thinklogical
A BELDEN BRAND

Generic HSI Architecture for Nuclear Control Room Modernization

A Summary White Paper

As Described in INL/EXT-20-61079:

Vendor-Independent Requirements for a

Boiling Water Reactor Safety System Upgrade [1]

[1] Hunton, Paul Joseph, & England, Robert T. *Vendor-Independent Design Requirements for a Boiling Water Reactor Safety System Upgrade*. United States. https://doi.org/10.2172/1755891

INL/EXT-20-61079

Vendor-Independent Requirements for a Boiling Water Reactor Safety System Upgrade

Light Water Reactor Sustainability Program

Paul J. Hunton, Research Scientist, Principal Investigator
Robert T. England, Research Engineer

MPR Associates, Inc.

Paul Heaney
David Herrell
William Jessup

May 2020

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy

Summary

The Display, Keyboard, and Trackball (DKT) Architecture described in this document was proposed as part of a larger, licensable, I&C upgrade License Amendment Request (LAR) Framework Document per the ISG-06 Rev 2 Process with the objective "to achieve a standard, universal, and flexible HSI solution while minimizing costs and regulatory risk."

This solution also provides maximum flexibility to support multiple transition states driven by SR and NSR I&C upgrades, which will by necessity occur over an extended period of time.

Disclaimer

When developing the research document from which the following excerpt is taken, the Idaho National Laboratory (INL) consulted with Thinklogical in the development of the design concept described within it.

Specific Thinklogical equipment is referenced as examples in the excerpt to tether the Display, Keyboard, and Trackball (DKT) concept to commercially available technology.

INL appreciates Thinklogical’s participation in this research, but cannot endorse the use any specific vendor technology.

Acronyms

10 CFR 50	Title 10 of the Code of Federal Regulations, Part 50, Energy
ABWR	Advanced Boiling Water Reactor
ADS	Automatic Depressurization System
AR	Alternate Review
ASAI	Application Specification Action Items
ATWS	Anticipated Transient Without Scram
BISI	Bypassed Indication and Status Indication
BWR	Boiling Water Reactor
BOP	Balance of Plant
CGD	Commercial Grade Dedication
CS	Core Spray
CBP	Computer Based Procedures
COSS	Computerized Operator Support System
CCF	Common Cause Failure
CFR	Code of Federal Regulations
CR	Control Room
D3	Diversity and Defense-in-Depth
DI&C-ISG-04	Digital Instrumentation and Controls Interim Staff Guidance #04
DI&C-ISG-06	Digital Instrumentation and Controls Interim Staff Guidance #06
DAS	Diverse Actuation System (function in a DCS)
DCS	Distributed Control System
DEG	Digital Engineering Guide
DKT	Display(s), Keyboard, and Trackball integrated Human System Interface
DR	Design Requirements
ECCS	Emergency Core Cooling Systems: Comprised of Core Spray, High Pressure Coolant Injection, the Low Pressure Coolant Injection mode of Residual Heat Removal, and Automatic Depressurization System. The Reactor Core Isolation Cooling System also provides emergency core cooling capability. It is identified as a separate system in plant design documentation. It is grouped under ECCS in this research document for convenience.
EIM	Equipment Interface Module
EMC	Electromagnetic Compatibility
EPRI	Electric Power Research Institute
FMEDA	Failure Modes, Effects, and Diagnostics Analysis
FR	Functional Requirements
GDC	General Design Criteria
GEH	General Electric - Hitachi
HFE	Human Factors Engineering

HPCI	High Pressure Coolant Injection
HSI	Human System Interface
I&C	Instrumentation and Control
LAR	License Amendment Request
LGS	Limerick Generating Station Units 1 and 2
LPCI	Low Pressure Coolant Injection (LPCI) - mode of RHR
LWRS	Light Water Reactor Sustainability (Program)
N4S	Nuclear Steam Supply Shutoff System
NRC	Nuclear Regulatory Commission (United States)
NSR	Non-Safety Related
O&M	Operating and Maintenance
PAMS	Post Accident Monitoring System
PPS	Plant Protection System
PSAI	Plant Specific Action Item
PWR	Pressurized Water Reactor
RCIC	Reactor Core Isolation Cooling
RHR	Residual Heat Removal
RISC	Risk-Informed Safety Class
RRCS	Redundant Reactivity Control System
RPS	Reactor Protection System
SCCF	Software Common Cause Failure
SE	Safety Evaluation
SOE	Sequence of Events
SLCS	Standby Liquid Control System
SPDS	Safety Parameter Display System
SR	Safety-Related
TBC	To Be Confirmed
TBD	To Be Determined
V&V	Verification and Validation
VOP	Vendor Oversight Plan
UFSAR	Updated Final Safety Analysis Report

