PROVIDING END-TO-END PROTECTION AGAINST DIGITAL THREATS WITH A KVM SYSTEM

How a cyber resilient KVM system protects mission-critical IT systems in control centers, industrial, government and military facilities from threats in a digital world

CYBER SECURITY

SECURE KVM SOLUTIONS ■ MISSION CRITICAL 24/7 ■ MADE IN GERMANY

ihse.

WHEN UNCOMPROMISING SECURITY IS REQUIRED

In government, military and other critical infrastructure facilities security is paramount. A cyber attack on an IT system or the loss of confidential information can quickly become a serious threat to local or national security. Data theft from IT systems can cause enormous damage to institutions in commercial, industrial and service sectors. Stringent cyber security precautions must be taken to safeguard information and assets at all times; a process that is made harder as staff increasingly work remotely from different locations and in mobile environments.

Companies of all sizes rely heavily on networked digital IT systems and are susceptible to cyber threats that take advantage of even the smallest vulnerabilities in the system. Incursions are increasingly common and cover a wide range of forms: from industrial espionage, data theft and data manipulation to ransomware attacks. To guard against these threats, companies must ensure that their IT systems have the highest level of data and access security by identifying weak points and securing them with cyber resilient IT systems.

Data protection and data integrity have top priority within critical national infrastructure sectors and are subject to comprehensive and strict guidelines. In Europe, the legislation for this is covered by the European NIS (Network and Information Security) Directive.

In response to ever-increasing cyberattacks, the new EU Directive NIS2 was introduced in January 2023. All EU countries are required to transpose this NIS2 directive into national law by October 2024.

The NIS2 Directive aims to establish a harmonized framework for cyber security across the EU, promoting greater resilience against cyber threats and enhancing the overall security of network and information systems. The NIS2 Directive extends its scope beyond traditional critical infrastructure operators to include a wider range of entities such as digital service providers, cloud computing services and search engines. Companies are required to take appropriate security measures to manage risks posed to the security of their network and information systems. This includes implementing measures to prevent and minimize the impact of cyber security incidents and maintain a secure digital environment.

IT hardware requirements for critical infrastructure systems vary depending on the sector and specific application. However, the supporting IT systems should be resilient, secure and capable of fully dealing with potential threats.

HOW CAN IT SYSTEMS BE PROTECTED AGAINST CYBER ATTACKS?

IHSE has developed a robust, easy-to-use cyber protection concept. This does not restrict users in any way. Conversely, it offers and delivers enhanced utility, additional features such as collaboration and supervisory oversight as well as enormous flexibility.

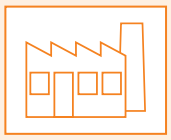
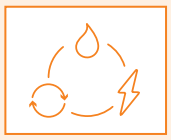
1. CYBER SECURITY

Cyber security is a part of an organization's total IT security regime. It refers to the protection of IT systems, comprising computers, networks, programs and data, against unauthorized access, attacks, damage or theft of information. The primary objective of cyber security is to ensure the continuous confidentiality, integrity and availability of data. This includes protection against a variety of threats, such as malware, hacker attacks, data leaks and other forms of cyber crime.

A successful cyber attack may lead to theft, falsification (spoofing) or destruction of sensitive data. In addition to operational disruption and financial loss it can also affect the trust of customers and partners. It may also have extended consequences, resulting in breach of contract with penalties under the GDPR and adversely affect the ability of the business or institution to continue operating.

REQUIREMENTS FOR CYBERSECURITY CONCEPTS

Cyber security is of crucial importance in all areas of society as digital attacks and threats can increasingly affect the normal functioning of organizations and institutions.

