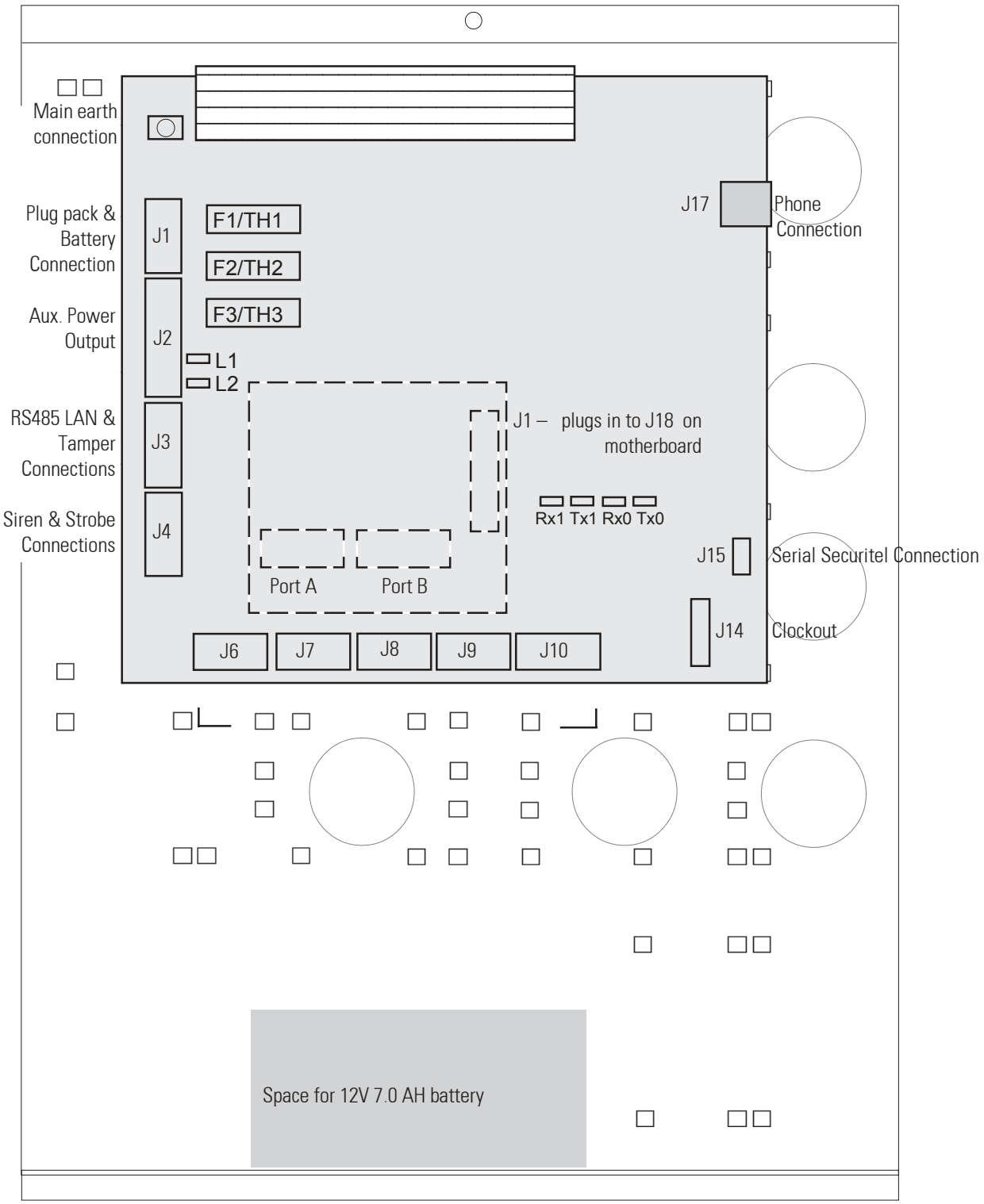
GE Interlogix

Version 8 Challenger Panel TS0816

Installation and Quick Programming Guide

Diagram : Challenger panel with major connection points



Note: *This equipment must only be installed and serviced by professional qualified personnel.*

Contents

Mechanical & environmental specifications

Enclosure dimensions:	360mm long, 260mm wide and 82mm deep.
Minimum clearance between equip. enclosures:	50mm (between equipment vents)
Minimum clearance between encl. & side wall:	25mm
Storage temperature:	-20 degrees C to +80 degrees C.
Operating temperature:	0 degrees C to +50 degrees C.
Humidity:	95% Non condensing

Note: Units should only be used in a clean environment and not in humid air.

