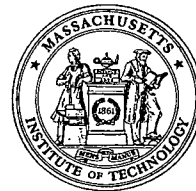


NUCLEAR REACTOR LABORATORY
AN INTERDEPARTMENTAL CENTER OF
MASSACHUSETTS INSTITUTE OF TECHNOLOGY



EDWARD S. LAU
Assistant Director of
Reactor Operations

138 Albany Street, Cambridge, MA 02139-4296
Telefax No. (617) 324-0042
Tel. No. (617) 253-4211

In-Core Experiment Loops
Activation Analysis
Nuclear Medicine
NTD Silicon
Facility Tours
Education & Training

12 May 2016

U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Attn.: Document Control Desk

Subject: Re: License Amendment Request for upgrade of the Nuclear Safety System in
the MIT Reactor Protection System, Docket No. 50-20, License R-37

The Massachusetts Institute of Technology hereby submits additional material to be placed on the docket in followup to the 30 September 2014 License Amendment Request (LAR) for its Facility Operating License No. R-37. The requested amendment is for upgrade of the reactor's nuclear safety system in the Reactor Protection System with new analog instrumentation and digital neutron flux monitors.

This submittal contains the following six documents:

- 1) Overview of New Nuclear Safety System with Integrated Supporting Modules
- 2) Signal Distribution Module (SDM)
- 3) <100 kW Key-Switch Module (KSM)
- 4) Withdraw Permit Circuit (WPC) Modification
- 5) Magnet Power Supplies and Rundown Relays
- 6) LED Scram Display, and Safety System Monitoring & Status Display PLC

And the drawings referenced by those documents:

- a) R3W-256-2 Rev. 1.4 for the SDM global connections
- b) R3W-258-3 Rev. 2 for the SDM V2 board
- c) R3W-254-4 for the Key-Switch Module
- d) R3W-203-4C Sheet 3-of-4 for the existing WPC
- e) R3W-203-4D Sheet 3-of-4 for the proposed WPC
- f) R3W-253-4 for magnet power supplies / rundown relays

A020
NRR

None of the drawing or text in this submittal contains any proprietary information. All of it has had previous thorough discussion with the appropriate branch of NRC. This submittal establishes official documentation of the additional material.

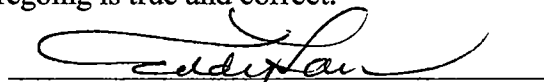
Sincerely,



Edward S. Lau, NE
Assistant Director of Reactor Operations
MIT Research Reactor

I declare under penalty of perjury that the foregoing is true and correct.

Executed on 05/12/2016
Date


Signature

EL/st

Enclosures: As stated.

cc: USNRC – Senior Project Manager
Research and Test Reactors Licensing Branch
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

USNRC – Senior Reactor Inspector
Research and Test Reactors Oversight Branch
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Q/A File #E-2012-1 — Digital Upgrade for Nuclear Safety System

"Overview of New Nuclear Safety System with Integrated Supporting Modules"

Description of Integrated Supporting Modules for New Nuclear Safety System

The proposed digital nuclear safety system consists of four independent neutron flux monitoring channels, which detect reactor neutronic power and reactor period, and compare those parameters against their pre-set values. If the pre-set values are reached, the flux monitors will output a trip signal. The following describes how these trip signals bring about a reactor shutdown, while they are also processed via independent modules for display and recording. These various modules are individually described and safety-evaluated in separate safety review documents*. Here the focus is on how the integrated system functions when all of these modules are connected together. See the block diagram in Figure One.

This describes the propagation of trip signals that are generated by the DWK 250 neutron flux monitors and travel throughout the various downstream modules until the signals attain their goal of scrambling the reactor. It is important to note that in all cases, the propagation manifests by de-energizing signal paths, not by energizing them.

When the reactor is operating at power within its prescribed envelope, no trip signals are generated**. — The relays that generate trip signals on the DWK 250 monitors are closed, and the signal paths downstream all are energized (to 24 volts DC). These signal paths go through the Signal Distribution Module (SDM), the Scram Logic Cards, the <100 kW Key-Switch Module (KSM), the Withdraw Permit Circuit (WPC), the Magnet Power Supply System, and the Rundown Relay System. The signal paths through these various modules remain energized, and there is no scram.

If the reactor is operating outside its prescribed envelope, a trip signal is generated. — Relays on the DWK 250 monitors are opened, de-energizing (to zero volts DC) a series of signal paths downstream. With these signal paths de-energizing, the ultimate effect is that electrical power stops going to the electro-magnets that support the neutron-absorbing shim blades, dropping the blades into the core by gravity and achieving shutdown of the reactor.

- * "Signal Distribution Module"
- "<100 kW Key-Switch Module"
- "Withdraw Permit Circuit Modification"
- "Magnet Power Supplies and Rundown Relays"
- "LED Scram Display, and Safety System Monitoring & Status Display PLC"

- ** Whenever the reactor is operating above 100 kW in Full Power Operation mode, each DWK 250 will generate the "100 kW High Power" trip signal. This signal is received by the Scram Logic Cards, where it performs a logic comparison that results, in this case, in no output of a scram signal. This is described in further detail later on.

Each DWK 250 neutron flux monitor outputs trip signals in binary form, via eight binary output relays. Two of them are used for high power warning and short period warning. The other six are for trip functions: high power level, short period, high power 100 kW operation, low count rate, test status, and fault / equipment malfunction. These eight output relays have a 24-volt DC source applied across them, from an independent external source, rather than from the DWK 250 chassis. The relay outputs are electrically isolated from the internal circuitry of the DWK 250. The external source is a pair of 24-volt DC power supplies, which are set up in parallel, connected via an auctioneering diode array, so that if one fails, the other will take over without interruption. The 24-volt DC power energizes the relays via the SDM. (See the Global Connection schematic diagram R3W-256-2 Rev. 1.4.)

The DWK 250 outputs a trip function signal by opening one or more of its binary output relays. This de-energizes the signal path on the SDM that connects to Scram Logic Card 1 and Card 2. Each DWK 250 has six trip signal paths through the SDM to the Scram Logic Cards, one for each of the six trip conditions listed in the previous paragraph. Together there are 24 such signal paths going through the SDM from the four DWK 250 chassis, passing the trip signals on to Scram Logic Cards 1 and 2.

Scram Logic Cards 1 and 2 perform identical logic comparison functions, and are connected to the SDM in parallel, with optical isolation at their inputs. Each Card uses discrete logic components, and is therefore non-programmable. Each features a two-out-of-four voting logic in hardware to prevent false trips from a single DWK 250 failure; this also eliminates the need for a safety system channel bypass switch. For instance, if one DWK 250 outputs one or more trip signals, then the Scram Logic Card will receive the signal(s) for logic comparison, and will make a decision not to output a scram signal. If two or more DWK 250s output trip signals, the two-out-of-four voting logic is now satisfied, and the Scram Logic Card will make the decision to output a scram signal. The Scram Logic Cards themselves have optically isolated outputs. They de-energize relays in the Withdraw Permit Circuit (WPC) and the Magnet Power Supply modules. Scram Logic Cards 1 and 2 work in parallel for redundancy.

The scram signal travels downstream from the Scram Logic Cards and reaches the <100 kW Key-Switch Module (KSM). The KSM chassis is mounted within the same Nuclear Instrument Module (NIM) bin as the Magnet Power Supply modules (NIM Bin 2 in Figure One). When a scram signal reaches this NIM bin, it is distributed to both the KSM and the Magnet Power Supply modules. This scram signal opens six relays in the Magnet Power Supply modules and five in the KSM. Opening of any of the six relays in the Magnet Power Supply modules will interrupt electrical power to the shim blade magnets directly, as will one of the relays in the KSM. Opening any of the four other relays in the KSM will open existing circuits Scram Loop A and Scram Loop B in the WPC, which in turn also results in interruption of shim blade electromagnet current, shutting down the reactor. These four relays also activate the "Safety System Scram" alarm on the main control room annunciator panel. Opening of the WPC activates the "Withdraw Permit Circuit" annunciator alarm there as well.

Whenever electric current to a shim blade electromagnet is interrupted, the Rundown Relay System moves the corresponding shim blade drive to its "full in" position at its normal speed. This takes place automatically to ensure that the released blade reaches its bottom position and stays there following a scram, completing the protective action once it is initiated.

When the KSM's key switch is turned to <100 kW Operation, signals indicating the key switch position are sent to the Scram Logic Cards, to the Safety System Monitoring & Status Display Programmable Logic Controller (PLC), and to the control room's main annunciator panel. This key switch position also automatically bypasses all three of the low flow primary coolant scrams. If reactor power reaches 100 kW, the DWK 250 will output the 100 kW high power trip signal, which will be logically interpreted by Scram Logic Cards 1 and 2. When the KSM's key switch is turned to Full Power Operation, the PLC's <100 kW Operation message will clear, and the low flow scrams are no longer bypassed. If reactor power reaches the nominal full power (6 MW), the DWK 250 will continue to output the 100 kW high power trip signal, while the Scram Logic Cards will receive the signal but will not interpret it as grounds for outputting a scram signal.

The two Scram Logic Cards and the LED Scram Display module are mounted within the same NIM bin (NIM Bin 1 in Figure One). Whenever a trip signal reaches the Scram Logic Cards from the DWK 250 chassis via the SDM, the Cards capture it and send it along to the LED Scram Display (again via the SDM), regardless of the logic decision. The LED Scram Display indicates the trip signal even if it came from a transitory condition, such that it cleared immediately at the DWK 250. This latching can be reset only by manually pushing a Channel Reset button on the LED Scram Display, one for each of the four DWK 250s. The Channel Reset button also resets the Scram Logic Cards (as they do not have their own reset buttons), and thus the lights on the LED Scram Display. This reset function is a necessary prerequisite for a reactor startup.