3.3.5 Modernized HSI (DI&C-ISG-06 D.2.2)

3.3.5.1 Purpose of Modernized HSI

The advantages of a modernized, integrated, digital safety-related and non-safety solution include improved visibility of data in the CR and AER and the resultant plant staff flexibility. To provide this visibility, video displays will replace the traditional indicator lamps, annunciator windows, meters, and recorders in the CR. The expectation in most NRC documentation is that the CR will have strictly separate traditional safety-related video displays and separate, traditional non-safety related video displays. These separated, classified, spatially dedicated video displays show plant status as reflected in the data sampled by the systems, internal plant system status, and active control actions. Soft controls are also possible, where the operator performs manual functions on soft control implemented in the video display.

The requirements for the safety-related content of the DKTs will be evaluated by HFE. The DKT displays will be simple, usable, and easily navigated by ROs and SROs. The information displayed will be meaningful and necessary for use in monitoring and controlling LGS.

The traditional video display includes an interface to the logic solver, a video generator, a display, a keyboard, and an operator input device (e.g., touchscreen, trackball, or mouse) as an integrated unit, similar to a personal computer. Implementing this traditional approach in the CR has a weakness in that the design provides video display functionality only in spatially fixed CR locations. Safety-related video displays are assigned inflexibly to one of the several divisions (along with the divisionalized channels) and placed in fixed locations by division. There is a strict segregation of non-safety from safety-related video displays. The typical design installs safety-related video displays in fixed locations with specific functions, which the vendor designs into the equipment, to interface with the safety-related systems. The typical design installed non-safety related video displays as part of their DCS. These provide essentially unlimited non-safety related control system flexibility for the DCS video displays. While the modernized design will install DCS video displays in fixed locations, these video displays will be capable of interaction with any system within the DCS (as described in Sections 3.3.5.2 and 3.4.5), unless HFE requires fixed functionality on some of the DCS video displays.

As shown in Figure 3-24 below, the modernization proposes the use of a digital DKT architecture that enables sharing data on safety-related DKTs with any control and data system that watchstanding operators could need in the CR. This will include the safety-related systems (any channel or any division), the non-safety related DCS, and other systems such as the corporate business network. The DKT Switches will have redundant internal controllers and redundant power supplies, to maximize reliability. The redundant power supplies will be fed from separate safety-related power feeds for single-failure tolerance. The DKT switching design will ensure that no single failure and most double failures prevent data display and soft control in the CR.

To support this architecture, the DKT interface in the associated, serviced systems will be separate from the DKT. The serviced divisional DKT Interface will connect to both DKT Switches. The DKT Switch is a solid-state implementation of the traditional keyboard, video, and mouse (KVM) switch, which establishes the connection mechanism to the safety-related DKTs distributed throughout the CR. The DKT Interface transmits video signals to the display and receives data from the DKT keyboard and trackball through the DKT Switch. Once a DKT user in a particular location selects a DKT Interface and the equipment connects the DKT with an available DKT Interface, the user cannot tell whether there is a switching network or a direct connection between the DKT and the selected DKT Interface. Each serviced system will provide a sufficient number of DKT Interfaces to support the intended number of simultaneous DKT locations requiring access to a particular serviced system.

