

and confusion.[2] Ground stations are far from immune to attack and can also be targeted if proved to be the weaker link.

The satellite communication industry collectively, at every stage of the supply line, shares the responsibility to take actions to mitigate vulnerabilities and protect critical end-to-end data connectivity through integrating cybersecurity standards and protocols. Data breaches caused by malicious attacks are said to be responsible for 51% of data breaches in 2020.[3] Whether it is about corporate espionage, ransom demands, or defense, a threatening agent will study a system and its supply chain for vulnerabilities and cause a chain reaction of interception, manipulation, and suspension of industry assets. Independent studies have also estimated that the average cost of a malicious data breach by the average malicious attack is around $4.27 million USD[2]. Lowering the risk of cybersecurity violations is not only a task of these organizations and states but a priority for the satcom supply line worldwide.

THE VULNERABILITIES OF RF AT THE GROUND STATION

SatCom ground terminals were not designed for anticipating remote cybersecurity vulnerabilities. Design features were largely based on a closed network model with security at the data level. But as the Cloud Hopper case strikingly demonstrates, the ground station can become the weakest link because of this common oversight. Today, many terminals either carry smart BUCs or simple BUCs, commonly referred to as “dumb BUCs” by many in the industry.

THE DIFFERENCES BETWEEN SIMPLE BUCS & SMART BUCS

Simple BUCs may have minimal access points. However, this exposes a large weakness for physical attacks and disruptions at the ground terminal level. In fact, many simple BUCs on the market can be successfully hacked in a few minutes because of the exposed hardware ports and low-security clearance levels. On the other hand, there are ground terminals with integrated smart BUCs, Block Upconverters with various points of access from serial to Ethernet ports. Smart BUCs do have an added level of protection compared to simple BUCs. But when it comes to nefarious actors armed with the tools and know-how of terminal vulnerabilities, the best level of options for industries is to tighten security for critical data by optimizing cybersecurity countermeasures and protocols as the complexity of cybersecurity continues to evolve.

Almost every component in the satellite communications link is addressable via IP technology. Most of the equipment in the communications chain has hardened to prevent security intrusions by outsiders. Unfortunately, although BUCs have updated to allow access via ethernet/IP technology, almost all BUCs have relatively simple password protection. With over 15 years of engineering premium reliable and superior performance BUCs, Terrasat Communications has released a line of Cyber Hardened Intelligent BUCs to increase satellite ground terminal security for industries who need optimized flexible protection.

The race to upgrade terminal equipment to modernize with cybersecure terminal equipment has proven to give industry leaders an advantage in an uncertain world.

AIRBUS UPGRADES WITH TERRASAT

Airbus is an international reference in the aerospace sector who designs, manufactures, and delivers industry-leading commercial aircraft, helicopters, military transports, satellites, and launch vehicles. Airbus also provides data services, navigation, secure communications, urban mobility, and other solutions for customers on a global scale. Industry leaders, such as Airbus Defence and Space, rely on secure multileveled connectivity performance and reliability to integrate into their extensive portfolio. With the challenge of optimizing cybersecurity for critical ground satellite terminals, Airbus in partnership with Terrasat Communications detail the challenge and successful application of upgrading satcom terminals with Terrasat's Cyber Hardened IBUCs.

In late 2019 Airbus Defence and Space AS was tasked by a customer to provide a number of quick, deployable, tactical satellite antenna systems. One of the system requirements was for SNMPv3 compliancy to improve cyber security of the satellite terminals, incorporating message authentications, privacy monitoring and control management over open networks.

The engineering team contacted Terrasat and quickly concluded that the IBUC, although not yet in full production, provided a good solution to the customers' requirements due to its SNMPv3 compliancy and cyber hardening. While the Covid-19 situation brought with it some delays, the cyber hardened IBUCs arrived on time and was tested and approved for installation.

The handover of the project and virtual demonstration of the terminals took place in December 2020, at which point Airbus supplied 12 complete quick

deployable 2.4m tactical satellite antenna systems, all with stand-alone lightning conductor kits, field swappable X-band and Ku-band RF kits. Also included in the handover was the Airbus Pheonix L-band to fibre media converter system, enabling the user to place the IDU and modem equipment up to 500m away from the terminal to reduce potential exposure. The handover and virtual demonstration went ahead as planned and resulted in a satisfied customer.

