

White Paper

High Security Networks Isolation and Secure KVMs

Non Classified Document

Table of Content

Overview.....	3
1. The environment – the challenges.....	4
1.1. Physical Network Separation.....	4
1.2. High-Security organizations and internet	5
1.3. Integration between different organizations	6
1.4. Networks integration risks	7
2. Available Solutions.....	9
2.1. Option 1 – LAN Switching	9
2.2. Option 2 – Multiple PCs and peripherals.....	11
2.3. Option 3 – Commercial KVM.....	13
2.4. Option 4 – Conventional Secure KVM (2 nd Generation)	18
2.5. Option 4 – HSL Secure KVM (3 rd Generation).....	21
2.6. Option 5 – HSL Secure KVM Combiner.....	24
2.7. Option 6 – Modular Secure KVM Combiner	26
2.8. Option 7 - Virtualization and mixing networks at the server	28
3. Aspect of Secure KVMs	29
3.1. The KVM as a target for attackers	29
3.2. The SKVM as a gateway or peripheral filter	30
3.3. The Trusted SKVM.....	30
3.4. The use of SKVM for Copy – Filter - Paste	31
3.5. KVM Users - Work flow and non-work flow users.....	31
4. Appendix A - The design of the modular KVM Combiner	33
5. Appendix B – Security Gaps and Common Criteria Levels.....	35
6. Appendix C - Intrusion Scenarios Analysis	36

Overview

This document describes HSL view of network separation – integration dilemmas and solutions.

In the first chapter deals with the environment, the need for physically isolated networks, the need for networks integration with mixed security levels or security gaps. In particular we will try to explain the driving forces in opening secure organizations to the hostile outside world of the internet.

In the second chapter we would describe the options to provide integration between isolated networks to enable efficient user access. With each optional solution we will cover potential risks and benefits. Options described will cover multiple PC and user consoles, KVMs, Secure KVMs , KVM Combiners and soft isolation (such as virtualization).

In the third chapter we briefly discuss the various security and operational aspects of secure KVMs in isolated networks environments.

Appendix A discusses the design of the KVM combiner as an example of secure KVM.

Appendix B provides an example of intrusion scenarios of the KVM Combiner.

As this white paper is non-classified, references and description of classified features omitted here. If you would like to receive references or further information please contact: info@highseclabs.com

The effort invested by governments and agencies to crack KVMs is comparable to the effort invested to crack crypto codes, keys or firewalls. In many cases it would be easier to leak information through an attacked KVM compared to leak it through deciphering data that was encrypted using strong encryption.

1. The environment – the challenges

1.1. Physical Network Separation

Computer networks in many organizations are continuously challenged by various security threats. The popularity of the internet and the availability of portable mass-storage devices introduce severe internal and external threats to most organizations. Defense and government organizations with higher security networks and much less tolerance for data leakages are forced to physically isolate their secure networks from other less secure networks thus creating a situation that a single organization or a single employee need to operate in several different isolated networks having different security levels. Isolation between these networks is a key concern as a small leakage of data between two networks may cause catastrophic results to the organization involved.

In the older days of the cold-war, defense organizations were challenged by electromagnetic emanations eavesdropping or leakages. TEMPEST standards for products and building were formed and enforced to assure that critical data would not leak through electromagnetic fields to the wrong hands. Physical separation of Red – Black networks was common practice with proper positioning of end equipment to minimize the radiation leakage risks. Today TEMPEST is a smaller threat to information security compared to the new software related “soft” threat such as viruses and Trojans. In the last 10 years, TEMPEST equipment is used mostly in tactical platforms (submarines, aircraft, vehicles) and in only key locations for office desktop users.

The reasons that organizations are physically separating networks today:

1. **It is the only reasonable way to assure separation (no leakages) between networks. All other “soft” methods are breakable.** Desktop computers and servers are un-trusted by definition! Every method that relies on code – can be attacked or modified to cause leakage.
2. Segmentation – if one network was successfully penetrated by an attacker, the effect would not propagate to other networks. The damage is limited.
3. Many less secure networks may have external access or even internet access. Leakage to these networks may mean perfect gateway to the outside world.
4. Different network security and user authentication and security may be needed for different networks having different security level.
5. Electromagnetic leakage between networks.
6. Reliability and disaster recovery – independent networks may be designed to provide higher availability.
7. Networks coming from several different organizations or operational units.

As there is a high installation and maintenance cost for multiple isolated networks, in recent years there was a trend to consolidate networks and reduce their number in some organization. Still network consolidation in high security organization is not very common due to the growing security risks involved. In many high security organizations today it is not uncommon to see 10 different networks routed to a single user.

The industry is now providing creative security products to keep networks fully isolated while handling key operational issues such as:

1. **User operational issues** - Integration for the user through secure KVMs and KVM Combiner.
2. **Infrastructure cost** – Integration of physical networks having different security level through products like NOA (Network Overlay Appliance).
3. **Approved data export / import** - “Copy – filter – paste” for user efficiencies through lower cost data-diodes and better KVMs.

1.2. High-Security organizations and internet

The introduction of the internet and e-mail forced many high-security organizations to open their internal information system to the outside world. Many organizations opened access to the internet through procedures while others open through exceptions or procedure violations.

This access became a necessity. It is very difficult to think about any organization that may operate as an independent IT island in the world of networked IT infrastructures.

There may be many reasons to open the IT systems to external networks / internet:

- Lower cost communications with remote branches or sites possible through the internet (as opposed to expensive and limited leased lines).
- Access for home users or remote employees
- Enabling user access to internet resources for information collection, analysis, updates, news etc.
- Enabling users access to external emails
- Enabling limited remote access for partners, sub-contractors, affiliated organizations etc.
- Synchronization with web-sites and remote data-bases
- Voice over IP and Video over IP applications (such as Skype and Messenger)
- Users access to entertainment or social resources (for example on board an aircraft carrier to provide crew entertainment at off-duty hours).

There may be many other valid reasons that require certain level of access to external networks. Each organization is challenged by daily users request to open access to various external resources.

Without this access user will be inefficient or would not be able to perform certain job tasks or simply will be bored. There may be many arguments why not allowing such access (wasting of users time is a strong one) but still the most dominant reason would be – Security Threats.

Network integration enables simultaneous user access to two or more networks. Network integration can be achieved through several mechanisms that will be presented in this document.

1.3. Integration between different organizations

Another complex challenge is the case of integration between two different organizations. This case is specifically challenging not only due to technical issues but also due to political and organizational responsibility issues.

In many real-world environments it is necessary to enable access from one secure organization to another secure organization. An example for this is a city emergency room having access to ministry of defense system on one side and the police at the other side. Needless to mention that in real world there may be many networks involved that that makes things much more complex.

High-security organization that allows access to their network by another organization may be very sensitive and fearful due to the following concerns:

1. The risk that intruders will intrude the organization network through the other attached organization network. This scenario is typically the biggest fear. Trusting another organization security outside the organization jurisdiction is very problematic issue. “We don’t know what they are doing and therefore we cannot trust them.”
2. The risk of data leakage between networks
3. The difficulties in managing user’s permissions at another organization.

Only one weak point is needed to leak the organization sensitive information into the wrong hands. If this weak point exists in another (connected but uncontrolled) organization. This typically causes tension between connected organization information security officers. Even if the security level of the two organizations is similar, the challenge will be similar as no side will fully trust the other side’s security measures.

There are 3 available solutions to this challenge:

1. To provide remote presentation of the specific applications needed using Citrix presentation server or Microsoft RDP. This option removes the immediate risk of networks leakage but still information may leak and intruders may access sensitive resources.
2. To use a secure KVM to enable specific users access to both networks.
3. To use unidirectional data diode to ensure that the other connected organization will have “view only” pushed data. Unidirectional data flow may reduce the risks of data leakages in the reverse direction and solve many of the issues.

Regarding the first method it should be noted that in recent security evaluations it was shown that capable intruders could intrude the presentation server through a session. From the presentation server the intruder access to the attached secure network was a straight forward task.

1.4. Networks integration risks

Integration or consolidation between networks having different security levels raises immediate concerns about potential data leakages from the higher to the lower security networks. Intruder may penetrate the lower security network and through the integration point, he/she may access or attack the higher security network from the inside.

Integration of networks having different security levels may cause various information security threats:

1. The potential for intruders to access the secure networks or classified data through that opened (externally attached) network.
2. The potential of malicious code to enter and operate in the organization’s networks. For example: PC or server infected by spy-ware or virus.
3. The potential of unaware users to leak secure information between the internal and external networks (for example users sending classified files on outside non-secure email).
4. The potential of fully aware users to leak secure information between the internal and external networks (for example users installing a spy ware program on their desktop).
5. The potential of attacking a network from the inside causing overloads and failures.
6. *The potential of intruders or internal users to install a temporary or even permanent leakage between internal and external networks.*

In general when two isolated networks are getting closer, it is clear that only one weak point is needed in order to leak data between these networks or penetrate the higher security network. That weak point has higher probability to exist if there are multiple points of vulnerability or points of integration between the two isolated networks.