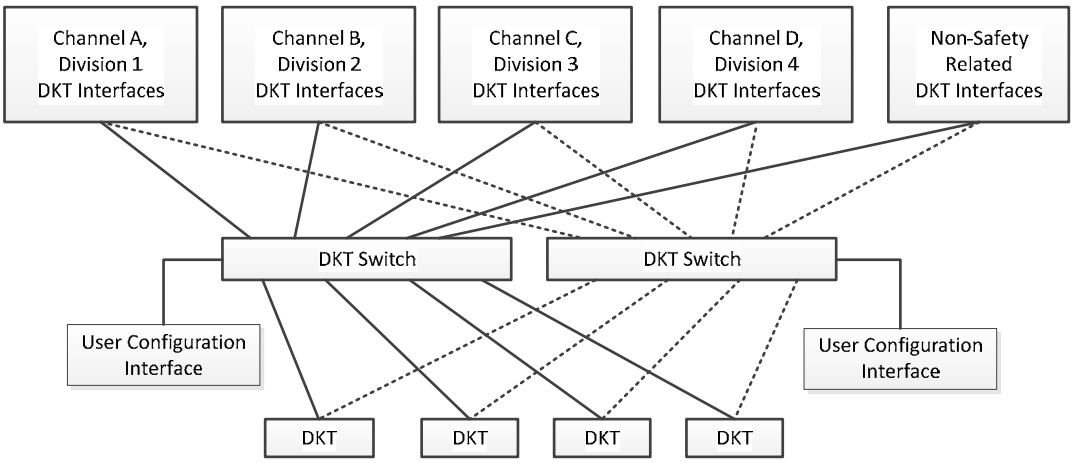

Figure 3-24. Proposed Display Switching Architecture

The only information retained in the DKT Switch system is the set of allowable connections between serviced system DKT Interfaces and DKTs in the internal configurable table. The DKT Switch system switches (i.e., directs) the information between the DKTs and the serviced system DKT Interfaces without retaining any information. The DKT Switch vendor designed and tested the DKT Switch to ensure that no cross linkage between DKT Interfaces or DKTs is possible, including cross-coupling between switched connections on the printed circuit boards within the DKT Switch.

DKT Interfaces will be powered from divisional power and interface with the DKT Switches through optical fibers. Similarly, DKT Switches will interface with the DKTs through optical fibers. The fiber optic connections provide electrical isolation between the DKT Interface and the DKT Switches and ensure that the DKTs have electrical isolation from the DKT Switches. The design of the DKT Switch ensures data isolation between DKT Interfaces.

To the extent practical, all CR and AER data and status display will be through the DKTs. The DKTs will provide soft controls for all operator actions. The required manual operator controls will be retained and reconfigured to support the modernized PPS. One or more reduced functionality DKTs will be provided in the AER to simplify maintenance by providing indication

of the PPS data for calibration or other maintenance activities. These DKTs may also be used to support the PPS EWS.

All DKTs and the DKT Switches (e.g., Thinklogical TLX80) will be commercial grade dedicated and evaluated to ensure compliance with critical characteristics that include separation of video streams and no cross linkage between streams. All of the DKT Interfaces (e.g., Thinklogical redundant video transmitters and receivers), DKT Switches, and DKTs are thus basic components. Thus, there are no concerns about controlling safety-related systems from non-safety related displays, since the design will not include non-safety related DKTs or multi-divisional DKTs. While DKTs can be connected to any safety or non-safety related system, no DKT can be connected to more than one DKT Interface, and, thus, the DKT is limited and restricted to accessing only one system at a time. The DKT Switch behaves as a traditional, mechanical A-B KVM switch, albeit with many more ports, more switching capabilities, software restrictions concerning connections, and much more flexibility. This design resolves DI&C-ISG-04 (Reference 44) concerns about multidivisional displays and use of non-safety related displays to control safety-related systems by eliminating the potential of occurrence of the base concern.

DI&C-ISG-04 (Reference 44) strongly discourages implementing safety functions from non-safety related video displays, especially in DI&C-ISG-04 Section 3.1 Item 3. The proposed DKT Switch architecture used with DKT and DKT Interfaces addresses this concern directly, while at the same time providing for a common and flexible HSI in the CR.

3.3.5.2 Generic HSI Architecture

TBD/TBC 18: LGS to define the current BISI indicators in the control room (and AER) that are related to RPS, N4S, ECCS, or DAS

TBD/TBC 19: The PPS BISI indicator lamps and annunciator windows will be removed by this mod (we are not going to add discrete outputs to drive indicator lamps)

For the proposed switched DKT architecture, each DKT Interface will provide distinct standard communication links from each safety-related division and channel to the DKT Switch. Each non-safety related DKT Interface will have communication links to the DCS virtual terminal server. Fiber optic communication links will connect each DKT Interface to a DKT Switch port and a DKT Switch port to each DKT. As many DKT Interfaces as are required will be implemented. The locations of DKTs will be known, and restrictions will be configured into the DKT Switches to preclude defined locations from performing defined functions.

All data and status sampled by and computed by each channel and division will be available for display by the DKTs in the CR and AER. Data will not be presented in volts, mA, or logical state (e.g., True or False). Analog data will be presented in engineering units. Discrete contact state will be displayed as a meaningful message that provides easily understood meaning (e.g., valve closed, pump running). As an example, the LDS temperature data will be presented with a clear identification of the plant location with the high temperature.