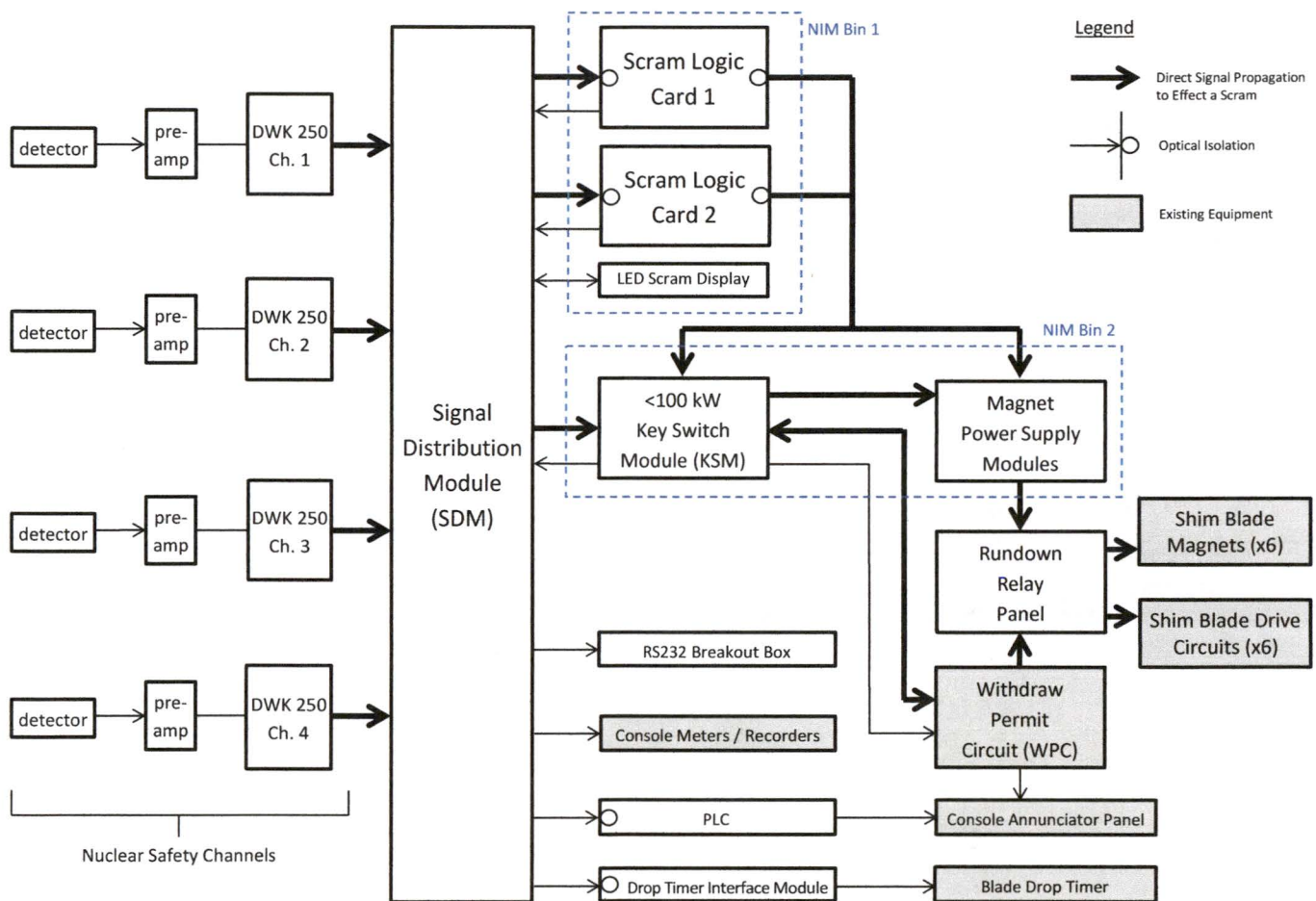
All of the above trip signal handling and scram signal handling functions take place via bi-stable, discrete components. There is no system clock or other timing function. In order to register the date and time of a trip event, a digital Safety System Monitoring & Status Display PLC panel is employed for real-time event logging. Each DWK 250 chassis outputs trip signals to the SDM, where the trip signals are routed separately to the PLC, as well as to the Scram Logic Cards. The two warning signals from the DWK 250 also go directly to the PLC, via the SDM. The PLC will then display and record the names of all of these alarm indications that come in, and will pass two types (warnings and fault alarms) to the control room's main annunciator panel. The PLC has a physical, common reset button to acknowledge and reset any alarms it registers. This reset button does not affect the LED Scram Display nor the Scram Logic Cards. The PLC has a built-in optical isolator on each of its signal input connections from the SDM, ensuring the signal flow is unidirectional into the PLC.

The six trip signals from each DWK 250 are passed via the SDM to a Drop Timer Interface module, which is equipped with optical isolators at the signal inputs, and in turn passes the signals to activate a Blade Drop Timer. The Drop Timer measures the time from initiation of a trip signal to 80% insertion of a shim blade, per Technical Specification

requirements. The Drop-Timer Interface module is a new piece of equipment that conditions the trip signals so that they are electrically compatible with the existing Blade Drop Timer.

All the modules described above, including the DWK 250 channels, are new equipment for the proposed nuclear safety system, with the exception of the WPC (which is modified in a few places) and the Blade Drop Timer. The control room's main annunciator panel is also existing equipment. All shaded blocks depicted in Figure One are existing equipment.

Figure One: Block Diagram of Nuclear Safety System with Integrated Support Modules



Safety Evaluation

The integrated system is highly redundant and will ensure that trip signals are propagated throughout the system to achieve their goal of scrambling the reactor, meeting their intended safety functions as defined by Chapter 7 of the Safety Analysis Report. If any of the components along the scram signal path should fail, the result will be an interruption of signal path, thereby resulting in shutdown of the reactor. Components that are not along the scram signal path will not interrupt the signal paths if they fail; furthermore, their failure will not interfere with trip propagation or scram processing. These latter components include the Safety System Monitoring & Status Display Programmable Logic Controller (PLC), the LED Scram Display, the Drop Timer Interface module, and the Blade Drop Timer.

Redundancy of scram relays and independence of activation(s) applies throughout the Nuclear Safety System, hence minimizing the risk of common-mode failure. All scram relays are mechanical relays that fail open, thereby minimizing the impact from EMF and radio frequency interference on their function.

Except the PLC, all the modules downstream of the DWK 250 chassis use low voltages and are built with discrete components that do not use microprocessors. The components are constructed only with non-programmable solid-state and discrete passive devices. As a result, signal propagation and handling are not subject to software processing delays. Additionally, there is no cybersecurity risk to this part of the system.

All the discrete components are standard industrially-rated devices. The low voltage nature of the system will maximize their operational life span, minimize EMF production, and reduce electrical hazards to Instrumentation personnel.

The Signal Distribution Module (SDM) reduces the use of excessive wiring and cable connections for signal transmission. Where possible, optical isolators are used at interfaces between modules to ensure signal flow is unidirectional.

The Scram Logic Cards use 2-out-of-4 voting logic in order to avoid unnecessary scrams from neutron flux monitoring channel faults. This increases stability and reliability of the nuclear safety system. If one of the two Scram Logic Cards fails such that it interrupts continuity from the 24-volt DC power supply, a scram signal is the result. The Scram Logic Cards were designed to provide an active output (24 volts) at each stage of the signal processing when a Scram condition does not exist. A scram signal from either Scram Logic Card is sufficient to result in a reactor scram. Whenever a scram signal is produced, it will indicate and be logged on the PLC, including in which Card(s) it originated.

All the modules in the Nuclear Safety System, including the DWK 250 chassis, will be rack-mounted within the protective metal cabinets of the control room console. The console cabinets will continue to provide the equipment with physical defense comparable to that for the current systems, including against seismic disturbance. Routine maintenance and inspection will be performed only by licensed reactor staff or under the supervision of licensed reactor staff. Where necessary, certain interactions can be performed only by or under the supervision of reactor Instrumentation staff members.

The control room is attended whenever the reactor is operating. At all other times when the building is unoccupied, it is protected as per the Physical Security Plan. Therefore, access control and configuration control are assured.

All the modules in the Nuclear Safety System, including the DWK 250 chassis, provide many indications of their operational status, trip signals, and scram signals. The console operator has a ready view of all of these, for instance, on both the LED Scram Display and the PLC. Therefore, human interface is improved. Additionally, the system is designed and constructed to require as little disconnection of cables, modules, and components for routine operation as possible. This is a major improvement over the existing Nuclear Safety System.

The new Nuclear Safety System will receive pre-operational and operational testing under a Test Plan. Individual modules will be bench-tested. Global system testing will be performed both on the bench and after installation in the control room.

Once it is operational, the functions of the Nuclear Safety System will be tested periodically as per the Technical Specifications. Therefore, regular surveillances will ensure its continued integrity.

The Nuclear Safety System provides one of the functions of the Reactor Protection System. Even if the Nuclear Safety System fails, there are other independent and redundant reactor protective functions that will continue to provide an automatic scram of the reactor based on high temperature, low primary coolant flow rate, low core tank level, etc., as described in the existing MITR Safety Analysis Report. Therefore, the Reactor Protection System is highly robust and diverse.

Q/A File #E-2012-1 – Digital Upgrade for Nuclear Safety System

"Signal Distribution Module"

Description of the Signal Distribution Module

The Signal Distribution Module (SDM) is a passive interface circuit between the DWK 250 digital neutron flux monitors and all components downstream. As can be seen in schematic diagram R3W-256-2 Rev. 1.4, and circuit board diagram R3W-258-3 Rev. 2, the SDM has a total of thirteen connections. In terms of signal flow, four of those connections are strictly input (signal coming from each of the four DWK 250 units), seven are input/output bidirectional, and two are strictly output. The following is a list of the connectors as they are labeled:

1. X10: Receives signal from DWK 250 channel #1.
2. X11: Receives signal from DWK 250 channel #2.
3. X12: Receives signal from DWK 250 channel #3.
4. X13: Receives signal from DWK 250 channel #4.
5. X14: Receives power from two 24-volt DC power supplies which are set up in parallel, connected via an auctioneering diode array, so that if one fails, the other will take over without interruption. The X14 connector then passes 24-volt DC power as output to three downstream components: Scram Logic Card 1, Scram Logic Card 2, and the <100 kW Key-Switch Module. The X14 connector also passes the 24-volt DC power via connectors X10 through X13 to energize the output (scram/alarm) relays of the four DWK 250 channels. (The DWK 250 output relays are electrically isolated from the internal circuitry of the DWK 250, and rely on an external power source for their operation.)
6. X15: Passes signals from the four DWK 250 channels to Scram Logic Card 1. The X15 connector receives signals back from Scram Logic Card 1 and routes them to other non-safety-related monitoring and display devices.
7. X16: Passes signals from the four DWK 250 channels to Scram Logic Card 2. The X16 connector receives signals back from Scram Logic Card 2 and routes them to other non-safety-related monitoring and display devices.
8. X17: Passes signals to and from the <100 kW Key-Switch Module.
9. X18: Passes signals to and from an LED Scram Display module, which captures scram signals from any of the four DWK 250 channels via the Scram Logic Cards, and keeps them latched in until the Scram Display module is used to reset the two

Scram Logic Cards. (Once the scram condition no longer exists, the DWK 250 will not show what the scram was.)

