PERSONNEL AND MACHINE PROTECTION SYSTEMS IN THE NATIONAL IGNITION FACILITY (NIF) *

R. Reed, J. Bell, G. Lau, C. Karlsen, S. Montelongo, J. Rouse, J. Wheeler, B. Loll, A. Thakur,
LLNL, Livermore, CA 94550, USA

Abstract

The National Ignition Facility (NIF) is the world's largest and most energetic laser system and has the potential to generate significant levels of ionizing radiation. The NIF employs real time safety systems to monitor and mitigate the potential hazards presented by the facility. The Machine Safety System (MSS) monitors key components in the facility to allow operations while also protecting against configurations that could damage equipment. The NIF Safety Interlock System (SIS) monitors for oxygen deficiency, radiological alarms, and controls access to the facility preventing exposure to laser light and radiation. Together the SIS and MSS control permissives to the hazard generating equipment and annunciate hazard levels in the facility. To do this reliably and safely, the SIS and MSS have been designed as fail safe systems with a proven performance record now spanning over 12 years. This presentation discusses the SIS and MSS, design, implementation, operator interfaces, validation/verification, and the hazard mitigation approaches employed in the NIF. A brief discussion of common failures encountered in the design of safety systems and how to avoid them will be presented.

NIF OVERVIEW

The National Ignition Facility (NIF) is the world's largest and most energetic laser system. The NIF laser consists of 192 laser beams which are housed in a ten story building the size of three football fields at the Lawrence Livermore National Laboratory (LLNL). NIF can deliver up to 1.8 million Joules and 500 Terawatts of ultraviolet laser light on to mm-sized targets centered in the ten-meter-diameter target chamber. Experiments using NIF's 192 laser beams are making significant contributions to national security, fusion energy, and basic science. During these experiments significant radiation fields can be generated within the Target Bay, along with potential laser light, high voltage hazards, and explosion hazards in various areas of the facility all presenting a hazard to personnel in the affected areas. If not properly configured the laser can also be a hazard to itself if back reflections propagate off of improperly positioned equipment causing damage to laser components.

* LLNL-CONF-644612. This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. #LLNL-ABS-631632

SAFETY SYSTEMS OVERVIEW

In order to mitigate the potential hazards presented to personnel, NIF uses a distributed Safety Interlock System (SIS) and a separate Access Control System that functions in conjunction with the facility SIS to control access into the facility. The purpose of the NIF facility Safety Interlock System (SIS) is twofold: 1) to work in conjunction with administratively controlled procedures to protect personnel from exposure to high-voltage, laser light, radiation, asphyxiation, and other hazards, and 2) where feasible, to minimize or eliminate equipment damage in the event of a failure in a monitored component in the NIF. The NIF ACS is a commercially available Access Control System which employs an on line database configured to identify personnel qualified to enter the facility and to track their location within the major operational areas of the NIF.

The facility SIS provides permissive signals for the operation of process power supplies, alignment lasers and other devices necessary to perform target shots. It monitors the status of safety related elements in each area of the facility, including shutters, doors, crash buttons, sweep status, oxygen levels, radiation alarms, etc. The SIS does not control any process devices, but simply provides a permissive signal for each device interlocked by the system. If the interlock logic chain for a device is not satisfied, the permissive signal will not be enabled, operation of the device will not be permitted, and it will stay in its fail-safe state or position. If the interlock logic chain for a device is satisfied, the permissive signal will be enabled, and operation of the device will be allowed. The actual operating state of the device is determined by the process control system within the constraints imposed by the SIS.

SIS functionality is distributed along the boundaries of NIF subsystems as appropriate. This allows SIS's to be handled in smaller more manageable units to simplify their management including validation and verification. Each of the distributed SIS's communicates key status to the facility SIS. The facility SIS manages facility wide alarms and paging functions to alert key personnel to system alarms. A simplified view of the SIS architecture is shown in Fig. 1.

Similar to the SIS, a Machine Safety System (MSS) is employed to mitigate possible damage to critical facility components that could be caused by shots when the facility is not configured properly for a system shot. As an example such damage could be caused by a back reflected laser beam from the target shroud which failed

ISBN 978-3-95450-139-7

to open at shot time. Such devices are monitored by the MSS which passes a permissive to the SIS or other systems preventing shots unless the system is configured properly.