LEDs

L1: **Slow flashing** indicates the panel is operational. (Microprocessor is running)
L2: Factory diagnostic use only.

Rx1: **Flashing Rx1** LED indicates remote units (RASs & DGPs) replying to polling.
Tx1: **Flashing Tx1** LED indicates Challenger panel is polling remote unit/s.
The Tx1 LED should always be active.

Rx0: **Flashing Rx0** LED indicates data being received from device connected to the Line (J17) (remote monitoring station or dial-up modem) or J15 Serial Port (Securitel interface or PC).

Tx0: **Flashing Tx0** LED indicates data being sent from the Challenger to a device connected to the Line (J17) or J15 Serial Port.

Parts list

The checklist below details all the items included in your Version 8 Challenger Panel and the installation kit.

1	x	V8 Challenger panel in metal enclosure	☐
1	x	16 Volt AC plug pack	☐
1	x	V8 Challenger installation guide	☐
1	x	V8 Challenger user guide	☐

Installation kit

1	x	tamper switch	☐
6	x	M3 screws	☐
6	x	spring standoffs	☐
1	x	1K 1/4 watt resistors	☐
17	x	3-way plug-on screw terminal connectors	☐
3	x	2-way plug-on screw terminal connectors	☐
1	x	red battery lead with QC terminal	☐
1	x	black battery lead with QC terminal	☐
40	x	10k 1/4 Watt resistors	☐

Cover

The Panel cover can be removed by unscrewing the four Allen head bolts securing it.
Note: When removing the cover after system is installed, be aware that tamper alarms are fitted to detect cover removal and the removal of the base from its mounting surface.

Mounting

The unit is mounted via screws or bolts through the 4 mounting holes in the base.

Ensure that the unit is mounted on a flat, solid, vertical surface such that the base will not flex or warp when the mounting screws/bolts are tightened.

