POTENTIAL USE OF THINKLOGICAL'S KVM TECHNOLOGY IN SAFETY APPLICATIONS

Richard Turk
Senior Project Director, Technology Resources LLC
3478 Ahern Pl. Melbourne FL
rick.turk@comcast.net
(860) 819-0392

Richard Cooper
Vice President, Thinklogical LLC
1001Washington St, Milford CT 06460
richard.cooper@thinklogical.com
(484) 467-5633

James Gleason
President, GLSEQ, LLC
13220 S. Shawdee RD, Huntsville, AL 358003
jim.gleason@glseq.com
(256)-369-8857

David Herrell
Executive Engineer, MPR Associates
320 King St, Alexandria, VA 22314
dherrell@mpr.com
(703) 519-0512

[Digital Object Identifier (DOI) placeholder]

ABSTRACT

A recent study conducted as part of the Light Water Reactor Sustainability (LWRS) Program, sponsored by the U.S. Department of Energy (DOE)[1] identified and proposed practices and principles to support industry Digital Instrumentation & Controls (DI&C) Modernizations. One practice proposed was the use of a safety qualified switching architecture, based on Keyboard-Video Mouse (KVM) components, referred to as a Display Keyboard Trackball (DKT) Architecture. The DKT architecture envisioned by the DOE research provides for a flexible Human System Interface (HIS) solution for the Main Control Room (MCR) that supports both the interim states during phased implementation and the envisioned analog-digital hybrid end-state for the MCR.

The purpose of this paper is to present a conceptual configuration for the DKT architecture and describe potential implementation of this architecture to achieve the benefits of:

- Simplification of the control room layout,
- improvement of the Human System Interface (HSI),
- Cost reduction from fewer displays,
- Consolidation of operator functions.

MPR and Technology Resources are currently assisting Thinklogical in assessing the process of developing a DKT configuration and qualifying a KVM/DKT system as a basic component for nuclear control room modernization. In addition to equipment qualification. This paper describes the results of that assessment and the potential nuclear safety offering Thinklogical will be pursuing.

1. INTRODUCTION AND BACKGROUND

New Plant control rooms and operating plant control room modernization are increasing employing screen images generated by a computer or other electronic device referred to as Visual Display Units (VDU). These control rooms represent a change in the Human System Interface (HIS), moving away from many functionally-dedicated HSIs to single multifunctional integrated HSI screens and consoles. This has proved very successful in other industries, such as defense and oil and gas Where multifunctional displays have been used to provide status overview and situational awareness. 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. Non-safety related application of a KVM network of extensions and switches, are also being used in new nuclear plant such as AP-1000 to provide operators with 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-safety-related Distributed Control System (DCS) and control of the large panel multiple screen wall displays. Meanwhile the KVM technology has continued to advance with increasing capabilities for signal transmission range, fidelity, security and reliability. Thinklogical is currently supplying Keyboard-Video-Mouse (KVM) technology to several industries to improve control center data visibility for operating staff.[2] These applications require very high reliability under challenging conditions, such as controls for military operations including U. S. Naval combatant ships. 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

2. DKT ARCHITECTURE AND ADVANTAGES

The existing US nuclear plant control rooms were designed with analog meters, discrete lamps, analog displays, and various types of switches to interface with the original analog protection and control systems. The industry has, over the years, replaced some of the analog control systems with digital systems. Some of the early digital control system replacements retained the original control room indications and switches, but most of the newer digital system modernizations updated the control room with a video display and some form of keyboard or pointing device as the human-system interface (HSI), eliminating most, if not all, of the original physical interface elements (e.g., meters, lamps, switches).

However, there is limited space in the control room to add one or two new HSI displays, keyboards, and pointing devices for each modernized non-safety related system and two new HSIs for each safety division of reactor trip and engineered safety features systems, for single failure tolerance. Further, for many control rooms, the location of the existing analog interface elements would not be appropriate for a digital HSI, based on performing a new human factors evaluation.

In a modernized control room, the design must still comply with regulatory requirements, including the single failure criterion and concerns for software common cause failure (SCCF). Separate indication and controls unaffected by the SCCF must still be provided for the operators. The controls must provide a diverse means to shut down and maintain the reactor in a safe state based on the situational awareness provided by the diverse indications.

A recent set of DOE LWRS reports and studies note that achieving an end state vision of a hybrid control room (i.e., mostly video displays with limited number of required diverse indications and manual controls) will be an iterative process, with many outages required for implementation. With many years required to modernize and transform both the protection, control, and monitoring systems and the control room, the end state of the overall modernization must be planned, and the plan must consider the intermediate states. As the plant iterates to a final solution, each intermediate state must ensure that human factors are maintained and that operators are trained and can monitor and control the plant in each of the intermediate states as well as in the final state. Each of the intermediate states must support and enable the end-state vision. Multiple human factors evaluations are required for the intermediate goals, as well as for the end-state vision. The design process must focus not just on the short-term goal (the next intermediate state), but on the end vision for the control room.

