LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-415541

Ultra Safe and Secure Blasting System

Mark M. Hart

July 27, 2009

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

CONTENTS

EXECUTIVE SUMMARY

The Ultra is a blasting system that is designed for special applications where the risk and consequences of unauthorized demolition or blasting are so great that the use of an extraordinarily safe and secure blasting system is justified. Such a blasting system would be connected and logically welded together through digital code-linking as part of the blasting system set-up and initialization process. The Ultra's security is so robust that it will defeat the people who designed and built the components in any attempt at unauthorized detonation. Anyone attempting to gain unauthorized control of the system by substituting components or tapping into communications lines will be thwarted in their inability to provide encrypted authentication. Authentication occurs through the use of codes that are generated by the system during initialization code-linking and the codes remain unknown to anyone, including the authorized operator. Once code-linked, a closed system has been created. The system requires all components connected as they were during initialization as well as a unique code entered by the operator for function and blasting.

INTRODUCTION

Current blasting systems typically employ safety fuzes crimped into blasting caps, electrical initiation of blasting caps, shock tube initiation of blasting caps, or detonating cord running to a booster to initiate the blasting charges. While this is an economical blasting design, any individual can connect their own fireset to electric blasting caps, initiator to shock tubes, or blasting cap to detonating cord to initiate the explosive charges. The only means of protecting this type of blasting system from unauthorized or accidental detonation is by controlling access to that system. Some blasting systems are widely distributed over terrain or distributed throughout structures. A determined malevolent individual can effectively work to gain access and bring about unauthorized detonation of part or all of the blasting system. This is particularly important in a large blasting system where the set-up is staged over time. The Ultra Blasting System would allow staged placement of charges and detonators without risk of accidental or unauthorized firing of the detonators on the pre-positioned explosive charges. It also permits secure placement of explosive charges over extended periods of time. A partially or completely disconnected Ultra system is designed to prohibit initiation of any detonator. With the Ultra System, authorized detonation can only occur following complete assembly of the Ultra and command code entry by the authorized operator.

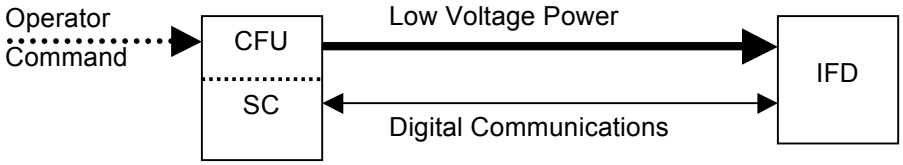
The following is a brief tutorial describing the design and function of the Ultra.

ULTRA SYSTEM ARCHITECTURE AND GENERAL FUNCTION

For purposes of illustration the Ultra Safe and Secure Blasting System architecture will be described using one detonator. It will be readily apparent how the system can fan out to accommodate an unlimited number of detonators. All components, including the integrated fireset detonator, have on-board intelligence that is necessary for code-linking and ultimate function under authorized control. The Ultra one-detonator system would consist of two major components listed below:

- Command Fire Unit & System Controller (CFU/SC)
- Integrated Fireset Detonator (IFD)

The CFU can be connected to the IFD to provide low voltage power. The SC is an integral part of the CFU and communicates with the IFD by copper wire, fiber optic line, or radio signal. When radio communications are used, the IFD can be powered by a long-life internal battery for improved flexibility and simplicity in its placement. The IFD can be viewed as a very intelligent blasting cap. The IFD is integrated in that it contains a microprocessor with a communications interface, fireset, slapper bridge circuit, pressed PETN initiator, and appropriate booster. The fireset is a miniature capacitor discharge unit (MCDU) that consists of a low to high voltage charging circuit, miniature storage capacitor, and trigger circuit. The slapper Kapton-copper bridge circuit is burst by the capacitor discharge through the high voltage trigger circuit. The small Kapton flyer impacts the pressed PETN pellet. The PETN pellet runs to detonation, sending an aluminum flyer into the booster that initiates the main charge high explosive. All the above can be mounted on a single integrated circuit or multi-chip module (MCM).



In the example configuration, the CFU provides low voltage to the SC and IFD for powering internal logic, communications, and the integrated fireset on the IFD. The SC communicates with the IFD, designating an encryption key and generating authentication codes. The detonator is connected with low voltage power and digital communications provided by the CFU/SC. The operator commands the SC to initialize the system through the CFU. As part of this process, the SC randomly generates a pointer for an encryption key stored in a firmware register on the SC and IFD. Encrypted communications are established and the SC randomly generates two authentication codes. One is the authentication code for the SC, the other is an authentication

code for the IFD. The encryption key pointer and two authentication codes are stored in non-volatile memory on the SC and the IFD. Once this is accomplished, the SC and IFD take on a parent-child relationship. The SC parent "owns" the IFD children and the IFD child will only communicate with its parent. The CFU/SC can be powered down and disconnected from the IFD with the IFD remaining immune to any attempt at unauthorized detonator initiation.

When ready for blasting operations the CFU/SC is reconnected to the IFD and/or powered up if it remained connected. As the system is powered, the SC executes firmware re-establishing encrypted communications with the IFD. The IFD first receives and verifies the SC's authentication code and then sends its authentication code to the SC for verification. If the authentication codes are not verified, the IFD ceases logic operation and the detonator will not fire. Once the authentication codes are verified, the IFD is under control of the CFU/SC. During the following processes, the IFD and SC are communicating with each other, frequently challenging and re-verifying each other's authentication code. The arm command is input by the authorized operator. The SC passes instructions to the IFD to charge its integrated fireset. The operator takes the safety off. The SC passes instructions to the IFD to move a mechanical shutter out of line with the firing train. The operator presses the fire button and the SC provides a digital command for the integrated fireset to fire, initiating detonation.

COMPONENT FUNCTION DETAIL

Command Firing Unit

The CFU provides operator interface and low voltage power to the IFD fireset and internal microprocessor. The battery powered CFU accepts a code input by the operator verifying authorized commands. In the absence of that code, the CFU will not function with effect. Once the correct operator code is entered, the Ultra blasting system can be armed with switch function on the CFU. Following confirmation of arming, the Ultra system is taken off-safe with switch input on the CFU. Following confirmation of off-safe, the system will detonate with switch input on the CFU.

System Controller Initialization

The SC provides the digital command interface and communications between the CFU operator input and the IFD. The SC consists of a digital microprocessor containing firmware instructions and algorithms, encryption key list registers, and non-volatile memory. When connected to the IFD and powered, the SC establishes open communications with IFD. Once communications have been established, the SC randomly selects a pointer to the key list in firmware and transmits that pointer value to the IFD. The IFD selects the key by the pointer register value and encrypted communications are established between the SC and IFD. The encryption flag is set in both the SC and IFD. The SC then passes its authentication code and the IFD's authentication code to

the IFD. The IFD stores these encrypted authentication codes in non-volatile memory. The SC and IFD set their code-linked flags. At this point the SC and IFD are logically welded together as a closed system, taking on a parent-child relationship.

System Controller Operation

Once the Ultra is initialized and code-linked the system controller verifies system integrity prior to blasting operations. With power-up the SC establishes open communications with the IFD. Once communications have been established the SC verifies initialization by checking the encryption and code-linked flags on the IFD. The SC and IFD establish encrypted communications by selecting their encryption keys using the key register pointer value stored in non-volatile memory. The SC transmits its encrypted authentication code to the IFD. The IFD verifies the correct SC authentication code and then transmits its encrypted authentication code to the SC. With verification of the IFD authentication code in the SC, the system is ready to take operator commands leading to detonation or unlinking the system.

Integrated Fireset Detonator

The IFD fireset converts low voltage supply to high voltage stored in a miniature capacitor discharge unit (MCDU). The initiation train consists of a slapper flyer, mechanical safety link, PETN pellet initiator, and booster. The detonator is manufactured with the mechanical safety link interfering with the initiation train and the microprocessor incapable of accepting instructions to fire the initiation train except from its parent CFU/SC and only after code-linking initialization and authentication code verification.

The IFD microprocessor contains firmware instructions, encryption key list, and non-volatile memory. The CFU or internal battery provides power to the IFD. The SC provides communications to the IFD. The IFD responds to a sub-communications “tickle” from the SC by announcing its presence on the SC network and transmitting its flag status. The SC acknowledges the presence of the IFD and begins communications. During initialization the SC transmits the encryption key pointer. The IFD stores the pointer value in non-volatile memory, reads the designated key from a firmware register and begins encrypted communications with the SC. With this action, a flag is set indicating configuration for encrypted communications.