Sector		Endangered asset	Aim
Commercial and industrial		▪ Sensitive customer and supplier data ▪ operational information	▪ Protect confidential information ▪ Secure financial transactions ▪ Ensure business continuity
Government and military		▪ Personal data ▪ National security information	▪ Maintain data integrity and secrecy ▪ Protect national security
Critical infrastructure		▪ Security of supply (water, power, transportation, ...)	▪ Ensure continuous and uninterrupted operation
Financial institutions		▪ Personal data ▪ Transactional information	▪ Maintain customer trust ▪ Prevetion of fraud
Medical and Healthcare		▪ Sensitive patient information ▪ Functioning of equipment ▪ Data communication	▪ Guarantee patient safety and privacy ▪ Continuous availability of medical services

RISKS	SYSTEM FAILURE	LOSS OF IMAGE	ESPIONAGE	INFRASTRUCTURE DAMAGES
TYPE OF ATTACK	▪ Denial-of-Service-Attack (DoS) ▪ Blackmail and Ransomware	▪ Manipulation of information ▪ False media reports ▪ Identity theft	▪ Theft of trade secrets and sensitive data ▪ Theft of technology and research information	▪ Terrorism ▪ Unauthorized manipulation of resources
CONSEQUENCES	▪ System damage and reinstallation costs ▪ Loss of assets	▪ Loss of trust in information channels (e.g. media or government sources)	▪ Loss of competitiveness	▪ Disruption of critical infrastructure, e.g. electricity, gas, water, airports ▪ Disruption to public safety and security

2. WHAT IS KVM?

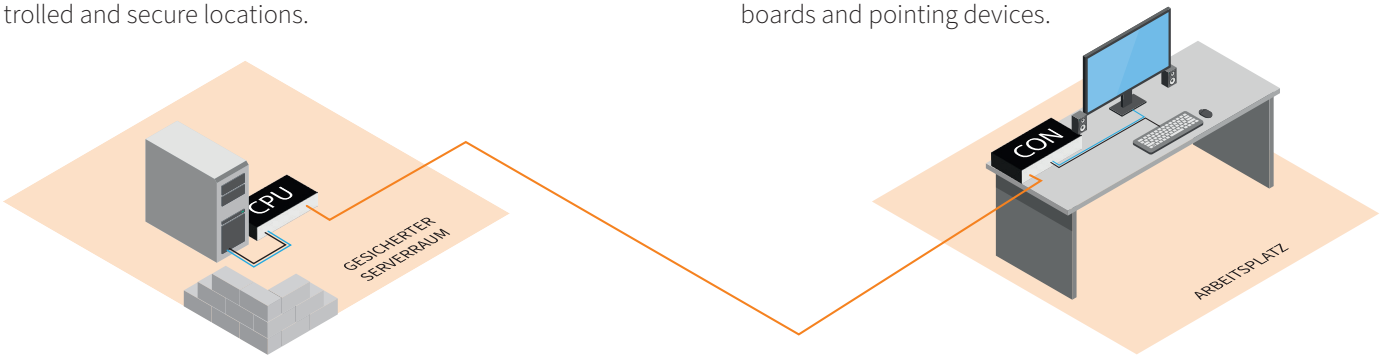
KVM refers to keyboard, video and mouse, the standard computer input and output devices used in the workplace. KVM technology enables real time operation of one or more computers or servers from a central workstation. The primary elements of a KVM system are the extender and matrix switch. Extenders enable remote connection of users to computers over a long distance, a matrix switch allows individual users to connect to any desired computer on the installed system; subject to strict permission and authorization parameters.

Direct KVM systems operate independently of the in-house IP network. The two systems function in isolation with an air gap between them. Where required, bridges are available to connect KVM systems to TCP/IP networks, allowing internet-enabled devices to be accessed from a KVM workstation.

KVM EXTENDERS

KVM extenders enable the physical separation of computers and workstations over hundreds, or even thousands, of meters with no detriment or adverse effects on the operation of the computer. This makes it easy to locate computers in environmentally-controlled and secure locations.

Removing noisy, bulky, heat-producing computers from the operator workplace creates a more pleasant, less-cluttered, working environment. Users' desks simply require a small receiver box together with basic computer peripheral devices: monitors, keyboards and pointing devices.

