Division / Business Unit: Safety, Engineering & Technology
Function: Signalling
Document Type: Standard

Level Crossing Monitoring Requirements

ESD-05-05

Applicability

ARTC Network Wide

SMS

Publication Requirement

Internal / External

Primary Source

SPS 08 v1.3 and ESD-05-02

Document Status

Version #	Date Reviewed	Prepared by	Reviewed by	Endorsed	Approved
1.0	09 May 22	Standards	Stakeholders	Manager Signalling Standards	Acting General Manager Technical Standards 26/05/2022

Amendment Record

Amendment Version #	Date Reviewed	Clause	Description of Amendment
1.0	09 May 22	All	Aligned to Australian Standard AS 7705 Level Crossing Monitoring Systems. Other minor editorial changes.

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this standard is to specify the minimum requirements for the monitoring of level crossings that are fitted with active protection and warning systems on the ARTC network.

1.2 Scope

The scope of this standard includes the monitoring system, data logging, remote monitoring and alarming, battery testing, design, power supply, interface, and functional requirements.

1.3 Document Owner

The General Manager - Technical Standards is the Document Owner. For any query, initial contact to be made at standards@artc.com.au.

1.4 Reference Documents

The following documents support this standard:

ARTC ESD-03-01 – Level Crossing Design
ARTC ESC-03-01 – Level Crossing Construction
ARTC ESM-03-01 – Level Crossing Maintenance
ARTC ESD-09-01 – Signalling Power System
ARTC EGP-03-01 – Rail Network Configuration Management
ARTC ESM-07-02 – Track Circuits and Train Detection Devices
ARTC ESM-07-04 – Unreliable Track Circuit due to Infrequent Train Operations
ARTC SPS 01 - Standard Requirements for Signalling Electronic Systems
ARTC SPS 02 – Environmental Conditions
ARTC SPS 06 - Connections for Signalling Interface
ARTC SPS 04 - General Requirements for Labelling of Signalling Equipment
ARTC SPS 07 - Vital Indication Optoisolator
AS 7770 - Rail Cyber Security
RISSB CoP Rail Cyber Security in Train Control Systems.
AS7705 – Level Crossing Monitoring systems
AS7703 – Signalling Power Supplies
AS 7718 – Signal Design Process Management
AS 7770 – Rail Cyber Security
HIMA HIMatrix Checklist for Inputs v2.00
HIMA HIMatrix Checklist for Outputs v2.00
HIMA HIMatrix Checklist for Programs v2.00
HIMA HIMatrix F Safety Manual for Railway Application, HI 800 437 E, Rev. 3.03.00 (1806)
HIMA HIMatrix System Manual – Compact Systems, HI 800 141 E, Rev. 2.02

HIMA HIMatrix F3 AIO 8/4 01 Manual, HI 800 161 E, Rev. 2.00

HIMA HIMatrix F3 DIO 16/8 01 Manual, HI 800 177 E, Rev 2.00

HIMA HIMatrix F35 03 Manual, HI 800 477 E, Rev. 3.00.00 (1823)

HIMA HIMatrix F Maintenance Manual for Railway Application, HI 800 673 E Rev. 1.03.00 (1806)

HIMA HIMatrix Safety Manual, HI 800 023 E, Rev. 4.01.01 (1714)

HIMA HIMatrix Safety-Related Application Conditions (SRACs) Addition to the HIMatrix Safety Manual for Railway Applications, HI 800 575 E, Rev. 3.03.00 (1806)

HIMA HIMatrix H7013: Main Filter, HI 800 269 E, Rev. 1908

HIMA SILWorX Communication Manual, HI 801 101 E, Rev. 6.01 (1351)

HIAM SILWorX First Steps Manual, HI 801 103 E, Rev. 6.04 (1549)

HIMA SILWorX Smart Safety Test Manual, HI 801 495 E, Rev. 1.00.00

1.5 Definitions & Abbreviations

For the purposes of this document, the following terms and definitions apply:

Term or acronym	Description
ARTC	Australian Rail Track Corporation
AS	Australian Standard
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DC	Direct Current
I/O	Input / Output
LED	Light Emitting Diode
mA	Milliamp
MTBF	Mean Time Between Failure
NTP	Network Time Protocol
OS	Operating System
OSL	Operating System Loader
PB	Push Button
SNTP	Simple Network Time Protocol
V	Voltage
VPN	Virtual Private Network

2 General Requirements

The level crossing monitoring system, monitors the status of a level crossing, logs events, reports warning or failure conditions to a central location, provides facilities to remotely test the level crossing battery supply and to support improved maintenance practices.

The level crossing monitoring system shall be designed in such a way as to minimise the risk of providing incorrect information or of reducing the integrity of the level crossing.

The level crossing monitoring system should prevent false alarms being generated during maintenance activities.

ARTC level crossings are constructed and maintained to provide the highest levels of reliability and safety. Nevertheless, reports of failure to operate correctly are received from time to time. Any such incident is required to be investigated exhaustively, to determine what the cause of the reported failure might be, and to provide urgent repair of any fault revealed by the inspection. If, as often occurs, no fault is found, the question remains unresolved whether the failure report was prompted by an intermittent fault, or an error of observation by the person making the report.

Likewise, any accident or incident on a level crossing calls into question the safety of the system. The subsequent enquiry would benefit from the ability to provide a detailed record of the operation of the equipment at the time of the incident.

There is an evident need for a method of data recording that will enable the recent operational history of a level crossing to be 'read', after the report of that level crossing equipment having failed to operate properly.

