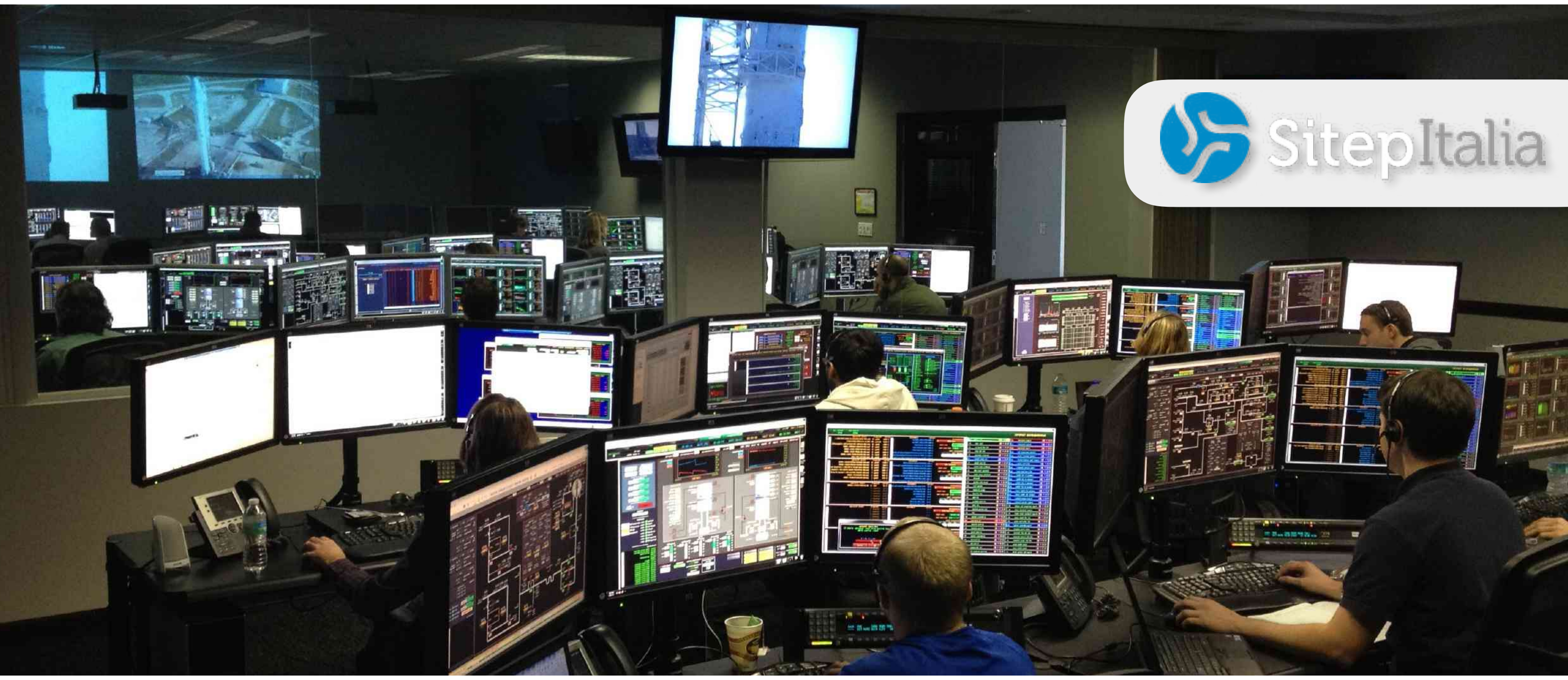
Case Study

SEdesk™

Secure Command & Control for non-lethal weapon installations



Background

Isolated systems are the least liveable solution for security and law enforcement applications. Initially, systems were using specialised hardware and software in an isolated environment relying on proprietary command and control protocols. Digitalisation together with the prevailing IoT (Internet of Things) approach, are reshaping the landscape of law enforcement operations. Changes are in progress and more critical law enforcement physical devices, collecting and sharing data, are being connected. Unmanned sites and systems such as USV, ULV and UAV require a further effort to deploy security in a flexible and effective way. The technology advancement makes feasible the optimising of operations, reducing reaction time, turning field data into useful intel information and much more. Such new scenarios require a more flexible approach to deliver the mandatory security level, protecting both systems and information from security leakage and cyber attacks.

Challenge

Unmanned systems, still use the approach to completely isolate domains not taking advantage of the integration opportunities and efficiency. Due to increasing need from law enforcements to monitor and control a variety of sensors and connected systems as well as easily analyse, manage and monitor informations from remote, this separation model has been increasingly compromised. So, how to make integration a real opportunity for command & control systems bypassing the existing old-style paradigms while increasing security and yet thwarting cyber-attacks?

Industry

Defence & Law Enforcement
Command & Control

Challenges

- Optimise the effectiveness of secure remote Command & Control for systems, designed to be deployed in multiple locations and potentially difficult to reach with suitable infrastructure

Goals

- Securing connections among multiple sites hosting critical systems with an effective, flexible, hardware based, military grade solution
- Bypassing typical limitations of VPN or other traditional networking tools

Solution

SE*desk*™ is a unified workspace providing secure remote access to whitelisted resources and on-device isolation to reduce the surface of attacks in a perimeterless digital workplace.

Solution

The protection of borders, coastal areas and critical infrastructures as well as the need for new ways to control riots and to manage critical law enforcement situations, led to the development of MASS systems. Designed to be installed on board of vessels, military fast boats or USV (Unmanned Surface Vehicles), land vehicle or land positions, MASS are the suitable device to engage potentially hostile targets with non-lethal emissions. Designed to generate different emissions to engage targets during critical missions, MASS allows acoustic emissions such as voice messages (pre-recorded or live) to be sent over a long-range path and disturbing sounds to grant a degree of deterrence. Furthermore, a green Laser Dazzler with associated Laser Range Finder and a powerful Search Light are used as additional deterrents against threats or as supporting tools during missions. The MASS are also equipped with cameras, for day and night operations, to watch over and to record events in real time. The equipment is designed to meet the most severe military specifications.

The requirement is therefore for an effective, secure and centralised command and control of MASS systems alongside with the need for complete remote management of all actions on the terrain, with minimised overhead.

In this scenario, SE*desk*™ finds its perfect place as being the right combination of application and network layer protection by isolation. By defining a controlled perimeter, SE*desk*™ not only provides authenticated service isolation and access control, but also data protection through delivery and storage leveraging the SE*link*™ technology to protect data transfer from the remote MASS systems to the central server in the control room. SE*desk*™ delivers a multi-layer approach to protect both the network and the endpoints from data exfiltration. Moreover the simplicity of the implementation allows for fast and effective deployments.

Benefits

- **Complete isolation** of data and applications on endpoint devices
- **Fine-grained access control** to the central network through context-based policies and User-Device-Server multi-factor authentication
- **Hardware based, military grade** security
- **Reduced maintenance** on endpoint devices
- **Zero configuration** on endpoint devices for easy deployment (VPN free)
- **Optimisation of operational costs**
- **Future proof technology,** ready for resilience against quantum computer attacks

SitepItalia

Sitep Italia is a worldwide leading solution provider of specialised defence and commercial navigation, communication and security systems for maritime applications. Sitep Italia can boast a long tradition of design, development, manufacturing and support of advanced electronic systems for military and commercial applications since 1975. Continuous investment in human and capital resources allowed the company to gain a leading role as a supplier to the Italian naval market, export its innovative technology all over the world, diversify its technology and expand into commercial application.

Blu5 Group
info@blu5group.com
www.blu5group.com