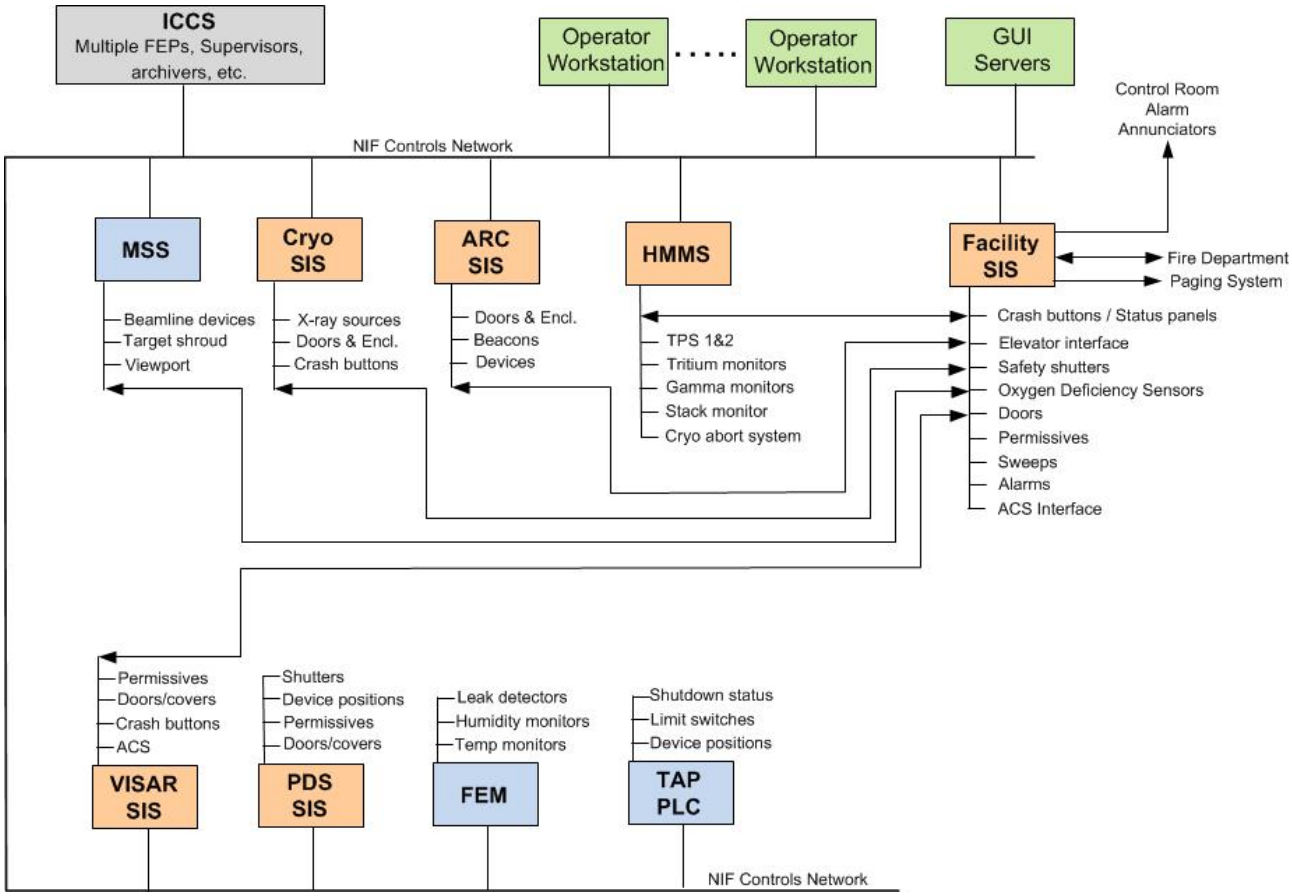

Figure 1: Simplified architecture of the NIF MSS/SIS.

SAFETY SYSTEMS STATUS

During the past two years, the NIF SIS has been expanded to support high yield shot operations, and to support a variety of new diagnostic systems including the Advanced Radiographic Capability (ARC) [1]. The SIS was modified to support three shot modes for shots to the Target Bay. Shot Category A is defined as no or low yield ($<10^{14}$ neutrons). Shot Category B is defined as moderate yield ($>10^{14}$ and $<=10^{16}$ neutrons). Shot Category C is defined as high yield ($>10^{16}$ neutrons). Depending on the shot mode, SIS requires various combinations of shield doors to be closed and various areas of the facility to be swept.

The SIS monitors 19 primary shield doors for the Target Bay that are required to be closed for category B shots. It also monitors 27 additional secondary shield doors for the switchyards that are required to be closed in addition to the primary doors for category C shots. For each shield door the SIS monitors the closed position of the door and the engaged position of the seismic pin. For a valid closed signal SIS must see both (redundant) position switches indicating closed and the seismic pin switch indicating that the seismic pin is in the engaged position. Additionally, the SIS provides a permissive to each shield door allowing it to be operated.