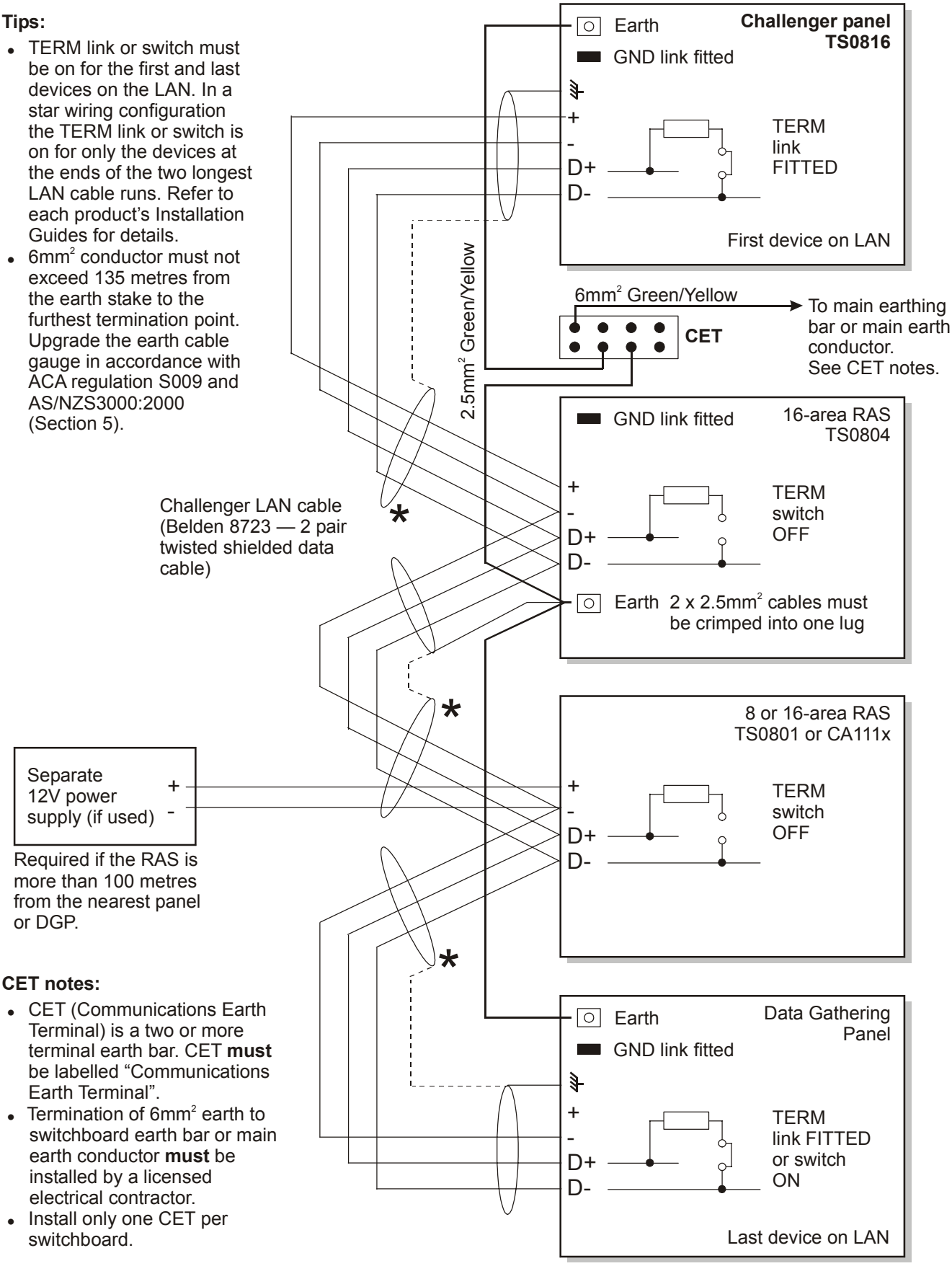
- 50mm clearance should be allowed between equipment enclosures mounted side-by-side and,
- 25mm allowed between the enclosure and the side wall.

LAN System & Protective Earth Connection Block Diagram

Be sure to read the protective earthing system recommendations first!

Tips:

- TERM link or switch must be on for the first and last devices on the LAN. In a star wiring configuration the TERM link or switch is on for only the devices at the ends of the two longest LAN cable runs. Refer to each product's Installation Guides for details.
- 6mm^2 conductor must not exceed 135 metres from the earth stake to the furthest termination point. Upgrade the earth cable gauge in accordance with ACA regulation S009 and AS/NZS3000:2000 (Section 5).