It is considered inevitable that once a unit is installed, it will eventually be required to provide data acceptable as legal evidence, for instance in the event of an enquiry following a level crossing fatality. In that case the normal software design and testing will need to have been augmented by a stringent process of design specification, documentation and independent validation, to produce a record that can be presented and accepted by the court as reliable evidence.

As a minimum, level crossing monitoring system is required to monitor and record the below:

- Visual and audio warning, boom barriers and/or pedestrian gates where applicable
- Timing of operation as per level crossing design
- Associated train detection systems and circuitry
- Controls that operate, override or test the level crossing system
- Availability of primary power supply and voltage
- Battery voltage

2.1 Design Requirements

As a minimum, the design shall:

- provide functionality as required by AS and ARTC standards and practices
- minimise the risk of detecting and reporting incorrect status information
- minimise the risk of interfering with the systems being monitored
- be safe, fit for purpose and feasible

- detect, indicate, and log faults as per AS and ARTC standards and practices
- have been documented as per AS and ARTC standards and practices.
- minimise the risk of unauthorised manipulation of the system

In addition to this standard, design of the level crossing monitoring is required to be compliant with AS 7705 and AS 7718.

The level crossing monitor shall interface to the level crossing signalling control equipment in accordance with the approved designs for connecting the Level Crossing monitor to ARTC Level Crossings.

2.2 Environmental Requirements

Monitoring system shall comply to ARTC standard SPS 02 – Environmental Conditions.

3 Functional Requirements

3.1 Operation and self-checking

The level crossing monitor shall:

- Automatically start-up and commence monitoring on initiation of electrical power.
- Automatically re-start if the software ceases to operate correctly.
- Alarm and shut-down if more than 3 re-starts occur without 300 seconds of continuous operation.
- Check all configuration data on start-up and indicate a system fault if it is invalid.
- Alarm if the power supply is out of limits for correct operation.
- Alarm on loss of communication
- Continuously check that the software, and real time clock are operating correctly.
- Log the events with date and time

3.2 Digital inputs

The Level Crossing monitor shall have a minimum of 32 digital inputs (48 digital inputs preferred) that are logged and 8 inputs that are not logged.

As a minimum, the following digital inputs shall be connected to the Level Crossing monitor when available at the particular Level Crossing:

- All train detection system that control the operation of the level crossing.
- Direction stick relays.
- The level crossing control and repeat relays.
- Level Crossing timer function
- Test switch.
- Gate (Boom Arm) Up and Down state.
- Pedestrian gates – Open state, Closed state, lights and control relays (if different from the level crossing control relay)
- Lights, Bell and Gate (Boom Arm) emergency switches.
- Primary Power supply state.
- Low battery voltage indication from charger.
- Any other function that qualifies the operation of the Level Crossing (for example approach signals).
- Audible warning equipment state.
- Crossing normal relay.
- Reset fault or warning.
- Output state of each flasher.

Other relays/contacts of interest may be required depending on the local requirement or if requested by ARTC based on existing practice.

The state of each digital input shall be checked at least once every 0.25 seconds.

3.3 Digital outputs

The Level Crossing monitor shall have a minimum of 8 digital outputs. All digital outputs shall be logged.

The current state of the outputs shall be indicated on the level crossing monitor.

The Level Crossing monitor shall provide outputs as follows:

Battery Test	Used to control battery test where provided.
No fault	This output is ON when no fault condition has been detected with the level crossing equipment. The fault indication remains until acknowledged.
No warning	This output is ON when no warning condition has been detected with either the level crossing monitor or the level crossing equipment. The warning indication remains until acknowledged
System fault	This output operates in conjunction with the No Warning output. This output is ON when a fault has been detected with the level crossing equipment. The output remains on until the fault condition has been acknowledged.
Low battery	This output operates in conjunction with the No Fault and No Warning outputs. This output is ON when a fault or warning condition has been detected with the level crossing battery. The output remains on until the fault or warning condition has been acknowledged.
Lamp problem	This output operates in conjunction with the No Fault and No Warning outputs. This output is ON when a fault or warning condition has been detected with the level crossing lamps. The output remains on until the fault or warning condition has been acknowledged.
Logic Problem	This output operates in conjunction with the No Fault and No Warning outputs. This output is ON when a fault or warning condition has been detected with the operation of the level crossing equipment. The output remains on until the fault or warning condition has been acknowledged. This output FLASHES to indicate that the Level Crossing monitor is maintenance disabled.

3.4 Analogue Inputs

The Level Crossing monitor shall have a minimum of 8 analogue inputs.

Analogue inputs shall be protected against reverse polarity connections and surges.

The first analogue input shall be electrically conditioned for a 0 to 20 volts DC input voltage. This input shall be used to monitor the Level Crossing battery voltage.

At least 4 Analogue inputs shall be provided to monitor the Level Crossing lamp currents in the range of 0 to 20 amps DC.

Normally two sets of lamps are connected to each circuit which is monitored by one analogue channel. An electronic flasher changes between the sets of lamps at about 45 times per minute when the lamps are operating. The two sets of lamps may be identified as Flasher Up and Flasher Down for the purposes of the Level Crossing monitor. A digital input may be used to monitor the state of the flasher.

It is expected that both the flasher state digital input and the lamp current input will be used to determine the number of lamps operating in each set of lamps for each circuit.

A change shall be considered to have occurred on a lamp analogue channel when a different number of lamps are determined to be operating for either set of lamps to the previously determined number.