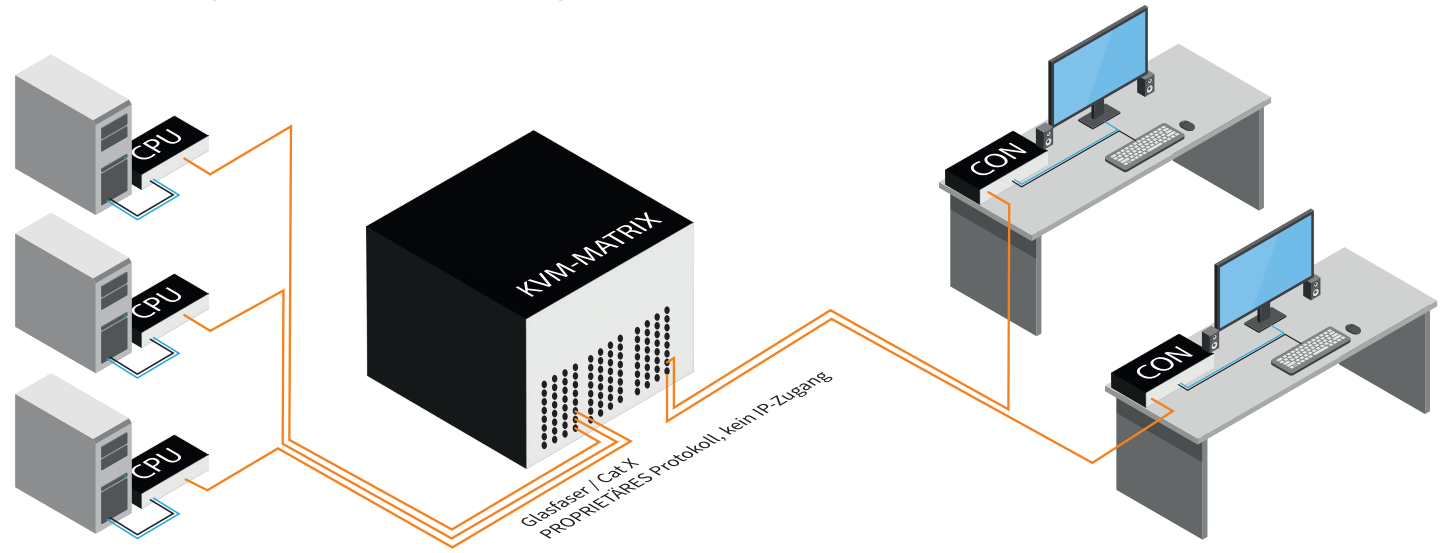


KVM MATRIX SWITCHES

KVM matrix switches are used to simultaneously connect several users to multiple computers. The switches allow uninhibited access to sources and the ability for users to switch instantly between them. All operations are independent of the IP network. Operators can access any appropriate computer from their own console subject to access rights.

Expensive equipment and software licenses can be shared between multiple users, reducing infrastructure investment. It allows users to access single sets of data thereby ensuring they access up-to-date information and limiting errors caused by multiple data versions. Data can be shared and duplicated across several endpoints for supervisory monitoring, shared workload and large videowall display capability.

KVM solutions are used in various industries, such as air traffic control and management, healthcare, finance, education, broadcast and environments that rely on highly secure control centers.



3. PROTECTION AGAINST CYBER ATTACKS BY IHSE KVM SYSTEM

As a technology leader in flexible and highly secure KVM solutions, IHSE is committed to cyber security at the highest level. The multiple award-winning IHSE products deliver outstanding manufacturing quality from Germany, high availability, reliability, robustness and certified protection against internal and external threats through a range of measures. The KVM system creates a secure and isolated operational area without restrictions.

- A KVM setup prevents unauthorized physical access by locating sensitive devices and computers in a secure environment, with no access to computer hardware from the workstation area.
- Connection between devices is secured by proprietary encrypted data procedures in accordance with the highest military standards and the national criteria for critical infrastructures.
- Operators must authenticate themselves at their consoles.
- The KVM system provides access management which authorizes individual users and permits their access to specific computers.
- The central matrix switch contains Secure Core technology to physically separate it from the IP network. This prevents potential external attacks via IP.
- The modular system design of the switches permits system expansion and upgrades to be carried out easily and at low cost, even during live operation. Newly emerging standards or interfaces can be quickly integrated into the existing architecture.