10. X19: Passes analog signals from the four DWK 250 channels to existing console chart recorders and meters.
11. X20: Passes signals from the rear input/output terminal blocks of the four DWK 250 channels to and from a breakout module containing four 9-pin RS-232 ports (one per channel), plus a 15-pin RS-232 port that can interact with all four smaller ones. The breakout module will be secured from unauthorized access.
12. X21: Passes signals from all inputs of the SDM to a non-safety-related programmable logic controller (PLC) for monitoring and status display.
13. X41: Passes signals to and from all four DWK 250 channels to a Drop Timer Interface Module, which in turn passes signals to activate a Blade Drop Timer. This setup will measure the scram time from initiation of a scram signal to 80% insertion of a shim blade. The Drop Timer Interface Module conditions an input signal for compatibility with the previously-existing Blade Drop Timer, and includes optical isolation of the SDM from the Blade Drop Timer. The Drop Timer Interface Module and the Blade Drop Timer are both mounted in a "NIM bin" rack which provides them an independent power source.

Safety Evaluation

The Signal Distribution Module (SDM) is a new passive circuit board which facilitates passing of signals between various components of the new nuclear safety system. If the board fails, such as by physical damage or other disruption to a scram signal path between a DWK 250 and the Scram Logic Cards, there will be a loss of the signal, thereby causing the Scram Logic Cards to produce a scram. The physical damage could include puncture, impact, fire, or high voltage surge, while other types of disruption could include radio frequency interference, overheating, or corrosion. All would result in a scram.

Because the SDM is a passive circuit board, it does not include any optical isolators. However, there are optical isolators built into Scram Logic Card 1, Scram Logic Card 2, the Drop Timer Interface Module, and the PLC panel.

The connection to the two 24-volt DC power supplies only passes power to the two Scram Logic Cards and the <100 kW Key-Switch Module. The SDM board does not use the power for its own functions. The two power supplies are fed from a common 120-volt AC source, and have an internal fuse which will protect against surges that exceed 250 volts AC on that line. They also have an output overload that will trip at no more than 35 volts DC. In the unlikely event of an excessive line voltage surge, both power supplies will likely trip to protect themselves, interrupting power to the two Scram Logic Cards, scrambling the reactor. If the surge affects the SDM board directly, it will create physical damage as described above, again resulting in a reactor scram.

Signals input to the SDM board from the two Scram Logic Cards are passed along to other display and status monitoring devices. If the board should be damaged in these areas, there is no effect on nuclear safety. The console operator may observe a partial loss of indications of reactor power and reactor period, but will not receive false information. There are redundant displays of reactor power and period, such as on the face of each DWK 250 chassis, that will remain operable. There are also four existing independent non-safety-related neutron flux channels or N-16 gamma channels displaying reactor power. Likewise, loss of signal output from the SDM to existing console chart recorders and meters has no effect on nuclear safety. There is redundant recording of reactor power history from the non-safety-related neutron flux channels.

Signals to and from the RS-232 breakout box will be lost should the SDM board be damaged. However, this again has no nuclear safety consequence. The breakout box allows access to each of the four DWK 250 channels to set adjustable parameters by computer. Such adjustments are done only by authorized individuals, and only when the channel is off line or the reactor is shut down. The box has a cover and is secured when not in use. The computer used for this purpose is a standalone unit and is not connected to the internet. The interface software is provided by the manufacturer of the DWK 250s. Therefore cybersecurity is maintained.

The SDM will be bench-assembled on one circuit board in a controlled environment. The new board will then be connected to the rest of the new nuclear safety system while everything is de-energized. The module will be constructed with standard industrially-rated components. The two 24-volt DC power supplies meet medical qualifications. The SDM contains no digital components, and is therefore not subject to cybersecurity threats.

The SDM will be mounted within the protective metal cabinets of the control room console. The console cabinets will provide the module with physical defense, including against seismic disturbance. Routine maintenance and inspection will be performed only by licensed reactor staff or under the supervision of licensed reactor staff. The control room is attended whenever the reactor is operating. At all other times when the building is unoccupied, it is protected as per the Physical Security Plan. Therefore, access control and configuration control are assured.

The control room and its metal instrumentation cabinets are in an air-conditioned environment. The temperature is continuously maintained within a desirable setting (approximately 68 F). There is a temperature alarm (setpoint no higher than 78 F) that is monitored whenever the reactor is operating, or shut down with the control room attended. This air-conditioning control easily satisfies the operating requirements for all the components in the SDM board.

All cables to the SDM and cable connection points on the SDM will be labeled, as will the circuit board. These markings improve the human interface for purposes of installation and maintenance. Once it is installed, there will be no regular human interface with the SDM board. It will be handled only by or under the supervision of license reactor staff. Therefore, human factors engineering remains adequate.

The SDM contains a continuity wiring feature that recognizes when each DWK 250 is connected to its correct connector on the SDM. Specifically, DWK 250 Unit 1 is supposed to connect to X10 via cable K-10, DWK 250 Unit 2 to X11 via cable K-11, DWK 250 Unit 3 to X12 via cable K-12, and DWK 250 Unit 4 to X13 via cable K-13. If a cable is unplugged, or plugged into the wrong connector, the continuity circuit will report the misconfiguration via a fault message on the PLC that handles safety system monitoring and status display. The same error message will be generated by the PLC if this continuity circuit fails open.

A dummy cable plug will take the place of a DWK 250 chassis in cases where one chassis is physically removed for repair/maintenance. The absent chassis will appear as a trip signal on the Scram Logic Cards. If any one of the remaining three chassis should output a trip signal, then the Scram Logic Cards will produce a scram signal. The purpose of the dummy plug is merely to allow the continuity circuit to continue to verify that the three remaining chassis are connected to their correct connectors.

The new SDM board will be tested for wiring verification using a written procedure prior to first use, and periodically as part of operational checks of the nuclear safety system. Therefore, these pre-operational and routine surveillances are sufficient to assure the completeness and integrity of the circuitry.

Q/A File #E-2012-1 – Digital Upgrade for Nuclear Safety System

"<100 kW Key-Switch Module"

Description of the <100 kW Key-Switch Module

The <100 kW Key-Switch Module (KSM) provides positive indication to the console operator if the reactor is set up for the <100 kW mode of operation vs. the Full Power mode of operation. The KSM chassis is labeled "Reactor Operating Mode", as shown in Figure 1 and Figure 2.



Figure 1



Figure 2

There are only two positions for the key switch: Full Power mode, and the <100 kW mode. The switch is mechanically spring-loaded for positive detent, so it will move to rest in one of these two positions, making it extremely difficult to leave the key in a neutral position.

When the key switch is turned to <100 kW Operation, a local <100 kW Operation indicator LED light will illuminate. (See key switch pole KS1C on Reactor Drawing R3W-254-4.) Likewise, also from pole KS1C, a signal will be sent to the Status Display programmable logic controller (PLC), and from pole KS1B, an alarm will illuminate on the control room's main annunciator panel. Furthermore, when the key switch is selected to <100 kW, the KSM transmits signals via pole KS1D to bypass any scram that comes from Low Flow Primary, Low Pressure MP-6, or Low Pressure MP-6A (each of which activates its own indicator on the control room's main annunciator panel). The 100 kW High Power Trips

from the DWK 250s will, if on, be interpreted as channel trip signals by Scram Logic Card 1 and Scram Logic Card 2. (Note: As shown in Drawing R3W-254-4, pole KS1A exists but is not used.)

When the key switch is turned to Full Power Operation, the <100 kW local indicator, the <100 kW annunciator alarm light, and the PLC message will all clear, and the three primary flow scram bypasses are automatically removed. A local Full Power Operation indicator LED light will illuminate via key switch pole KS1C. Furthermore, when the key switch is selected to Full Power, the KSM sends a signal via pole KS1C to Scram Logic Card 1 and Scram Logic Card 2 which causes the DWK 250 100 kW High Power Trips to be bypassed.

The front of the KSM chassis has two LED lights that indicate "Loop A Scram" and "Loop B Scram", as seen in Figure 1 and Figure 2. These lights come on only when there is a scram condition in the Withdraw Permit Circuit's (WPC's) Scram Loop A or B, respectively.

Reactor Drawing R3W-254-4 illustrates all the above functions of the KSM. The module receives power from two 24-volt DC power supplies which are set up in parallel, connected via an auctioneering diode array, so that if one fails, the other will take over without interruption. When the KSM chassis is powered, the "24V D.C. Power" indicator LED light will be lit.

The KSM chassis is mounted within the same Nuclear Instrument Module (NIM) bin as the Magnet Power Supply modules. When Scram Logic Card 1 or Card 2 outputs a scram signal, the signal reaches this NIM bin via connector X40, which distributes it to both the KSM and the Magnet Power Supply modules. This scram signal opens all relays downstream of the Scram Logic Cards as indicated on Drawing R3W-254-4. This set of ten 24-volt relays includes GM1A, GM2A, GM3A, GM1B, GM2B, and GM3B in the Magnet Power Supply modules, and RY5, RY6, RY7, and RY8 in the KSM. In fact, any one of the RY5 – RY8 relays opening will open 120-volt relay B3 or B4 in the WPC's Scram Loop A or Scram Loop B (physically located in the WPC), thereby resulting in a scram. Additionally, opening of an RY5 – RY8 relay contact illuminates the "Loop A Scram" or "Loop B Scram" indicator LED light on the KSM chassis, and activates the Safety System Scram annunciator alarm. Opening of the RY4 relay (coil physically located in the KSM), or the GM1 – GM3 relays listed above, will directly interrupt electrical power to shim blade magnets as covered in the Magnet Power Supply System description.

Built into the back of the KSM chassis is one multi-pin connector, which combines the connecting functions of X28, X40, and X43, as they are labeled on schematic diagram R3W-256-2 Rev. 1.4. These connecting functions are as follows:

1. X28: Transmits signals to the Status Display PLC, and to Scram Logic Card 1 and Scram Logic Card 2 via the Signal Distribution Module.
2. X40: Receives 24-volt DC power. Receives signals from Scram Logic Card 1 and Scram Logic Card 2.
3. X43: Transmits signals to the Withdraw Permit Circuit, the Magnet Power Supplies, and the control room's main annunciator panel.

Safety Evaluation

The <100 kW Key-Switch Module (KSM) is constructed entirely of discrete components, uses no digital devices, is not programmable, and is therefore not subject to cybersecurity threats. The KSM is not responsible for originating any scram signals. It uses 24-volt DC power. If power is lost, the 24-volt LED power indicator light and any other LED indicator light on the front of the chassis will all go out. However, when the key switch is in the <100 kW mode, the main annunciator panel will continue to have its "<100 kW Operation" alarm light on, as that alarm is powered from the annunciator panel itself. If the chassis were damaged, the effect would be the same as a loss of power.