The preferred way to achieve the required flexibility and to constrain the number of displays in the control room would be to design the display system to support connectivity from any display to any system, with appropriate capabilities provided on Reactor Operator (RO) displays and with restricted system control capabilities on the Senior Reactor Operator (SRO) and Shift Technical Advisor (STA) displays.

Most distributed control systems (DCS) already provide a means of sharing data from multiple controllers with many video displays, thus minimizing the number of non-safety related video generators. To avoid crossing channel or division boundaries in safety systems, video generators will have to be assigned to a single electrical division. Providing the channel and division data to a pair of video generators can be structured to be acceptable, as long as independence is maintained.

Since the switching matrix connects only one display, keyboard, and pointing device to one video generator at any time, and since the display, keyboard, and pointing device do not provide a path for malicious software to be transported between video generators, the concern that one video display unit could adversely affect safety system channels or divisions and/or multiple non-safety systems is eliminated, satisfying the base requirement established in Digital Instrumentation and Controls Interim Staff Guidance 4, “Highly-Integrated Control Rooms – Communications Issues.”

Providing a highly reliable DKT that allows the operator to switch an individual display between the video generators provides the SRO the ability to pull the data needed from any single channel or division in a safety protection or monitoring system or from any non-safety control or monitoring system, which includes non-safety related display of all safety protection and monitoring system data. With a safety-related DKT, the RO has access to all data the SRO has, in addition to the capability of providing control actions to any channel or division in a safety system (one channel or division at a time), and to issue commands to the control systems. This flexibility of a safety-related DKT, when combined with the equivalent of trained ROs and SROs in other industries, has been demonstrated to provide enhanced control room capabilities, by allowing the ROs and SROs to see data previously unavailable to them, increasing situational awareness.

Since the intermediate control room states are likely to be different from the final control room state, the flexibility provided by a safety-related DKT and this approach supports the intermediate and final states locations of flexible display functions, where displays are not allocated to specific functions. This flexibility is not provided if displays are allocated to specific functions, potentially requiring display locations to after their initial installation, as the control room morphs through intermediate states to a final hybrid configuration.

Using current US regulatory guidance, the DOE INL reports conclude that a redundant switching matrix, with redundant fiber optic feeds between the video generator and the switch and between the switching matrix and the user's display would be classified as safety, and the equipment qualified to current guidance. With that approach, safety systems are controlled by safety displays, safety displays provide safety data on which operational decisions are made by SROs and ROs, and ROs issue commands to safety systems through safety displays. High quality safety displays, and the same matrix switches, provide the RO and SRO with data display access to non-safety monitoring and control systems, and ROs command access to non-safety related systems. The safety-related DKT design provides the required electrical and data isolation between the safety switching matrix and the non-safety related video generators.

The benefits of safety-related DKT would be available to any existing reactor that intends to modernize their existing analog systems and control rooms as well as being a design base for control room designs for new Small Modular Reactors (SMRs). The simplicity of use is slightly offset by the human factors engineering and costs of establishing and maintaining safety classification of the safety-related DKT networks. The DOE reports and this paper conclude that the increased functionality and capabilities outweigh the costs associated with a safety classification of safety-related DKT.

3. DKT CONCEPTUAL CONFIGURATION, SAFETY FUNCTION AND QUALIFICATION

In support of the DOE work reported in Reference 1, the conceptual DKT configuration shown in Fig. 1 was developed by Thinklogical.