OPERATE ANYWHERE AT ANYTIME WITH CYBER HARDENED IBUCS

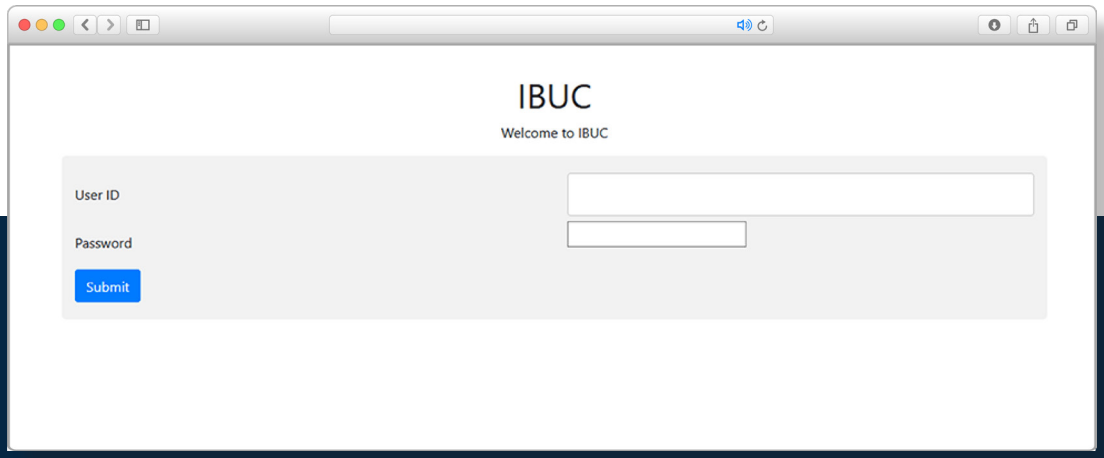
Terrasat Communications is leading the push for cybersecurity advanced Intelligent Block Upconverters to monitor, deter, and strengthen end to end communication data for critical infrastructure at the satellite ground terminal level. Cyber Hardened IBUCs are Intelligent BUCs with heightened cybersecurity protocols for critical data satellite communications for satellite ground terminal applications with hardened physical ports and a 3-year warranty. With the exposed vulnerabilities of remote site locations sporting limited protection, Terrasat's Cyber Hardened IBUCs are equipped with Ethernet ports and an RS232 auxiliary interface connected through hardened access ports using ASCII protocol.

Users can confidently access & connect each session through cryptographic network protocols with SSHv2, HTTPS, & SNMPv3.

Integrated Cryptographic Secure Remote Terminal Sessions

As Operation Cloud Hopper has demonstrated to the industry, resilience to cyber threats starts with multi-level security. Cyber Hardened IBUC units are accessible through secure remote terminal sessions by providing authentication, privacy, and access control to users. Users can confidently access and connect each session through cryptographic network protocols with SSHv2, HTTPS, and SNMPv3.

SSHv2 operates by connecting first, then encrypting the connection before login over an unsecured network. Another point of access for is through embedded webpages through Internet browsers connecting via HTTPS protocols. The newly designed and responsive Cyber Hardened IBUC interface portal makes it difficult for outside threats to access transferring

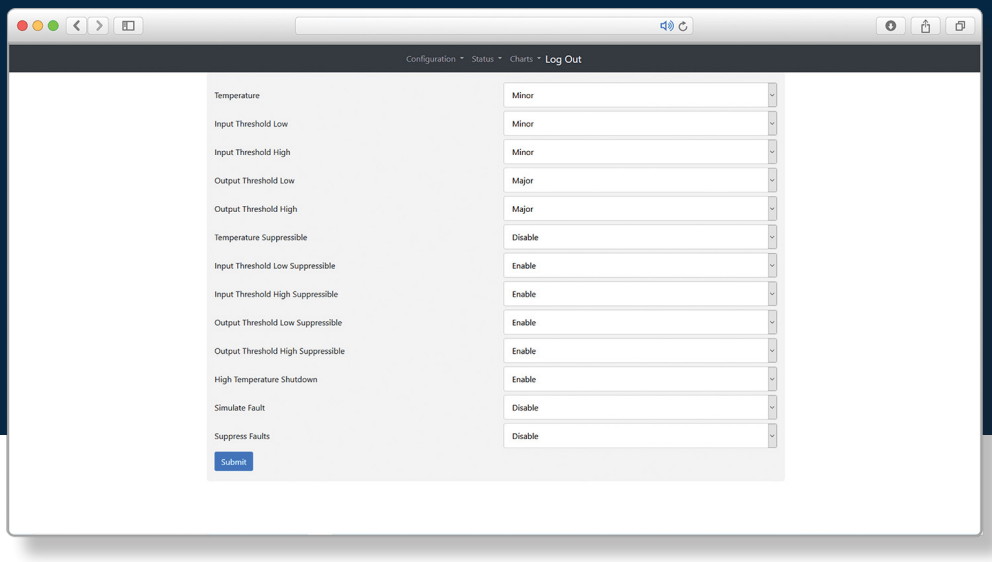


packets and add heightened levels of security protected with key encryption and password-base authentication.

