SystemX

Onboard Cyber Defence and Security Platform

Defending your cyberspace has never been more challenging or important. With critical data moving around the globe, you need to understand the security posture of your air, land or sea networked and distributed assets.

Introducing SystemX™: Flexible, Capable, Secure

Protect your networks and connected devices with CCX Technologies' SystemX Cyber Defence and Security platform. Designed to operate in bandwidth- and latency-restrictive channels, like satellite and terrestrial radio links, SystemX is a flexible solution that can either be integrated directly on hardware, or in the cloud. The appliance-server architecture is built to improve the security posture of a variety of equipment on air, land and sea vehicles. Protecting critical networks and assets, the platform features a robust intrusion detection system (IDS), bespoke and easily customized rules-sets, logging and reporting, and automatic defense and mitigation capabilities.

CCX TECHNOLOGIES

SystemX

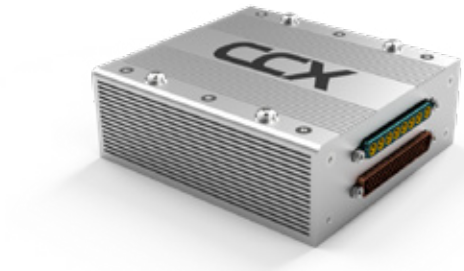
Onboard Cyber Defence and Security Platform

A New Way Forward in Cyber Defence & Security

What makes SystemX unique? Flexible and robust, it resides directly on an asset, and features a comprehensive cyber security solution that includes hardware, software and services.

Hardware

The solution has two hardware components. The AP-150 Secure Wireless Gateway (AP-150) is a small, standalone, SystemX software-enabled, device that provides an easy way to add cyber defence and security, plus other secure networking services to your deployed assets.
The DataPHY™ Secure IOT Data Transmission Appliance (DataPHY) is small and powerful, enabling secure data transmission over WiFi or Ethernet. When installed on an aircraft, DataPHY securely transmits vehicular data to the AP-150. Initially avionics focused, these two elements can easily be implemented on land and sea assets.



AP-150 Secure Wireless Gateway

Flexible Implementation Options

SystemX Software is delivered on the CCX Technologies AP-150, providing a straightforward installation option. SystemX Software can also be installed as a virtual machine (KVM, ESXi, VMWare, or VirtualBox) on existing networked avionics equipment such as a router, server, or radio. The server software can run in any data center, including popular cloud systems like the Google Compute Engine (GCE) and Amazon Web Services (AWS).

Software Suite

The SystemX Software suite of cyber defence and security applications is compatible with most modern networked avionics equipment and provides:

+ Simultaneous cyber-attack detection to and from the asset
+ Robust intrusion detection system
+ Vehicle-tailored PKI
+ Advanced firewall capabilities
+ Secure upgrade, configuration and logging facilities.
+ Automatic attack mitigation with key stakeholder notifications
+ Monitors all networked systems on the asset

Services

The SystemX Services offer extended capabilities including:

+ Secure Satellite and GSM airtime services (with voice and text)
+ Secure Passenger and crew data
+ Secure Airtime
+ Mission-tailored Rules-sets
+ Security Operations Center
+ Secure Home Country data and call termination
+ Remote technical support
+ Real-time configurable alerts
+ Cyber Security Test Lab