Initialization code-linking proceeds as the SC transmits encrypted authentication codes for itself and the IFD. The IFD stores these values in non-volatile memory. With this action, a flag is set indicating initialization code-linking. Following this action, the IFD is code-linked to the SC and takes on the child-parent relationship. In any following operation, the IFD will verify the SC’s encrypted authentication code and then transmit its encrypted authentication code to the SC. Once the SC verifies the IFD’s authentication code the SC can communicate encrypted arming, off-safe, and firing instructions to the IFD. In summary, this is a fail-safe blasting system. It will

not function with detonation unless it exists in the configuration that was originally initialized and code-linked.

When the IFD receives the encrypted arming instruction, it enables the oscillator in the charging circuit to convert low voltage direct current provided by the CFU, to high voltage for charging the miniature capacitor discharge unit (MCDU). When the SC transmits the encrypted off-safe command, the IFD moves the mechanical safety link out of line in the initiation train. When the SC transmits the encrypted firing signal, the IFD fires the MCDU, bursting the slapper bridge and in turn firing the initiator and booster.

METHODOLOGY

Encryption Protocol

Identical encryption algorithms are located in firmware on the SC and IFD microprocessor. The encryption keys are located in identical firmware registers on the SC and IFD microprocessors. Flag registers are located in non-volatile memory. As part of initialization and setting up encrypted communications, the SC randomly generates a register pointer. This points to the register location both on the SC and IFD microprocessor that contains the key that will be employed in encryption. The register pointer is transmitted to all IFDs and stored in their non-volatile memory. The key itself is not transmitted. The encryption algorithm on the SC and all IFDs use the same selected key. Both the SC and IFD microprocessors set their encryption flags as they begin encrypted communications.

Initialization And Code-Linking Protocol

Three steps are involved in code-linking.

1) The SC initiates a sub-communications “tickle” with all IFDs recording their presence on the network and their flag status regarding encryption and initialization.

2) The SC begins open communications with all IFDs, and then establishes encrypted communications with all IFDs.

3) The SC randomly generates its authentication code and all of the authentication codes for the individual IFDs. The authentication codes are transmitted to each IFD where they are stored in non-volatile memory. The code-linked flag is set in the SC and IFD on non-volatile memory. Thereafter, and only following mutual verification of authentication codes by the SC and IFD, instructions can be transmitted by the SC and acted on by the IFD.

With the completion of initialization and code-linking, the blasting system has become a closed system that is logically welded together. Disconnecting any IFD or exchanging an initialized IFD with another IFD will prohibit the blasting system from functioning. The system will not function when an initialized CFU/SC is replaced with another CFU/SC.

Random Authentication Challenges

Both the SC and IFD will transmit challenges to each other at frequent and random intervals to verify that there has been no substitution or replacement of these components. When a random challenge is verified, communications and control continues. If the transmitted authentication code is not verified, function ends and detonation cannot take place.

Unlink and Dissever Protocol

In the event it is desired to dismantle the code-linked Ultra Blasting System, the SC and IFDs can be returned to the as-manufactured state and used in a new set-up. When the code-linked Ultra is powered it checks flag status, establishes encrypted communications using the key register pointer stored in non-volatile memory, and verifies authentication codes. The IFDs can now receive and act on commands. The dissever command is input through the CFU by the operator. The SC acts on this command by instructing the IFD's to erase the encryption key pointer and authentication codes from non-volatile memory and to reset all flags. The SC erases its encryption pointer and authentication codes from its non-volatile memory and resets all flags. The system is now unlinked. The system has been logically dissevered and has been returned to the as-manufactured state. It can now be dismantled and reused in whole or in part at a later time in a new blasting system set-up. These parts can be mixed and matched with other SCs and IFDs. This new system will be initialized and code-linked into a new code-linked, logically welded, closed blasting system. Dismantling a code-linked blasting system without first unlinking, yields a collection of unusable detonators and a useless system controller.

You-First Protocol

If encrypted communications were not used between the SC and the IFDs, the you-first protocol would be used by the IFDs. The IFD will wait for and validate the authentication code from the SC before transmitting the IFD authentication code to the SC. This practice reduces the ability of a substituted SC gaining control over the IFD.