Terrasat Communications remains committed to prioritizing tightening security and installing confidence for users navigating the uncertainty in an evolving world. The new units also support Simple Management Protocol, or SNMPv3, with integration of IP M&C in existing network management systems. SNMPv3 is commercial-grade security for ease of administration, including authentication, authorization, access control, and privacy. SNMPv3 is established during network configuration and incorporates secret-key authentication to prevent eavesdropping. This assures that a received message was genuinely transmitted by the identified source of the message and that it was not tampered or replayed. Security measures include AES & DES encryption keys, user authentication, password hashing, and timeliness checks to counter hack attempts. With the latest versions of reliable encryption integrated into Cyber Hardened IBUCs, satcom operators can not only tighten security for ground satellite terminals but perform secure firmware updates and deter loss of critical assets confidently and efficiently.

The Terrasat Advantage of Ultimate Management and Controls

Inside the BUCs' interface, the new cybersecurity enhanced IBUCs is Terrasat's extensive management and controls (M&C). The M&C allows satcom operators in-depth analysis with statistic logs, 1,000 sensor readings, alarm configurations, and data graphs. The Cyber Hardened IBUC 2, IBUC 2e, IBUC 2G, IBUC R, or IBUC G monitors and controls numerous



parameters and has features that simplify installation, use, and enhance system performance. A notable feature within the interface is the Automatic Gain Control (AGC). The IBUC continuously monitors input and output levels. When AGC is enabled, the gain of the system is maintained at a constant level by an internal algorithm.

Engineered to Endure with Confidence

Terrasat Communications prides themselves with engineering field proven IBUCs with superior performance and reliability. With the dangers of cyber threats expanding throughout industries in an uncertain world, Terrasat Communications remain a leader in the supply chain to continue to bridge the gap with technology advancements and dynamic integration. Satellite ground terminal operators can confidently navigate the uncertainty that is to be expected. Each IBUC unit undergoes extensive testing at our vertically integrated modern manufacturing facility in California, including a 24–48-hour automated testing protocol over temperature and frequency band. Transparent specifications backed by test data guarantee key performance indicators such as low phase noise, high linearity, & rated output power over temperature. Internal sensors plus a microprocessor with advanced software enable a rich feature set including local & remote management so operators can support SLA while minimizing site maintenance costs.

SUMMARY

Terrasat's Cyber Hardened IBUCs Protect Against

- Session Hijacks
- Password Attacks
- Eavesdropping

Cyber Hardened IBUCs Key Features

- Cryptographic Network Protocols with SSHv2, HTTPS & SNMPv3
- Secret-Key Authentication
- Multi-Level Security Access Control
- Hardened Physical Ports with ASCII
- Timeline History Logs
- Enhanced Management & Control

THANK YOU

TO OUR PARTNERS

Terrasat Communications designs and manufactures innovative RF solutions for Satellite Communications systems. Our ground-breaking IBUC-the Intelligent Block Up Converter- brings advanced features and performance to C-band, X-band, Ku-band, & Ka-band satellite earth terminals and VSATs. Find out more about us at TerrasatInc.com

Terrasat Communications Inc.
Spring 2021

Terrasat Communications, Inc.
315 Digital Drive, Morgan Hill, CA 95037
+1 (408) 782-5911
Sales@Terrasatinc.com
www.TerrasatInc.com

References

[1] Richmond, Nathaniel. "Operation Cloud Hopper Case Study." Web log. Software Engineering Institute (blog). Carnegie Mellon University, March 9, 2019. https://insights.sei.cmu.edu/sei_blog/2019/03/operation-cloud-hopper-case-study.html.

[2] Doffman, Zak. "U.S. Military Satellites Likely Cyber Attacked By China Or Russia Or Both: Report." Forbes. Forbes Magazine, July 5, 2019. https://www.forbes.com/sites/zakdoffman/2019/07/05/u-s-military-satellites-likely-cyber-attacked-by-china-or-russia-or-both-report/?sh=1e09459add32.

[3] Zorabedian, John. "What's New in the 2020 Cost of a Data Breach Report." Security Intelligence, July 28, 2020. https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/.

FURTHER READING

"Cybersecurity and the New Era of Space Activities." Council on Foreign Relations, 2018. https://www.cfr.org/report/cybersecurity-and-new-era-space-activities.

"Cost of a Data Breach Report: 2020." Ponemon Institute LLC. https://www.ibm.com/security/data-breach.

"Cybersecurity of NATO's Space-Based Strategic Assets." Chatham House – International Affairs Think Tank, https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets.