

USE INFORMATION *SECURELY*, MANAGE COMPLEXITY

As armed forces become increasingly digitalized, the number of systems, security classifications and information sources converging within command structures continues to grow. IHSE Managing Director Dr. Thomas Niessen explains how access to this information can be organized without compromising security boundaries.

Text Miriam Rauh

Dr. Niessen, where do you currently see the greatest challenges for secure command-and-control infrastructure?

Today, vast amounts of information are available. The key challenge is making the relevant information available at the right time. This becomes increasingly challenging as more systems and security domains are involved. In an operational environment, no one can afford to spend time determining which system provides which information or what access authorization is required.

At the same time, every additional system increases complexity and creates potential attack surfaces. Maintaining command capability therefore also means keeping information flows manageable.

What role does KVM technology play in this?

KVM stands for Keyboard, Video and Mouse. Put simply, we provide controlled remote access to different computer systems. Users can access the sources they are authorized to use from a single workstation, while the actual computers remain physically remote and securely protected. The systems are not consolidated into a shared data platform. We enable access without merging the underlying data sets.

What does this mean when different classification levels are involved?

This is exactly where multi-class workflows come into play. The military, intelligence services, police and emergency response organizations work with different data sources, security domains, access rules and protection or classification requirements. Users should be able to easily access the information required for their task, even if it originates from several different security domains. The data remains within the respective systems and subject to their existing access controls. The KVM system establishes the connection to the relevant system. Anyone who is not authorized to access a particular source will not be granted access.

How does red/black separation work in this context?

Black information is unclassified or more broadly accessible, while red information is protected or classified. The key point is that both domains remain technically isolated and that no data can be exchanged between them in an uncontrolled manner. Our KVM matrix controls which workstation is permitted to connect to which computer source. An authorized user, for example in an operations or command center, should be able to access the required information, while the physical systems remain logically and spatially separated in the background.

“ESPECIALLY UNDER STRESS, TECHNO- LOGY SIMPLY HAS TO WORK.”

Dr. Thomas Niessen
Managing Director, IHSE

Does this architecture also provide protection against cyberattacks and insider threats?

KVM does not replace the cybersecurity measures of the respective data source. In other words, we do not encrypt the entire network. However, an additional layer of security is created by physically separating computers from the workstation and controlling access to them. For example, a USB headset can be permitted while copying data to a USB flash drive is blocked. This also makes direct tampering more difficult.



Foto: AI generated

How important are certifications for systems like these?

Security properties must be verifiable. In our case, EAL4+ relates to IT security and describes the depth and rigor with which the intended security functions are evaluated. For our system, this includes ensuring that information only travels along the intended path from a verified source to a verified workstation. TEMPEST addresses electromagnetic emissions and therefore protection against electromagnetic eavesdropping. IEC 60945, in turn, relates to resilience under demanding environmental conditions, such as humidity, vibration or temperature. Taken together, these standards address different dimensions of operational security.

What do Multi-Domain Operations mean for the command infrastructure of the future?

Land, air, sea, cyber, space and civilian information are increasingly being incorporated into situational assessments. However, this should not result in a single all-encompassing “super system.” Such structures can create new attack vectors and significant risks of system failure. In my view, what is needed are distributed, modular and interoperable systems that respect security boundaries while still enabling the necessary access to information. This includes controlled access rights and redundancy. For the operator, the technical complexity in the background should remain as invisible as possible. Especially under stress, technology simply has to work. That is exactly what our solutions at IHSE are designed to deliver.

For further information, please visit:
www.ihse.com

Advertisement

KVM. MULTI-CLASS. MULTI-DOMAIN.

Separate where it matters Connected where it counts.

PUBLIC AUTHORITIES

DEFENCE

COMMUNICATIONS

CRITICAL INFRASTRUCTURES

SECURE ACCESS TO
CRITICAL SYSTEMS.



SECURELY SEPARATED.
Strict separation of
security domains.



EFFICIENTLY CONNECTED.
All systems in view –
on a single console.



SOVEREIGN CONTROL.
Controlled access.
Maximum security.

ihse.
www.ihse.com