System Function Check

The Ultra blasting system, once initialized and code-linked can be field checked at any time to verify all components are functional. The operator momentarily closes a normally open switch on the CFU. This pulls an optically isolated input line on the SC microprocessor low, instructing it to run a system function check. The SC microprocessor verifies encrypted communications and valid authentication codes with all IFDs and responds by illuminating a green LED. Failure to verify encrypted communications and authentication codes would cause it to illuminate a red LED signifying that the Ultra blasting system will not function with detonation. If the red LED is illuminated following a full system function check, a diagnostic laptop can be connected to the SC

to determine the nature and cause of system failure. The laptop will provide a display interface for identifying components needing replacement.

If the system is designed with a common clock originating at the SC, the actual firing timing of all IFDs whether simultaneous or sequential, can be rehearsed and confirmed to within a fraction of a microsecond.

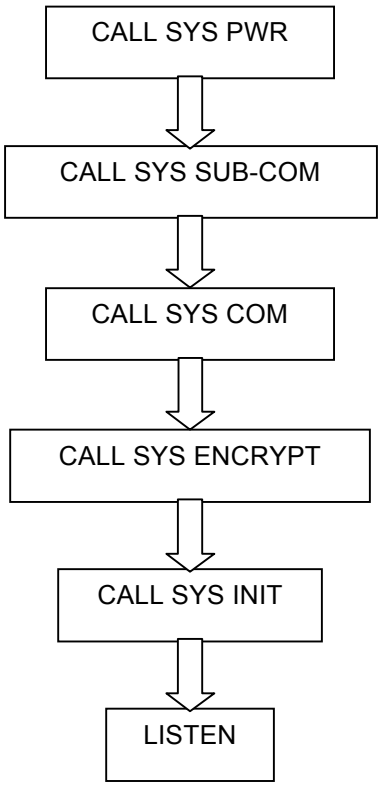
System Function Diagnostics

System function diagnostics can leverage on the use of intelligent microprocessors in the Ultra Blasting System. Connecting a diagnostic laptop to the SC will permit diagnostics showing status of the SC and all IFDs. This laptop interface would only have diagnostic capability and the SC would not accept function commands from the diagnostic laptop.

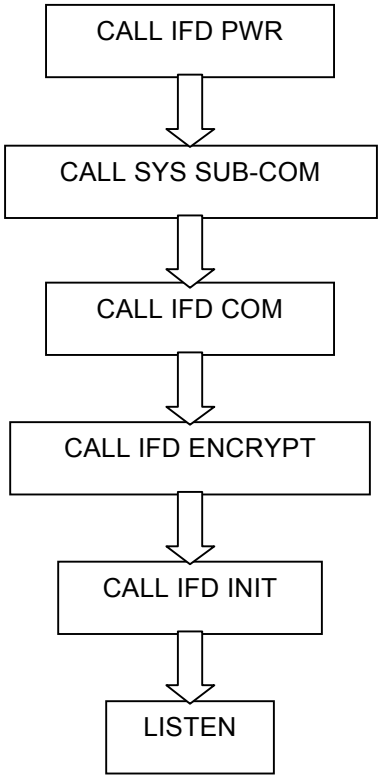
EXAMPLE PROGRAMMING FLOWCHARTS

The following programming flowcharts serve as examples of subroutines that illustrate Ultra function. The flowcharts shown provide a basic framework for logic function and firmware programming.

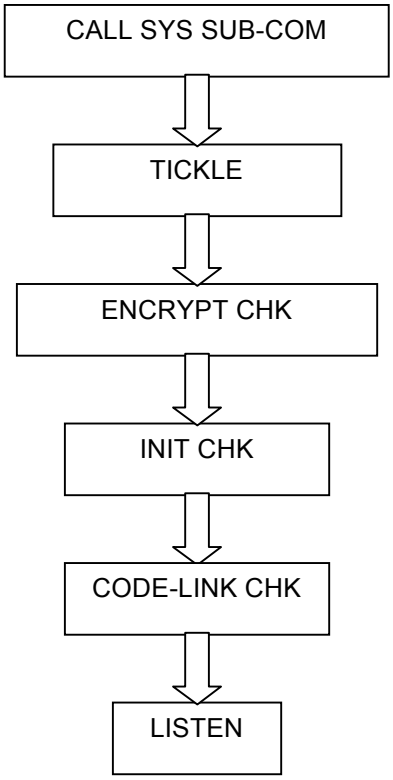
System Controller Power-up Firmware Flowchart:



