Expanded Keyboard-Video-Mouse (KVM) Technology Implementation for Advanced Reactors

Richard Turk
Technology Resources LLC

Richard Cooper
Thinklogical LLC

1 Abstract

With the widespread use of video displays in the most recent Generation III+ Instrument and Control (I&C) systems, Keyboard-Video-Mouse (KVM) technology has been and important enabler in providing a centralized Human System Interface (HSI). Large multiple screen "wall" displays are the center pieces of the control rooms. The wall displays and other screen displays are selected and accessed from control stations using KVM networks. Their use however, was introduced as a solution only after the basic I&C architecture had been established and licensed. This often limited their application to non safety system. Meanwhile the KVM technology has continued to advance with increasing capabilities for signal transmission range, fidelity, security and reliability This paper will describe the advance features of KVM technology that can be applied at the outset of Advance Reactor I&C design to help fulfill the promises of Advanced Reactors.

2 Introduction

The Generation III+ Advanced Light Water Reactors now coming on line are the first designed to, and reviewed against, the Human Factors Engineering guidance of NUREG -0711 "Human Factors Engineering Program Review Model." These control rooms represent a large step change in the HSI, moving away from multiple functionally dedicated panels to single multifunctional integrated consoles. As has been done in other industries, such as defense and oil and gas Large wall pane displays to provide status overview and situational awareness have been added. Keyboard-Video-Mouse (KVM) technology has facilitated the improved HSI for these plants, making it possible for any operator to access and operate multiple digital inputs with only one set of mouse, keyboard and displays. With the use of the KVM network of extensions and switches, operators have dynamic control of the information displayed on the large wall panel screens. Likewise, at individual operating consoles, operators have the ability for functional selection of displays on multiple screens. KVM use however, was introduced as a feature only after the basic I&C architecture had been established and licensed. This has limited their application so far to the non-1E Distributed Control System (DCS) and control of the large panel multiple screen wall displays as shown in Figure 1. Meanwhile the KVM technology has continued to advance with increasing capabilities for signal transmission range, fidelity, security and reliability. Advantages currently be realized installations like military command and control centers, electric grid transmission control centers and Oil and gas production real time operations centers include:

- Control Station layout optimization
- Less heat & noise
- Fiber optic isolation
- No electrical emanations
- Secure, no eavesdropping
- Safer– no sparks
- No interference with other equipment
- Lightweight
- Non conductive
- Solid state drives for storage
- FPGA architecture

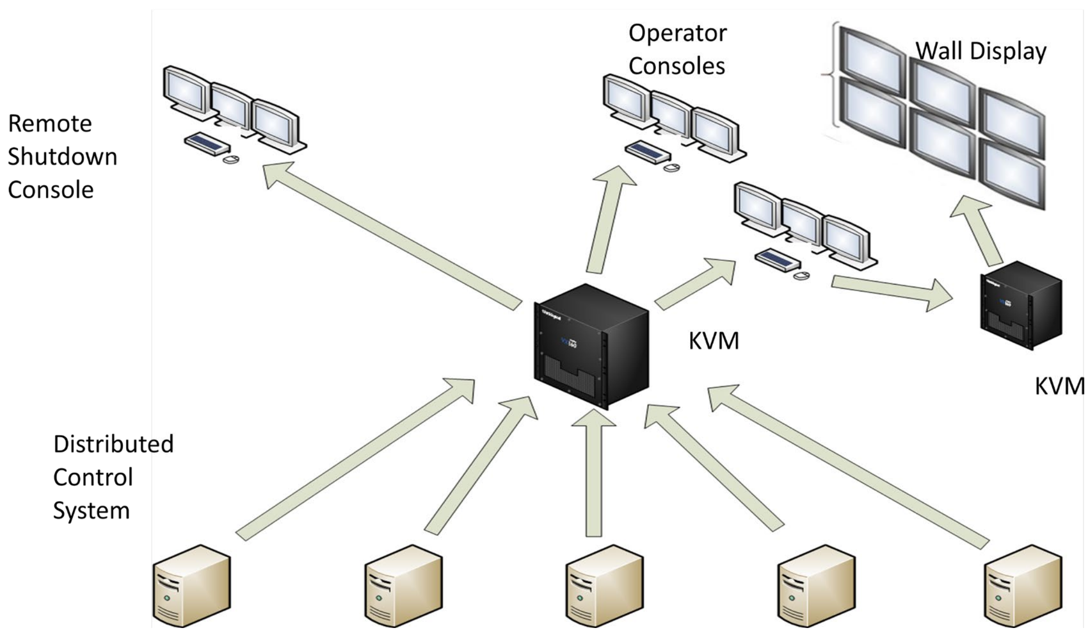

Figure 1 - Typical use of KVM in Gen III+ LWRs

3 Further Integration in SMRs and ANLWRs

As noted above application of KVM networks to centralize and integrate operator control consoles and wall displays on Generation Iii+ NPPs was limited to the non1E DCS. KVM networks are widely used in other industries for applications requiring high reliability and rigorous qualification such as military command centers and oil and gas drilling Real-Time Operations Centers. Small Modular Reactors and Advanced Non-Light Water Reactors (ANLWR) will have reduced, or even eliminated Class 1E I&C Systems. This will allow for significant further integration of control stations and facilities and, as in these other industries, integration of the overall management of the power generation asset.