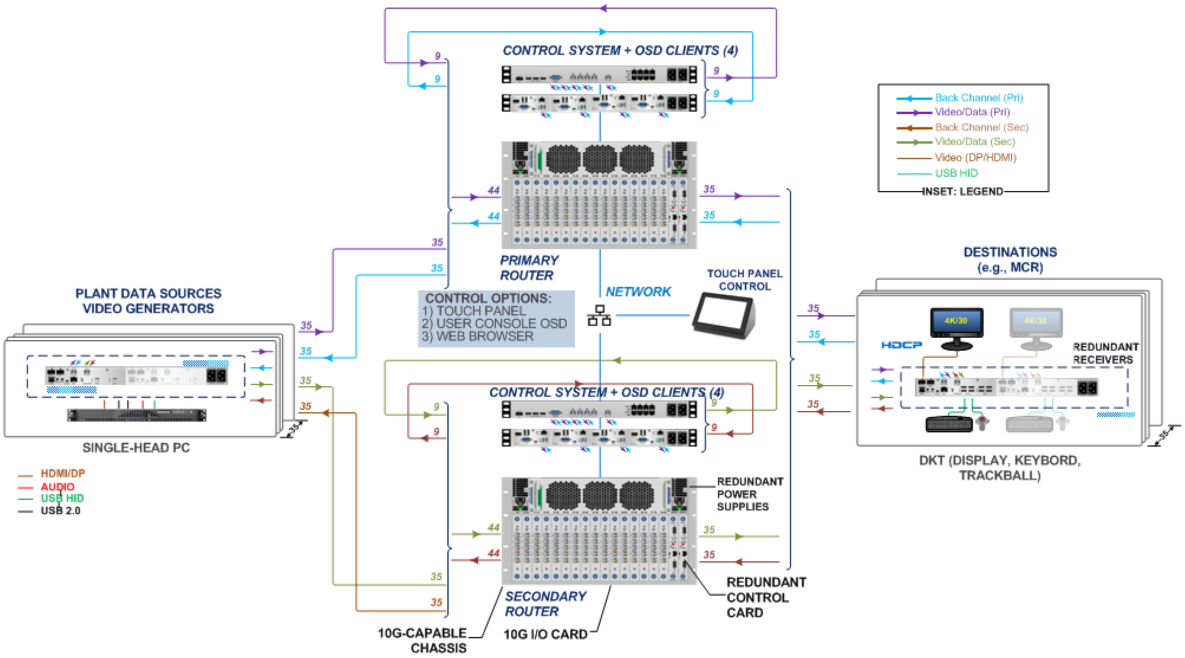

Figure 1. Conceptual DKT Configuration

The solution shown features a fully redundant Display, Keyboard, Trackball “DKT” configuration to . Thirty-five single-screen PCs displaying a set of plant information are connected to redundant matrix switches via diverse fiber paths. The diverse fiber paths then run to 35 operator workstations in the MCR and elsewhere through out the plant.

The left side of the drawing shows source PCs connected to DKT transmitters via standard copper cables. These cables are video, analog audio, keyboard, and trackball. The Thinklogical transmitter converts the electrical signal to an optical signal and distributes it via diverse fiber paths to duplicate, redundant Thinklogical matrix switches seen in the center of the drawing. Both matrix switches work synchronously, switching sources to destinations as requested by control system. In the event of a failure the “backup” switch becomes the primary. Each matrix switch is controlled by a dedicated control system. Both control systems are running synchronously.

Fiber cable runs from each matrix to each receiver. The optical signals are converted back to electrical at the receiver and distributed to the DKT. Should any fiber path or matrix switch fail, the system automatically switches to the back up.

The sources can be any number of PCs (with any number of Displays) or data inputs and destinations (operator workstations) can handle any number of video displays from these multiple sources as required. The Thinklogical matrix switch is non-blocking, meaning any source can be displayed at multiple destinations simultaneously without technical restrictions. The control system is configured to allow source selection to destination switching by an operator only as allowed by the system administrator based on security or policy protocols. All transmitters, matrix switches and receivers all utilize N+1 redundant load sharing power supplies for reliability and resiliency.

DKT’s provide the digital function to connect separate safety-related and non-safety related video displays and separate safety-related and non-safety related keyboards and pointing devices. The safety-related functions of the DKT’s consist of processing safety-related command functions to safety-related displays and preventing the processing of non-safety command functions to safety-related displays, as follows:

- Process safety-related commands from safety-related keyboards to safety-related displays
- Process safety commands from safety-related pointing devices to safety-related displays
- Prevent commands from non-safety-related keyboards to safety-related displays.
- Prevent commands from non-safety-related pointing devices to safety-related displays.

The qualification of DKT’s will be performed to comply with IEC and IEEE Standards and NRC Regulatory guides on Independence, Environmental Qualification, Seismic Qualification, Computers in Safety-related applications, and Electromagnetic and Radio-Frequency Interference.

4. RESULTS AND CONCLUTIONS

The recent set of DOE LWRS reports and studies on Digital Instrumentation & Controls (DI&C) Modernizations in nuclear power plants has highlighted the use and advantages of KVM, now known as DKT, to simplify the modern nuclear plant control room. The safety-related functions of the DKT’s consist of processing safety-related command functions to safety-related displays and preventing the processing of non-safety command functions to safety-related displays. With a safety-related DKT, the RO has access to all data the SRO has, in addition to the capability of providing control actions to any channel or division in a safety system (one channel or division at a time), and to issue commands to the control systems. This flexibility of a safety-related DKT, when combined with the equivalent of trained ROs and SROs in other industries, has been demonstrated to provide enhanced control room capabilities, by allowing the ROs and SROs to see data previously unavailable to them, increasing situational awareness.

Experience with similar application in other industries that require very high reliability under challenging conditions, such as controls for military operations provides high confidence that current technologies such as Thinklogical's KVM Switched and extenders can meet nuclear requirements for safety-related application.

5. REFERENCES

1. INL/EXT-20-61079 Vendor-Independent Design Requirements for A Boiling Water Reactor Safety System Upgrade May 2020 U.S. Department of Energy Office of Nuclear Energy. https://doi.org/10.2172/1755891
2. R Turk, R Cooper "Experience with Group-View, Wall Panel Displays Outside the Nuclear Industry" 11th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies Feb 2019