



The Critical Role of Ground Control Stations in Drone Operations

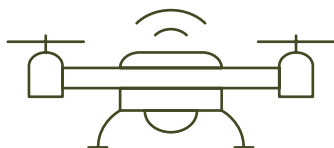
Why rugged devices are the essential tools for UAV success.

The success of drone missions heavily depends on the reliability and performance of the ground control stations used by operators in the field. Learn how rugged devices hold the key to ensuring ground control stations can securely maintain control, communicate effectively, and process mission-critical data without interruptions.

Taking Control of the Battlefield with UAV Technologies

In modern military operations, Unmanned Aerial Vehicles (UAV), or 'drones' have become indispensable tools, with their capacity for both autonomous and remotely piloted missions significantly enhancing the efficiency and safety of military personnel.

As the power and versatility of drone capabilities increase and their designs and control systems make them more portable, drones are no longer just reconnaissance tools, but an instrumental item in everyday offensive and defensive operations.



The Modern Battlefield

Swarm drones

Multiple UAVs working together to overwhelm enemy defences.

Manned-Unmanned Teaming (MUM-T)

Drones collaborating with human-operated systems for enhanced operational efficiency.

Signal Repeater Drones

UAVs acting as airborne communication relays, extending control range and minimising interference risks.

As the demand for commercial drones and unmanned aerial vehicles for defence use increases, the market is projected to grow at a compound annual growth rate (CAGR) of 13.74%, reaching

\$27.9 billion
by 2033.*

*Fortune Business Insights
Unmanned Aerial Vehicle (UAV)
Ground Control Stations (GCS) Market



Ground Control Stations (GCS)

A Critical Component

GCS play an essential role in operating drones, making it possible for operators to monitor and control their vehicles safely from a distance. Not limited to just an interface for operators to pilot drones, GCS are used to visualise, analyse, and share operational data from these drones with the wider operational unit and intelligence teams.

Given the varied and demanding environments in which drone operators are deployed, the ability of rugged mobile devices to withstand the rigours of military operations makes the preferred choice for GCS over consumer-grade devices.

Over the following pages we'll explore in greater depth four key areas where rugged field devices must meet the highest standards to serve as GCS solutions for military drone operators.



Reliability Under Harsh Conditions

[Jump to section >](#)



Data and Device Security

[Jump to section >](#)



Dependable Connectivity

[Jump to section >](#)



Advanced Interfaces and Operability

[Jump to section >](#)



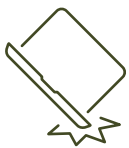
Reliability Under Harsh Conditions

Drone operators could be called into action anywhere in the world. Whether it's the scorching sands of the deserts or the subzero chill of an arctic tundra, GCS devices must be able to withstand every conceivable weather condition, as well as the rigours of day-to-day military activities.



Environmental Challenges

Extreme temperatures, dirt, dust, rain, sea water, and sand could all be features of the deployment zone.



Battlefield Conditions

The highly dynamic nature of field deployment and unpredictability of operations mean that impacts, knocks, and vibrations are commonplace.

Mission Criteria

Standard commercial devices aren't built to withstand these rigours of the field, and are likely to fail fast in such conditions, leading to mission-critical failures.

The unpredictability of weather and warfare call for rugged devices that can endure the environmental extremes and unrelenting physicality of frontline military usage.



Data and Device Security

As with all military operations, security of equipment, information, and personnel, is of the highest priority. Operating drones in the field for either training or live missions introduces additional mobile endpoints that could potentially be exploited as security vulnerabilities.



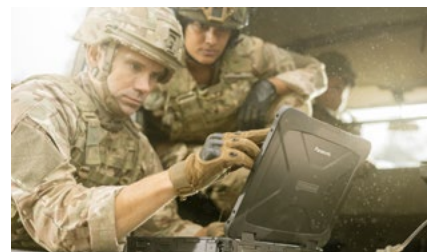
Hijacking and Counter-Drone Threats

As counter-UAS technologies increase in sophistication, adversaries will attempt to disable or even take control of drones, which could have severe consequences if the drone is carrying live ordnance.



Communication Interception

With GCS acting as relay points sending drone information to troops and bases, any interception or disruption to these communication lines could endanger troops, as well as threaten wider military security.



Lost and Captured Devices

In the event of GCS devices being lost, seized, or damaged in the field, the ability to remotely disable devices and wipe their hard drives to protect sensitive data and the wider military network is a fundamental requirement.

Mission Criteria

Owing to the sensitive information transmitted between drones and control stations, and the physical control systems themselves, GCS must therefore be equipped with the highest levels of security and encryption.