At least 2 Analogue inputs shall be provided as general purpose analogue inputs. These shall be configurable to monitor temperature, currents, lamps, or voltages.

One Analogue input shall be used to monitor the battery test load current in the range of 0 to 20 amps DC. A change shall be considered to have occurred when the current is more than 0.5 amperes different to the last recorded value.

The state of each analogue input shall be checked at rates which is high enough to accurately reflect both the flashing and not-flashing states of the lamps. Analogue inputs shall be continually monitored, regardless of the current state of the level crossing.

3.5 Logging

The Level Crossing monitor shall detect changes in its analogue inputs, digital inputs and it's digital outputs. Details of these changes shall be stored with their date and time (to the tenth of second) of occurrence. At least the last 8000 changes shall be stored.

The log shall be maintained in a non-volatile storage medium. The log shall still be retrievable after the Level Crossing monitor has been removed from service, transported to another location, and left without power for at least 31 days.

The oldest event shall be automatically replaced by the next new event when the event log is full.

Changes to the state of the flasher inputs shall not be logged. This is solely to prevent wasting log space.

3.6 Monitoring

The Level Crossing monitor shall check the digital inputs and analogue inputs for correct relationship, sequence and timing.

The Level crossing monitor shall process logic with, internal intermediate states and timer facilities.

The logic shall be configurable for each particular level crossing.

The Level crossing monitor shall determine the number of lamps operating on each lamp circuit; check the number of lamps operating against the number that should be operating; provide a fault indication when the number of lamps detected is more than expected on any particular lamp circuit, or two or more less than the expected; and provide a warning indication when the number of lamps detected is one less than the expected.

The Level Crossing monitor shall provide for the use of additional fault or warning inputs.

The Level crossing monitor shall provide an indication that remote battery testing is in progress.

The Level crossing monitor shall provide spare inputs for logging additional track circuits and control relays.

In general, the logic shall be as follows:

In normal operation the level crossing monitor will display two green LEDs which indicate NO FAULT and NO WARNING. If the monitor reports its status to a computer these two indications are combined to give a status of NORMAL. If a designated FAULT occurs then the LED for NO FAULT shall extinguish indicating that a FAULT has occurred. If a designated WARNING occurs then the LED for NO WARNING shall extinguish indicating that a WARNING has occurred. As well as WARNINGS or FAULTS being indicated on the front panel appropriate messages are reported to allow remote reporting of FAULTS and WARNINGS.

The NO FAULT status indicates that the battery voltage is not low, no more than one lamp is out, more lamps than expected have not been found, and that there is no other designated fault condition detected by the level crossing monitor logic. The Fault indication is latched until the fault reset push button is pressed or the fault reset command is received.

The NO WARNING status indicates that none of the designated warning conditions are present. The Warning indication is latched until the fault reset push button is pressed or the fault reset command is received.

A status indication of WARNING shall be indicated if one or more of the following has occurred:

- No remote test or local test of the level crossing has occurred as per the requirement of the level crossing design specific to a particular location and battery back-up capacity in consultation with corridor engineer for any other maintenance requirement.
- No train has traversed the level crossing for infrequent train operations as per ESM-07-02 and ESM-07-04. Where provided, Emergency switches/Isolation switches have been activated
- There has been a failure of some nominated item of signalling equipment near the level crossing e.g. points detection failure, signal lamps out or track failure.

A status indication of WARNING & LAMP shall be indicated if:

- One of the lamps is not working.

A status indication of WARNING & BATTERY shall be indicated if:

- The AC Supply has been OFF for more than 6 hours 30 minutes.

A status indication of WARNING & SYS_FAULT shall be indicated if:

- The Level Crossing Monitor itself has an internal fault. A possible internal fault could be due to failure of the clock, CPU, memory, log data, analogue input, EPROM, a test output being ON without a test being requested.

A status indication of FAULT & LOGIC shall be indicated if the level crossing has:

- not started operating 6 seconds after the time that it should start operating.
- not stopped operating 6 seconds after it should have stopped operating.
- not had a change of state on the flasher inputs within the last 5 seconds when the level crossing should be operating.
- operated continuously for more than 20 minutes.

- the Boom normal when it should not be, or not normal when it should be normal.
- either direction stick relay is energised when no train is present.
- Battery Test relay is faulty or not present (possibly causing the battery charger to be without power).

A status indication of FAULT & LAMP shall be indicated if:

- Two or more of the lamps are not working.
- More lamps are operating than expected on any lamp circuit (a possible short circuit).

A status indication of FAULT & BATTERY shall be indicated if:

- the battery voltage is below its configured alarm point, generally 15% below the charging voltage and based on the design requirements for a specific application, as measured by the level crossing monitor for more than 3 seconds.
- the low battery alarm card input is off for more than 3 seconds.
- the remote testing of the level crossing battery has not drawn sufficient test current for more than 7 seconds.

Due to track maintenance vehicle considerations, the following entry is to be recorded in the log but not alarmed:

- level crossing lights have been operating for less than 20 seconds before the train arrives at the level crossing.

It is possible to have multiple status indications which would indicate that more than one fault has occurred. For example, a failure of a flasher unit will give FAULT & LAMP & LOGIC.

A status indication with LOGIC flashing once per second indicates that the monitor has had its reporting of status changes disabled temporarily. When in this state the monitor will not report changes of status to the control centre. This state, if available is entered by holding the Fault Reset button pressed for 5 seconds. It is cancelled by a momentary push of the Fault Reset button or at a pre-programmed interval after activation. Normally this time-out is set for 45 minutes. All Faults and Warnings must be cleared before cancelling this mode otherwise they are to be reported to the remote site (Control Centre).