Another capability implemented to support category C shots is the SIS Access Key Stations (AKS). The AKS are used in the entry process for the Target Bay prior to and after category C shots. The AKS contain tokens that are checked out by an operator prior to gaining access to the Target Bay. The AKS maintains an on-line database that may be queried by the control room operator to determine how many tokens are checked out and who has them. The AKS also furnishes a signal to the SIS that is true when all AKS tokens are present. The SIS uses this signal in its permissive generation logic to prohibit permissives unless all AKS tokens are present.

Prior to engaging in category C shots several additional protocols are followed for gaining access to the Target Bay. This is to further reduce the likelihood that someone could be accidently left in the Target Bay during a high yield shot when the consequences are much greater. At least seven hours prior to a category C shot the Target

ISBN 978-3-95450-139-7

Bay is placed into "Restricted Mode". In this mode the SIS Target Bay entry panels are backlit in yellow and indicate that the bay is in Restricted Mode. To gain access while the Target Bay is in Restricted Mode an entrant must:

1. Call the control room from the door which they desire entry
2. The control room operator observes the entrant on the entry surveillance monitor
3. The control room operator verifies each entrant has an Access Key Station token
4. The control room operator verifies each entrant has a valid Rad Work Permit (RWP)
5. The control room operator buzzes the entrant(s) in through the selected door
6. The control room operator verifies that each entrant scans their ACS badge and that they are entered into the ACS transaction log
7. The control room operator verifies that no one tailgates into the Target Bay with the entrant(s)
8. The control room operator verifies that the Target Bay door closes after the entry

After a category C shot, a re-entry procedure for the Target Bay is executed. This procedure includes testing of all the SIS devices in the Target Bay that may be susceptible to damage by radiation in order to ensure that they remain operational prior to releasing the Target Bay for general access.

The newly commissioned ARC SIS (see Fig. 1) implements the ARC laser SIS functions. These include device position monitoring, door positions, diagnostic enclosure monitoring, warning beacon control, ARC laser source permissives, and communication of ARC SIS status to the facility SIS.

FACILITY SIS

The facility SIS is a distributed Programmable Logic Controller (PLC) based system. It consists of four PLCs, one controlling interlocks for Laser Bay #1, Switchyard #1, and Capacitor Bays #1 & #2. The second controls interlock functions for Laser Bay #2, Switchyard #2, and Capacitor Bays #3 & #4. The third controls interlocks for the Target Bay. The fourth "Master" PLC coordinates activities of the other three, performs additional error checking, controls the digitized voice warning system, interfaces oxygen alarms to the Fire Alarm Control Panel, and handles interlocks for the balance of the facility.

A critical function of the facility SIS is to implement the sweep functions for operational areas of the facility and to monitor the perimeter of those areas. Engineered sweeps controlled by the SIS require personnel to physically enter an area to ensure that a sweep of the area has been conducted and that it is unoccupied. This requires a sweep team to traverse the area being swept in a predefined pattern actuating the sweep key-switch in each status panel in an area. Completion of the required actions, in the specified sequence and allotted time, is required prior to issuing permissives for potential hazard generating operations.

The facility SIS enforces engineered perimeter control for operational areas of the facility that are subject to sweep. Once the sweep perimeter is established, the system provides an alarm indication in the control room if the perimeter has been violated, and drops any associated permissives. Areas of the facility subject to sweeps (depending on shot mode and configuration) include:

1. Capacitor bays (4 each)
2. Laser bays (2 each)
3. Switchyards (2 each)
4. Target bay (7 levels)
5. Diagnostic mezzanines (4 each)
6. LB1 Viewing gallery
7. Level 3 and level 5 Target Bay mechanical equipment rooms
8. Core elevator vestibules (2 each)
9. NEL lobby

CRYO SIS

The Cryo SIS is based on the same architecture as used by the facility SIS. It communicates safety status to/from the facility SIS via a set of defined hardware communication bits. It handles safety functions related to the Cryogenic Target Positioner (CTP). This includes monitoring x-ray shielding components, camera tray position, vessel door monitoring, glovebox monitoring, local crash button monitoring, and x-ray source permissive generation to support radiography of the cryogenic targets.

HAZARDOUS MATERIALS MANAGEMENT SYSTEM (HMMS)

The HMMS also shares a common architecture with the facility SIS. HMMS implements the facility tritium monitors (22 ea.), gamma detectors (10 each), the facility stack monitor, the cryo abort volume, and the tritium processing system.