Some of the relays associated with the Withdraw Permit Circuit (WPC) have their coils and/or contacts physically located within the KSM. These include relays RY4, RY5, RY6, RY7, and RY8. If this part of the KSM fails, such as by loss of power, physical damage, or other disruption to a circuit path, there will either be a loss of signal in the WPC, thereby causing a scram, or a power cutoff to Scram Loop A or Scram Loop B, equally causing a scram. Likewise, if the 120-volt AC power supply path to the magnet power supplies within the KSM is physically interrupted, the loss of magnet power will cause the shim blades to drop into the core, thereby causing a scram. The physical damage could include puncture, impact, fire, or high voltage surge, while other types of disruption could include radio frequency interference, overheating, or corrosion. All would result in a scram.

The key switch is mechanically spring-loaded for positive detent, so it will move to rest in one of its two positions, making it extremely difficult to leave the key in a neutral position. However, if the key switch should fail and not be in full contact with either of its two designated positions, neither mode indicator LED light will be illuminated, no respective main annunciator or PLC alarms will be lit, and none of the bypasses associated with either position be in effect. Accordingly, if the primary pumps are not on, all the associated low flow scrams will be in effect (WPC open) and will prevent a reactor startup or continued operation. If the primary pumps are on, and reactor power exceeds 100 kW, the 100 kW High Power Trips on the DWK 250s will take effect and scram the reactor.

Another failure mode of the KSM is if it no longer transmits a signal because of physical damage or other disruption as discussed above. This would have the same effects as lack of full contact within the key switch, as described in the previous paragraph. All such abnormal effects are either not safety-related, or produce outcomes more conservative than the normal configurations.

The KSM shares use of the 24-volt DC power supplies with the Scram Logic Cards. If the 24-volt power fails, the Scram Logic Cards will produce a scram.

The KSM will be bench-assembled in a controlled environment. The new assembly will then be connected to the rest of the new nuclear safety system while everything is de-energized. The module will be constructed with standard industrially-rated components. The two 24-volt DC power supplies meet medical qualifications.

The KSM will be mounted in the same Nuclear Instrument Module (NIM) bin as the Magnet Power Supply modules. They are all within the protective metal cabinets of the control room console, which will provide the modules with physical defense, including against seismic disturbance. Routine maintenance and inspection will be performed only by licensed reactor staff or under the supervision of licensed reactor staff. The control room is attended whenever the reactor is operating. At all other times when the building is unoccupied, it is protected as per the Physical Security Plan. Therefore, access control and configuration control are assured.

The control room and its metal instrumentation cabinets are in an air-conditioned environment. The temperature is continuously maintained within a desirable setting (approximately 68 F). There is a temperature alarm (setpoint no higher than 78 F) that is monitored whenever the reactor is operating, or shut down with the control room attended. This air-conditioning control easily satisfies the operating requirements for all the components in the KSM.

All cables to, and cable connection points on, the KSM will be labeled, as will the NIM bin. These markings improve the human interface for purposes of installation and maintenance. Once it is installed, there will be no regular human interaction with the KSM chassis other than the key switch itself. The key switch is a standard industrial component. The LED indicator lights adjacent to it confirm when it is latched in either of its two designated positions. Therefore, human factors engineering remains adequate.

The new KSM assembly will be tested for wiring verification using a written procedure prior to first use, and periodically as part of operational checks of the nuclear safety system. Therefore, these pre-operational and routine surveillances are sufficient to assure the completeness and integrity of the circuitry.

Q/A File #E-2012-1 – Digital Upgrade for Nuclear Safety System

"Withdraw Permit Circuit Modification"

Description of Withdraw Permit Circuit and Modification

The Withdraw Permit Circuit (WPC) is a startup interlock that consists of a string of relays and contacts in series. Each corresponds to either a startup requirement or to a reactor scram condition. If any of the relays and contacts in this series lineup is open, the circuit interrupts electrical current to the electromagnets that hold the six shim blades, thereby decoupling the shim blades from their drives and effecting a scram. See MIT Reactor Drawing R3W-203-4 (Sheet 3 of 4; Revision C for the existing WPC, and Revision D for the proposed modification).

The WPC will be modified in this upgrade to the digital nuclear safety system in the following areas:

1. Removal of the relays and contacts that produce a two-out-of-three logic for the Period Channel Level Signal Off-Scale scram. These are no longer needed for the new nuclear safety system. (An earlier approach was to bypass all of these relays and contacts, but leave them physically in the circuit. Later we decided to remove them for simplification and maintainability of the circuit.) Twelve contacts will be removed as a result.
2. Addition of three relays that bypass the primary flow scrams when in the <100 kW operating mode, which uses no forced flow, as allowed by Technical Specifications. These relays are designated RY1 (for the Core Inlet Pressure MP-6A scram), RY2 (for the Low Flow Primary Coolant scram), and RY3 (for the Core Inlet Pressure MP-6 scram). These relays will perform bypass functions that are currently implemented manually using individual upstream key-switches. For the upgrade, the relays will be permanently installed into the WPC.
3. Addition of three relays that operate through the rundown relay panel. The first of these relays, designated B2A, interrupts magnet current to shim blades 1 and 2. The second, designated B2B, interrupts magnet current to shim blades 3 and 4. The third, designated B2C, interrupts magnet current to shim blades 5 and 6. Each of these is a redundant addition in series with existing relays B1A, B1B, and B1C respectively.
4. Addition of one contact that opens the WPC redundantly in the case of a scram trip from the nuclear safety system. This new contact, designated B4-1 or "Safety System Scram (Loop B)", will serve a redundant function with existing contact B3-1 "Safety System Scram (Loop A)". A scram signal from Scram Logic Card 1 will open relays B3 and B4 in Loop A and Loop B respectively. Likewise, a scram signal from Scram Logic Card 2 will also open relays B3 and B4 in Loop A and Loop B respectively. In the existing system, the Safety System Scram opens only one contact (B3-1).

Safety Evaluation

The removal of old relays and contacts, instead of bypassing them, helps prevent cluttering the Withdraw Permit Circuit (WPC) with unused components. The removal process will be done with the circuit completely de-energized, and will not exert undue physical stress on the other existing components in the circuit.

The addition of new relays and contacts will be done by building them into several separate circuit modules in a controlled environment. These new modules will then be connected to the rest of the new nuclear safety system while the reactor is shut down and the appropriate circuits are de-energized. All existing and new relays in the WPC are standard industrially-rated mechanical relays, hence minimizing the impact from EMF and radio frequency interference on their function. All are configured to open when de-energized or upon failure. The WPC remains non-programmable and non-digital, consisting only of discrete bi-stable components, and is therefore not subject to cybersecurity threats.

New relays RY1, RY2, and RY3 (mentioned in Item 2 above) bypass three different scrams that all represent the low primary coolant flow condition when operating the reactor in the <100 kW mode. When the <100 kW mode is selected on the <100 kW Key-Switch Module, these three relays will be energized to close and bypass the scrams. A failure of any of these three new relays during a low flow condition will result in a reactor scram. When the Full Power mode is selected on the <100 kW Key-Switch Module, these three relays will remain de-energized and open, and will have no effect on the WPC.

New relays B2A, B2B, and B2C interrupt electrical current to the electromagnets of their respective pairs of shim blades. Their functions are redundant to existing relays. Like those existing relays, if they fail during operation, they will cause their pairs of shim blades to drop into the core, shutting down the reactor.

The WPC will remain mounted in its original location within the protective metal cabinets of the control room console. The console cabinets will continue to provide the circuit with physical defense, including against seismic disturbance. Routine maintenance and inspection will be performed only by licensed reactor staff or under the supervision of licensed reactor staff. The control room is attended whenever the reactor is operating. At all other times when the building is unoccupied, it is protected as per the Physical Security Plan. Therefore, access control and configuration control are assured.

The control room and its metal instrumentation cabinets are in an air-conditioned environment. The temperature is continuously maintained within a desirable setting (approximately 68 F). There is a temperature alarm (setpoint no higher than 78 F) that is monitored whenever the reactor is operating, or shut down with the control room attended. The air-conditioning control easily satisfies the operating requirements of all the components, which are of standard industrial qualifications. When the reactor is shut down and the building is secured, the WPC is de-energized.

All cable connections to the WPC will be labeled, as will the new circuit modules. These markings improve the human interface for purposes of installation and maintenance.

Human interface with the WPC is via key-switches in plain sight on the front of the console. The existing array of key-switches for individual scram bypasses will now be supplemented by one that switches between <100 kW and Full Power modes of operation. When this <100 kW key-switch is turned to the <100 kW mode of operation, which automatically bypasses the three primary flow scrams, it provides one indicator light on the <100 kW Key-Switch panel, and an alarm on the main annunciator panel denoting "<100 kW Ops Mode On". Additionally, the main annunciator panel will have the "Withdraw Permit Bypass On" alarm illuminated. These indications reinforce the console operator's awareness of operating the reactor in <100 kW mode. Furthermore, there will be indicator lights turning on at each of the three primary flow scram bypass key-switches, providing visual confirmation to the console operator of the flow scram bypasses. Therefore, human factors engineering remains adequate and more than equivalent to the current system.

The new WPC will be tested with a written procedure prior to first use, and periodically as per the Technical Specifications for the nuclear safety system and process system scrams. Therefore, regular surveillances will ensure the integrity of the circuit, and the WPC will continue to perform its safety function as defined by the SAR.

Q/A File #E-2012-1 – Digital Upgrade for Nuclear Safety System

"Magnet Power Supplies and Rundown Relays"

Description of Magnet Power Supply System

The function of the magnet power supplies is to provide current (~80 milliamps DC) to the electromagnets for all six shim blades (i.e., absorber sections of the control devices) in the reactor core. Each magnet holds the weight of its shim blade, attaching it to its drive mechanism via the magnet. When current to the magnet is interrupted, the shim blade will decouple from its magnet and drive, and travel vertically by gravity into the reactor core, scrambling or shutting down the reactor in less than one second.

In the existing nuclear safety system, power for the magnets originates in the electronic circuitry of the six nuclear safety amplifiers. These amplifiers provide the necessary trip signals, three on high power and three on short period, and use those signals to interrupt current to the magnets. The interruption is first applied to the magnets for a pre-selected pair of shim blades (blades 1 & 4, or blades 2 & 5, or blades 3 & 6), and then to the remaining four magnets.