From all the bad scenarios described above, it seems that the worst scenario is number 6 – this is the real nightmare of any IT security officer. **The potential that someone may receive on a daily basis the most classified and up to date information in that organization, without any physical site intrusion (and even without leaving a trace behind) is definitely the worst threat.**

There is only one threat that may present a higher risk – the capability of bad guys not only to receive data but also to inject data back or to damage the organization’s IT system at a critical time. For many defense organizations this is the ultimate threat and fear – having wartime hidden “remote control” or “time bomb” code inside their secure IT system.

2. Available Solutions

2.1. Option 1 – LAN Switching

The term LAN switching applies here to an electromechanical switch rather than to electronic switch (layer 2 or layer 3). This solution is shown in the block diagram in figure 1 bellow. A single PC with a single LAN card connected to a switch box attached to 2-3 different copper LANs.

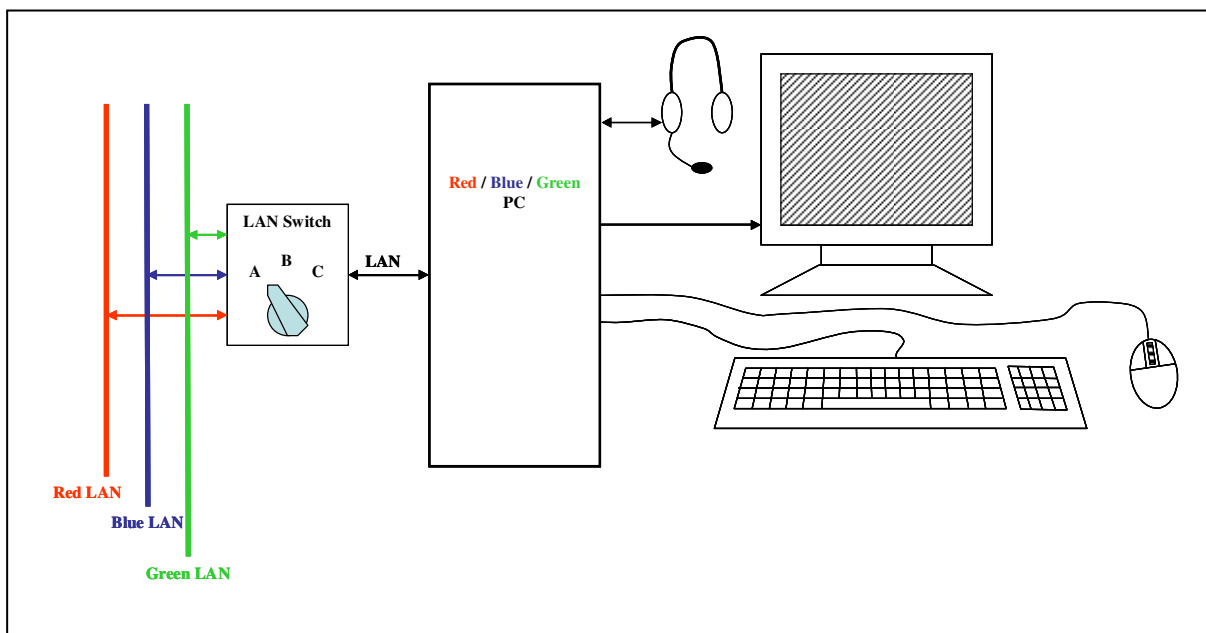


Figure 1 - Multiple networks separation using LAN Switching

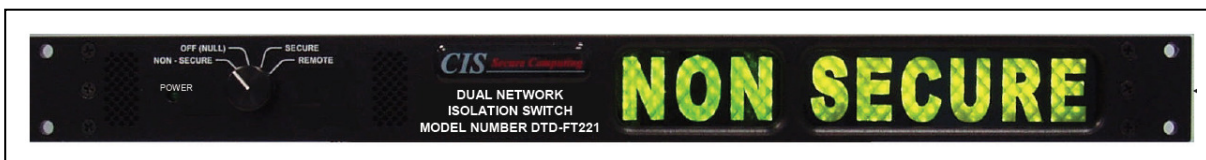


Figure 2 – CIS Dual network isolation switch

This method was very popular in high-security organizations in the 80's and 90's but almost disappeared several years ago. It became a major threat as security organization found the easiness of making data leakages in a single computer attached to two isolated networks. Some organizations requested users to reboot their computers before switching but still is regarded as the most

dangerous way of isolating networks. The CIS dual network isolation switch shown in figure 2 is an example of such device that enables four functions at once –

1. Physically switch between isolated networks.
2. Provides clear visible indication of the user selected network (color coded Non Secure – Secure light).
3. Forces the computer to reboot by modulating their power input.
4. Mechanical assurance that networks cannot be crossed.

Advantages	Disadvantages
Low cost (switch is cheap, single PC, single set of peripherals).	Significant security risks as a single computer connect to two isolated networks. Standard PC is regarded as huge security hole... Even after reboot
Strong galvanic isolation between networks. Possible due to the simple electromechanical design.	Does not support mix of copper and fiber LANs. Normally does not support Giga LAN.
The possibility to provide mechanical solution to avoid advertent or inadvertent LAN crossing.	Difficult to use – long time to switch between networks due to reboot time.

Table 1 – LAN Switching isolation advantages and disadvantages

In general, this method regarded as safe when electrical emanations were the primary risk, today viruses and malicious code is the primary risk and therefore this type of isolation is not in common use anymore and regarded as very unsafe.

To further illustrate the potential danger in this concept, in recent work done by HSL, laptop computer vulnerabilities were analyzed to find potential ways to use same laptop at different networks.

HSL found more than **20 different vulnerabilities** that need to be fixed / addressed at any level from chipset, motherboard, BIOS to OS and applications (assuming forced reboot and two isolated encrypted disks)!

2.2. Option 2 – Multiple PCs and peripherals

The most straightforward method is to connect two or more independent sets of computers and peripherals (see figure 3 below). This method becomes unpractical when more than three isolated networks are needed as the user desktop becomes a jungle of wiring, displays and peripheral devices.

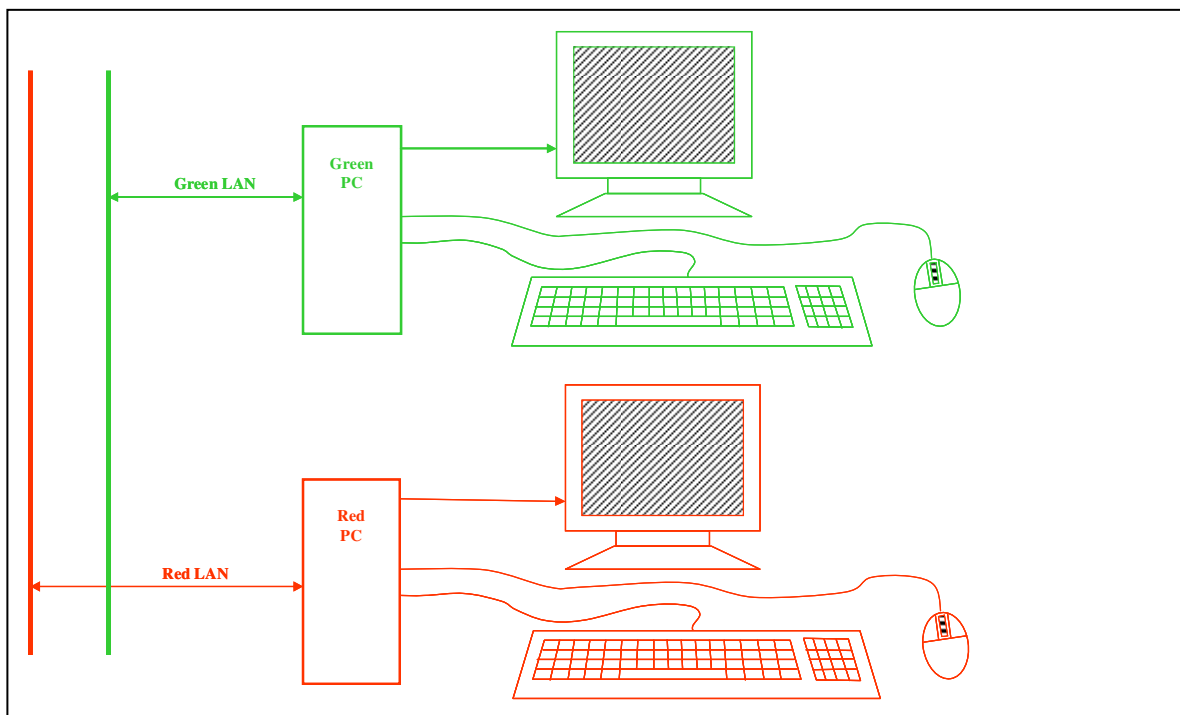


Figure 3 - Multiple networks separation using multiple PCs and peripherals

The use of this method is also causing real-estate problem as user displays becomes larger and larger. 15" LCDs are now replaced by low-cost 24" wide LCDs. Any attempt to arrange a user desktop with 2 displays like that will result office space rearrangement...

In addition to this problem, many of the users are using today multiple displays for each host and the resulted desk space leaves no place for the user anymore.