Additionally, mobile solutions featuring AI that can support rapidly adaptable countermeasures and communication protocols to guard against ever-evolving cyber threats and interception are emerging as must-haves in the domain of GCS.

Dependable Connectivity

During remote operation, maintaining a stable connection between the drone and the control device is vital. Any drop in communication between the GCS and the drone could result in loss of control, interruption to real-time surveillance, and the inability to report and respond to dynamic threats and situations.

But maintaining high-speed connectivity between GCS and the drones can prove problematic:

Environmental Interference

While the drones themselves may typically be flown in open environments, operators are often based in covert positions which can block or weaken the strength of signals. Even when operating in the open, natural obstacles such as mountains or dense urban environments can also cause connectivity disruptions.

External Threats

As well as the physical environmental challenges, there's the malicious threat. Adversaries may employ electronic warfare tactics such as jamming and signal interference to degrade or block communications, potentially rendering drones ineffective or even causing them to crash or be hijacked.

Mission Criteria

When interference or signal loss can compromise mission success, drone operators need GCS devices that feature reliable, versatile connectivity modules and networking capabilities to ensure uninterrupted operations, and the safety of both personnel and equipment.





Advanced Interfaces and Operability

Drones are some of the most advanced technologies in frontline military usage. Packing surveillance, communication, live video streaming, flight manoeuvrability, weaponry, and much more into highly covert airborne vehicles, they are very much at the leading edge of military – and technological – innovation.

But all that capability needs monitoring and controlling, and when ground personnel are embedded deep on the battlefield, they can't carry a full server room with them.

GCS controllers need portable devices that meet a demanding set of computing and operability criteria:



High-powered computing to run processor-intense AI applications and programmes.



Large sunlight-viewable screens that can display clear visuals and video feeds.



Touchscreen operation that works while wearing gloves.



Long lasting battery power that can sustain intense field usage for hours and even days.



Modular connectivity and customisable ports for external controls and accessories.

Mission Criteria

As the functionality and complexity of drones broadens, GCS must combine powerful processing, adaptability, and portability, with a highly intuitive and user experience that empowers operators to seamlessly move between applications and accessories to control drones and monitor their feeds without interruption.

TOUGHBOOK

A Reliable Partner for GCS

TOUGHBOOK devices are the ideal controller and mobile ground station for drone operations. With powerful processors, rugged design, extended connectivity, and cyber security features, they are engineered to tightly control drone flight and functionality, and securely stream collected footage, making them the ideal recruit for UAS and drone operations.

Designed closely with military experts, manufacturers and system integrators, the TOUGHBOOK range of rugged COTS tablets and notebooks are built to withstand the rigours of extended use in extreme environments and include several features designed specifically for military and covert use.

Combining the power of Windows 11 Pro, Red Hat certification, military level security, and reliable connectivity, TOUGHBOOK has a long-term product roadmap to give you the maximum value and lifetime from your investment.



Superior Screen Technology

TOUGHBOOK features low-reflection, high-resolution screen technology to provide outdoor-readable displays with patented 'rain mode' and glove compatibility to enable all weather working for drone operators.



Video and Communication

TOUGHBOOK devices are available with front- and rear-facing cameras, allowing operators to document situations with ease and seamlessly communicate with support teams and Command-and-Control bases.



Uninterrupted Connectivity

TOUGHBOOK features integrated wireless GPS as well as 5G-ready and enhanced 4G connectivity for downloading and uploading critical reports and data. The robust, long-lasting battery life ensures operators can stay on the job even in evolving situations.



Survive Extreme Environments

TOUGHBOOK is built to withstand heavy impacts, vibrations, dirt, water, and temperature extremes, so your operators can stay in control even in the most challenging of conditions.



Ultra-Secure Tech

TOUGHBOOK provides the highest level of security right out of the box, with deeply integrated hardware, firmware, Red Hat certification and Secured-core PC offering protection from highly advanced threats and cyberattacks.



Cloud, Edge, and Air-Gapped Operations

TOUGHBOOK devices offer Red Hat certification for seamless integration for cloud-based, edge computing, and air-gapped environments, ensuring data security and operational flexibility in mission-critical scenarios.

Tried. Tested. Trusted.

Militaries and defence integrators internationally have been choosing TOUGHBOOK for over 25 years because we know the challenges they face.

With a range of accessories and features tailored to meet different mission parameters and operational requirements, TOUGHBOOK is the perfect recruit for military mobile ground control systems.

Our solutions go beyond hardware. We work closely with industry experts, UAS manufacturers and system integrators to provide the best solution based on your needs.

Novadem



Get Ready for Takeoff

Speak to one of our UAS experts to discuss your requirements and learn more about TOUGHBOOK for UAC GCS.

Panasonic
CONNECT

TOUGHBOOK