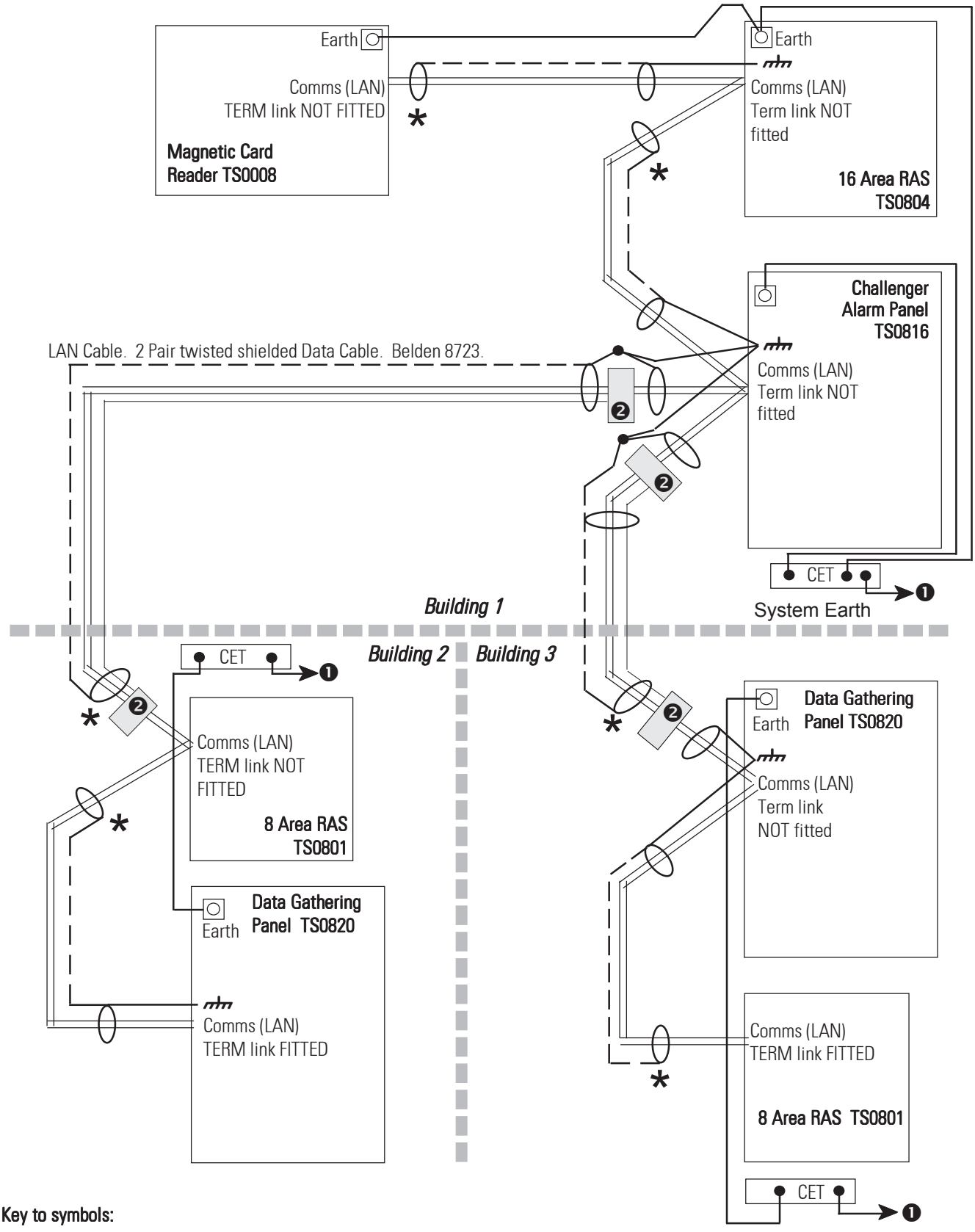


CET notes:

- CET (Communications Earth Terminal) is a two or more terminal earth bar. CET **must** be labelled "Communications Earth Terminal".
- Termination of 6mm^2 earth to switchboard earth bar or main earth conductor **must** be installed by a licensed electrical contractor.
- Install only one CET per switchboard.

* The data cable shield is **not** connected to earth at this end. The data cable shield is connected to earth at one end only.

LAN system & earth connection block diagram — Multiple Cable Runs



Key to symbols:

❶ Main/Sub electrical switchboard earth bar

❷ = TS0893 LAN isolation

✱ Shield of Data Cable NOT connected at this end.

LAN cable: 2-pair twisted shielded data cable, Belden 8723

See also: **LAN** & **Earthing** details on page 7 & the detailed diagram on page 5.

LAN connection

The LAN is used to connect Data Gathering Panels (to provide extra inputs) and Arming Stations to the Challenger panel. Remote units can be up to 1.5 km from the Challenger control panel.

Arming stations and Data Gathering Panels must be connected via a 2-pair twisted-shielded data cable from the LAN connection. (Belden 8723 is recommended)

The shield of the data cable connected to the Challenger panel should be connected to earth at the Challenger and not connected at any other end.

It is recommended that where the distance between the arming station and the nearest device is more than 100 metres, a separate power supply be used to power the arming station.
To power the arming station, **do not** connect '+' from the LAN. Connect '+' of the local power supply to '+' on the arming station and connect 0 volts from the power supply **and** 0 volts from the LAN connection to the arming station terminal marked '-'.