<i>Advantages</i>	<i>Disadvantages</i>
Physically secure - Strong isolation between networks as no integration point exist.	Operationally unsecure – users tend to make mistakes as desktop space becomes crowded.
Easy for the user to identify the security level (network) in use if keyboards and displays are marked properly.	Difficult to use – two isolated environments. Potential for “Fake GUI” threat.
	Large desktop space needed for PC and duplicated sets of peripherals. Unpractical for larger number of networks or for multiple displays for each host.
Fast switching time between environments.	Lower reliability, a lot of cabling.
Medium cost – no special equipment needed (still 2 or more sets of equipment needed to be maintained for each user)	User authentication in multiple networks is replicated.
	Higher maintenance costs due to the duplicated environments.

Table 2 – Multiple networks separation using multiple PCs and peripherals advantages and disadvantages

2.3. Option 3 – Commercial KVM

This method is by far the most popular one today even in high-security organizations as commercial KVMs are readily available for very low-cost. Many high security organizations are using commercial KVMs because they are completely unaware to the big security risks involved.

Typical commercial KVM setup is shown in figure 4 bellow. As shown in this figure the isolated networks integration takes place at the user's desktop. It is assumed that the integration is in the form of switching between sources but in reality many options exists to turn this integration into data leaking between the isolated networks.

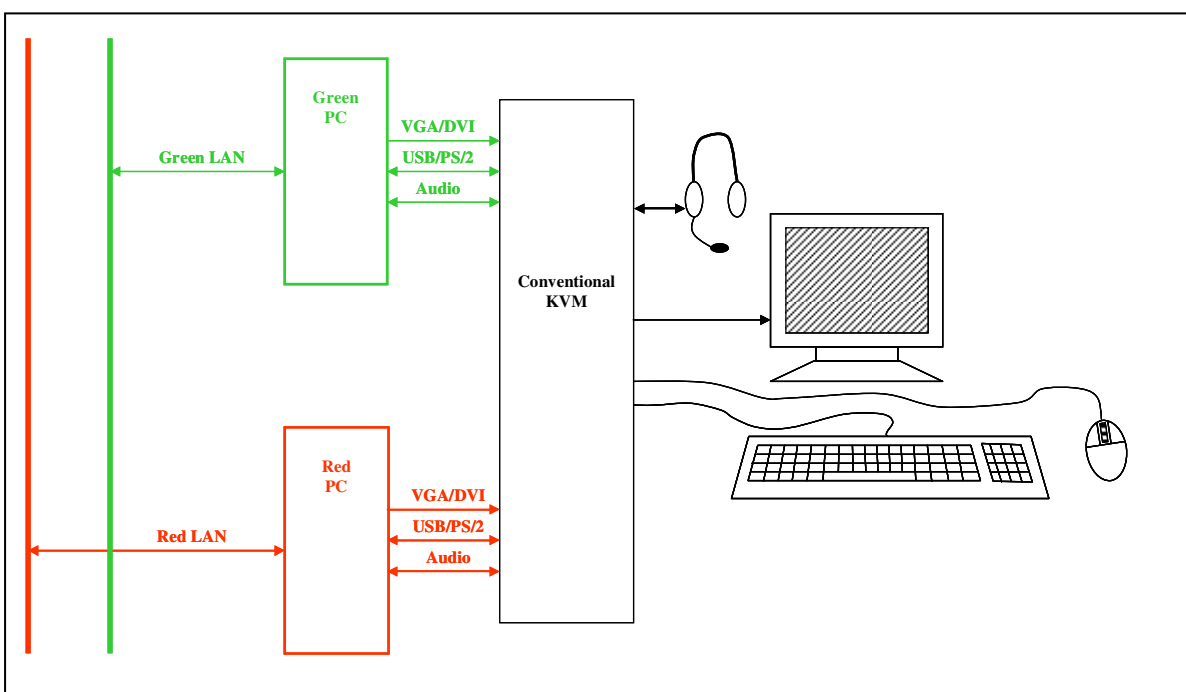


Figure 4 - Multiple networks separation through multiple PCs and a commercial KVM

Video and peripheral lines connected between the isolated PCs and the KVM by cables. Simple solid-state video MUX route one video input to the single video output based on user inputs. User can select one output through keyboard hotkeys detection or by pressing push-buttons.

Peripheral channels are normally connected to microcontroller to enable error free boot of connected PCs. This microcontroller setup is typically the vulnerable point in the commercial KVM as it may leak data between channels.



Figure 5 – An example of a 4-ports commercial KVM from Belkin

<i>Advantages</i>	<i>Disadvantages</i>
Secure to certain extent – some isolation between networks.	Security risk due to the use of COTS KVM. KVM may be tampered or abused to leak data.
Medium cost – low-cost KVM needed (still 2 or more PCs need to be maintained for each user)	Ease of use – medium. Two isolated environments but simple switching between.
Fast switching time between environments.	Difficult for the user to identify the security level (network) in use.
	Many low-cost commercial KVMs are manufactured by un-trusted sources.
	User authentication in multiple networks is replicated.
	Exposed data I/O (USB) ports at the KVM
	Poor galvanic isolation between PCs (unless one network is fiber)

Table 3 – Multiple networks separation through multiple PCs and conventional KVM advantages and disadvantages

The reliance on the older PS/2 protocol does not relieve the security risks of conventional KVMs as keyboard logging and bi-directional data-exchange can still happen in PS/2.

The use of commercial KVM can be a weakest link that may be abused by an attacker to cause data leakages between connected networks. In general high security organizations like to control the integration point between the networks and therefore many of them defined “Secure KVMs” as a controlled solution for this challenge. Still due to security vulnerabilities **many organizations would not allow commercial KVMs in sensitive environments.**

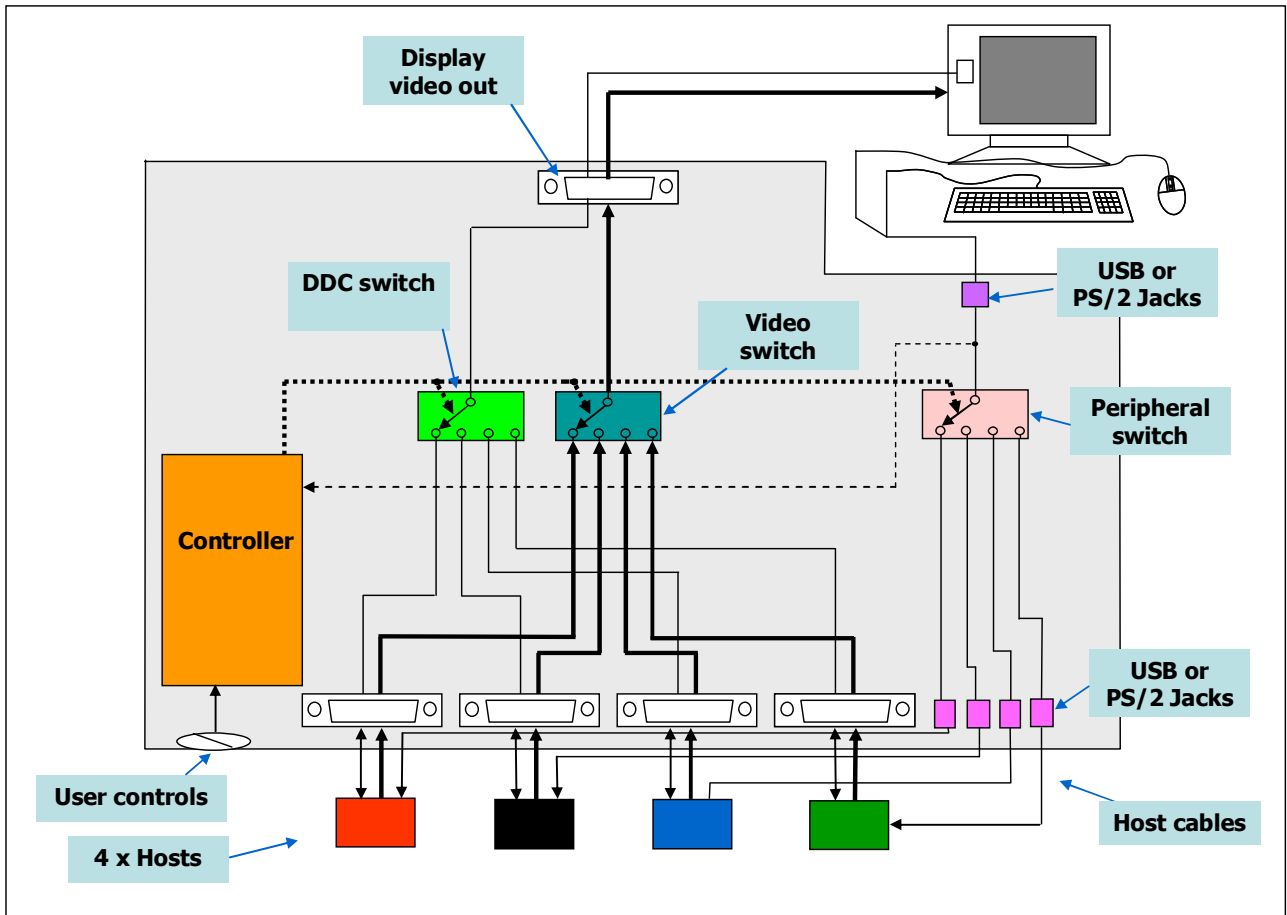


Figure 6 – 4-Ports commercial KVM Block diagram

No.	Security Risks
a)	Proper isolation between hosts cannot be guaranteed – hosts may leak to other hosts attached to same KVMs through multiple mechanisms like signaling.

b)	Firmware may be tampered or replaced remotely or physically
c)	Product may be physically tampered or completely replaced by a modified product
d)	Product may have buffers of keyboard strokes that may be used to create a leakage
e)	Display Plug and Play channel may be abused to cause data leakages.
f)	USB ports may be used for unauthorized peripheral devices such as mass storage devices or wireless keyboards.
g)	KVM may be used as key-logger to store keyboard data
h)	User confusion and poor situation awareness. User may be abused by a tampered host.