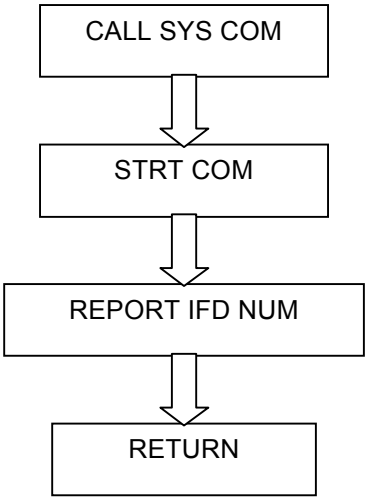
Integrated Fireset Detonator Power-up Firmware Flowchart:



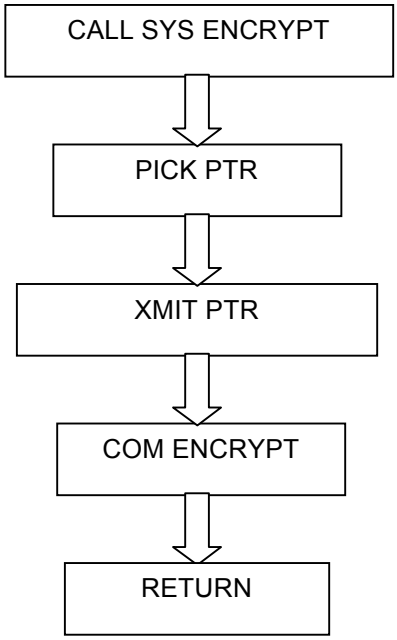
System Controller Sub-communications Firmware Flowchart:



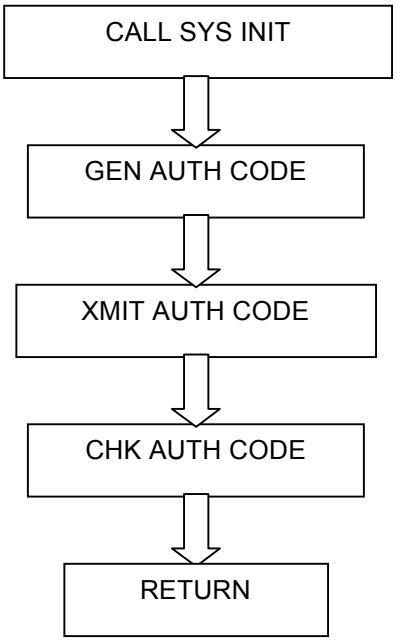
System Controller Communications Firmware Flowchart:



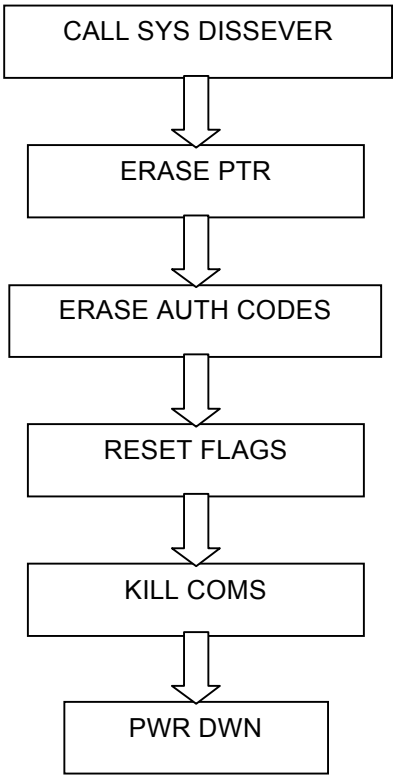
System Controller Encryption Firmware Flowchart:



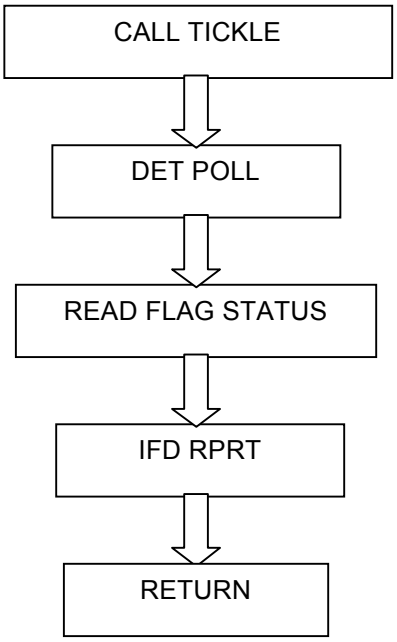
System Controller Initialization Firmware Flowchart:



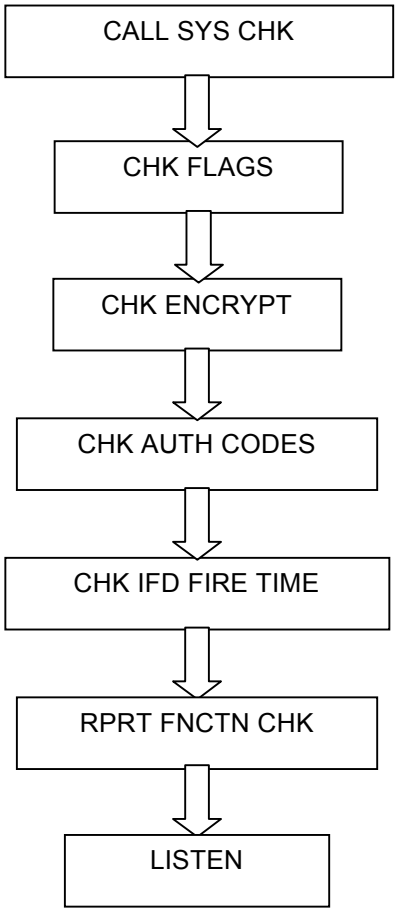
System Controller Dissever Firmware Flowchart:



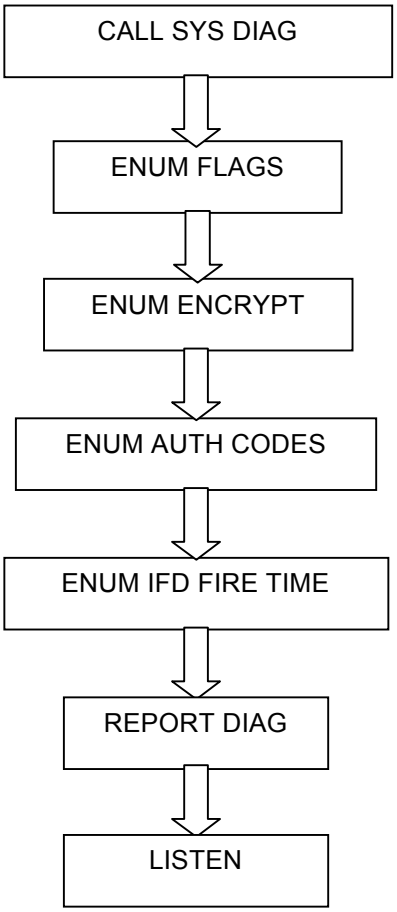
System Controller Tickle Firmware Flowchart:



Blasting System Function Check:



Blasting System Diagnostics:



SUMMARY AND CONCLUSION

While the above tutorial has provided a relatively complete description of a very safe and secure blasting system, design implementation can accommodate different levels of safety and security. The fundamental design of a safe system incorporates digital communications between the system controller and integrated fireset detonators. This intelligent communication supports decision making algorithms in both the system controller and the integrated fireset detonator that are responsible for system function and detonation. The degree of security in the blasting system can be varied according to the potential threat and consequence of attempts at unauthorized function of the blasting system. The first level of protection employs code-linking and authorization codes. The system can be further hardened against sophisticated attempts at unauthorized detonation by employing encryption in communications.

The Ultra Safe and Secure Blasting System provides safety and security beyond traditional blasting systems by incorporating microprocessor function at the detonator level. This microprocessor capability within the system can be leveraged to provide the operator with a high degree of confidence that the blasting system will function as designed. For blasting systems that are set up for long periods of time, the operator may want a simple field check to ensure proper system function prior to blasting. This is accomplished using diagnostics firmware embedded in the Ultra system controller. A simple closure switch will signal the system controller to execute its internal diagnostics firmware and go through a complete system check prior to blasting. At the conclusion of the internal system check, an indicator lamp will illuminate on the command firing unit verifying that the system is fully functional. In the event the internal check does not indicate a fully functional system, a laptop computer would be connected to the system controller to determine which components are malfunctioning and need replacement.

If you would like further explanations regarding any part of the Ultra Safe and Secure Blasting System design concept, you can contact Mark M. Hart at the Lawrence Livermore Laboratory, phone: 925-423-4770 or email: hart6@llnl.gov.