3.7 Status reporting

The Level Crossing monitor shall indicate its status locally using No Warning and or No Fault outputs. If a warning or fault occurs, it shall turn off the No Fault or No Warning outputs as appropriate and indicate the cause by turning on either system, lamp, battery, or logic output as appropriate.

A facility is required for local level crossing maintenance staff to temporarily disable the status reporting whilst maintenance is carried out. The maintenance staff shall not be required to have any equipment to use the temporary disable facility.

3.8 Battery Testing

Where required, the level crossing monitor shall have the facility for testing the current state of the level crossing battery and reporting the results to a remote location. If there are multiple batteries, then health of all batteries is required to be tested.

The level crossing monitor shall use outputs, for example, 1 and 8 (that is Battery Test, and Timer Test) to control the battery test. These outputs control the 120 V AC supply to the level crossing battery charger, and a test load for the level crossing batteries

The process of testing the level crossing battery and the level crossing monitor when requested shall be as follows:

- Perform a through check of the operation of the Level Crossing monitor which includes processor test, event log integrity check, program checksum, configuration check, and memory test. If all checks do not pass then abort the battery test, indicate a system fault and report it.
- Check battery voltage to determine if it is within limits. If it is too low, then abort the battery test, indicate a battery Fault and report it.
- Check that the battery test current is less than 1.0 amps and the Battery test cut-off indication is ON.
- Report that the test will commence.
- Turn on output 8 (that is Timer test). Check that the Battery test cut-off indication turns OFF between 270 and 330 seconds later. If it does not, then abort the battery test, indicate a Fault and report it.
- Turn OFF timer test output 8.
- Check that the battery test current is less than 1.0 amps and the Battery test cut-off indication is ON.
- If the crossing is operating, delay until at least 30 seconds after the crossing has stopped operating.
- Turn ON both timer test output 8 and Battery test output 1 at the same time, for 4 minutes.
- Monitor that the Battery test current is greater than 6 amps and battery voltage remains greater than alarm voltage.

If the battery voltage drops below the alarm voltage during the test, stop the test, and indicate a battery fault;

if the battery test current drops below 6 amps for more than 7 seconds during the test, stop the test, and indicate a battery fault; otherwise terminate the test at the end of 4 minutes and indicate and report that the test passed, and the current state of the level crossing.

- The previous step is terminated if the crossing starts operating and the process is restarted at “Turn ON both timer test output 8 and Battery test output 1 at the same time, for 4 minutes”, at least 30 seconds after the crossing has stopped operating.

3.9 Control and Interrogation

The control and interrogation facilities shall be via Ethernet or other communication methodology agreed by ARTC

The following facilities shall be provided:

- Display all logged events starting from the oldest and finishing with the most recent event. The user shall be able to pause, continue, and abort this display.

- Display all logged events starting from a given date and time and finishing with the most recent event. The user shall be able to pause, continue, and abort this display.
- Display all logged events starting from a given date and time and finishing with a given date and time. The user shall be able to pause, continue, and abort this display.
- Display time and date.
- Set time and date. This facility shall be protected by requiring the user to provide a predetermined operations security code.
- Display inputs, outputs, intermediate (internal logic states), and timer names and current state.
- Display current lamp status and configuration.
- Display current battery voltage and configuration.
- Set serial port configuration where applicable.
- Display serial port configuration where applicable.
- Reset warnings and faults. This facility shall be protected by requiring the user to provide a predetermined maintenance security code.
- Initialise the event log. This facility shall be protected by requiring the user to provide a predetermined maintenance security code.
- Perform a self test and battery test..
- Enable or disable the immediate reporting of changes to the user in addition to logging changes.
- Display name, data version, code version, status, and report state.
- Conduct a self test and report results.
- Download and Upload permanent configuration data.
- Calculate the location specific lamp offsets and apply them if they are valid. This facility shall be protected by requiring the user to provide a predetermined maintenance security code.
- Display lamp calculation details.

3.10 Configuration

There are two types of configurable items. One set may be changed during normal operation. The other set cannot. Both are stored in non-volatile memory.

Configurable items that cannot be changed during normal operation are:

- Name and date of the permanent configuration data.
- For each digital input, its name.
- For each digital output, and intermediate state their names and controlling boolean expressions.
- For each Timer its name, controlling boolean expression, and duration in hours, minutes, and seconds.
- For the battery analogue input, its name, fail voltage, and bus voltage correction.

- For each lamp analogue input, its name, analogue channel number, number of lamps expected on flasher up, number of lamps expected on flasher down, flasher input, and an intermediate state that identifies when the lamps should be on.
- For the battery test current analogue input, its name, analogue channel number, “on” current in amperes, “off” current in amperes.

The configuration details above shall have a checksum or equivalent mechanism that is checked to confirm that they are valid.

Configurable items that can be changed during normal operation are:

- Name of crossing
- Serial port setup where applicable
- Current date and time
- Battery bus offset from measured value
- Lamp offsets for each particular lamp set. This may be required to allow for variations in level crossing installations. This should be able to be manually entered as well as learnt from level crossing operation.

3.11 Replay Requirements

The level crossing monitor should be capable of providing a local and remote replay so that events stored in the system memory can be graphically represented following an incident.

4 Interface Requirements

4.1.1 Lamps

A non-invasive method of detecting the number of lamps operating shall be used. This method shall be designed so that any fault in the lamp detection is detectable.