Table 4 – Summary of security risks using commercial KVMs

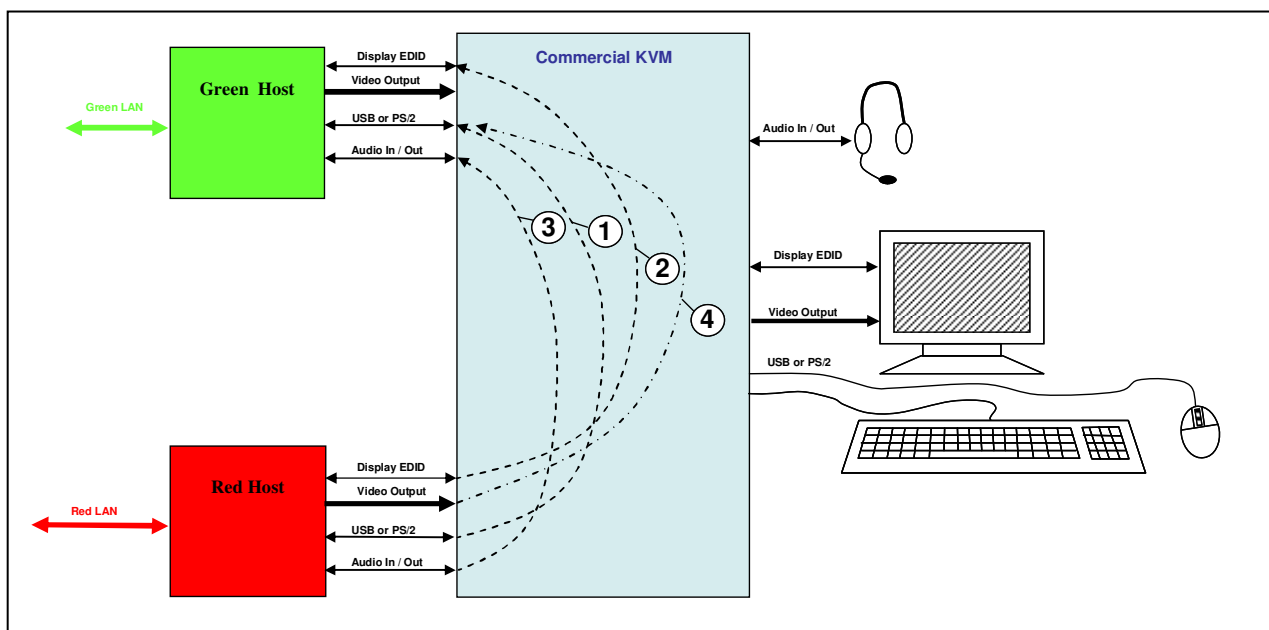


Figure 7 - Commercial KVM primary leakage modes

Figure 7 illustrates the primary leakage modes in commercial KVM. Needless to say that there may be other leakage modes but it is enough to understand the 4 modes shown in the figure to understand the wider risks picture.

In general leakages may be permanent, conditioned (based on time or specific triggering events) or may be delayed in time.

Mode 1 is leakage across peripheral ports. It may exist with both PS/2 and USB protocols with similar risks and results. This is by far to most tested mode that may be implemented even without KVM device tampering. Keyboard buffers inside KVM may be abused to cause this type of leakage.

Mode 2 is DDC leakage across video ports. It is using the bi-directional display Plug and Play serial lines to leak information between hosts. This is another popular mode that may be implemented even without KVM device tampering (using signaling methods).

Mode 3 is analog leakage across audio ports. It is using the bi-directional audio path (headphones to microphone) to deliver audio or even data across channels. This leakage is based on the capability of standard PC audio chips to perform audio analysis of simple soft modem. Red PC audio card is used to generate audible modem signals while green PC audio card is used to convert audio back to data. Small amplitudes of audio crosstalk between channels may be used to leak data without the need for physical tampering.

Mode 4 is conversion leakage across different ports. It is more complex to implement but its potential use may be dangerous due to the difficulty to detect it. In this example, a special circuitry is “planted” inside the KVM to capture video frames of red host and transfer (through slow streaming) this data into the green network. Although hardware to perform this conversion is complex, actual size may be small enough to fit inside small commercial KVMs.

The methods presented above are just typical examples of attacks on commercial KVMs. Secure KVM may be attacked by similar methods although new methods may be used to crack the advanced security features available in these products.

2.4. Option 4 – Conventional Secure KVM (2nd Generation)

For more than 10 years there are KVM products in the market that are classified as secure KVMs. These products are usually certified through Common Criteria to EAL 4+. Secure KVM products are special KVMs that were designed to operate between isolated networks based on the US NIAP published Protection Profile or other documents issued by other governments.

Conventional secure KVMs offers higher security compared to commercial KVMs in the following areas:

- Always-active anti-tampering sub-system to detect potential enclosure intrusion and deactivate the device. Most anti-tampering systems are battery powered and using a single micro-switch as a sensor.
- Read only firmware residing on OTP (One Time Programming) or ROM (Read Only Memory).
- No buffer or memory to prevent data leakages during switching (signaling).
- No hot keys or on-screen display – to prevent KVM leakages.
- Tamper-evident labels to indicate mechanical tampering.
- Circuits are soldered directly onto the Printed Circuit Board (PCB) to make tampering without soldering equipment impossible.
- Microcontroller per port for isolation.
- Electrical isolation between host ports. Avocent claims 60 dB separations between ports.
- Optional filtered CAC (Common Access Card) port for smart-card reader.
- Some basic isolation in EDID (Display Plug & Play) channels.
- Government (NIAP) approval through Common Criteria or TEMPEST evaluation.

While existing secure KVMs are better than commercial KVMs, still they are vulnerable to sophisticated attackers and becoming less and less effective against new intrusion techniques.

One particular problematic area is the Anti-tampering. Many of the existing EAL 4+ secure KVM devices are fitted with battery powered anti-tampering system. The purpose of this system is to detect potential mechanical intrusion and irreversibly disable the KVM functionality to warn the user. Most products are using a single micro-switch positioned between the enclosure bottom part and the top cover. An attempt to remove the top cover will release the micro-switch and activate the anti-tampering circuit and cause irreversible firmware modification that disable normal device use. The use of anti-tampering method without



Figure 8 – Avocent/Emerson SC540 4-ports Secure KVM

In this setup two or more PCs are connected to separate networks. The USB or PS/2 of each computer is connected to the secure KVM through a cable. Optional galvanic isolation enables the two computers ground planes to be floating (isolated). Each video input channel is passed through data diode to assure isolation and unidirectional flow. Monitor DDC (Plug & Play) is emulated by isolated devices (not shown here). Video switch implemented by MUX connect one video input to the video output port based on user selection.

USB or PS/2 keyboard / mouse connected to the Secure KVM via two isolated host emulators. These host emulators assures that all bi-directional protocols will be reduced to a uniform unidirectional data flow passed through a switch and another set of optical data-diodes. The unidirectional peripheral data stream is then routed to the device emulators connected to the attached hosts through cables. This peripheral path implementation enables absolute peripheral devices filtering – no storage devices will be supported.

Optional anti-tampering circuitry enables tampering detection and reporting when needed.

Optional TEMPEST interfaces enable fiber link to monitor and use of special TEMPEST peripherals.

Optical data diodes are electronic elements that converts electrical signals coming from one side to light, received by another side and converted back to electrical signals. These elements assuring uni-directional data flow by reliance on physics. They are also capable of creating galvanic isolation between the two sides if needed (no common ground).

Advantages	Disadvantages
High security – at least against basic attacks.	Security risks especially when used between big \security gaps.
Some protection of peripheral ports – USB / PS/2 ports are unidirectional by optical isolators. Strong peripherals filtering.	Ease of use – medium. Two isolated environments but simple switching between.
Medium cost – higher cost KVM needed (still 2 or more PCs need to be maintained for each user)	Difficult for the user to identify the security level (network) in use.
Fast switching time between environments.	User authentication in multiple networks is replicated.
Optional high galvanic isolation and anti-tampering.	

Table 5 – Multiple networks separation using HSL secure KVM advantages and disadvantages

2.5. Option 4 – HSL Secure KVM (3rd Generation)

As a result of extensive threats and existing KVM products evaluation, HSL designed a new generation of secure KVMs (third generation).

