A new interlock system for the Vulcan laser

C J Reason, W J Lester, P Holligan, D A Pepler, R W W Wyatt

Central Laser Facility, CCLRC Rutherford Appleton Laboratory, Chilton, Didcot, Oxon., OX11 0QX, UK

Main contact email address: *c.reason@rl.ac.uk*

Introduction

The provision of safety interlocks in the CLF has developed through stages, starting with a hardwired system, through to a computer system, 'Cerberus'[1)] using Arcnet and written in Borland Turbo Pascal V 3 running under DOS, to 'Cerberus'[2)] – rewritten as a computer system using Ethernet and written in Borland Turbo Pascal V 7 running under DOS.

This has had to be replaced for a number of reasons including

- Much of the hardware is no longer available (e.g. door displays, Amplicon IO cards etc).
- The computers with ISA slots are no longer easily available.
- DOS and Borland Turbo Pascal are no longer supported.
- The limits on code and data of 64 Kbytes were preventing necessary changes to the system.

Also a new international standard IEC 61508 - Functional Safety for E, E, EP (Electrical / Electronic / Electronic Programmable) systems[3)] has been published. It is recommended (but not mandatory) that safety systems should comply with this.

As it would have been very difficult to prove a system based on just a PC would comply, it was decided that the new interlock system would be based on a safety PLC system called Argus, while a totally re-written version of Cerberus would provide the display system.

Safety considerations and IEC 61508

The system was specified and assessed with the help of Dr. David J Smith of Technis who is a national expert in safety systems[4)].

Consideration was given to two scenarios. Blindness to an individual from an alignment laser either locally or from a different room was assessed at < Safety Integrity Level (SIL) 1 and blindness to an individual from a shot was assessed at SIL 1. Calculating the probabilities of the two cases and setting the compensation for blindness at the high figure of £100,000 for the purposes of this exercise (cf. the value of a life at > £1,000,000), ALARP (As Low As Reasonably Practicable) calculations showed that the levels at which further improvements should be considered were £15 in the first case and £55 in the second. It was therefore assumed that any further improvements were unnecessary.

It was decided to err on the side of caution and design the system to comply with the higher SIL 2 (also commercial components are available at this level). The safety system is provided by an industry standard PLC system with a SIL 2 PLC system monitoring the critical functions (see below). The PLC system was not suitable to provide the information to the operators so a computer system provides the layout diagram (see Figure 5) and door displays (See Figure 6 and 7), neither of which are 'safety critical'.

The architecture of the new system

The system is based on an interlock station in a room as shown in Figure 1. The display computers communicate with each other and the PLCs by Ethernet and the PLCs communicate with each other by digital signal levels. This architecture allows the rest of the system to continue providing safety functionality even when a room is 'turned off' (e.g. lost power).

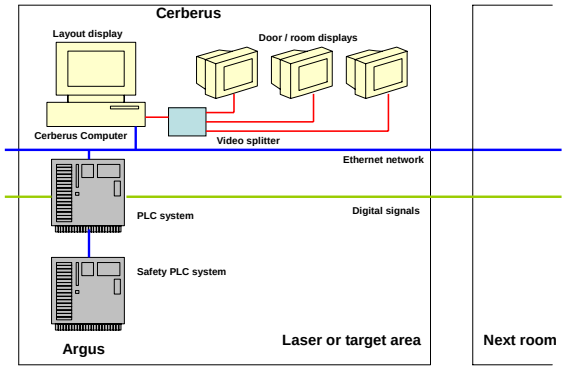

Figure 1. The system architecture.

The Argus PLC system

This was designed from the lifecycle developed from IEC 61508. Block 9 in the overall safety life cycle below is developed into 2 further lifecycles called the hardware & software lifecycles (See Figure 3).

The Vulcan Argus interlock system consists of six independent systems for the front-end room, laser room, laser room 4 and target areas West, East & Petawatt. (See Figure 2).