CCX TECHNOLOGIES

SystemX

Onboard Cyber Defence and Security Platform

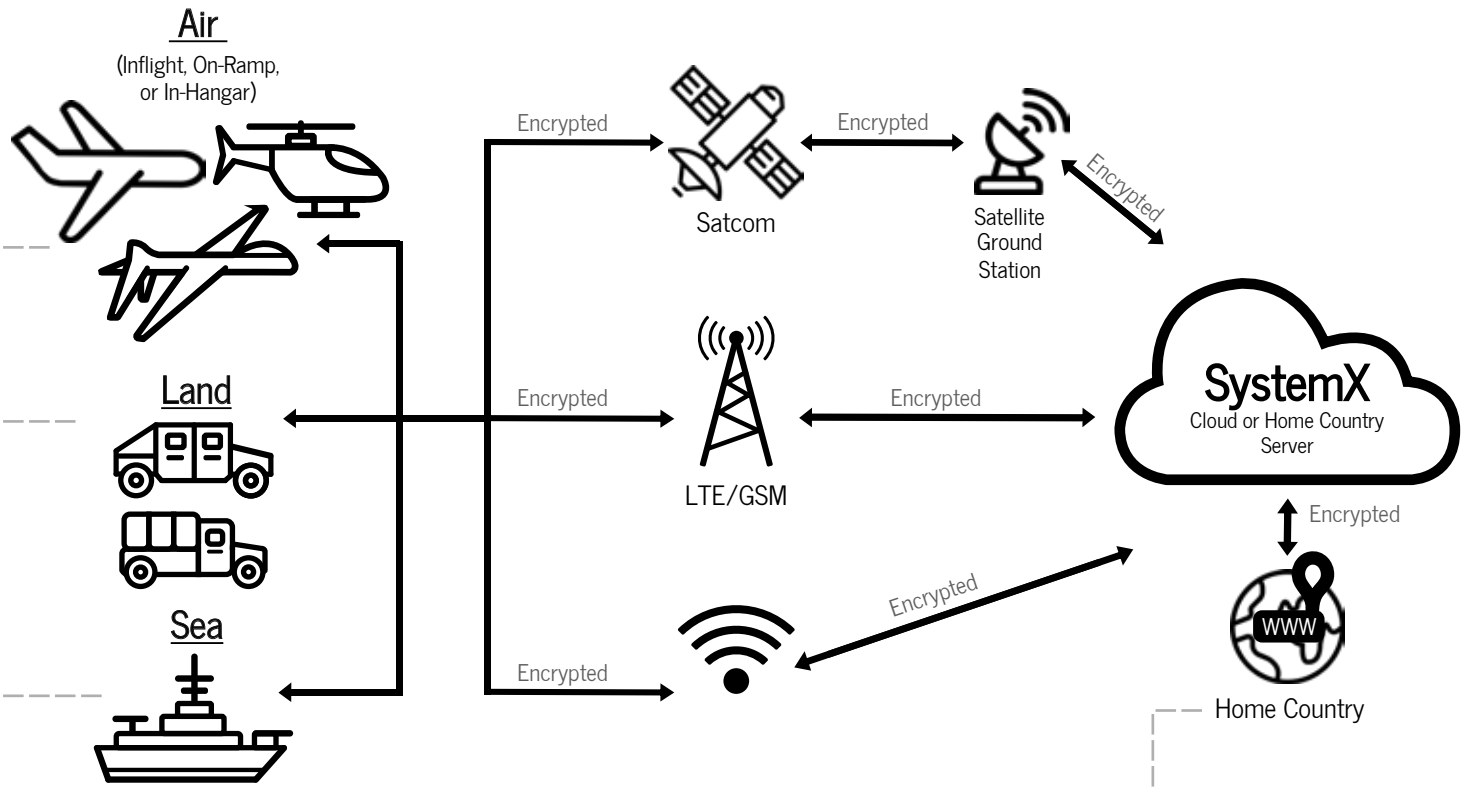
SystemX Platform Ecosystem

On-asset Monitoring

Residing directly on the asset, SystemX Software and hardware provide real-time, actionable information about the security posture of your air, land or sea vehicle's network. It monitors a variety of data-buses, including ARINC-429, ARINC-717, MIL-1553, and ARINC-664 (AFDX). Wherever your asset is on the globe, SystemX detects anomalies, potential cyber-attacks and alerts security experts while keeping critical data secure.

Customizable IDS

The IDS can monitor traffic on traditional Ethernet and WiFi networks and on a variety of avionics, defense, and industrial networks, including ARINC-429, ARINC-717, ARINC-664 and MIL-1553. SystemX can also monitor third-party equipment logs, which will generate cyber alerts, and even non-cyber security alerts such as over-temp or an equipment fault. All alerts are collected by the server and presented in a format that can be used by an SOC to gauge the severity of an alert.



Home Country Advantage

SystemX has the unique capability to ensure your critical data is routed through your home country with encrypted network transmissions from your asset (aircraft, vessel, vehicle) to your designated home country NOC (network control centre). The result? Your data never hits the open internet in a foreign country, and is kept ultra-secure.

CCX TECHNOLOGIES

SystemX

Onboard Cyber Defence and Security Platform

SystemX Addresses the Whole Cyber Defence & Security Cycle

Detection: Employs active monitoring onboard air, land and sea vehicles, providing customized alerts for an ever evolving and increasing range of cyber-attacks and anomalies.

Logging & Reporting: Tailored rules-sets, and real-time IDS log and reporting capabilities on the vehicle securely send alerts to operations centers and stakeholders for immediate action.

Analysis: Based on customized rules-sets, CCX Technologies' support team analyzes generated alerts and determines potential impact on the asset's environment including crew, users, network and overall system.

Mitigation & Defence: Implemented to match operational parameters that offer automatic mitigation and defence capabilities depending on the type of mission.

Need more information?

Call us: +1 (613) 703-6161
Email us: info@ccxtechnologies.com
Visit us: ccxtechnologies.com

CCX TECHNOLOGIES