The design goals behind these products were:

1. To provide better security compared to second generation (conventional) secure KVMs. In particular to address new attack techniques and new threats. HSL designed these products to meet **Common Criteria EAL 6/7**.
2. To support the latest display and peripheral devices available today.
3. To provide additional user functionality compared to second generation (conventional) secure KVMs.

This method developed and patented (pending) by HSL in 2008 as a safe KVM solution for very high security organizations.

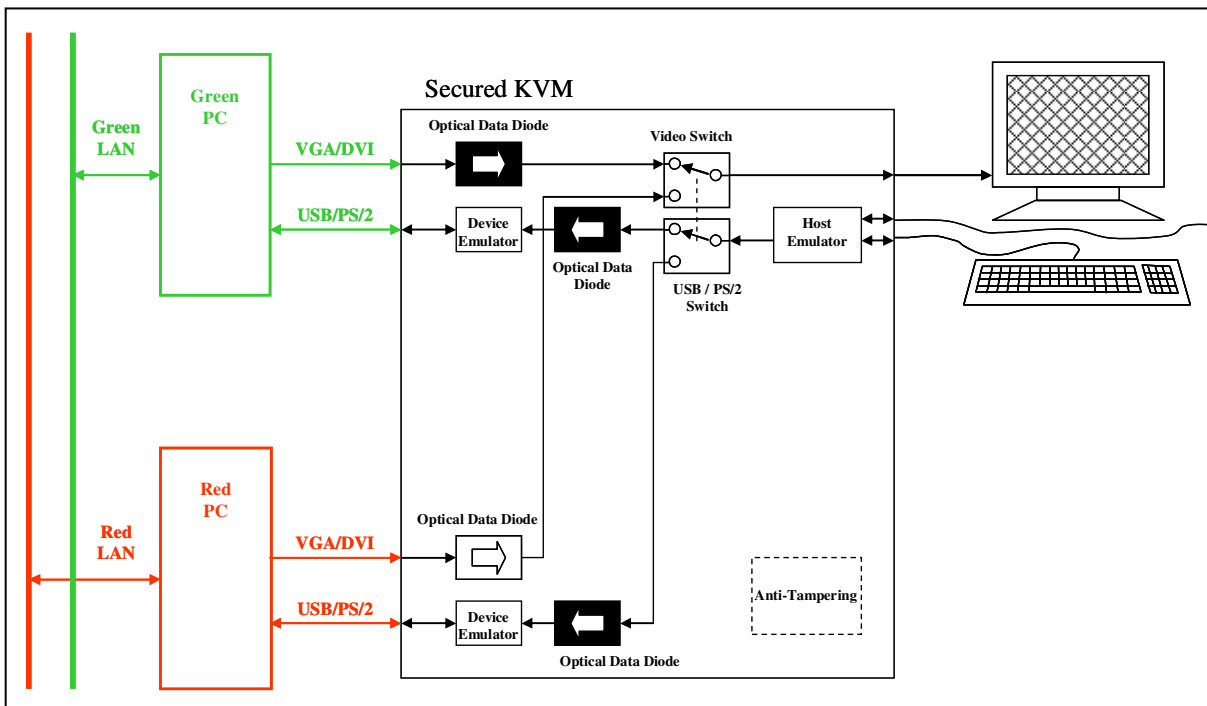


Figure 9 – Multiple isolated networks separation using HSL Secure KVM

In this setup two or more PCs are connected to separate networks. The USB or PS/2 of each computer is connected to the secure KVM through a cable. Optional galvanic isolation enables the two computers ground planes to be floating (isolated). Each video input channel is passed through data diode to assure isolation and unidirectional flow. Monitor DDC (Plug & Play) is emulated by isolated devices (not shown here). Video switch implemented by MUX connect one video input to the video output port based on user selection.

USB or PS/2 keyboard / mouse connected to the Secure KVM via two isolated host emulators. These host emulators assures that all bi-directional protocols will be reduced to a uniform unidirectional data flow passed through a switch and another set of optical data-diodes. The unidirectional peripheral data stream is then routed to the device emulators connected to the attached hosts through cables. This peripheral path implementation enables absolute peripheral devices filtering – no storage devices will be supported.

Optional anti-tampering circuitry enables tampering detection and reporting when needed.

Optional TEMPEST interfaces enable fiber link to monitor and use of special TEMPEST peripherals.

Optical data diodes are electronic elements that converts electrical signals coming from one side to light, received by another side and converted back to electrical signals. These elements assuring uni-directional data flow by reliance on physics. They are also capable of creating galvanic isolation between the two sides if needed (no common ground).

This solution is simple and safe for environments having top secret or national security networks. It is typically used for simple tasks users. Users working daily between networks (intelligence analysts or operations) may need easier solution such as KVM Combiner shown bellow.

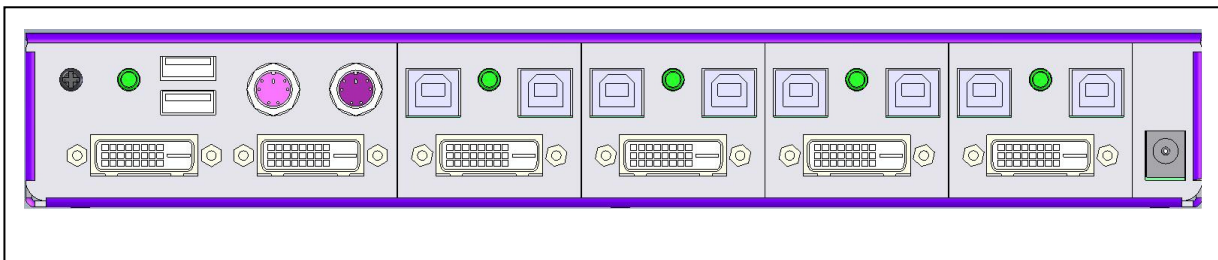


Figure 10 – HSL K224 Dual displays 4-Ports secure KVM

Advantages	Disadvantages
-------------------	----------------------

Very high security - Optical isolation between channels.	Ease of use – medium. Two isolated environments but simple switching between.
Complete protection of peripheral ports – USB / PS/2 ports are unidirectional by optical isolators. Strong peripherals filtering.	Difficult for the user to identify the security level (network) in use.
Medium cost – higher cost KVM needed (still 2 or more PCs need to be maintained for each user)	User authentication in multiple networks is replicated.
Fast switching time between environments.	
Optional high galvanic isolation and anti-tampering.	

Table 6 – Multiple networks separation using HSL secure KVM advantages and disadvantages

2.6. Option 5 – HSL Secure KVM Combiner

This method developed and patented (pending) by HSL in 2008 to further improve the user experience while maintaining highest level of security. It addressed the needs of specific users who are working daily in several isolated networks. These users are characterized by the need to enable structured processes between networks. A typical example would be intelligence analysts that their daily job involves data collection at one network to build a report on another network. Security gap between networks may be very high and therefore KVM Combiner should implement data security measures similar to HSL Secure KVM. To enable easy work across isolated networks, the KVM Combiner uses advanced video processor to create interactive “Windows like” user experience.