MULTI-LEVEL SECURITY CONCEPT

KVM SECURITY BENEFITS

- Physical separation
  - PCs in demilitarized zone (DMZ)
  - no LAN access for the user
- Interoperability
  - OS-independent
  - Large number of possible interfaces and devices, including cameras
- Increased efficiency
  - Collaborative through simultaneous operation of single device
  - Reduce costs by sharing resources
  - Centralized administration of separate networks
- Access control
  - Additional security layer through user roles
- Switching in real time
  - Instant response
  - No perceived user latency

ADDITIONAL PROTECTION WITH IHSE KVM SOLUTIONS

- Redundancy options
  - Fail-safe operation
  - Continuous availability
  - Maximum reliability
- Scalability
  - Future-proof investment security
- Secure core technology
  - Discrete data paths
  - No crosstalk
- Isolation from the IP world
  - Data transmission over isolated network
- Administration
  - Simple restoration of configuration (backup/recovery)
  - Two Factor Authentication (2FA) for administration
  - Controller isolated from signal paths
  - Operation possible without permanent administration
- Secure remote office solutions

CERTIFIED SECURITY SOLUTIONS

- CC EAL4+ certified devices
- Secure components
  - No back-channels (video, audio)
  - USB interfaces restricted to mouse and keyboard
  - Audio low-pass filter
- Tamper protection
  - No buffer memory
  - Sealing of the device
  - No command sets permitted
- Encryption of KVM signals
- Eavesdropping security according to TEMPEST standard (NATO SDIP-27 Level B/Zone 1)

CYBER SECURITY

4. SECURITY THREATS AND CORRESPONDING PROTECTIVE MEASURES

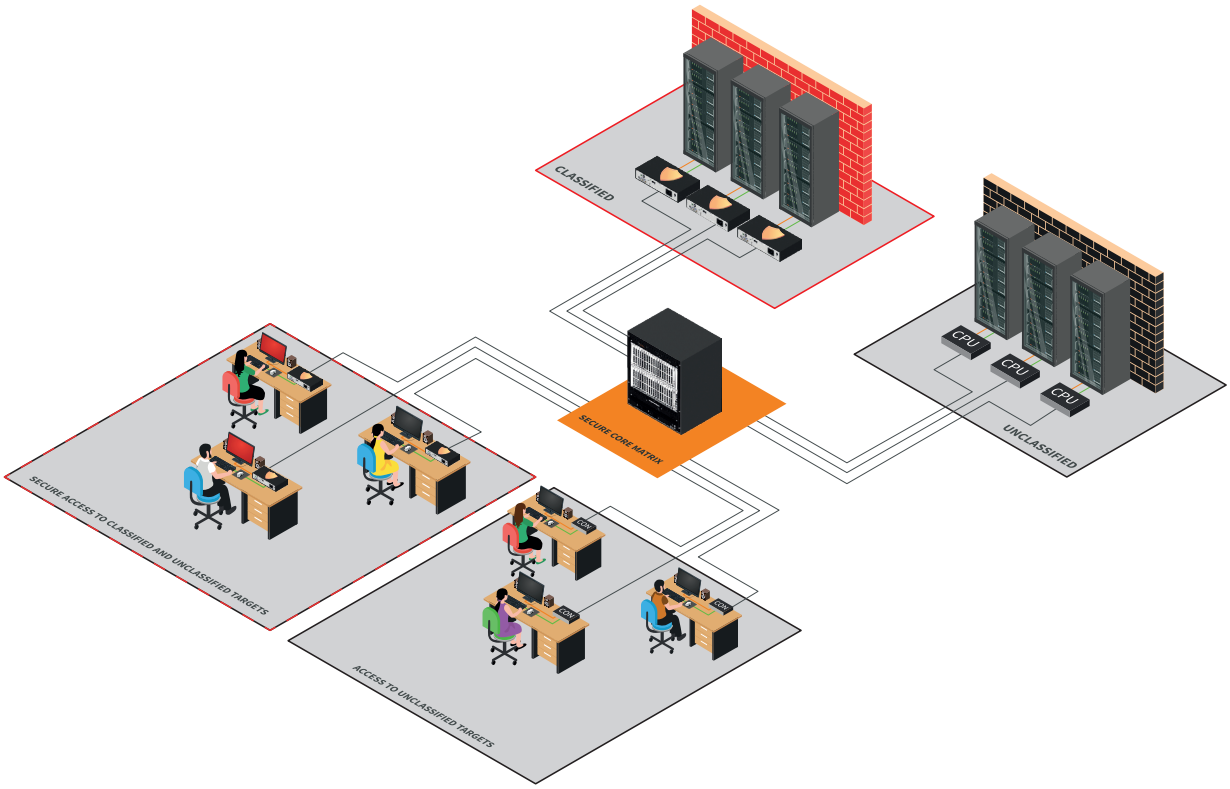
IHSE's R&D department maintains close contact with military IT security experts in order to identify potential threats to data security and systematically eliminate them during the development process.