The new nuclear safety system will not consist of safety amplifiers. Instead the high power and short period trips all originate from four independent Mirion DWK 250 neutron flux monitors. The new magnet power supply system will consist of three modules, with each module providing magnet current to two shim blades (blades 1 & 2, blades 3 & 4, and blades 5 & 6). Each module interfaces with its corresponding rundown relay circuit, with magnet current passing through the rundown relay panel on its way to the magnet. The function of the rundown relay system will be described in the next section.

Each magnet power supply module is a stand-alone electronic circuit, made of discrete solid-state components, with its own 24-volt DC power supply. (See Drawing R3W-253-4.) Each module has two "current adjust" regulators, one for each associated shim blade. The regulators are semiconductor devices. The adjusted current is displayed on a meter in series with the regulator, one for each shim blade.

Magnet current is interrupted in each magnet power supply module via two relays that are controlled by Scram Loops A and B from the output of the Scram Logic Cards. For instance, relay contacts GM1A-1 and GM1B-1 on Drawing R3W-253-4 for shim blade 1 belong to relays GM1A and GM1B in Scram Loops A and B respectively. If Scram Loop A, or Scram Loop B, or both A and B are open, i.e. in scram condition, these relay contacts will open to interrupt magnet current to shim blade 1. Likewise, contacts GM1A-2 and GM1B-2 for shim blade 2 will open to interrupt magnet current to shim blade 2.

The Withdraw Permit Circuit (WPC) interrupts magnet current via relays in the rundown relay panel, as described in the next section. For redundancy, when the WPC is open, the 120-volt AC line power from reactor electrical circuit L21 itself will be interrupted,

thereby simultaneously de-energizing all three 24-volt DC power supplies for the three magnet power supply modules. This can be seen on Drawing R3W-253-4, where relay RY4 from the WPC will open relay contact RY4-1 when the WPC is open, thereby interrupting current from all three 24-volt DC magnet power supplies. The independent interruption of the magnet power supply via the nuclear safety Scram Logic Cards and the WPC provides redundancy and prevents common-mode failure.

Description of Rundown Relay System

The function of the rundown relay system is to move each shim blade's drive mechanism to its "full in" position at its normal speed whenever magnet current to the shim blade's magnet is removed. When the blade's magnet current is interrupted, the blade is intended to drop by gravity into the core. Moving the drive in behind it automatically is to ensure that the blade reaches its bottom position and stays there following a scram, completing the protective action once it is initiated.

The magnet power supply circuits are constructed in three independently-powered modules, each supplying a pair of shim blade magnets. The rundown relay system, however, is all part of one panel, and uses its own 24-volt DC power supply to energize the circuits for all six shim blades.

When the magnet power supply circuit is energized, current goes through the rundown relay system via three relay contacts connected in series (B1A-1, B2A-1, & RR1-1 on Drawing R3W-253-4 for shim blade 1, or B1A-2, B2A-2, & RR2-1 for shim blade 2). Relays B1A and B2A are controlled by the Withdraw Permit Circuit (WPC). If the WPC is open, i.e. in scram condition, these relays interrupt magnet current to the associated shim blade. Relays RR1 and RR2 also interrupt magnet current, if the magnitude of that current drops below a pre-determined value which is set by an opto-relay (U1 for shim blade 1, U2 for shim blade 2).

The RR1, RR2, etc., relays perform two additional functions: controlling an indicator light that shows the status of the rundown relay circuit for its corresponding shim blade, and overriding normal control of the shim blade's drive motor. The indicator light stays out whenever the magnet current is at normal operating level. It comes on when the magnet current is low or near zero; the corresponding shim blade drive will be moving in, until it reaches its full-in position. Whenever the WPC is open, the indicator lights will stay on, denoting the control overrides which prevent any shim blade drive from being moved outward. Even after the WPC is reset and re-energized, this override condition will remain in effect until the rundown relay circuits themselves are reset by the console operator. Additionally, the rundown relay circuits cannot be reset if the magnet current is below a pre-determined value. When the circuit is reset, the indicator lights go out.

The rundown relay circuit for each shim blade can be individually reset once the blade drive has reached the full-in position and the WPC has been reset and re-energized. A master reset (pushbutton PB7, acting via relays MR1 and MR2 on Drawing R3W-253-4) is also available to reset all six rundown relay circuits simultaneously.

Safety Evaluation

Both the magnet power supply system and the rundown relay system will continue to perform their safety functions as defined by the SAR. Both systems were rebuilt with standard industrially-rated components. As was the case for their previous forms, they contain no digital components, being constructed only with non-programmable solid-state and discrete passive devices. Therefore, these systems are not subject to cybersecurity threats.

There are six independent ways to interrupt current to any given shim blade magnet: two relays from the Scram Logic system (via scram loops A and B), two relays from the WPC in the blade's rundown relay circuit, one relay in the blade's rundown relay circuit that opens upon low current, and one relay from the WPC in the line power supply. If there is a nuclear safety system scram, all six of these ways will have their relays open, to ensure a reactor scram. If there is a process system scram (e.g. low flow on the primary coolant system, low pressure city water, etc.), then only four of the above ways will apply: two relays from the WPC in the blade's rundown relay circuit, one relay in the blade's rundown relay circuit that opens upon low current, and one relay from the WPC in the line power supply. Most importantly, any one of these ways will cause a magnet current interruption to shut down the reactor, and will activate the rundown relay circuit to drive all the shim blades in. (The regulating rod will also be driven in when the WPC is open, but via the existing rod control circuit.)

Five out of six of the relays mentioned above in the magnet power supply circuit and the rundown relay circuit for each shim blade are wired in series. If any one of those is open, magnet power to that shim blade is interrupted.

The three magnet power supply modules have their own independent 24-volt DC power supplies. Likewise, the rundown relay panel has its own 24-volt DC power supply. They are independent except that the three units for the magnet power supply modules have a common relay immediately upstream that will open when the WPC is open.

In summary, redundancy of scram relays and independence of scram activation(s) minimizes the risk of common-mode failure of the magnet power supply system and the rundown relay panel. The two relays from Scram Loops A and B, and the three relays from the WPC, are all mechanical relays that fail open, hence minimizing the impact from EMF and radio frequency interference on their function.

Opto-relays, one for each shim blade, are used within the magnet power supply modules. For instance, they are shown as contacts U1-1 and U2-1 in Drawing R3W-253-4 for shim blade 1 and shim blade 2 respectively. The opto-relays were chosen for their sensitivity to low current, i.e., less than 5 milliamps. Upon sensing current dropping to a low value, the optical portion of the relay will then deactivate the solid-state portion to de-energize the coil of relay RR1 for shim blade 1, or RR2 for shim blade 2, etc.

Each 24-volt DC power supply for the three magnet current power supply modules and the rundown relay panel is protected by its own fuse against surges in line voltage on

circuit L21. In line with each shim blade magnet, downstream of the magnet power supply and rundown relay circuits, is a fuse that prevents any power surge from damaging the magnet. Each fuse is rated for no more than 0.25 amp. Therefore, the magnet power supply system and the rundown relay circuits are adequately protected from power surges in their operating environment.

The magnet power supplies and the rundown relay panel will be rack-mounted within the protective metal cabinets of the control room console. The console cabinets will continue to provide the equipment with physical defense comparable to that for the current systems, including against seismic disturbance. Routine maintenance and inspection will be performed only by licensed reactor staff or under the supervision of licensed reactor staff. The control room is attended whenever the reactor is operating. At all other times when the building is unoccupied, it is protected as per the Physical Security Plan. Therefore, access control and configuration control are assured.

The control room and its metal instrumentation cabinets are in an air-conditioned environment. The temperature is continuously maintained within a desirable setting (approximately 68 F). There is a temperature alarm (setpoint no higher than 78 F) that is monitored whenever the reactor is operating, or shut down with the control room attended. The air-conditioning control easily satisfies the operating requirements of all the components, which are of standard industrial qualifications. When the reactor is shut down and the building is secured, the magnet power supply system and the rundown relay circuits are de-energized.

Human interface with the magnet power supply system is via current-adjust knobs, and meters on the console showing the instantaneous magnet current for the corresponding shim blades. The interface with the rundown relay panel is via indicator lights and reset pushbuttons, as described in the previous section. These interfaces are in plain sight, and conveniently near the main part of the console for the operator. Therefore, human factors engineering is adequate and equivalent to the current system.

All cable connections to the magnet power supply system and the rundown relay panel will be labeled, and some will be color-coded. Individual modules and panels will also be labeled, as will key electronic components on circuit boards. These markings improve the human interface for purposes of installation and maintenance.

The functions of the magnet power supply system and the rundown relay panel will be tested periodically as per the Technical Specifications for the nuclear safety system. Therefore, regular surveillances will ensure the integrity of these systems.

Q/A File #E-2012-1 – Digital Upgrade for Nuclear Safety System

"LED Scram Display, and Safety System Monitoring & Status Display PLC"

Description of the LED Scram Display

The LED Scram Display features two 4x4 arrays of light-emitting diode (LED) indicator lights that allow, via the outputs of the two Scram Logic Cards, the console operator to readily identify which DWK 250 chassis has produced a trip signal from its binary outputs, as shown in Figure 1 below. The upper array shows the signals output by Scram Logic Card 1, and the lower array by Scram Logic Card 2.