Even if 1E qualification is not required, system reliability and redundancy can be integrated into the overall design of the system. For high criticality installations, it is possible to use endpoints with redundant matrix connection points. These connections can feed back to different I/O cards of a single matrix or to redundant matrices. For source endpoints, the signals from the source computers would be fed to both matrices simultaneously. For destination endpoints, the receiver would monitor the status of both of the inbound signals. Users can specify the signal to use when both are present. The receiver automatically fails over to the alternate signal if one of the connections is lost. The two matrices communicate with each other over the network to maintain the switch configurations in sync.

The Generation III+ NPPS still require dedicated Safety Console or panels. Their elimination will allow for significant simplification and optimization of the control spaces layout.

As the Generation III+ digital control rooms progressed through design, licensing and construction, other computer related aspect of managing the plant as an asset, not related directly to operational control were treated as independent systems. In many cases these system were not provided by Reactor supplier, but were left for the owner operator to develop and were incorporated into the control room With additional LAN workstation and desks These included computer systems for engineering document management, operating procedures, configuration management, maintenance and work management, etc. With SMR and ANLWR development still in the early stages of development and in many cases with the eventual owner operator a member of the development team There is an opportunity for further integration at individual control stations using an expanded KVM network. Since high KVM networks' transmission signals between the host computer and the operating station can be extended large distances, there is also the opportunity to share the operations and other information with and between offsite facilitates such as emergency support facilities, engineering conference room, executive office buildings, maintenance centers, etc.. Currently distances of up to 50 miles have been tested. Figure 2 shows a possible extended LVM network

4 Improved Human System Interface and Human Performance.

KVM network provide superior performance for the HSI. The transition to a centralized integrated operator console facilitated by the ability to access and operate multiple digital inputs with only one set of mouse, keyboard and screen, greatly simplifies tasks and increases productivity relative to moving between dedicated control panels. Functional selection of displays at the consoles enables simpler and faster task execution, reducing operator burden. Functional selection of the large wall pane Greatly aides in oversight and situational awareness Placement of computers, workstations and other digital hardware away from the operator consoles reduces heat, noise, and clutter for improved work environment.

Higher end KVM networks with high resolution, low-latency video distribution provide increased visibility and clarity. With high end KVM networks signal compression can be avoided leading to no frame dropping, Compressed solutions produce pixel shifts, video artifacts and fuzzy text from video conversion. If no processing is required to compress there is no added latency and overall latency can be reduced from milliseconds to microseconds. Latency produces jitter, such as inconsistent mouse movements that result in eyestrain

Additionally smooth keyboard and mouse performance provides accurate human/system interactions with reduced likelihood of error. KVM switching allows for display sharing for supervisory oversight, peer review or verification and Human Performance (HuP) monitoring.

KVM switches and extensions also allows for display sharing for supervisory oversight, peer review or verification and Human Performance (HuP) monitoring. An IP-connected KVM system has the ability to of make use of IP-multicast protocols to provide point-to-multipoint distribution of KVM feeds for monitoring or collaboration. Different types of connection modes include:

- SHARED MODE: All receivers are connected in parallel to a particular source. All human interface devices (HID), including keyboards, mice, tablets, etc. are connected simultaneously.
- EXCLUSIVE MODE: Multiple users can monitor the video and audio feed. However, the first user to connect to the source has exclusive rights to the HID connections (one keyboard and mouse).
- VIEW-ONLY MODE: A user can connect to a source only to receive the video/audio feed. No HID connections are possible.
- PRIVATE MODE: A single user is granted access to a particular source. Once that connection is made, all other user connection requests are rejected until the user releases the connection.

The various modes can enable the use of the KVM system in a number of different workflow scenarios outside of the standard one-to-one mode, such as status monitoring of alarm UIs, training or job shadowing, and signage throughout the facility. But they still provide users with the privacy and security capabilities needed for confidential use, such as email and confidential documents.

5 Enhanced Cyber Security

As the Generation III+ Nuclear control rooms have progressed through design, licensing and construction, Application of high end KVM networks in areas such as military command and control centers has resulted in significant security enhancements. These Networks employ fiber optic isolation, elimination of USB data ports, hard drives and network cables accessible at operator consoles

The networks are designed to achieve, over significant distances if necessary, separation of the threat (people) from the target of the threat (the content). They provide a robust and flexible suite of advanced security features and functions that allow for close management of user interaction in multi-domain environments to prevent attacks, and the resiliency necessary to withstand an attack There is the functionality required to allow for continuous monitoring of the system

Five key design criteria for most high end systems are

- The system architecture should physically secure and separate the target of the attack (content or system operation) from the threat: people.
- The technologies used in the system should eliminate the ability to attack from a distance; that is, sniff or eavesdrop on the system.
- The system should allow the administrator to closely manage and control access in accordance with the organization's security policies.
- The system should automatically and continuously monitor for and identify breaches.
- The system should be resilient; that is, it should be designed to not only withstand an attack, but also recover quickly following one.

6 Asset Management with Improved Onsite and Offsite Communications