4.1 INTERNAL THREATS (INSIDER THREATS)

Insider threats arise within an organization. For example, data theft, manipulation or betrayal of secrets by people who work on the premises and have access to sensitive data. Theoretically, all computers could be locked, but in practice in a modern control center, employees need to be able to share systems, information and data in order to analyze situations and make quick decisions.

The IHSE KVM system manages the balancing act between operational flexibility and effective data security.

- All computer systems, hard drives, USB and LAN ports are located away from employees in a secure area maintained by authorized personnel, accessible only with appropriate security clearance.
- USB ports on user workstations block all data transmission except keyboard and mouse signals. This prevents the installation of harmful malware or spy software.
- To prevent unauthorized access to sensitive data, access control restrictions managed by the system administrator determine which users and workstations have access to specific computers and levels. Mixed classified (multi-class) environments can be configured with areas at different levels of confidentiality,
- System logon is secured by means of two-factor authentication. A monitoring function can be used to display attempts to violate rights or trigger an alert.
- Certified IHSE secure extenders have integrated EAL4+ isolators that prevent bidirectional data flow. These prevent injection of malware into the computer via a computer monitor's return channel.
- Other attacks through audio, keyboard and mouse interfaces are also prevented within the IHSE Secure range.

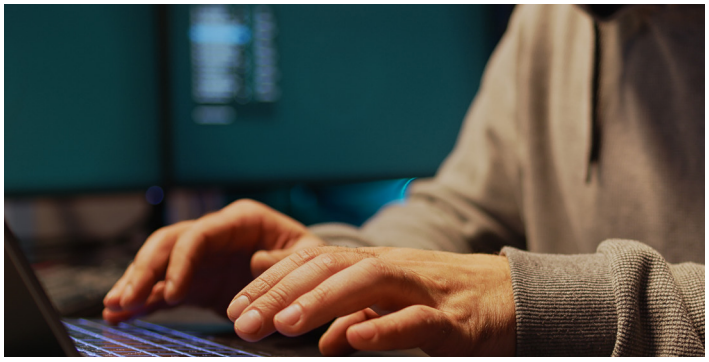


4.2 EXTERNAL THREATS

4.2.1 RISKS FROM IP AND EXTERNAL CONTROLS

Transmission of data via publicly accessible Internet Protocol (IP) networks represents a major vulnerability. Data can be intercepted or manipulated during transmission.

- Data transmission within IHSE KVM systems is based on a protected, proprietary network protocol.
- If required, IP access can be added to a KVM system, for example for remote maintenance or administration tasks. IHSE offers special IP gateways which act as isolators and continues the physical separation between KVM and IP networks. This enables IP connectivity while maintaining a fully secure system.
- The core KVM matrix is physically separated from the IP network and operated completely independently of the IP infrastructure. Network errors therefore have no impact on the overall system.
- Strict separation of control and data signals provides additional security for the system. Access to the matrix via external media controllers or systems can be restricted for security-critical installations (in-band control).



4.2.2 EAVESDROPPING ATTACKS

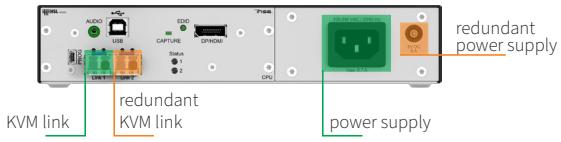
- In highly secure application scenarios, such as in the military sector, the use of certified IHSE security extenders is recommended. These restrict transmission of audio signals from the source to the user, making it impossible for the loudspeaker to be used as a microphone to listen to sound in the room.
- The use of fiber optic cables for signal transmission also prevents signal detection via electromagnetic radiation and is therefore recommended for installations in high-security areas.