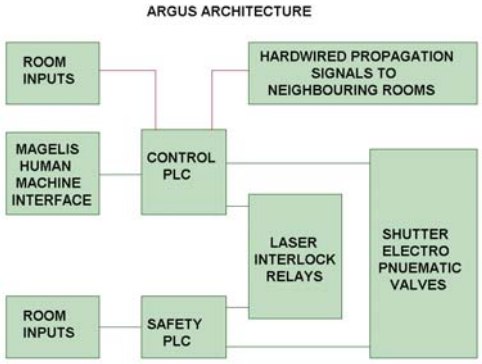

Figure 2. The PLC Architecture.

Each system is split into two parts, each part controlled by a programmable logic controller (PLC): -

The control PLC is a standard Schneider Momentum PLC which is connected to one or more Magelis human machine interfaces (see Figure 4), these are multi-page touch screen video displays which permit the operator to turn lasers on and off and to open & shut shutters. The graphics show the status of the lasers & shutters, authorisations needed, whether the room is hazardous, and displays any faults such as open doors, unresponsive shutters, faulty switches etc.

Propagation signals (room not tripped, room hazardous, authorisation, etc) are also sent & received digitally by the control PLC from neighbouring rooms.

The Momentum PLC is programmed in ladder logic and besides controlling the lasers & shutters monitors the system for malfunctions etc.

Each PLC system is built up of a processor module, a communication adapter plus a number of 32 way input & output modules. The size of the systems varies from 128 I/O for the front-end room to 256 I/O for the laser area.

The safety PLC is a Pilz PSS3047-3, which conforms to EN61508 safety integrity level 2. This PLC does not turn lasers on or open shutters but trips lasers & shutters, independently of the control PLC, if any room or enclosure interlock fails. This PLC has 3 processors (unlike the control PLC that has one) and all must agree. The PLC is programmed in statement list. Different input sensors are used for the safety PLC and the control PLC; e.g. a room door has two door switches, thus providing redundancy.

The Magelis page (see Figure 4) shows the TAW enclosed laser control (illustrative only as area could not be hazardous with room doors open). Laser 1 is shown on & its enclosure shutter shut. Laser 2 is on & its enclosure shutter open. The yellow high-lighted squares show interlock faults and would not normally appear on the screen when interlocks are healthy. Touching the grey 'Pulsed Lasers' square would change the Magelis page.

The Cerberus display system

The new version of Cerberus, re-written in Borland Delphi 7 running under Windows XP, takes its data from Argus over the Ethernet at a rate of 5 Hz and simply reports the information. From this information, it produces the layout diagram (the colour scheme being chosen by the writer) and door/wall displays which follow the agreed recommendations in the CLF. It does perform some consistency checks and warns the operator of data in conflict (e.g. a shutter between rooms reporting a different state from each room etc.). It has the optional ability to inform the user by voice output when certain functions change (e.g. a room tripping, becoming hazardous etc.). A basic bit pattern is provided to assist the operator in diagnosing the system.

Cerberus gets its knowledge of which room it is in from the name of the computer on which it is running and is completely defined by a table of information in simple text form (a file called layout.txt, editable by Word, Notepad etc.). This will define any configuration of up to 20 rooms and 100 each of doors, shutters, lasers and enclosures; with the associated layout diagram and door displays (these upper limits can be changed trivially). No changes to the code are needed. These text files can be saved and restored as required. The definitions of this text file are available in 'Instructions on how to use the new version of Cerberus' available on the CLF filing system. The file syntax is controlled by a number of keywords and is completely flexible as to the order of instructions and the choice of room numbers etc.

The program has an operational mode and a test mode. In the operational mode, the data is obtained from the PLC system. In test mode the operator can summon up a set of check boxes and change the settings of the bits at will in order to test the text file and code. The switch from test to operational mode is defined by a single line in the layout file.

Installation and commissioning

Meeting the new safety standard has meant replacing most of the wiring and devices feeding information to the PLCs (e.g. door switches have been replaced with two contact switches). This was completed during the Vulcan shutdown that was requested for other reasons in the first quarter of 2005.