The method used for detecting the number of lamps operating shall cater for the initial peak current each time a lamp is turned on, the tolerances in lamps, and fluctuations in battery voltage.

The lamp detection method shall be able to discriminate between number of lamps operating.

4.1.2 Voltage free contacts

The level crossing monitor shall have a minimum of 32 optically isolated digital inputs in accordance with SPS 06 Connections for Signalling Interface.

These inputs shall operate from a 12 volts DC nominal signalling power supply. Each input shall draw at least 5 mA. This is required to ensure reliable operation of the safety relay contracts.

4.1.3 Intermediate points in circuits

Digital inputs that monitor intermediate points in Signalling circuits shall use Vital Indication Optoisolators in accordance with SPS 07 Vital Indication Optoisolator.

4.1.4 Power supply

The Level Crossing monitor shall operate from a reliable primary source of power.

The Level Crossing monitor shall not earth the power supply or connect either polarity of the supply to the case.

The Level Crossing monitor shall have a breakdown voltage to earth of greater than 500 Volts DC.

4.1.5 Communications

Unless otherwise approved by ARTC, communications over Ethernet is preferred.

An approved router shall be used and connected to the ARTC Private Network unless another communication link is specified by ARTC.

Existing monitoring system which are not capable of communicating via Ethernet or radio, may utilise the Serial communication via dial-up modem in consultation with corridor signal engineer.

4.1.6 Time Synchronisation

Where possible, level crossing monitoring controller should be setup as:

i. An SNTP client, which connects and synchronises with ARTC's NTP time server.

ii. An SNTP server, which allows remote IO devices to connect to the CPU to synchronise their time.

All time synchronisation events are to be recorded in the Event Log.

5 Other Requirements

5.1.1 Mechanical Requirements

The Level Crossing monitor and its ancillary equipment should mount on DIN Mounting rail TS32, or BRB 930 style relay racking.

5.1.2 Integrity

The Level Crossing monitor shall detect all faults with itself that could reasonably be expected and indicate a system fault. The faults detected shall include: Memory faults - RAM and EPROM, CPU faults, Digital input faults, Analogue input faults, Digital output faults, corruption of memory contents, Real Time Clock failure, and current sensor faults.

Faults with the operation of most digital inputs shall be detected and indicated within the passage of one train. Digital inputs than are only logged are not required to have faults automatically detected.

Faults with the lamp detection shall be detected and indicated on the Level Crossing Monitors front panel and reported to the Control Centre within or immediately after the passage of one train.

Assurance shall be provided by an independent review of the system that it is improbable that the level crossing monitor will indicate that the level crossing is operating correctly after the passage of a train without both the monitor and the Level Crossing equipment being essentially operating correctly given that a self test and battery test is carried out every day.

The level crossing monitor shall be designed and tested to provide proof that the level crossing monitor will not reduce the safety, integrity of, reliability of, or public confidence in the level crossing.

The level crossing monitor shall turn off all its outputs if the monitor is not operating reliably.

The level crossing monitor shall have an independent method of disconnecting the battery test load and restoring power to the level crossing battery charger that is automatically tested as part of the battery test process.

5.1.3 Reliability

The designed Mean Time Between Failures (MTBF) for the Level Crossing monitor shall be greater than 50,000 hours.

6 Appendix 1 HIMA Level Crossing Monitor specific requirements

HIMA for level crossing monitoring application is capable of exceeding the minimum requirements of this standard. This Appendix provides guidance to the design engineer for specific requirements for HIMA level crossing monitoring design.

6.1 Reliability and Maintainability

a. All manufacturer's Safety-related Application Conditions (SRACs) are to be followed.

b. The monitoring system shall detect internal faults that indicate a system fault, including firmware, memory, data storage; processor faults; clock faults; input and output faults and communication faults.

c. The monitoring system shall be certified to operate correctly where its operating parameters are within its specifications.

d. The level crossing monitor shall be designed and tested in such a way as to minimise the risk of providing incorrect information, and of reducing the integrity of the level crossing.

e. The monitoring system shall be designed and tested to minimise the risk of unauthorised or unintended manipulation of the system

f. Maintenance staff shall be able to temporarily disable the status reporting whilst maintenance and/or testing is carried out.

g. The monitoring system should have a facility to prevent false alarms being raised during maintenance activities.

6.2 Design and data documentation

Design of the HIMA level crossing monitoring system shall include monitoring and logging of operation of the level crossing, visual and audible warning, where applicable boom barriers and/or pedestrian gates, primary power supply, battery testing, test switch, train detection system and remote alarming.

a. Design shall minimise the risk of interfering with the systems being monitored.

b. Application Logic Design Specification (ALDS) should be developed by projects/signal designers using the HIMA as a level crossing monitoring device.

c. All generated data documentation must contain the CRCs for all used function blocks.

d. A data control sheet shall be provided, and shall contain:

   i. The level crossing site location and ID;

   ii. The relevant network control centre;

   iii. The current revision and date of the application software;

   iv. The designer, checker, independent reviewer, and approver details and their signatures approving the data.

   v. What design stage the data is approved for. For example:

      i. For simulation testing;

ii. For factory acceptance testing; or
iii. For site acceptance testing.