4.3 RELIABILITY

Business interruption and system failures can cause significant damage, especially in mission-critical scenarios where real-time reaction is crucial.

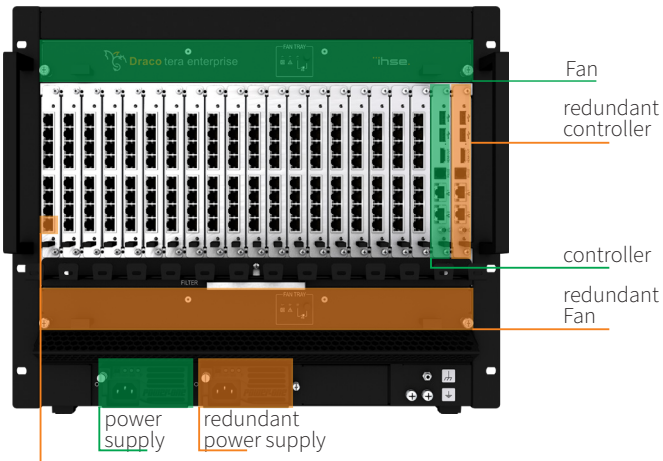
To prevent total system failure, IHSE products offer comprehensive system redundancy, that enables continuous operation or restoration as quickly as possible. In addition, many components and modules can be replaced during live operation (hot-swap), allowing quick and uncomplicated intervention without system downtime.

- The KVM endpoints on the user and source side can be provided with dual power supplies and redundant data paths.



- Each extender unit is available with two KVM network connections for primary and secondary network links. The secondary network is a fully functional backup network that immediately takes over operation if the primary network fails. The KVM matrices also have redundant power supplies and can be specified with multiple controller boards, with the secondary unit taking over control in the event of a failure.
- Full standby matrix redundancy can be implemented, which re-routes signal through a backup matrix in the event of a primary matrix failure.

The IHSE KVM system offers many additional design options that protect against system failures and meet specific application requirements.



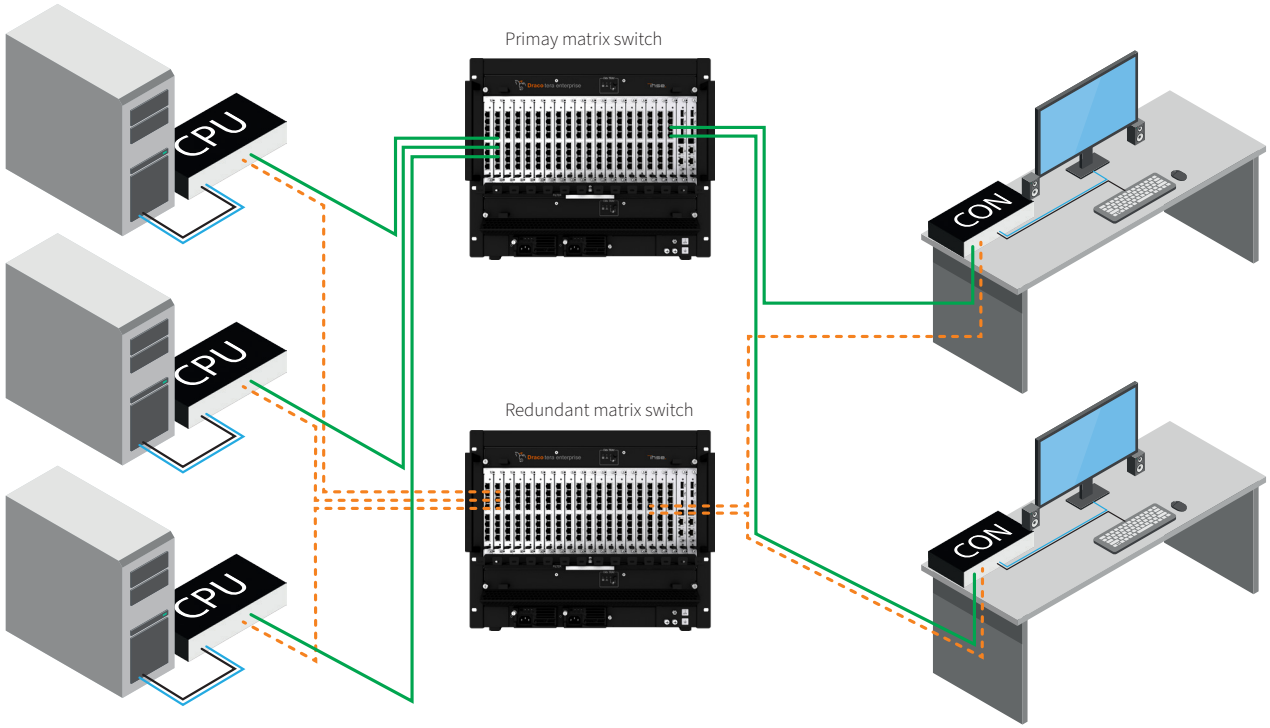
Ports freely selectable;
in case of failure, any other free port can be selected