Each PLC system is built according to a set of instruction and then is independently checked off. When completed, it is then tested in the specified room. The old interlocks in that room can be rapidly disconnected and the new system tested. At the end of the test period, the old interlocks are re-connected and minimally tested before operations can re-commence. This is done either during non-operational weekends or while areas are not in use.

The final stage of commissioning is to test the system with all rooms interconnected and again, this will be done in non-operational time.

The whole changeover of interlocks will be completed without requesting any additional operational time on Vulcan.

References

1. P Gottfeldt and C J Reason,
'Cerberus: a laser interlock system using Arcnet',
Computing and control engineering journal, December 1993, p 281

2. C Reason, E Divall, W Lester, D Pepler, R Wyatt,
'The implementation of the CLF Interlock System 'CERBERUS' on Vulcan',
CLF Annual report 1999 – 2000 (RAL – TR – 2000 – 034), p 194

3. 'Functional safety of electrical/electronic/programmable electronic safety-related systems', IEC 61508 / BS EN 61508 (7 parts)

4. D J Smith,
'Vulcan Laser Facility Interlocks',
Technis Report No T203 (Private communication).

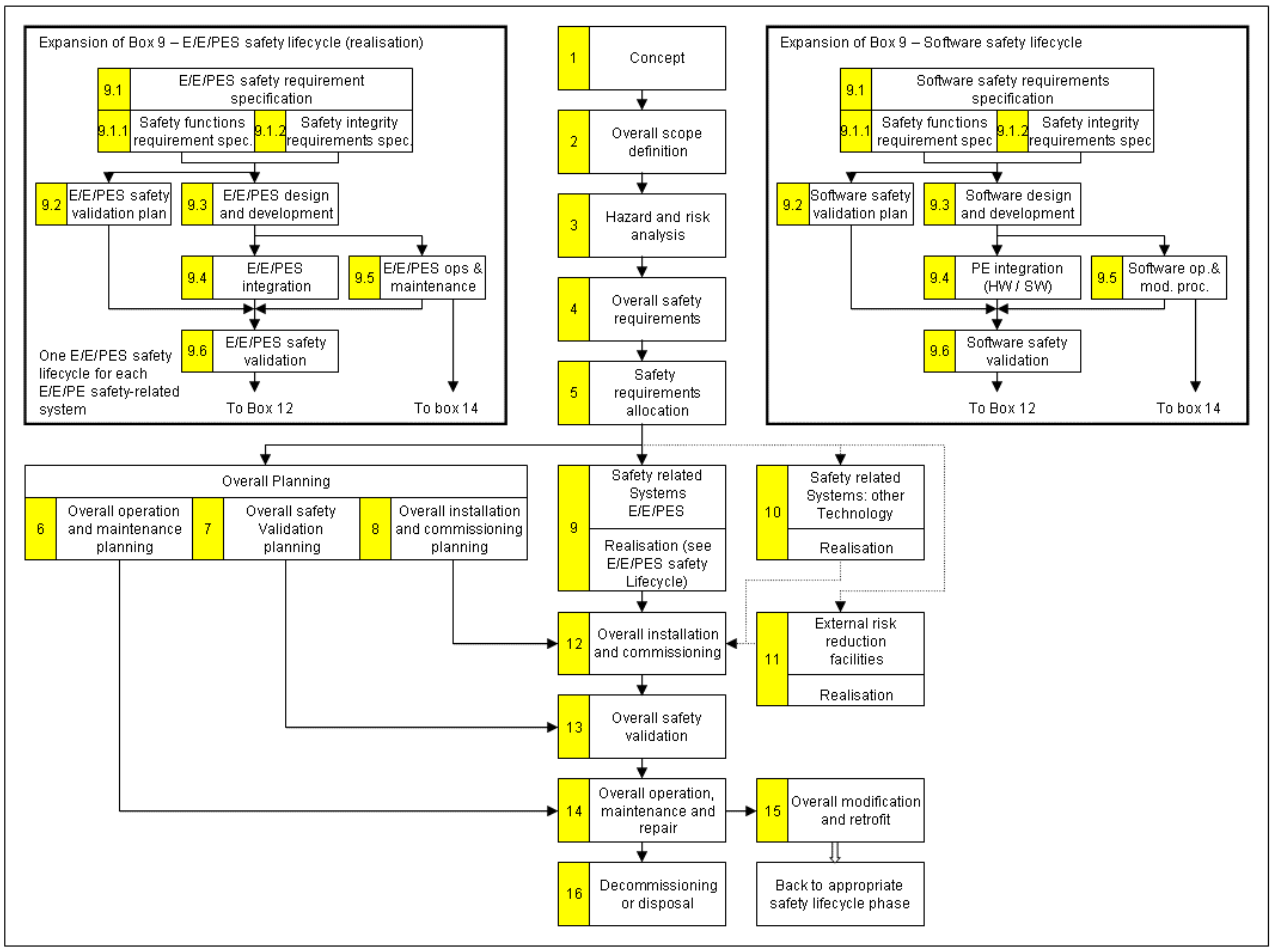

Figure 3. The overall safety lifecycle.

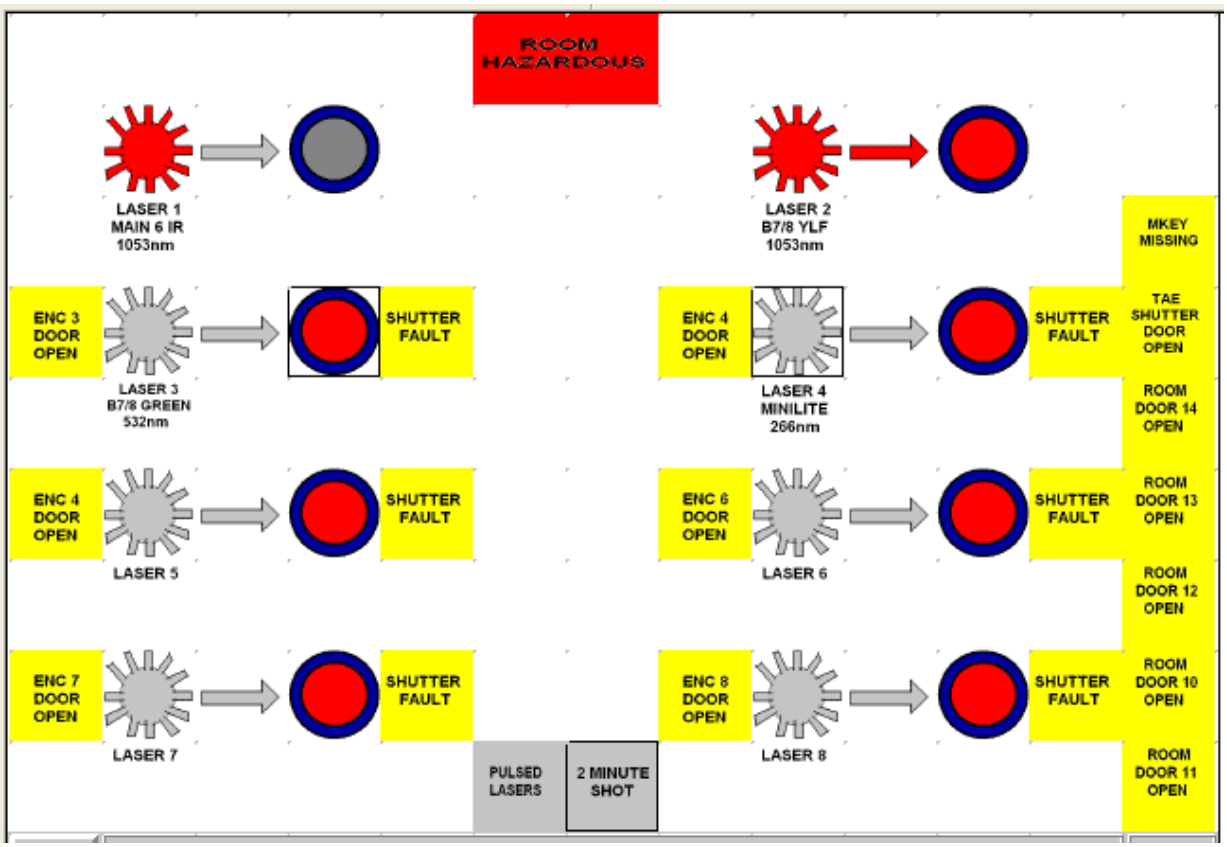

Figure 4. The Mangelis Screen.