See wiring diagrams on pages 5 & 6.

Protective earthing system — *recommendations*

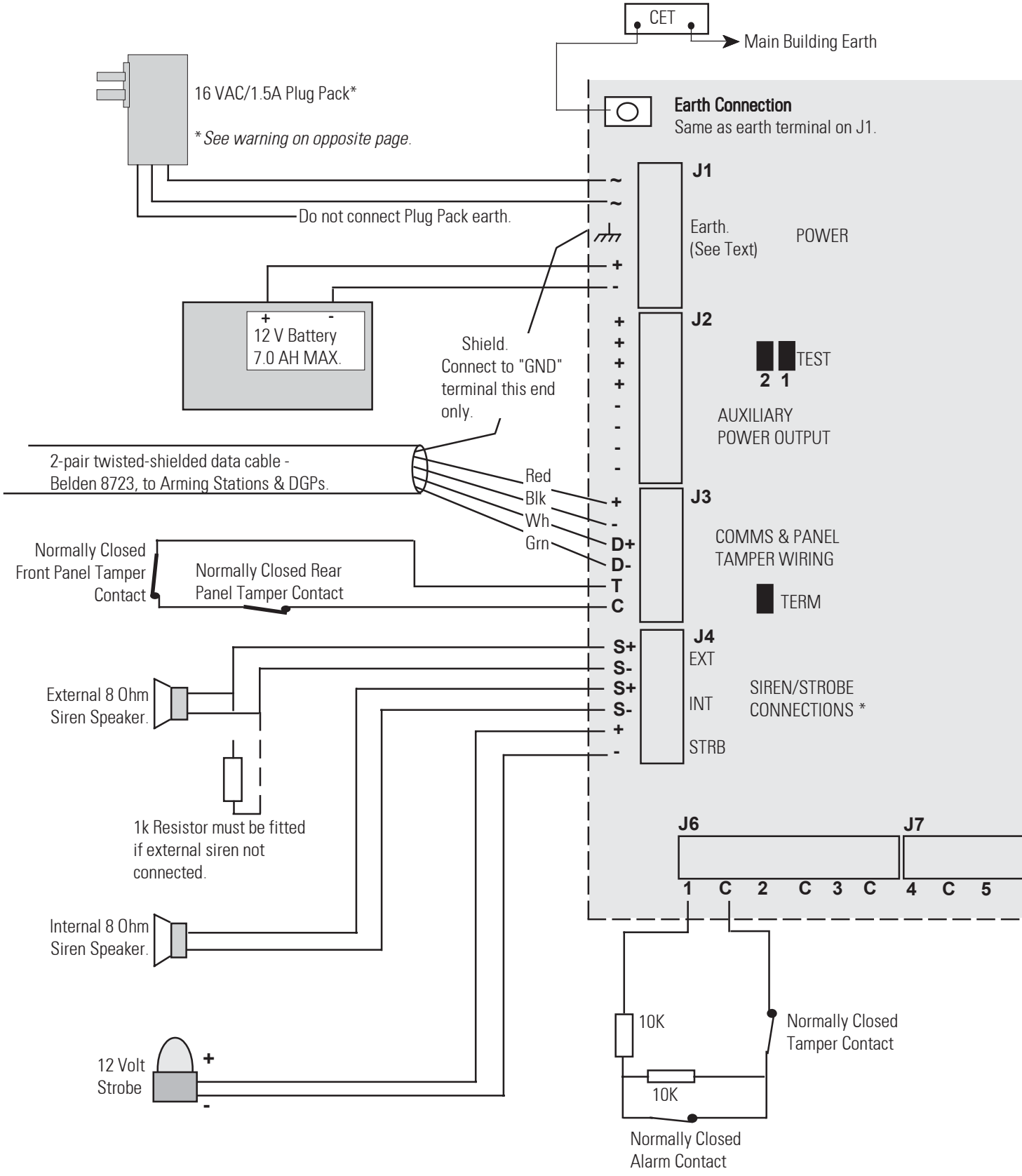
(The following recommendations are based upon Australian wiring regulations ACA AS/ACIF S009 Section 5 and AS/NZS 3000:2000 Section 5.)