HOT SWAPPABLE:
faulty components can be replaced during operation

DO YOU HAVE ANY QUESTIONS?

Would you like to find out more about how we protect against cyber attacks and make your KVM system fail-safe?

Ask our experts: gov@ihse.com



5. TESTIMONIALS

„As an IT system administrator, I use IHSE's KVM products to implement many scenarios and tools that make my work easier with little effort - including sandbox or air-gap environments for software testing. I can maintain my server landscape and workstation PCs directly from my workstation in the office. I can even work across different, isolated IP networks“

Niels S., IT system administrator

„As a security guard, I am responsible for the security of our company facility. Thanks to the KVM system, significantly fewer patrols are required in the office buildings, leaving more time for monitoring our critical data centers. The offices are free of PCs and storage media, and there are no entry points to the network via TCP/IP access.“

Günther F., facility manager

„In our IT company, the IHSE KVM solution enables us to simplify many organizational and security measures or make them obsolete. We no longer have any storage media or IP access in our offices. Thanks to KVM, everything is relocated to the data center.“

Andreas K., security officer

„In the past, we often had to spend weeks preparing for events in security-sensitive areas in order to achieve the required security levels in all conference rooms. The use of KVM technology saves us all this effort, as no changes to the cabling or hardware infrastructure are necessary - all that is needed is a simple adjustment of the configuration.“

Lena B., event manager

6. CONCLUSION

The strategies of cyber attackers are rapidly evolving and becoming more sophisticated. Their motives may be purely financial or may be in pursuit of geopolitical interests. Wars and acts of terrorism are increasingly fought in cyberspace and states use cyber attack as a means of gathering information, sabotage and to carry out disinformation campaigns. Critical infrastructure such as energy and water supplies, transport systems and healthcare are also increasingly being targeted to destabilize and weaken states. Governments and commercial entities need to be proactive in protecting their systems.

Nations and organizations must remain ahead of cyber criminals and be prepared for changes in the nature of threats. Security risks should be eliminated in advance by anticipating, identifying and eliminating potential threats to data security. Through the use of KVM technology, organizations can significantly mitigate the human risk factor; whether intended or accidental. KVM architecture completely isolates critical systems from the outside world without imposing any operating restrictions.

Security and user-friendliness considerations can be balanced. For the user, KVM offers fast access from their own workstation to all necessary resources in real time. For administrators, KVM means less maintenance and the removal of improper device use. For managers, KVM brings both security and cost savings through the shared use of resources and longer device lifecycles, along with reduced failure cycles and lower device downtime.

As conditions change, the modular design of the IHSE KVM system permits rapid and simple expansion without the need for complete replacement. The highly secure KVM system is future-proof and allows organizations to remain one step ahead of cyber criminals.

IHSE GMBH
Benzstr. 1
88094 Oberteuringen
Germany

Phone: +49 (7546) 9248-0
Fax: +49 (7546) 9248-48

info@ihse.com ■ www.ihse.com

SECURE KVM SOLUTIONS ■ MISSION CRITICAL 24/7 ■ MADE IN GERMANY