The modernized PPS will move the existing BISI in the CR for the PPS and DAS to DKTs. This design will add switched DKTs to provide the PPS engineering unit values, internal status,

actuated device status, results of self-tests and self-diagnostics, BISI, and other key information to the CR and to the AER on DKTs.

One use for at least one of the DKTs will be for continuously visible BISI, in accordance with NRC RG 1.47 (Reference 56) and NRC Generic Letter 85-06 (Reference 57). The administrative procedures under which the plant operates will be extended to a requirement for the watchstanding operators to choose one or more displays and always have the "continuously visible" BISI parameters on a DKT, which the watchstanding operators can easily identify. LGS concludes that this administrative requirement resolves the "continuously visible" regulatory requirement. Nothing in this LAR Framework Document or the design of the four systems of interest precludes this operation.

Redundant uninterruptible vital power will supply each DKT Interface, DKT Switch, and DKT, to avoid the potential for loss of CR data display. The power to the DKT Interfaces, DKT Switches, and DKTs will not fail with the loss of either electrical division source. At a minimum, the design will provide a power supply/DKT scheme, so that in the event of a loss of one safety-related electrical division source, sufficient DKTs remain operable to support full plant power operation.

Each DKT will be able to select one of the set of DKT Interfaces served by the DKT Switch if the switching network is configured to allow that connection. Each of the video links will provide sufficient bandwidth to support 4K video and will operate with imperceptible jitter. Each of the fiber optic links and the DKT Switches will maintain electrical isolation between electrical divisions as well as between safety-related and non-safety equipment on different power sources.

The expectation is that every DKT Interface and every DKT will provide acceptable video display and keyboard and trackball access to the DKT Interface. The user will be able to select each DKT Interface selection from the same keyboards and trackballs attached to the same DKT Switch, within the acceptable interconnection scheme configured in the DKT Switch.

The modernized design will use dual DKT Switches (e.g., Thinklogical TLX80). The DKT Interfaces will provide a dual fiber optic video interface to connect to each of the redundant DKT Switches, such that all DKT Interfaces can communicate with both DKT Switch chassis. Each of the redundant DKT Switches will not require reconfiguration when a switch module is removed and replaced, which reduces software complexity. To further increase reliability, a dual fiber optic DKT video interface will be attached to each DKT, such that each DKT Interface and each DKT can be reached even if one of the dual DKT Switch chassis fails or is taken out of service for maintenance. With this arrangement, the DKT user will be able to select any DKT Interface configured to be accessible from the DKT being used.

The design will provide dual controllers, dual power supplies, and extra switching modules in the DKT Switch, along with the separate, required modular Control System and On-Screen Display (OSD) Client rack mount chassis for each DKT Switch. The system administrator will use the modular Control System and OSD Client for the required password and controlled configuration capabilities for the DKT Switches, using the software supplied in the module. The DKT Switch

used as an example requires this module to operate. The module provides system wide, nonintrusive monitoring and control of the DKT Switch.

The design will be configured to support the EWS or maintenance computer associated with the PPS or DCS. In this case, the EWS or computer use DKT Interfaces, with appropriate password and physical protections in the EWS, will ensure the CR watchstanding operators are aware of any use of the EWS. Only a very limited number of DKTs will be allowed to connect to the EWS.

The cyber security team will evaluate the use of switched connections for EWS or maintenance computers for potential cyber security concerns as well as the design team evaluation for software change control and configuration management (CM).

The configuration will disable the ability to issue commands for the safety-related and non-safety related systems for the DKTs at the SRO workstation. The SRO will still be able to navigate to various screens and functions, but the SRO will not be able to use soft controls to initiate safety-related or non-safety related control functions. Similarly, the configuration will disable process commands for the safety-related or non-safety related system for any DKTs intended solely for maintenance or engineering use. To prevent the SRO, maintenance, and engineering staff from issuing commands, the DKT Switch will be configured to allow only certain DKTs to connect to certain DKT Interfaces. Thus, the DKT Switch software will restrict the DKT capabilities based on the port to which the DKT is connected. For example, when an RO workstation DKT connects to a DKT Interface, the DKT Interface will support soft controls for the safety function as well as screen navigation. The DKT Switch configuration for the SRO station will not allow connection to DKT Interfaces that support soft controls but will still allow screen navigation. This existing software function is already resident in the DKT Switch and will be qualified for safety-related use. For a non-safety related DCSs standard architecture implementation, the DKT Switch will connect to a DKT Interface (consisting of a Thin Client that communicates to a virtual machine) configured such that the SRO DKT operates in display only mode, disallowing commands to the non-safety related system but still allowing screen navigation. DKTs in the RO CR work area will be configured to connect to a DKT Interface that supports soft controls and screen navigation.