vi. Details of any modification sheets;
vii. Tester sign off for:
    i. Factory acceptance testing; and
    ii. Site testing;
viii. A completed HIMA HIMatrix Inputs Checklist should be referenced and attached;
ix. A completed HIMA HIMatrix Outputs Checklist should be referenced and attached;
x. A completed HIMA HIMatrix Program Checklist should be referenced and attached;
xi. A HIMA Rail Safety Application Conditions Checklist should be created, referenced and attached, which should list and demonstrates compliance to all safety related application conditions listed in HIMA document HI 800 575 E.
xii. A list of all references used for the preparation of the data design, including their revisions and dates;
xiii. References to any other relevant design elements, including the circuits.
xiv. A reference to the ALDS that was used to produce the data;
xv. A reference to all relevant tools and their versions, including SILWorX;
xvi. Details of the HIMA application data, including:
    i. The Project Configuration CRC;
    ii. The Program CRC(s); and
    iii. Details of the previous version and a reference to the difference list that was produced.

i. The CRC and version of the ComUserTask module;
ii. The CRC and version of the ComUserTask user configuration file;
iii. Details of any HIMA simulation application data;
iv. The version of firmware used on all HIMA devices[1], including:
    i. The Boot Loader (BL) version;
    ii. The BL CRC;
    iii. The Operating System (OS) version;
    iv. The OS CRC;

[1] For HIMA controller units the details of both the CPU and COM firmware must be included.

v. The Operating System Loader (OSL) version; and
vi. The OSL CRC.

e. Suitably rated bi-directional transient-voltage-suppression are to be used on digital outputs that drive inductive loads to reduce back EMF.

f. Application specific logic is not to be contained in function blocks and should instead be accessible in the main program.

g. The program cycle time is not be higher than 50ms.

h. Wherever possible, all monitored indications should fail/alarm due to a wire break, power supply failure, or other circuit failure.

i. Data changes require the confirmation of local presence at the level crossing, through the use of the local Maintenance Mode and the Data Change push buttons via digital inputs.

j. All HIMA unit's temperature states, power states, and CRCs are to be monitored and recorded in the event log, and continuously reported back to the level crossing monitoring system.

k. All Program CRCs are to be monitored and recorded in the event log, and continuously reported back to the level crossing monitoring system.

l. The ComUserTask User Configuration CRC shall be monitored and recorded in the event log, and continuously reported back to the central the level crossing monitoring system.

m. The forcing states of all HIMA CPUs are to be monitored, recorded, reported and alarmed. This includes the Force Switch State, Forcing Active, and Global Forcing Started bits.

n. All HIMA controllers are to be set to Auto Start.

o. Access to the HIMA controllers via SILWorX shall be restricted via PADT User Management, including:

i. The provision of Administration, Engineering, and Maintenance accounts with suitable access levels.
ii. The use of passwords provided and documented in the ALDS.
iii. Passwords must be at least 10 characters in length and must contains numbers, special characters, capital and lowercase letters.

p. Appropriate firewalling and other Cybersecurity techniques, in accordance with Australian Standard AS7770, and HIMA's Cybersecurity Manual are to be implemented.

q. Each HIMA unit is required to have a unique System and Rack ID. These IDs are to be unique across ARTC's network. These must be obtained from ARTC, such that they can ensure they can ensure unique numbers are issued and keep their HIMA ID database update to date.

6.3 Functional Requirements

6.3.1 Monitoring

a. The HIMA level crossing monitor application data shall be configurable for each individual level crossing.

b. The HIMA level crossing monitor shall determine:

    i. the number of lamps operating on each lamp circuit.

    ii. the number of lamps operating against the number that should be operating.

c. The HIMA level crossing monitor shall provide:

    i. a warning indication when the number of lamps detected is one less than the expected, and:

    ii. a fault indication when the number of lamps detected is more than expected on any individual lamp circuit, or two or more less than the expected.

d. The HIMA level crossing monitor shall log the start and end time of each level crossing operation.

e. The HIMA level crossing monitor shall provide for the use of additional fault or warning inputs. This shall be indicated via the local maintenance panel indications.

f. The HIMA level crossing monitor shall provide an indication that remote battery testing is in progress. This shall be indicated via the local maintenance panel indications.

g. The HIMA level crossing monitor shall provide an indication that local maintenance mode has been activated.

h. The HIMA level crossing monitor shall provide indications that lamp calibration is invalid or in progress.

6.3.2 Digital Outputs

In addition to digital output listed in Section 3, HIMA shall be configured to provide the Maintenance mode output. This output is ON when in maintenance mode.

6.3.3 Digital Inputs

In addition to digital input listed above, HIMA can be configured to provide the below inputs which should be used to improve the monitoring on level crossing.

The following digital inputs are to be monitored:

a. The Fault Reset, Warning Reset, Data Change, Calibrate, and Maintenance push buttons from the Local Maintenance Panel.

b. Level crossing normal relay.

c. Test Switch, Emergency Switch (if provided) and Manual Operation Switches (if provided).

d. Lights, Bell and Gate (Boom Arm) emergency switches where provided.

e. The health status of each flasher (if available).

f. Output state of each flasher.

g. Power Supply Unit failure alarm contacts.

h. Interfaces to traffic light functions, including:

    i. Traffic Light Train Demand (TD) function

    ii. Traffic Light Response (TLR) function

    iii. Pre-emption functions (if separate to the crossing control)

    iv. Advanced Warning Lights (AWL) status

i. Other relays/contacts of interest and any other ancillary systems (e.g. ELDs, Network Router etc.)