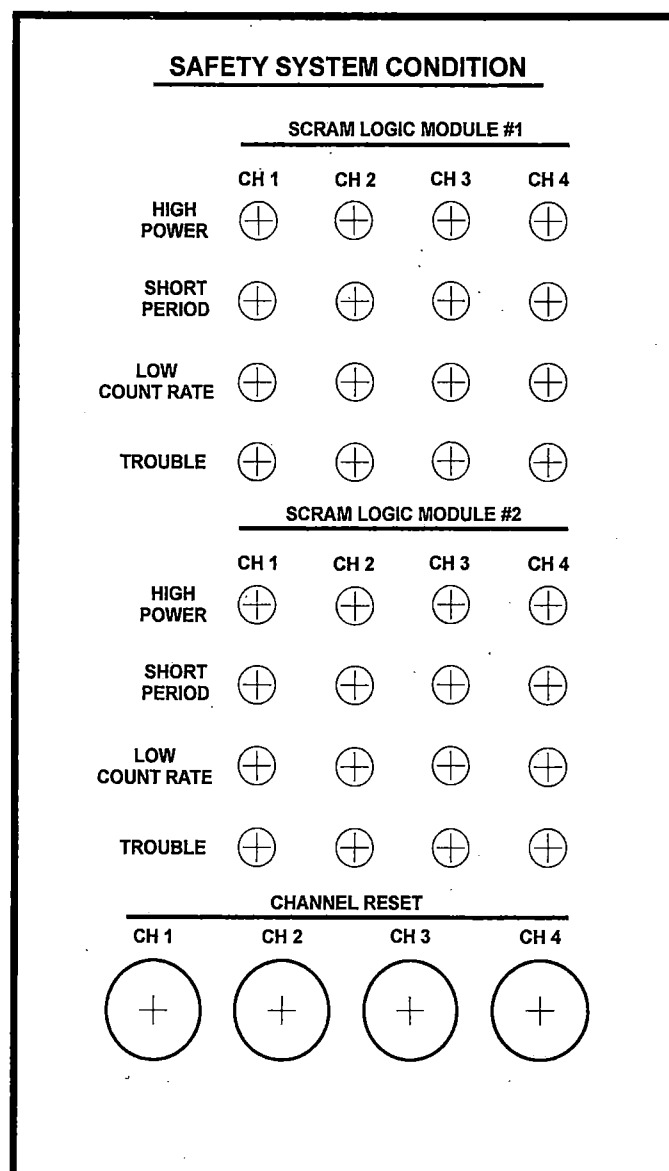


Figure 1 – Front Face Overlay for the LED Scram Display

The LED Scram Display module receives trip condition signals from Scram Logic Card 1 and Card 2 by way of the Signal Distribution Module (SDM). (See schematic diagram R3W-256-2 Rev. 1.4.) When a DWK 250 outputs a trip signal, the signal is indicated on the DWK 250 chassis itself. If this trip is transitory, such as a momentary high power, the indicator light on the DWK 250 will go out as soon as the trip condition clears. However, the trip signal will be retained (or "latched") in the Scram Logic Cards, which send it to the LED Scram Display module.

From each of the Scram Logic Cards, the LED Scram Display has four trip indications representing six trip conditions from each of the DWK 250 channels: High Power (full power or 100 kW set point, depending on the position of the <100 kW key-switch), Short Period, Low Count Rate, Test, and Fault / Equipment Malfunction, with the latter two combined as Trouble.

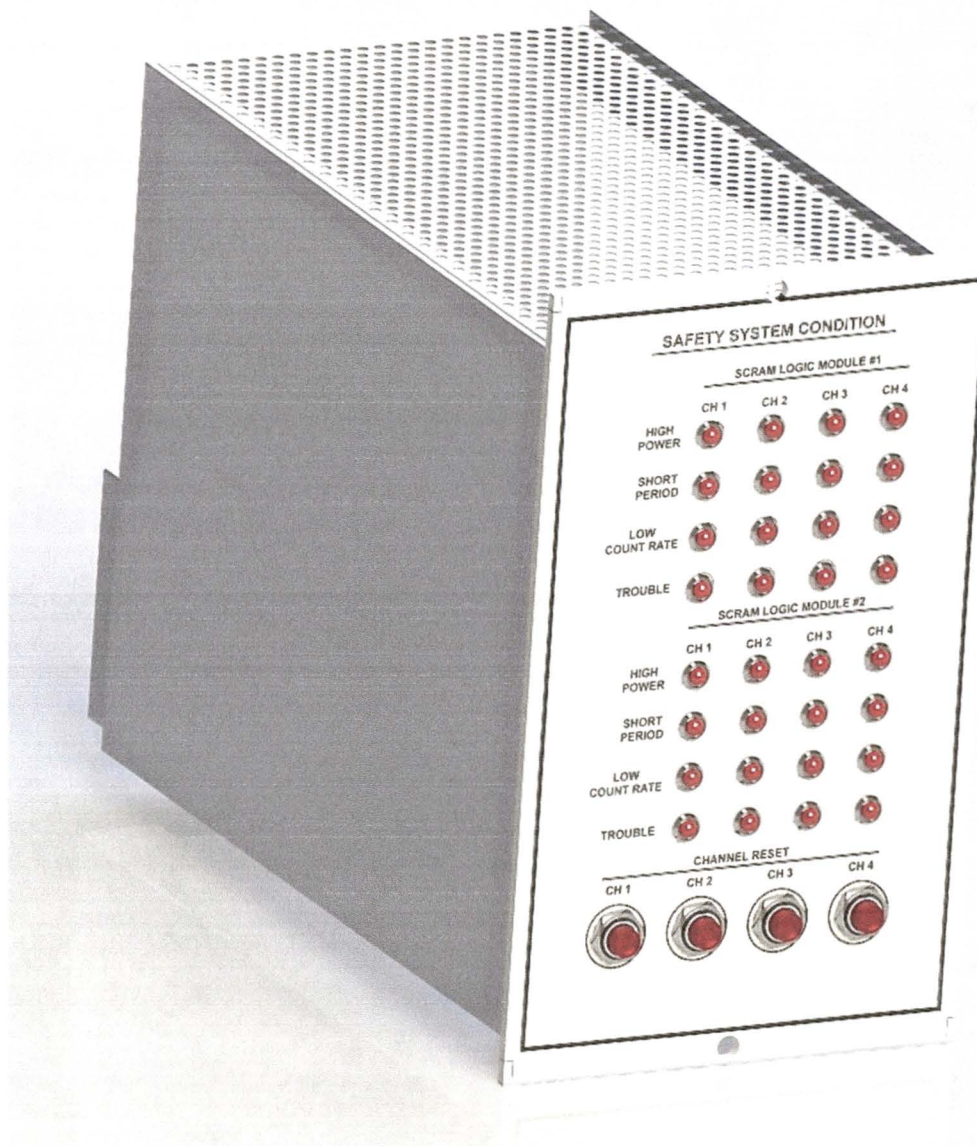


Figure 2 – 3-D Rendering of LED Scram Display Module

The High Power light represents one of two possible high reactor power conditions from the DWK 250 chassis – the [full power] High Power trip or the High Power 100 kW Operation trip – depending on which mode of operation is selected on the <100 kW Key-Switch Module (KSM). For instance, if <100 kW Operation is selected and reactor power reaches the <100 kW operation trip set point, then the DWK 250 chassis will output the High Power 100 kW Operation trip signal. The trip signal first arrives at the Scram Logic Cards, which then output the signal to the LED Scram Display module, illuminating the High Power trip light.

If just one of the four DWK 250 chassis outputs two or more trip signals, the two Scram Logic Cards receive the trip signals for logic comparison, but will not produce a scram signal. This will show up on the LED Scram Display as multiple lights lit up all in a single column, and no scram. However, if two or more of the DWK 250s produce trip signals, then the two-out-of-four voting logic designed into the Scram Logic Cards is satisfied, and the Scram Logic Cards will output a scram signal to shut down the reactor. This will show up on the LED Scram Display as multiple lights lit up in the same row, with a scram.

Therefore, the LED Scram Display provides a visual illustration for the console operator of the status of the Scram Logic Cards. It will be located on the control room console where it is easily visible by the console operator.

The LED Scram Display module contains reset buttons, one corresponding to each DWK 250 channel. The console operator needs to manually push the "Reset" button for the corresponding channel in order to clear the alarm for that channel latched in both of the Scram Logic Cards. The Reset buttons reset the Scram Logic Cards, and thus the lights on the LED Scram Display, particularly prior to restart of the reactor.

The LED Scram Display module and the Scram Logic Cards are composed of bi-stable, discrete components only, and therefore are not programmable and do not have a system clock or other timing function. Signal transmission between the LED Scram Display module and the Scram Logic Cards is via the Signal Distribution Module, which is functionally passive as covered in the Signal Distribution Module description. The Safety System Monitoring & Status Display PLC described below will register separately the date and time of alarms appearing on the LED Scram Display panel.

Description of the Safety System Monitoring & Status Display PLC

The Safety System Monitoring & Status Display PLC (a.k.a. "the PLC") operates independently of the LED Scram Display module. The main function of the PLC is to register and record the date and time when a trip signal is generated by any of the four DWK 250 chassis. In this way, the PLC provides indication of DWK 250 alarms, redundant with the LED Scram Display. The PLC is also equipped with a physical reset button that affects only the PLC itself.

Each DWK 250 chassis outputs to the Signal Distribution Module (SDM), where its trip signals will be routed to the Scram Logic Cards as well as independently to the PLC.

Each DWK 250 chassis can generate up to eight alarm conditions: High Power Trip, Short Period Trip, High Power 100 kW Operation Trip, Low Count Rate Trip, High Power Warning, Short Period Warning, Test Trip, and Fault / Equipment Malfunction Trip. The High Power Warning and the Short Period Warning do not warrant a reactor scram, and are routed to neither the LED Scram Display panel nor the Scram Logic Cards. However, all eight alarm conditions will reach the PLC by way of the SDM. The PLC will then display and record the names of all of these alarms that come in.

When the Withdraw Permit Circuit opens, the PLC will indicate it, based on a signal from the <100 kW Key-Switch Module (KSM). Additionally, the KSM outputs its key-switch position to the PLC. When the key-switch is set to <100 kW Operation, the High Power 100 kW Operation Trip, if generated, will reach the PLC and be displayed there. However, when the key-switch is on Full Power Operation, the PLC is programmed to ignore High Power 100 kW Operation Trip signals from the DWK 250 channels, and not display them.

The PLC generates three alarms on the control room's main annunciator panel: High Power Warning, Short Period Warning, and Trouble. An annunciator alarm of Trouble may include conditions of Low Count Rate, Test, or Fault / Equipment Malfunction. On the PLC, the console operator can see which one(s) it is. The PLC does not output any scram alarms to the annunciator panel; those come from the Scram Logic Cards via the KSM.

The PLC has a physical, common reset button to acknowledge and reset any alarms it registers. This reset button does not reset the alarms on the LED Scram Display nor the Scram Logic Cards. Furthermore, it does not by itself clear the alarms on the control room's main annunciator panel; to clear those, one must use the annunciator panel's own acknowledge and reset buttons as well.

The PLC has a built-in optical isolator on each of its signal input connections from the Signal Distribution Module. These ensure that the DWK 250 units are isolated from the PLC. Furthermore, the PLC is mechanically isolated by mechanical relays on its three outputs where it connects to the control room's main annunciator panel.

During the initial testing phase, the PLC panel will be installed in the control room but away from the main console. It will be moved near the main console for final installation. The PLC panel uses Secure Digital (SD) memory cards to store data.