The function of the Tritium and Gamma Area Monitoring System is to provide warning/information to operations personnel about potential radiation exposure by monitoring tritium concentrations and gamma dose rate levels and alarming when the concentration and/or dose rates exceed a predetermined setpoint. Once an alarm setpoint is tripped the alarm is sent to the facility SIS for annunciation. Tritium monitors are used to monitor rooms and enclosures where workers could be exposed. Gamma monitors provide real time gamma area radiation monitoring. The HMMA HVAC Monitoring System ensures that the Target Bay is held at a lower pressure than the surrounding areas to minimize particulate radiation in the surrounding areas. The cryo abort volume is a set of three tanks maintained at rough vacuum designed to contain the effluent of the target chamber cryogenic pumps during an off normal condition such as a power failure or control system failure. The tritium processing system is a subset of the HMMS. NIF

ISBN 978-3-95450-139-7

uses two parallel tritium processing systems each based on its own PLC.

The purposes of the NIF Tritium Processing System (TPS) are to:

- Process the effluent from the vacuum pumps in the target area vacuum system and glove boxes in the HMMA.
- Catalyze tritium from residual gases and convert to tritiated water, including the case of tritiated methane.
- Transfer tritium onto a removable dryer bed that can be processed as radwaste.

TPS uses the well-established recovery process involving catalytic oxidation of the tritiated effluent with the resultant water species collected on molecular sieve beds. The Tritium Processing System (TPS) is a tritium gas recovery system with two parallel absorption trains used to remove tritium from air evacuated from the NIF target chamber and other affected volumes.

MACHINE SAFETY SYSTEM (MSS)

The MSS is also implemented on a distributed PLC platform. The MSS handles only machine safety and does not implement any personnel safety functions. Its primary purpose is to prevent damage to hardware and laser system components due to detected failures or incorrect system configurations. The MSS monitors the position of the cryo target shroud and stops the shot if the shroud does not reach the fully open position during the last 5 seconds prior to the system shot. It monitors various beamline devices including the fiducial arm, phase plate, and rubble plate positions in each of NIF's 192 beamlines. The MSS passes permissive information to the facility SIS which grants or withdraws system shot permissives accordingly.

VALIDATION AND VERIFICATION (V&V)

NIF maintains an independent V&V organization that is chartered to conduct V&V activities on high quality level systems within NIF such as the SIS's and selected MSS's. Systems are tested periodically per their Configured Systems Maintenance Plans (typically semi-annually). The periodic tests emphasize exercising the field hardware to locate covert faults while regression testing concentrates on logic testing and is executed when the logic in a system is revised. Test results are reviewed and accepted by the SIS manager and the NIF Operations Manager.

CONCLUSION

The NIF SIS is designed as a fail-safe shutdown system. When a failure is detected, permissives are removed and operations requiring those permissives are halted until the issue has been corrected. SIS incorporates redundancy through key components of the system. Doors (shield doors and personnel doors) are monitored with redundant switch pairs. Crash buttons incorporate two sets of contacts that function redundantly. SIS incorporates redundant 24Vdc power supplies supporting its field devices. Critical SIS devices are powered by Uninterruptable Power Supplies (UPS) backed by a standby generator which allows the system to remain operational in the event of an extended power failure. The SIS uses diagnostic input/output modules on critical points to allow for additional error checking such as open circuit detection.

An extensive Failure Modes and Effects Analysis (FMEA) has been conducted to search out single points of failure that required mitigation. This analysis is updated when changes are made to the SIS and has been used to guide the SIS design.

An extensive Fault Tree Analysis (FTA) was conducted to confirm that the probability of someone being left behind in any of the operational areas was at an acceptable level, and to ascertain if additional controls were required.

The NIF SIS and related systems are subject to strict configuration management and are tested regularly in order to reveal covert faults. Regression tests are executed when programming changes are made on the systems.

SIS/MSS provides comprehensive operator interfaces consisting of facility overviews, operator help screens, alarm screens, troubleshooting aids, trending and archiving of selected data. Self-help screens provided to the operators have proved to be invaluable as they allow operations personnel to do much of their own troubleshooting and question resolution.

The NIF SIS/MSS has been in operation for over 11 years, operating 24/7/365. Its technology is proven with a large installed base worldwide. The system has been optimized for operations over its lifetime and continues to be optimized to support NIF operations. The system has reached a mature level with minor changes occurring a couple times a year. The system has been reviewed by both internal and external reviewers. Analysis has confirmed that it is a fail-safe system and that the probability of someone being injured due to being in a swept area is at an acceptable level.

During its lifetime the fail-safe response has been as designed. The systems are under strict configuration management and are tested regularly. The system is in place and is ready to support high yield experiments at the National Ignition Facility.

REFERENCES

[1] G. Brunton et al., "The Advanced Radiographic Capability, a Major Upgrade of the Computer Controls for the National Ignition Facility," MOCOBAB04, ICALEPCS'13, San Francisco, CA, USA, Oct. 2013, to be published.

ISBN 978-3-95450-139-7