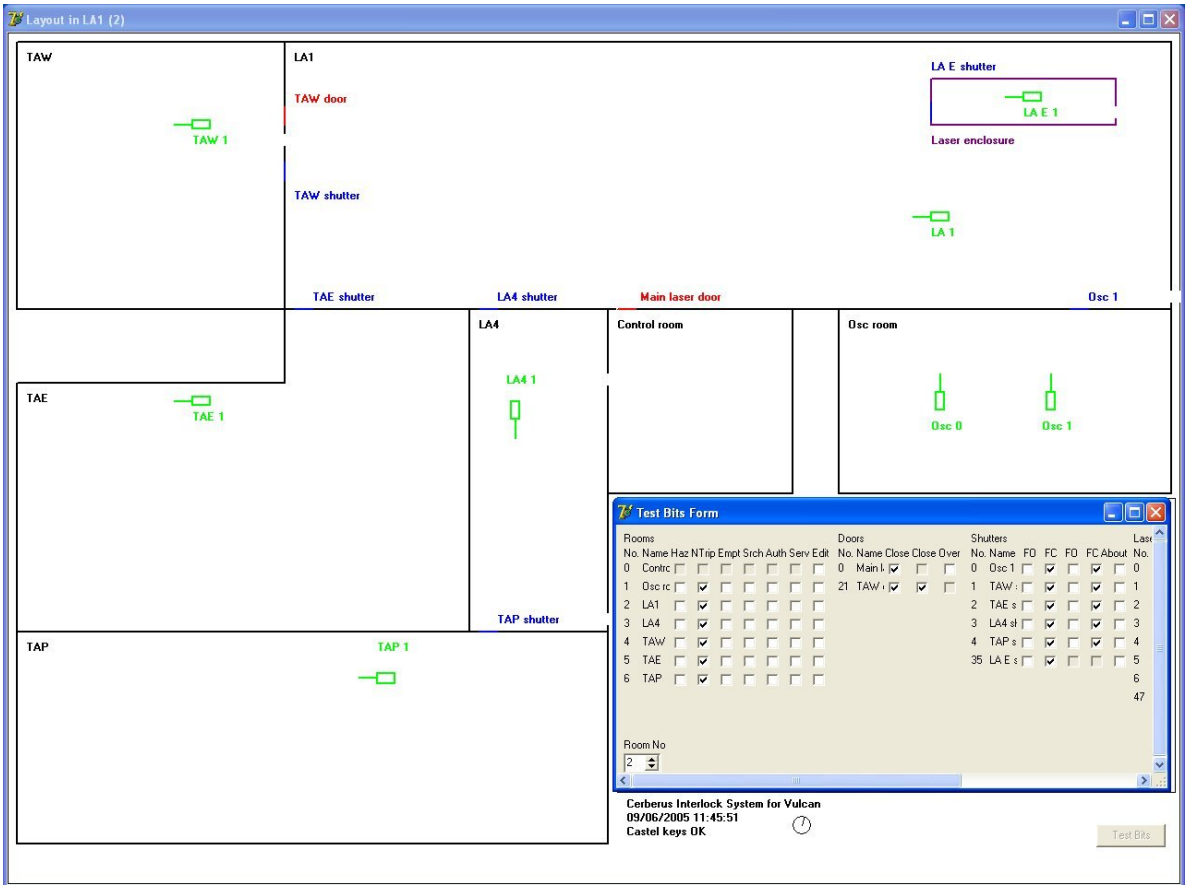

Figure 5. An example of Cerberus Layout Screen with Bit Testing Window.

Figure 6. An example of a non hazardous door display.

Figure 7. An example of a hazardous door display.