Each DKT Switch will provide internal redundancy and 100,000-hour mean time between failure.

For each configuration, the DKT Switch raises the question of software common cause failure. From a software point of view, the issue is similar whether the design uses a dual DKT Switch or single DKT Switch since both are internally redundant. This question also exists for the software (including firmware and programmable logic) in the DKT Interfaces and DKTs. The issues with software common cause failures will be addressed for the DKT Switch, since supporting the RPS, N4S, and ECCS functions will require the DKT Switch, DKT Interface, and the DKT to be included in the D3 Analysis (Reference 7). The DKTs are based on commercial designs of proven pedigree and from vendors with acceptable, proven obsolescence strategies. The NRC has approved the Westinghouse Common Qualified (Common Q) platform that uses the same video generators in all four safety-related divisions, so there is precedent for this design.

Two internally-redundant DKT Switches will provide true redundant communication for all DKTs, as shown in Figure 3-24 above. This design requires redundancy in the communication paths between the DKT Interfaces, DKT Switches, and DKTs to ensure a signal path exists, even with one DKT Switch out of service.

The safety-related channels and divisions, along with the non-safety related DCS all will provide data to both DKT Switches through individual dual fiber optic connections, one to each DKT Switch. Each DKT Switch fans the connections out to each safety-related (qualified) DKT. With redundant DKT Switches, the design supplies dual fiber optic interfaces on each DKT Interface and dual fiber optic interfaces on each DKT. The dual fiber interface ensures that each DKT can route to any DKT Interface if either of the DKT Switches fails. In that manner, each DKT Switch will have access to all data and each DKT will have access to the data through either DKT Switch. With this arrangement, the highly reliable single DKT Switch now will become significantly more reliable.

Any DKT will be able to interface with any safety-related or non-safety related systems, including issuing commands to both the safety-related and the non-safety related systems. Interfaces to other systems, such as the LGS corporate network, would also be possible.

Each DKT Interface, DKT Switch, and DKT will be qualified and commercial grade dedicated as a safety-related device, such that issuing commands to safety-related equipment occurs from safety-related equipment and commands to non-safety related equipment occur from safety-related, qualified equipment, which meets the expectations of DI&C-ISG-04. Thus, any DKT in the CR can be used for any function.

The detailed design will determine the power source for the DKT Interfaces, DKT Switches, and DKTs. Uninterruptible power is supplied to all of the PPS, but vital power may only be required for part of the DKT system. A Failure Modes and Effects Analysis will verify that the chosen power solution is acceptable and will not result in the loss of display or have the potential to propagate failures from one division to the other.

Vital power will be provided from both divisions for the DKT Switches and DKTs.

3.3.5.3 Use of HSI for PAM

The PPS DKTs will provide the capability to group PAM data available in the PPS logically for display to the CR operator and to other locations where DKT access is provided. All PAM data will be isolated and provided to and sampled by the DAS. The DAS then will provide a diverse display of safety-related information on the DAS DKTs on a system implementing AQ, thus providing a diverse means of CR display of the PAM data available in the PPS, in addition to the diverse non-safety related means provided on the DCS using data communicated from PPS.

By providing PAM data on the PPS DKTs, there will no longer be a need for those existing, separate safety-related meters and recorders in the CR that supply data from the existing RPS, N4S, and ECCS, since the data will be displayed redundantly and diversely on PPS and DAS DKTs. Having safety-related displays on the PPS DKTs will support the existing meters and recorders to be either removed or abandoned in place.

About Thinklogical, A Belden Brand

Thinklogical manufactures secure and resilient video distribution and KVM switching systems for nuclear control room, training and simulation applications.

Thinklogical products support DOE digital control room modernization recommendations with DKT (display-keyboard-trackball) technology that enables human factors improvements and reduces operational costs.

An ISO 9001:2015 certified company, Thinklogical products are designed and engineered in the U.S.A.

Thinklogical, A Belden Brand
100 Washington Street, Milford, CT 06460 USA
Phone: (800) 291-3211 or +1 (203) 647-8700 Fax: +1 (203) 783-9949
info@thinklogical.com www.thinklogical.com