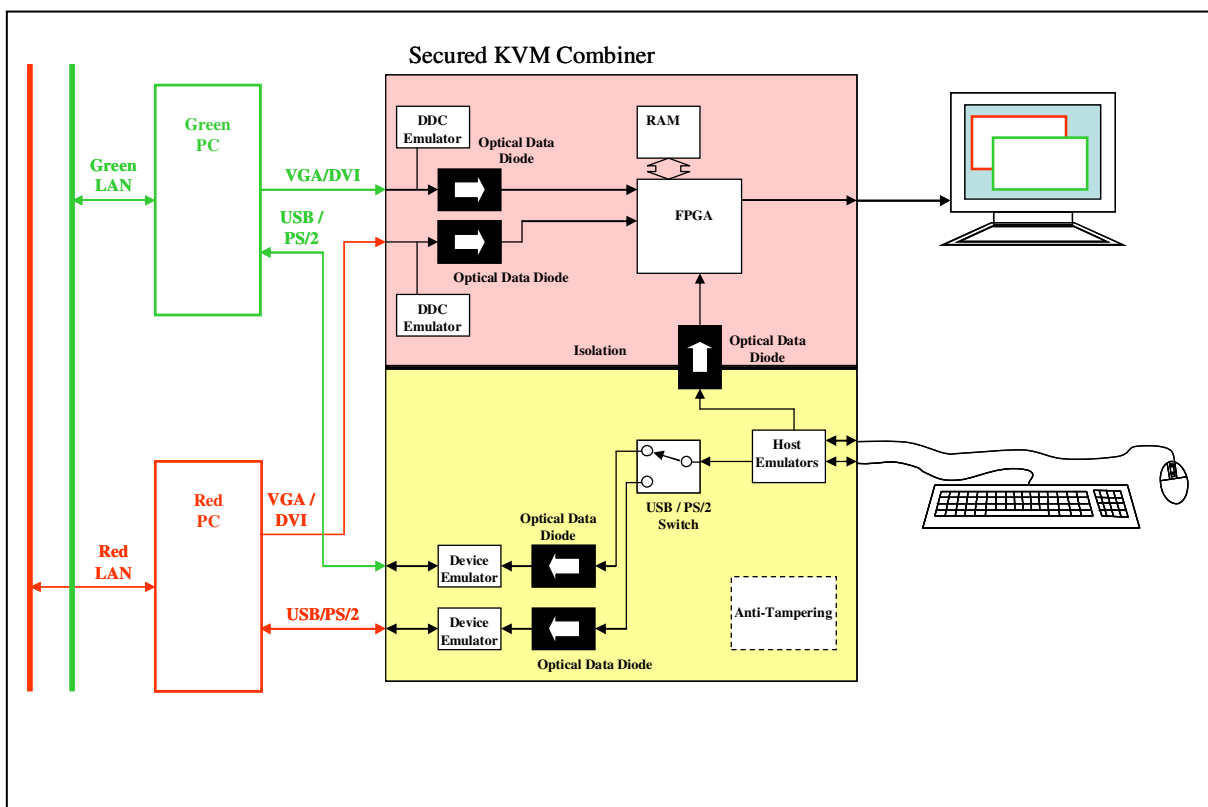


Figure 11 – Multiple PCs and Secure KVM Combiner

The video section of the KVM Combiner uses fast Field Programmable Gate Array (FPGA) and DDR memory to process video received from connected sources and generate high-quality high-resolution dynamic desktop at the connected display. Windowing commands and interaction data received by the video processor via optical data diode connected to the peripheral controller section.

Host emulators connected to the keyboard and mouse managing the user interaction. USB / PS/2 switch couples the active channel to the appropriate device emulator of that channel through optical data diodes.

Advantages	Disadvantages
Very high security - Optical isolation between channels.	User authentication in multiple networks is replicated.
Simultaneous work in windowing environment between different networks	Higher cost – higher cost KVM needed (and 2 or more PCs need to be maintained for each user)
Easy for the user to identify the security level (network) in use through colored frames.	
Complete protection of peripheral ports – USB / PS/2 ports are unidirectional by optical isolators	
Optional secure Copy – Paste between networks (controlled by policy and regulated by other systems)	
Fast switching time between environments.	

Table 7 – Multiple networks separation using HSL Secure KVM Combiner advantages and disadvantages

2.7. Option 6 – Modular Secure KVM Combiner

This method developed and patented (pending) by HSL in 2009 to further address high security organizations needs for improved efficiencies. HSL integrated in a modular chassis the KVM Combiner, isolated power supplied and 4 bays for hosts / hosts interfaces. These bays could use any combination of offered modules called *Nano-Blades*.

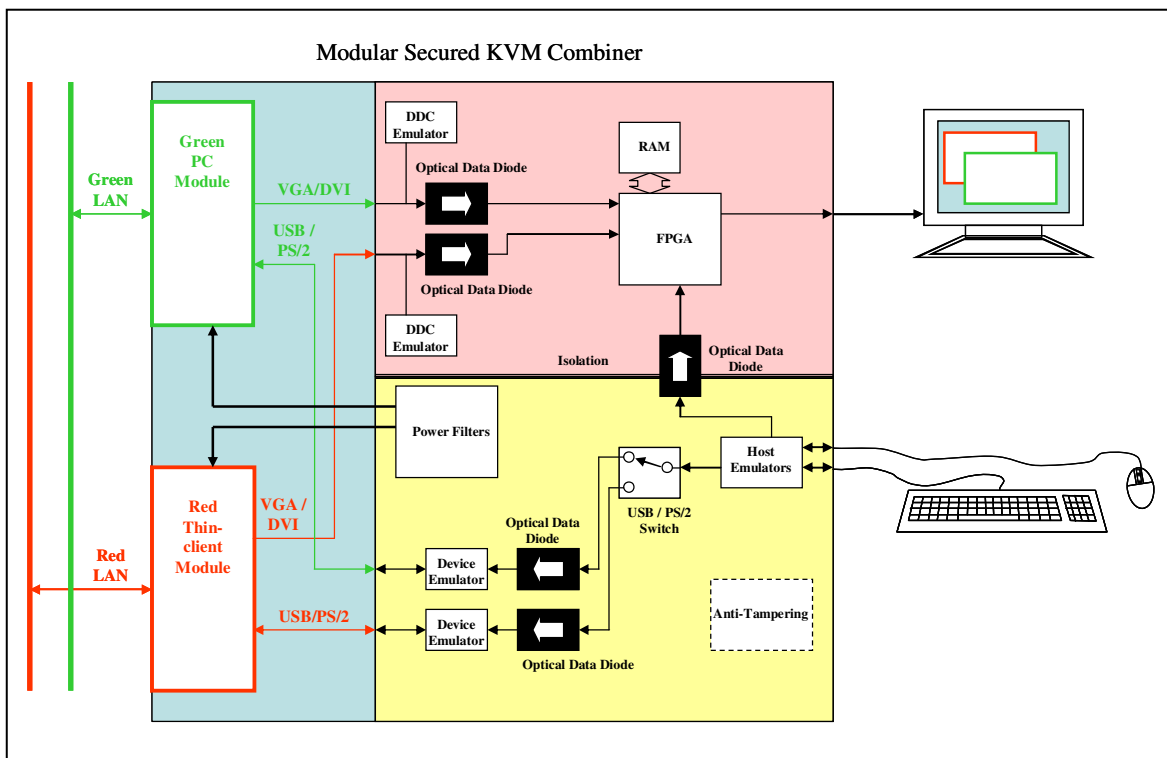


Figure 12 - Multiple PCs and Modular Secure KVM Combiner

HSL developed several *Nano-Blades* compatible with the product:

- AUX DVI to connect external PC, thin-client or docking station through DVI / HDMI.
- AUX VGA to connect external PC, thin-client or docking station through VGA.
- LNB – Linux based thin-client to run remote sessions, virtual desktop and local multimedia.
- LNBF – same thin-client module as LNB but with fiber LAN interface.
- ANB – Intel Atom based secure PC running Windows XP / XP embedded or Linux.
- Blank panel to plug unused bays.

Integrating the clients (thin or fat) as needed inside the KVM chassis enabled endless configurations to match the requirements of different user groups.

This modular approach also ease the maintenance and support of large deployments as many organizations tends to “paint” computers and peripherals by the class of networks that they touched.

The modular design accepted as safe to identify specific modules by their color. The chassis accepted as no-color. Maintaining the different groups inside the organization become easier with painted Nano-blades stocks.

Advantages	Disadvantages
Same as above (KVM Combiner)	Same as above (KVM Combiner).
Secure Hosts as part of an integrated solution – risks are easier to manage	Higher cost of KVM.
Minimum cabling – only LAN exposed	
Flexibility in deployment and maintenance	
Future growth path	
Isolated power option	
Reduced risk of exposed USB	
Smaller installation footprint	
Much lower power consumption	
End to End TEMPEST solution. No integration needed	
Single (secure) management platform across different isolated networks	
Cost effective solution	

Table 8 – Multiple networks separation using HSL Modular Secure KVM Combiner advantages and disadvantages

2.8. Option 7 - Virtualization and mixing networks at the server

The introduction of virtualization technology provided a strong temptation to secure organizations – the possibility to use a single server farm to mix between different networks on different virtual machines. Can virtual machines be partitioned enough to isolate different users and different security levels?

At first look the server and desktop virtualization may be the perfect solution for network isolation / integration. But a second look will reveal the major risks of this method.

As discussed above, from economy standpoint it makes perfect sense to integrate networks at the data-center or server.

Advantages	Disadvantages
Single desktop to access multiple virtual machines. Lowest implementation and maintenance costs.	The high risk of software code to bridge between different security levels or networks. This risk is similar in nature to the risk of desktop infection as the virtual machines coexist on a single operating system and single physical platform.
Single network infrastructure to the desktops.	No air-gap or physical separation. Intruder may propagate from server OS to virtual client OS to client to another virtual OS or to another server.
Intuitive an efficient user environment with mixed windows on a single display.	
Scaleable and easier to deploy – everything is done on software – no physical deployment or changes needed.	

Table 9 – Multiple networks separation using virtualization

The advantages of this solution are clear and attractive; still this method is not widely in use due to the severe security risks described above.

3. Aspect of Secure KVMs

3.1. The KVM as a target for attackers

As networks become isolated, KVMs becomes a focused target for attacks. There are several reasons for that:

- KVMs are almost the only point in the IT system that isolated networks are getting close to each other
- There are large numbers of similar KVMs – larger opportunity to attack. Better chance for success.
- Commercial and secure KVM products are readily available in the market and are easy to buy, analyze, and reverse engineer.
- KVMs may be easier attack target compared to firewalls or crypto equipment. Attacker will always prefer the weakest link to attack.
- Many organizations not fully understand the vulnerabilities of KVMs. Awareness is key factor in protection.
- Some commercial KVMs are designed in such way that practically bridging the hosts.
- Many of the KVM products can be detected on one of the host and therefore exposed as targets.
- Once a KVM had been tampered or leaked – it would be very hard to detect it. Secret information may easily leak through the internet.