Safety Evaluation

The LED Scram Display module is composed entirely of discrete components. It is a passive device that is used for visual indication only. Therefore, it is not subject to cybersecurity threats. It does not produce any scram signals, but does have the major secondary function of resetting the Scram Logic Cards. If the module fails, such as by physical damage or other disturbance, the LED indicator lights will not light, and the reset buttons may not function. In this case if the Scram Logic Cards produce a scram, there will be no means to reset the Cards, resulting in a conservative outcome. Furthermore, because the module is a passive device, it will not generate heat or produce interference in the Signal Distribution Module or other neighboring devices.

The PLC is optically isolated at its input from the SDM. It transmits only to the control room's main annunciator panel. Optical isolators built into the PLC's inputs will protect the DWK 250 units from being affected by any potential malware in the PLC's operating software. If this isolation fails, the PLC will be left completely disconnected from the SDM. In that case, none of the trip alarms generated by the DWK 250 units will reach or be registered by the PLC.

Likewise if the PLC itself fails, none of the trip alarms generated by the DWK 250 units will be registered there. Conditions of High Power Warning, Short Period Warning, or Trouble would not be output to the control room's main annunciator panel. In that case, high power warning capability would come from another existing neutron flux monitoring channel that is not part of the nuclear safety system. Furthermore, the DWK 250 chassis have their own indicator lights for these conditions. The existing nuclear safety system does not have any high power warning or short period warning functions. Therefore, the lack of these warning capabilities in the case of PLC failure or failure of its optical isolators will not degrade operational safety. Most importantly, since the PLC is not responsible for generation of any scram signals, its loss will not affect nuclear safety or reactor operation.

If the PLC fails, or one or more of its input optical isolators fail, a DWK 250 Trouble condition (Low Count Rate, Test, or Fault / Equipment Malfunction) will not reach the PLC, but will still light the relevant indicator(s) on the LED Scram Display. Trouble conditions from two or more DWK 250 units will still result in a scram output from the Scram Logic Cards, shutting down the reactor.

If malware corrupts the PLC, the PLC screen may provide or record inaccurate information, including the date and time, and the PLC may fail to output actual alarms, or may output any of its three annunciator alarms when they are not warranted. However, in all cases the console operator has other means in the control room to verify reactor conditions and the status of the nuclear safety channels. This failure mode of the PLC does not interfere with reactor scram functions and therefore has no impact on nuclear safety.

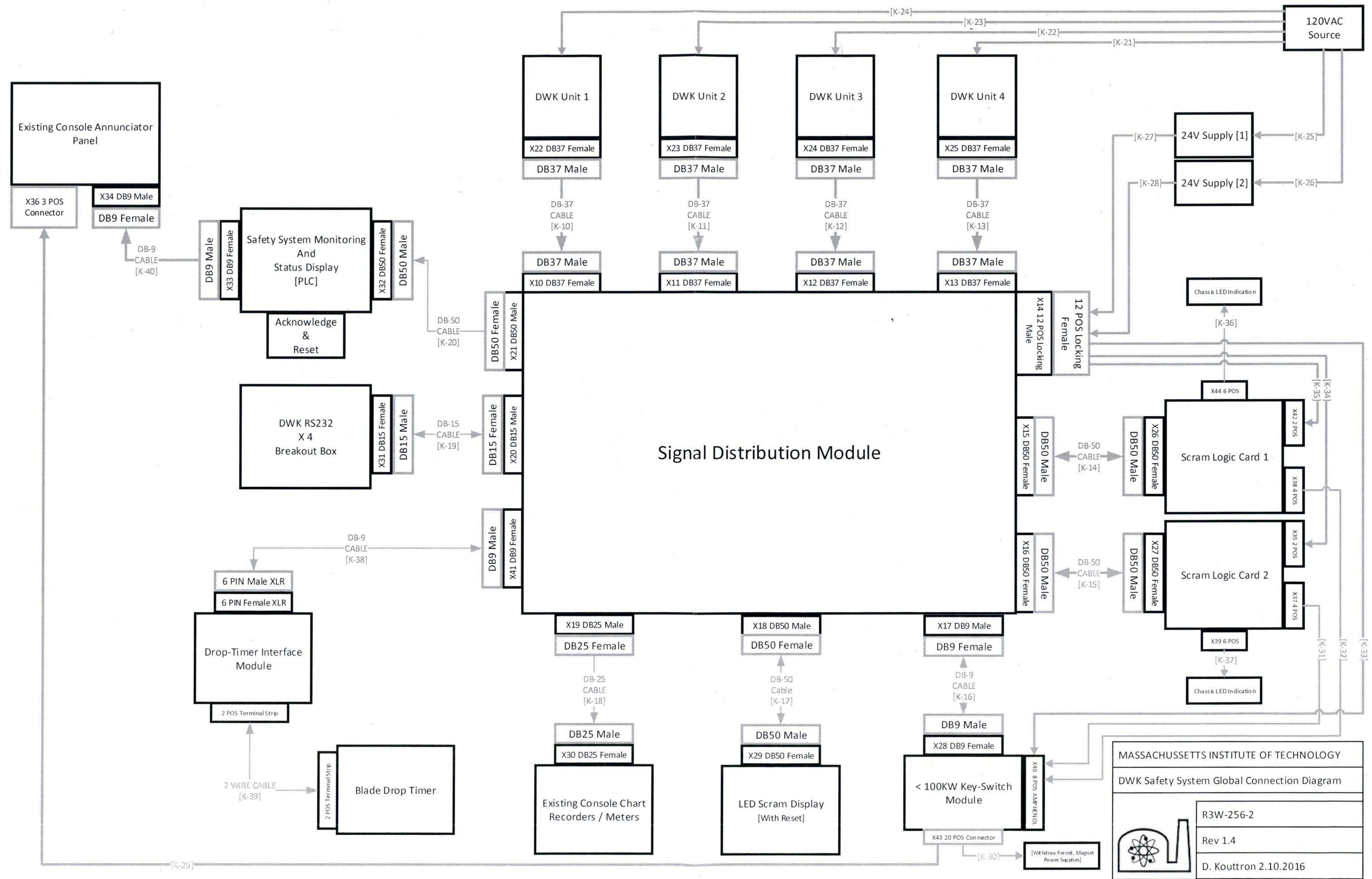
The PLC has network connection capability. However, there is no plan to place it on a public network, where it would have a higher probability of compromise by malware. The PLC writes its recorded data onto a Secure Digital (SD) card that has sufficient memory for the life of the equipment. In the case that the SD card will be removed for download, it will be used with a lab-specific secure computer.

The LED Scram Display module and the PLC module will be bench-assembled in a controlled environment. The new assemblies will then be connected to the rest of the new nuclear safety system while everything is de-energized. After that, the new system will be re-activated for testing. These modules will be constructed with standard industrially-rated components. They will be mounted on the control room console, which will provide them with physical defense, including against seismic disturbance. Routine maintenance and inspection will be performed only by licensed reactor staff or under the supervision of licensed reactor staff. Password protection will be used to secure the PLC logic. The control room is attended whenever the reactor is operating. At all other times, when the building is unoccupied, it is protected as per the Physical Security Plan. Therefore, access control and configuration control are assured.

The control room and its metal instrumentation cabinets are in an air-conditioned environment. The temperature is continuously maintained within a desirable setting (approximately 68 F). There is a temperature alarm (setpoint no higher than 78 F) that is monitored whenever the reactor is operating, or shut down with the control room attended. This air-conditioning control easily satisfies the operating requirements for all the components in the modules.

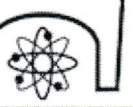
All cables to, and cable connection points on, the LED Scram Display module and the PLC module will be labeled. These markings improve the human interface for purposes of installation and maintenance. The arrangement of the LED Scram Display module's indicator lights and reset buttons are easy to see and use. The PLC's display screen conforms to modern industrial display standards. Therefore, human factors engineering is adequate.

The LED Scram Display module and the PLC module will be tested for wiring verification, including the proper level of illumination of LED lights and PLC display screen, using a written procedure prior to first use. There will also be periodic operational checks. Therefore, the pre-operational and routine surveillances are sufficient to assure the completeness and integrity of these modules.



MASSACHUSETTS INSTITUTE OF TECHNOLOGY

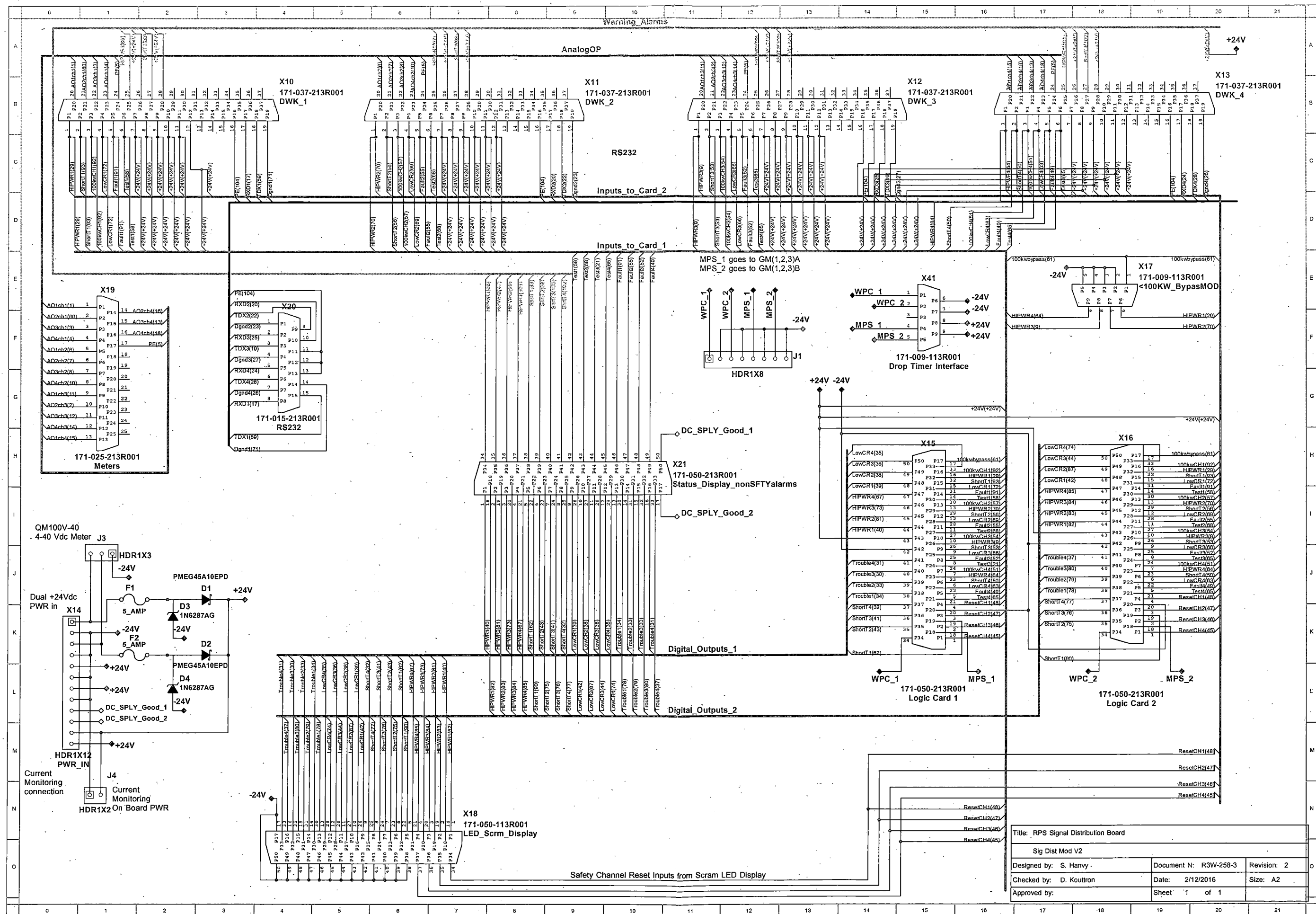
DWK Safety System Global Connection Diagram