- Challenger system equipment **with earth terminals** must be earthed via a Communications Earth Terminal (CET) by either connecting to the protective earthing system earth bar in the main or sub-electrical switchboard or, connecting directly to the main building earth conductor.
- All Challenger earth wiring must be Green/Yellow at least 2.5mm^2 or greater, to comply with Australian wiring regulations *(see wiring diagram)*.
- The device's "GND" link must remain fitted.
- **Do not** connect the plug pack earth to any device's earth terminal.
- This method of protective earthing is the only way to minimise earth potentials between any two Challenger products by using a common building earth system.

☞ **Tips**:
- **Do not** install multiple earth stakes in the same building (electrical installation).
- Install Challenger TS0893 LAN isolation devices between multiple buildings.

See wiring diagrams on page 5 & 6.

Challenger Alarm Panel Connection Diagrams



* See: Connection details on pages 10 & 11.

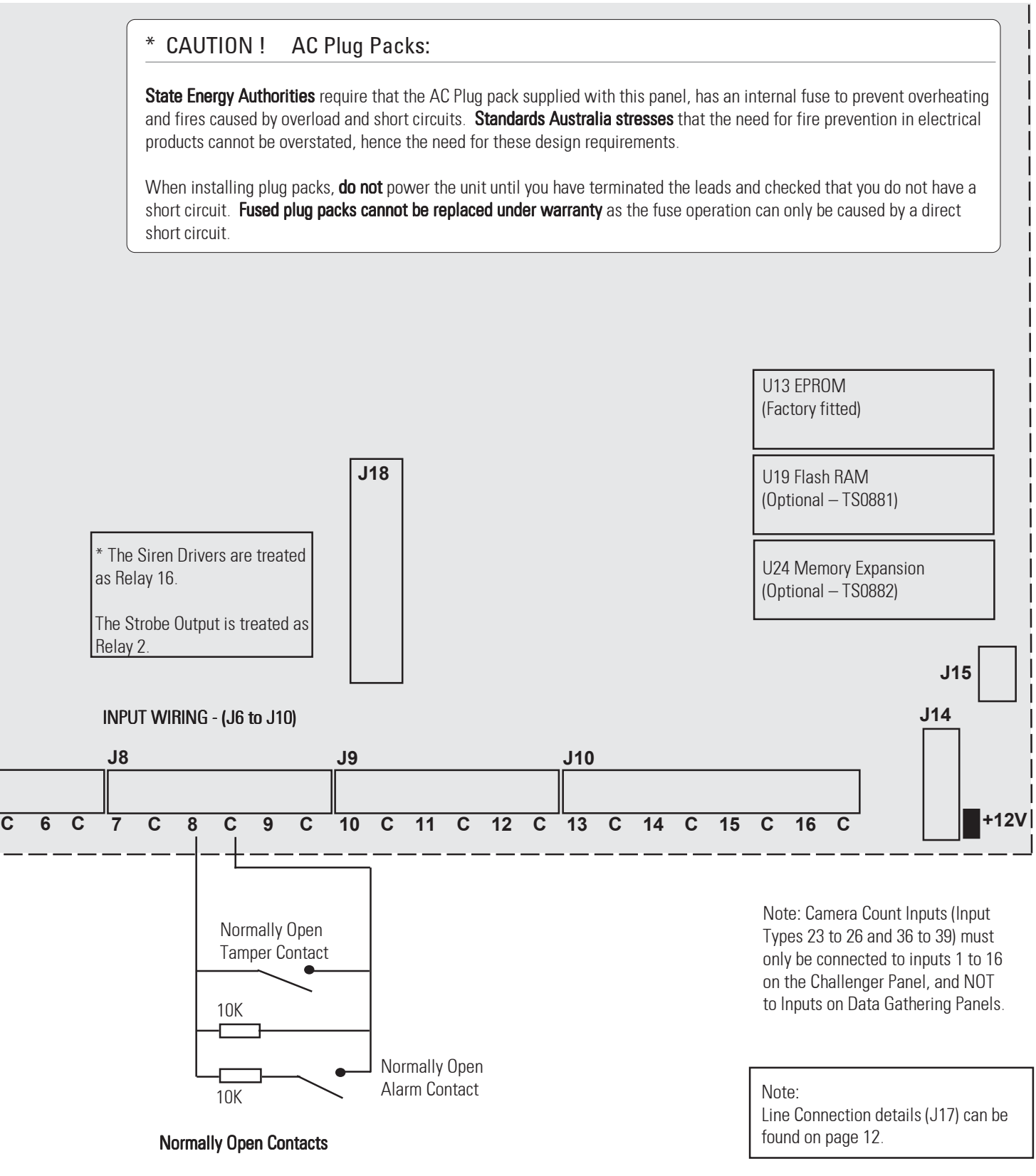
Normally Closed Contacts

Challenger Alarm Panel Connection Diagrams

* CAUTION ! AC Plug Packs:

State Energy Authorities require that the AC Plug pack supplied with this panel, has an internal fuse to prevent overheating and fires caused by overload and short circuits. **Standards Australia stresses** that the need for fire prevention in electrical products cannot be overstated, hence the need for these design requirements.

When installing plug packs, **do not** power the unit until you have terminated the leads and checked that you do not have a short circuit. **Fused plug packs cannot be replaced under warranty** as the fuse operation can only be caused by a direct short circuit.



Note: Camera Count Inputs (Input Types 23 to 26 and 36 to 39) must only be connected to inputs 1 to 16 on the Challenger Panel, and NOT to Inputs on Data Gathering Panels.

Note:
Line Connection details (J17) can be found on page 12.

Connections: 5mm plug-on screw terminals

J1 AC:
J1 Earth:

Connection of the 16 Volt, 1.5A, AC Plug pack supplied with the panel. *(See warning & connection diagrams on pages 8 & 9)*. Maximum current drawn by the panel with no peripheral devices fitted is 200mA.