6.3.4 Internal Variables

a. The error codes for all used inputs and outputs are to be monitored and included in a controller health indication, which when true indicates that the controller, and all of its remote I/O are healthy and have no system or input or output errors. If the controller health indication is false, a warning or error (as appropriate) shall be indicated on the Local Control Panel.

b. The error codes for all HIMA modules are be monitored and included in the controller health indication.

c. All communication links are to be monitored, including any redundant connections, and an alarm generated if any link is down.

d. If a ComUserTask module is used, a health bit for establishing.

e. All program, controller and configuration CRCs are to be shared over the link to level crossing monitoring system.

6.3.5 Lamps

a. Level crossing lamps are to be monitored to allow detection of any lamp failure.

b. The failure of any level crossing lamp shall be alarmed.

c. Whenever the crossing activates or deactivates, the current status of the lamp monitoring and any related alarms are to be recorded in the event log.

d. Flashing light lamp currents are to be monitored using isolated DC Hall Effect current sensors. These sensors are to be 4mA to 20mA, as they allow a sensor failure to be detected.

e. Lamp current sensor analogue inputs are to be directly connected to the HIMA CPU's analogue inputs; such they can be filtered at a higher frequency than would be possible if using a remote unit's analogue inputs.

f. All battery buses that supply lamps and/or their flashing units shall be monitored using isolating voltage transducers. If the bus voltage drops below a voltage that will reliably turn the lamp on, then a critical flashing light alarm shall be generated.

g. All lamp currents are to be adjusted for changes in the lamp bus bar voltages.

h. A minimum time-based filter with a 200ms filter window shall be applied to all measured lamp currents to filter out noise and start-up spikes in the lamp current sensor readings.

i. Separate lamp monitoring should be provided for:

    i. The up side left flashing lights

    ii. The up side right flashing lights

    iii. The down side left flashing lights

    iv. The down side right flashing lights

    v. The boom barrier tip lights

    vi. Optionally, and where specified by ARTC, the left boom barrier flashing light bank(s)

    vii. Optionally, and where specified by ARTC, the right boom barrier flashing light bank(s)

j. The following flashing light alarms to be provided:

    i. A non-critical (warning) alarm when a single flashing light lamp or any boom barrier lights are detected out;

    ii. A critical alarm (fault) when more than one flashing light lamp is detected out. Multiple boom barrier lights being out is considered a non-vital failure, and thus shall not cause a critical alarm to be raised; and

    iii. Individual indications for the up and downside flashing lights must be provided to allow maintainers to distinguish whether a flashing light failure has occurred on either the up or downside of the crossing.

6.3.6 Boom Barriers

a. Wherever possible, and in all new installations, both the up and down state of the boom barriers are to be monitored.

b. Boom barrier drive and fall times are to be monitored using the boom barrier detection. Alarms should be generated whenever the drive or fall times are outside a configurable time window. To enable predicative maintenance, separate non-critical alarms are also to be provided when the system detects the boom barriers rise or fall times have drifted over a number of measurements by a configurable percentage from their last calibrated values.

c. Where boom barrier up detection is provided, a failed to rise alarm shall be raised after a configurable period of time after it has been commanded to rise.

d. Where boom barrier down detection is provided, a failed to drop alarm shall be raised after a configurable period of time after it has been commanded to drop.

6.3.7 Pedestrian Gates

a. Wherever possible, and in all new installations, both the open and closed state of the pedestrian gates are to be monitored individually.

b. If the pedestrian gate control relay differs from the level crossing control relay, it shall be monitored and recorded.

c. Where pedestrian gate open (85-90 degree state) detection is provided, a failed to open alarm shall be raised after a configurable period of time after it has been commanded to open.

d. Where pedestrian gate closed (0-10 degree state) detection is provided, a failed to closed alarm shall be raised after a configurable period of time after it has been commanded to close.

6.3.8 Start-up

a. All alarms are to be appropriately conditioned during the application start-up to avoid false alarms.

b. All indications, including all digital input and output statuses, are to be logged at start-up.

c. All start-up events are to be recorded in the Event Log.

6.3.9 Configuration

a. All alarm thresholds are to be configurable.

b. All analogue thresholds are to be configurable.

6.3.10 Calibration

a. All calibration data shall be stored in non-volatile memory, using retain variables in the Application Data.

b. The calibration parameters for each lamp shall be configured, this shall include the calibration curve for the item (e.g. a lamp). This may be used for voltage or

temperature adjustment, based on readings from a voltage (e.g. the flashing light or battery bus voltage) or temperature sensor.

6.3.11 Control and Interrogation

a. The SILWorX application can be used remotely or locally to interrogate the level crossing monitor.

b. A web browser can be used to view and download the current crossing status, alarms, and events from the ARTC HIMA Level Crossing Monitor ComUserTask module.

6.4 Local Maintenance Panel

a. A local maintenance panel displaying all the diagnostics LEDs may be provided in conjunction with a centralised level crossing monitoring workstation.

b. The maintenance panel is also to be fitted with each of the level crossing monitor's push buttons.

c. The maintenance panel is required to be laser or water cut, and laser etched in 316 stainless steel with rounded corners and have no sharp edges.

d. The name of each output and push button shall be labelled on the panel.

e. A legend is to be laser etched to show the meaning, and wave form, of each flashing diagnostics indication.

f. All components on the front panel should be rated for IP67 or IP68.

g. All LEDs and Pushbuttons are to use screw type terminals.

h. All connections to the panel are to be insulated so that water or condensation cannot create a short circuit to the panel.

i. The panel shall be mounted inside a location case or annexure box.

j. The installation of the panel should ensure that rain while it is being used, or condensation while it is not, cannot cause water ingress on any other electronic or water sensitive components of the level crossing.

k. All pushbuttons, especially the Data Change pushbutton, are to be protected from accidental activation.

l. The mechanical design of the panel is approved by ARTC local signal maintenance engineer prior to fabrication. A concept layout for this panel is shown below, where red lines indicate the laser or water cut pattern. The push button (PB) and LED mounting holes are also required to be laser or water cut.