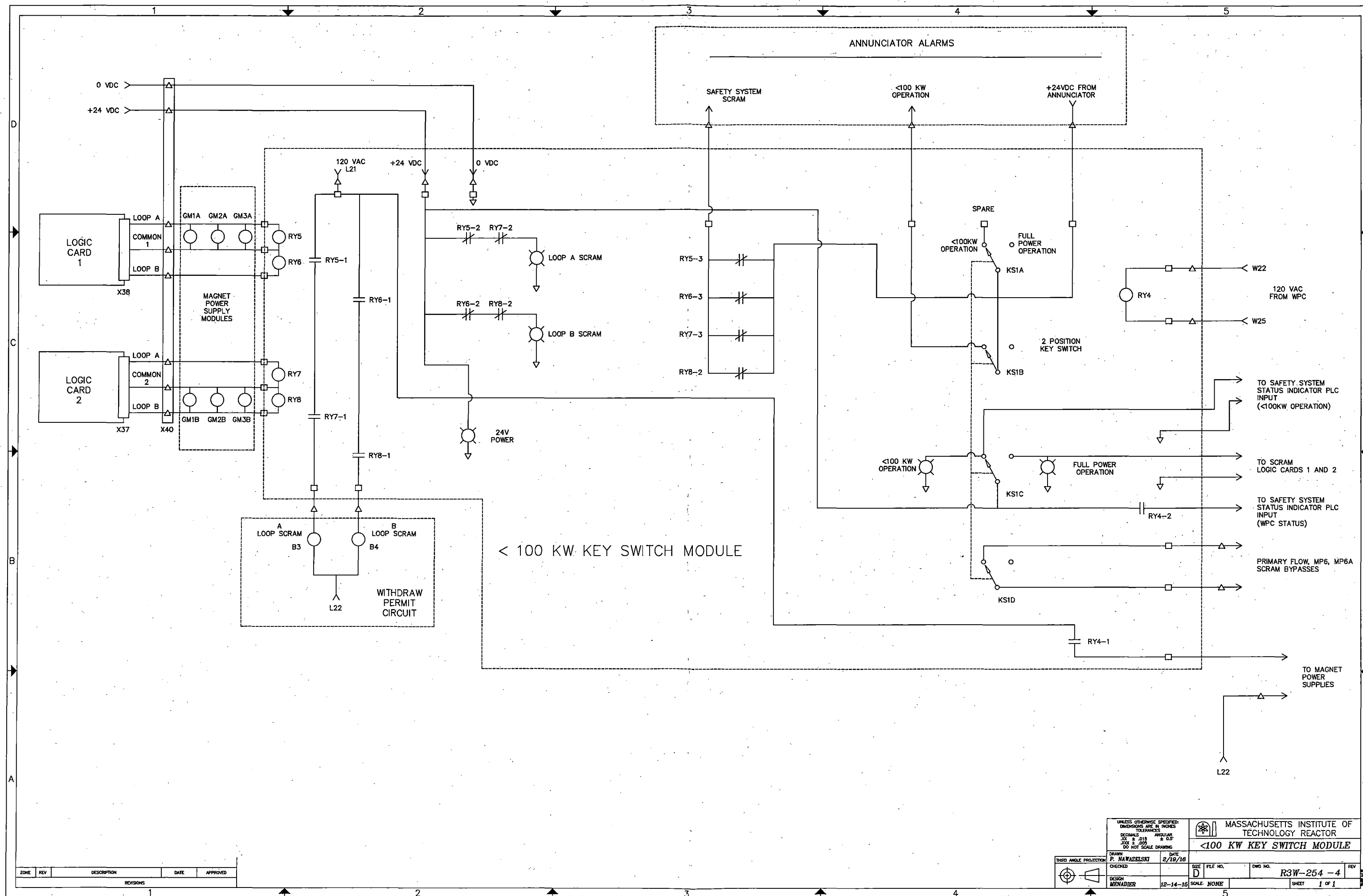


R3W-256-2

Rev 1.4

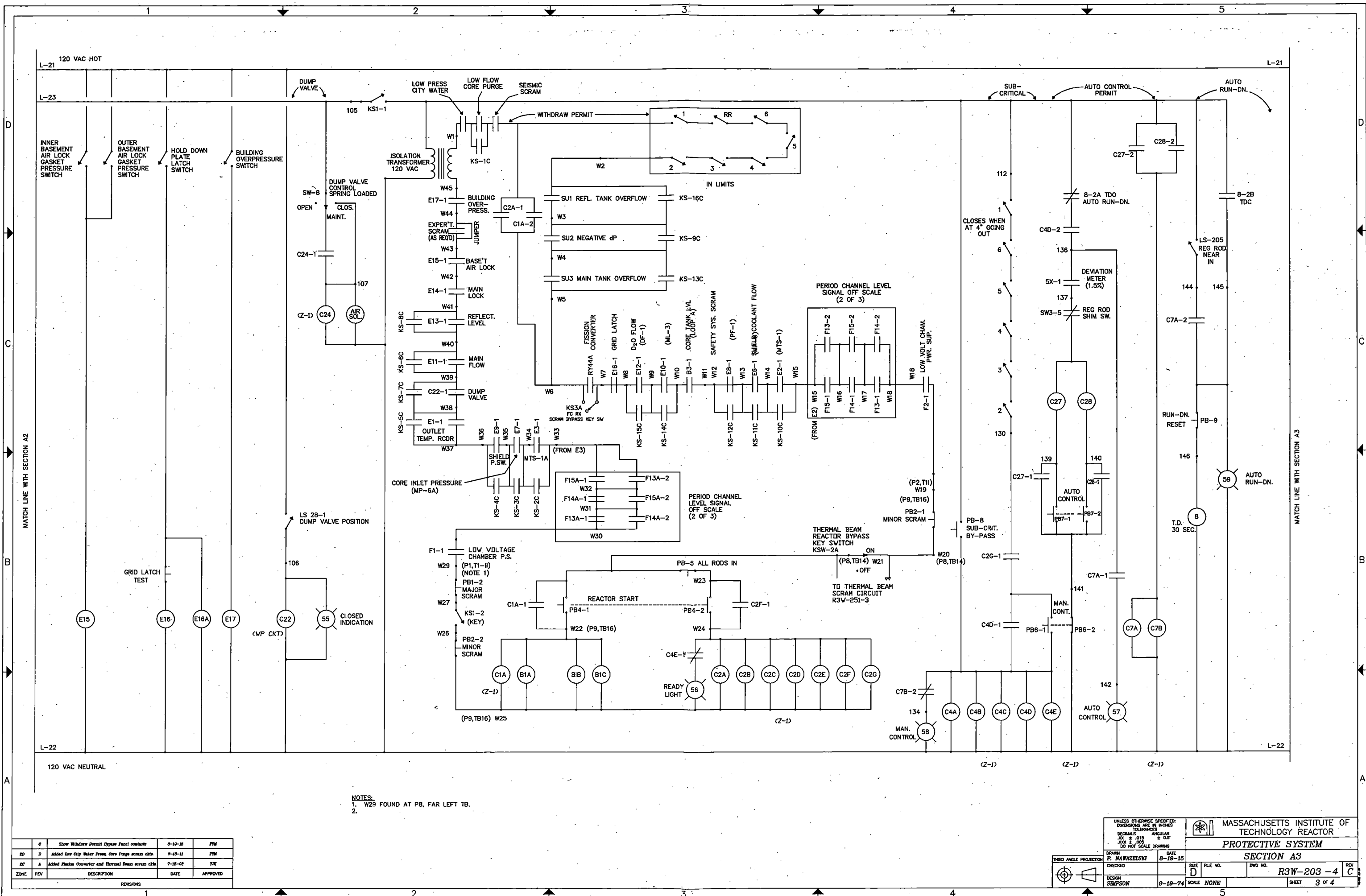
D. Kouttron 2.10.2016





ZONE	REV	DESCRIPTION	DATE	APPROVED
1				

THIRD ANGLE PROJECTION		UNLESS OTHERWISE SPECIFIED: DIMENSIONS ARE IN INCHES TOLERANCES DECIMALS .XX ± .015 ANGLES .005 ± .005 DO NOT SCALE DRAWING		MASSACHUSETTS INSTITUTE OF TECHNOLOGY REACTOR	
DRAWN P. MAWAZELSKI	DATE 2/19/18	CHECKED	SCALE NONE	FILE NO. D	DWG NO. R3W-254-4
DESIGN MENADIER	12-14-15				SHEET 1 of 1



NOTES:
 1. W29 FOUND AT PB, FAR LEFT TB.
 2.

REV	DESCRIPTION	DATE	APPROVED
1	Added Low City Water Press, Core Purge across chn.	7-10-74	PTM
2	Added Fission Converter and Thermal Beam across chn.	7-10-74	PTM
3	Added Fission Converter and Thermal Beam across chn.	7-10-74	PTM

UNLESS OTHERWISE SPECIFIED: DIMENSIONS ARE IN INCHES TOLERANCES DECIMALS .015 ANGLES .005 DO NOT SCALE DRAWING		MASSACHUSETTS INSTITUTE OF TECHNOLOGY	
SECTION A3		R3W-203-4	
DATE 8-19-74	FILE NO. D	SCALE NONE	SHEET 3 of 4