In general the effort invested by governments and agencies to crack KVMs is comparable to the effort invested to crack crypto codes, keys or firewalls. In many cases it would be easier to leak information through attacked KVM compared to leak it through deciphering data that was encrypted using strong encryption.

For this reason larger efforts are invested today by governments and agencies worldwide to increase the security of KVMs than ever before – these products are just in the wrong place at the wrong time...

3.2. The SKVM as a gateway or peripheral filter

Many organizations are starting to adopt the Secure KVM as a key component highly controlled and secure user desktop. The Secure KVM is used as a gateway for user access. Implementation of this concept is typically made from the following layers:

- a) All computers in use are having USB ports locked through proper USB lock software and strict policy. Only allowed USB devices are: USB Keyboard, USB mouse and sometimes CAC reader.
- b) Unused peripheral ports are either physically removed or deactivated through software / hardware.
- c) User computers are typically locked to prevent physical user access.
- d) The Secure KVM in use features strong USB device filtering to enable only USB keyboard and mouse.
- e) If needed – the Secure KVM in use supports CAC reader or other user authentication device through a dedicated peripheral port that is characterized by:
 - a. Strong filtering of USB devices – only user authentication devices are enabled. All other devices are rejected and deactivated.
 - b. Continuous monitoring of USB devices to prevent “hot swapping”.
 - c. CAC port is completely isolated from all other ports and it uses a separate set of USB cables to connect to the computers.
 - d. Computers that do not require user authentication through CAC reader are not connected through CAC USB cables.

This implementation prevents the use of mass storage devices and any other unauthorized peripherals. With proper deployment it is possible to create a site that has no exposed USB port vulnerability.

3.3. The Trusted SKVM

Some high security organizations use standard Trusted Platform Module (TPM) or proprietary crypto module in their PCs to create a trusted system in one or more networks. Since the Secure KVM “interfere” in the trusted platform chain of trust, HSL secure KVMs are equipped with optional TPM coupled to one channel.

This TPM located inside the Secure KVM allows the coupled PC to interact with KVM and authenticate it, thus to securely extend the trust chain all the way from the servers to the PCs, to the KVMs and finally to the coupled user peripherals.

3.4. The use of SKVM for Copy – Filter - Paste

Secure KVMs with integrated thin-clients are used in many applications to enable Copy-Filter-Paste processes. The thin-clients are configured to send clipboard content to a special copy server at the same network. Then the clipboard content is passed through various policy based filters and scans. Once qualified the content is passed through a data diode into the target network copy server where it is further passed into the target thin-client clipboard. Depending on user authorization level it is possible to copy and paste items such as text, images, video content etc.

It should be noted here that in any case the Secure KVM itself does not provide any internal path for these processes to avoid potential security risks.

3.5. KVM Users - Work flow and non-work flow users

KVM Users can be generally divided into 3 groups when it comes to accessing isolated networks:

1) *Work flow users* – users whose majority of their daily tasks / shifts includes:

- Monitoring of several networks at once
- Data collection and transferring of data across networks

Examples of Work flow users:

- a) Intelligence collection analysts
- b) Operations center users
- c) Counterterrorism Analyst
- d) Open source officer

2) *Non-work flow users* – users whose daily tasks include occasional switching between networks or data transfer between networks.

Examples of non-work flow users:

- a) Defense agency users with internet access or external email accounts
- b) Defense contractors
- c) Intelligence officers

3) *Exception users* – users who need access to other networks on exception basis (once per week for example).

Examples of exception users:

- a) Defense agency users with very limited access to external mail

b) Defense contractors with limited access to government network

During several experiments that were done with work flow users there were several disturbing findings:

- 1) Work flow users can lose as much as 50% of their time with data delivery overheads, struggling with internal security and processes.
- 2) Work flow users work is affected by these overhead. Resulting delays in data collection and bureaucracy filtering of data.
- 3) Rapid switching and multiple transfers causing excess users fatigue. User's tends to lose focus on their job due to rapid transitions.
- 4) Many of the daily processes are manual (not automated). This may result frequent mistakes and internal security failures.

As a result of the job study findings above, some organization defined a wider concept than just network integration - Process Based Network Integration (PBNI). An integration solution that takes into consideration the monitoring and transactions that the users should do and provides a complete process based solution. Policy based Copy-Paste across network is one of the key features of this solution.

For additional information see product specification.

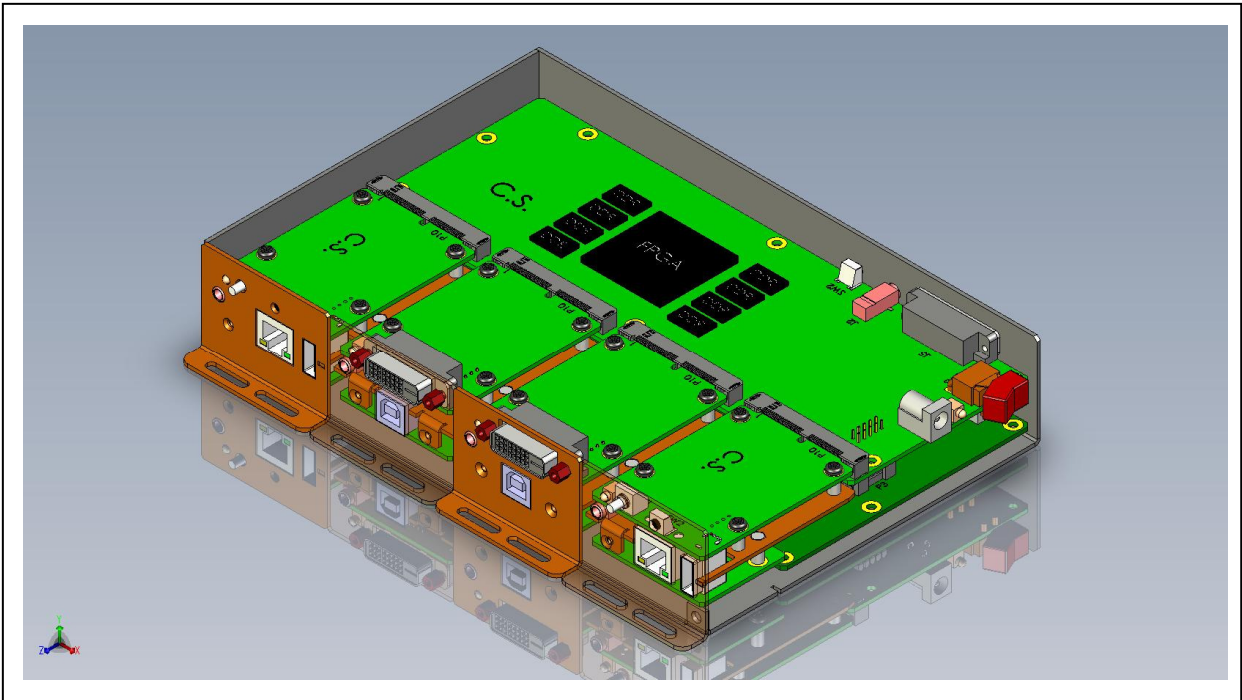


Figure 14 – Modular KVM Combiner internal structure

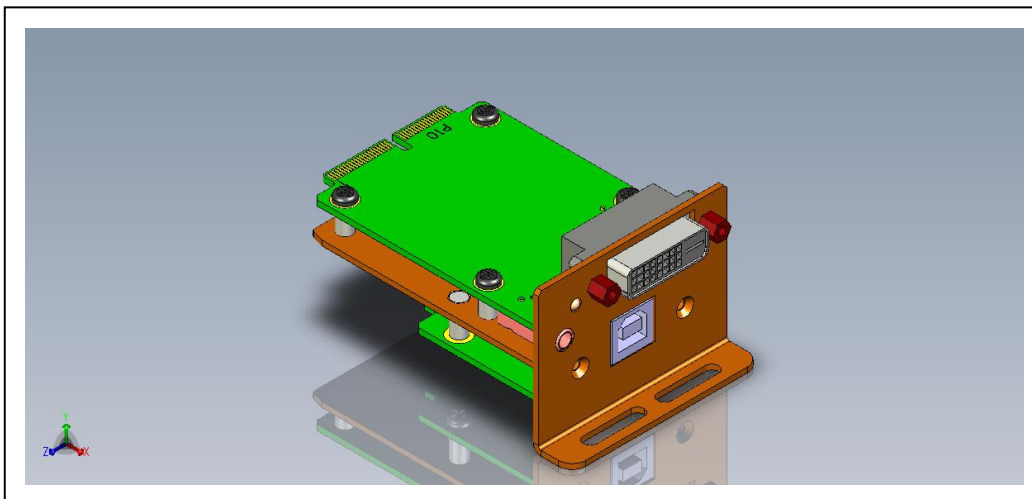


Figure 15 – AUX DVI Nano-Blade design

5. Appendix B – Security Gaps and Common Criteria Levels

This appendix deals with the relationship between specific KVM installation scenario and the required Secure KVM certification level.

The risk in KVM is from potential digital leakage between two coupled computers or their networks.

The following table provides some guidance to the secure KVMs security levels required across different security gaps.