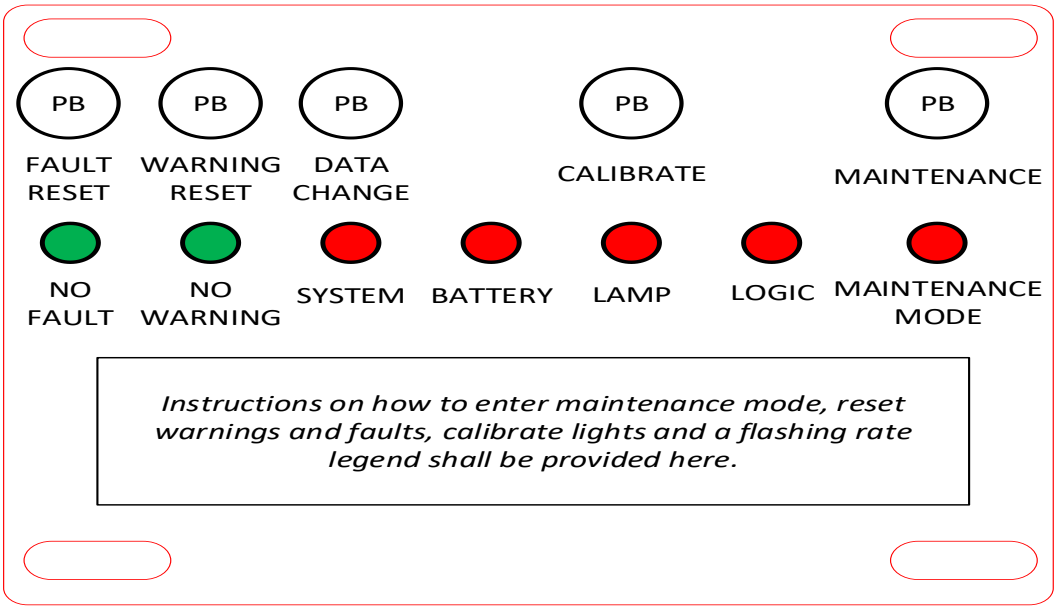

Figure 1 - Local Maintenance Panel Concept Layout

6.5 Installation and mounting

a. The installation and mounting requirements in the HIMA HIMatrix Compact Systems Manual are to be adhered to.

b. To ensure efficient cooling HIMA devices must maintain:

   i. A clear distance of at least 100 mm above and below the devices; and

   ii. A clear distance of at least 20mm to the left and right of the devices.

c. The ventilation slots of the housings must not be obstructed.

d. HIMA devices are to be mounted horizontally.

e. Mechanical coding pins shall be used for all HIMA I/O plugs and sockets. Standard coding pin configurations, provided by or developed with by ARTC, are to be used for each HIMA unit type, such that consistent of coding of ARTC's HIMA units can be maintained for each type.

6.6 Power Supply Requirements

a. The HIMA equipment's 24V DC power supply shall be:

   i. Electrically isolated from all other equipment.

   ii. Supplied by a suitable isolating DC to DC converter.

   iii. Isolated from earth.

   iv. Isolated from all other signalling busbars, with a separate busbar for hardwired inputs into the Level Crossing monitor.

   v. The level crossing monitor and its power supply are to have a breakdown voltage to earth of greater than 500 Volts DC.

   vi. The power supply must be smoothed. Any ripple must be confirmed to be within the limits allowed by each HIMA device.

vii. Meet the requirements of the HIMA manual.

b. The HIMA's 24V DC power supply shall be monitored by an Earth Leakage Detector.

c. The HIMA H 7013 24Vdc external surge filter is required on the HIMA device's 24Vdc bus, unless:

viii. An approved surge absorber from another manufacturer if used, which provides equal or better protection and filtering and is rated for at least -20°C to 70°C operation; or

ix. The HIMA is supplied from an internal 24Vdc bus, with no external circuits fed from that bus, and the DC to DC converter supplying that bus, filters the power supply with equivalent or better protection and filtering.

6.7 Remote Monitoring

6.7.1 Remote Level Crossing Monitoring Workstation

a. A remote level crossing monitoring workstation(s) shall be used for the centralised monitoring of the level crossing warning, alarm status and retrieve event logs.

b. The indications on the remote level crossing monitoring workstation shall relate to the level crossing maintenance panel indications. However, separate warning (yellow) and alarm (red) indications shall be provided for the following status indications:

a. System;

b. Battery;

c. Lamp, and;

d. Logic.

c. Alarms shall remain active and be repeated and/or escalated until the alarm has been acknowledged.

6.7.2 Remote Maintenance Workstation

a. A remote Maintenance Workstation with a SILWorX license, for remote access to the HIMA units via SILWorX, and a web browser, will also be provided to allow for remote diagnostics. The Maintenance Workstation will also allow for remote data changes, providing the local Data Change button is pressed on-site.

b. A dedicated programming port shall be provided on the network router in the level crossing monitor's locations. This port shall be a secured layer 2 VPN connection, which is only used when a HIMA unit needs to be re-programmed remotely.