		System one ↔					
		UNCLASSIFIED	IN CONFIDENCE	RESTRICTED or SENSITIVE	CONFIDENTIAL	SECRET	TOP SECRET
System two ↑ ↓	UNCLASSIFIED	EAL-2					
	IN CONFIDENCE	EAL-2	EAL-2				
	RESTRICTED or SENSITIVE	EAL-2	EAL-2	EAL-2			
	CONFIDENTIAL	EAL-7	EAL-4	EAL-4	EAL-4		
	SECRET	HIGH GRADE	EAL-7	EAL-7	EAL-4	EAL-4	
	TOP SECRET	HIGH GRADE	HIGH GRADE	HIGH GRADE	HIGH GRADE	HIGH GRADE	EAL-4

Matrix of KVM Assurance Levels

Table 10 – Required KVM security level as function of security gaps (adopted from Australian documents)

6. Appendix C - Intrusion Scenarios Analysis

This chapter analyses potential intrusion scenarios to further understand the design robustness of the Modular KVM Combiner.

Before the KVM Combiner project started, HSL performed structured sets of attacks on existing KVM equipment (including CC EAL 4+ certified devices). The results collected from these attacks led to many of the design requirements implemented in the design of the KVM Combiner.

The design of the KVM Combiner assumed a sophisticated intruder gaining full access to up to 2 connected blocks.

Additional analysis and tests were conducted on the physical level (tampering, power supply, electromagnetic) but these are still classified.

Modular Secured KVM Combiner

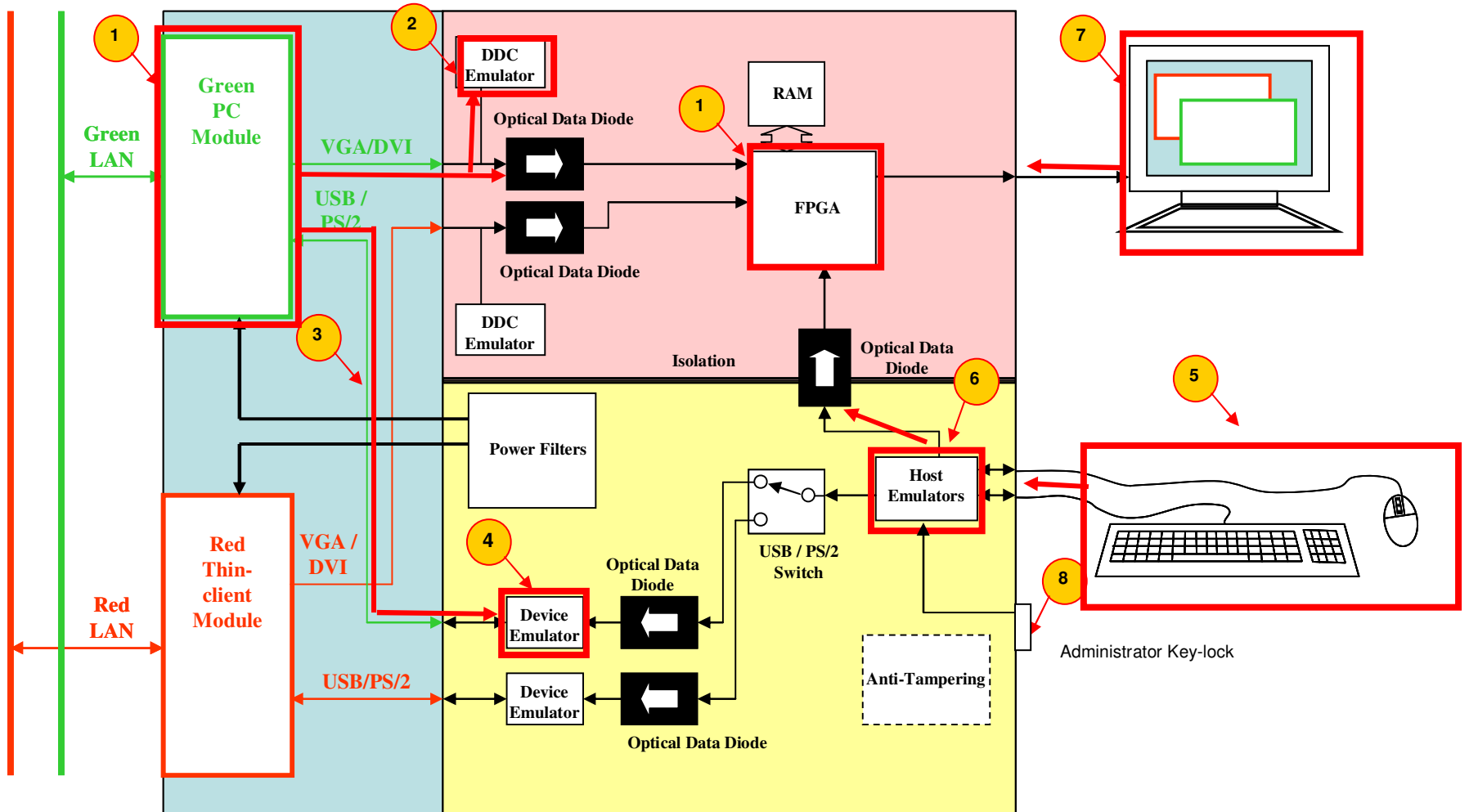


Figure 16 – Modular KAV Combiner Intrusion paths analysis

Potential intrusion paths with the assumption of no physical intrusion:

- 1 Assuming the Green PC invaded and fully controlled by intruder.
 - VGA and DVI output to the KVM Combiner manipulated by the intruder through the intruded PC.
 - Video input to the KVM Combiner does not allow any other data other than valid video signal. No where in the KVM Combiner the video data is being recognized or interpreted or processed. All valid video data will be converted to output image on the display.
- 2 Attack from the intruded PC 1 to the DDC emulator of the KVM Combiner cannot reprogram the emulator.
 - Even if DDC Emulator is being (somehow) manipulated, still it cannot impact leakages as it is only connected to the Green PC. **No leakage potential.**
 - DDC data does not reach the Optical data diode or FPGA. **No leakage potential.**
- 3 Attack from the intruded PC 1 follows the USB interface to attach KVM Combiner Device emulator.
 - Device emulator cannot be reprogrammed.
- 4 - Even if (somehow) device emulator firmware will be manipulated the effect of this will not propagate to any other block due to the attached Optical data diode. **No leakage potential.**
- 5 Assuming that connected keyboard / mouse is being intruded / controlled by intruder.
 - Note: Intruded keyboard may leak internally or externally – keyboard is not part of the system. We only evaluated the potential to affect the KVM Combiner integrity by fully intruded keyboard. If keyboard is one of security concerns – special keyboards may be used. Intruded keyboard may result leaked keyboard data by definition.
 - Intruded keyboard / mouse attack the Host emulator in the KVM Combiner. Host emulator cannot be reprogrammed.
- 6 - If Device emulator was (somehow) reprogrammed, resulted leakage is equivalent to the intruded keyboard leakage. No other leakages or propagated affects possible.

- Access to the KVM Combiner FPGA is unidirectional and therefore cannot leak any video information (even if the FPGA was reprogrammed).
- Device emulator cannot affect FPGA as communication is limited to predefined control protocol.

7 Assuming that connected display is being intruded / manipulated by intruder.

- Display interface (DVI) is unidirectional. Display may not affect FPGA in any way other than loading DVI output chip.
- Even if FPGA firmware is (somehow) manipulated, the effect cannot propagate to any other direction as the FPGA is surrounded by optical data diodes.

8 Assuming administrator key is being attacked (mechanically or electrically).

- Intruder cannot gain access to any setting that may cause leakage

7. Secure KVM Generations

	1 ST Generation	2 nd Generation	3 rd Generation
Years (design)	1999 - 2005	2005 - 2010	2010 -
Common Criteria	None, EAL 4+	EAL 4+	NIAP EAL 2+ , Rest of the world – EAL 4+
Interfaces	PS/2 and VGA, some DVI	DVI, USB	DVI-I dual-link, USB, DisplayPort, HDMI
Assumptions	Naïve – attacker is the user? Asset under attack is the user's data. No tampering. TEMPEST is the primary risk...	Attacker may be remote. Anti-tampering needed. Signaling attack is the primary risk.	KVM is under attack by 2 infected computers. Peripherals cannot be trusted. User cannot be trusted. Strong anti-tampering.
Primary protection means	Discrete circuitry (electronics)	Microcontrollers (firmware)	Physics (optical data diodes)
Strong USB filtering	No	No	Yes
EDID protection	None – display direct switching	Simple emulation	Highly isolated emulators, content firewall
Approved network gaps	Do not use today!	Use only between same classifications. Do not use for secret and above.	Can be safely used between internet and top secret networks
Products	<ul style="list-style-type: none"> • Cybex / Avocent / Emerson older products. • Belkin OmniView Secure. 	<ul style="list-style-type: none"> • Cybex / Avocent / Emerson current products. • Aten / IOGear secure KVMs 	<ul style="list-style-type: none"> • All HSL KVMs. • Belkin latest DVI-I models. • Adder / Black-box OEM new models