Terminal for earthing. This terminal is connected to **LAN system earth**. (Shield of the LAN cable). *(See: diagrams on pages 5 & 6 & Earthing" details on page 7)*

J1 BATT:

Positive and negative connections to 12V sealed lead acid battery. (7.0 AH maximum)
(See connection diagram on page 8)

J2 AUX PWR:

+12 Volt DC auxiliary power output to supply detectors, etc. 700mA maximum including any current drawn by devices connected to the J3 LAN + terminal, the J3 LAN – terminal, and to the internal siren speaker.

J3 LAN:

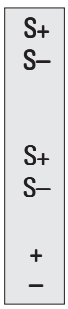
+12V DC supply conn. to remote arming stations. Max. current - see "AUX PWR". –ve DC supply connection to RASs & common 0 Volt connection of the RS485 LAN.

J3 LAN:

Data positive and data negative connection of the RS485 LAN. Remote units can be up to 1.5 kms from the Challenger control panel. *(See: Diagrams on pages 5 & 6 & "LAN connection" details on page 7)*

J3 Tamper:

Input and common connection for panel tamper switches. Short cct for seal. Open circuit for unsealed. (Must be sealed if not used). Can only be used with normally closed contacts such as the panel tamper switches.
(See connection diagram on page 8)



J4 EXT SIREN:

* Positive and negative connection to external 8 ohm siren speaker. A 1k resistor must be fitted across these terminals if the siren is not connected. The siren output is relay 16.
Max current: Ext. siren & strobe + is 700mA.

J4 INT SIREN:

* Positive and negative connection to internal 8 ohm siren speaker. The siren output is relay 16.
Max current: see "AUX PWR".

J4 STRB:

* Positive and active low connection for strobe switching. The strobe output is relay 2.
Max current: Ext. siren & strobe + is 700mA. *(See connection diagram on page 8)*

J6 to J10: Alarm Inputs 1 to 16

etc.

Require 10k End-Of-Line resistor for seal. 5k or 20k for unsealed.

Open or short circuit for tamper condition if "Input Tamper Monitoring" enabled in the system options.
(See connection diagrams on pages 8 & 9)

*** Strobe and siren limitations**:
The maximum current draw for the external 8 ohm siren and the strobe is 700mA.
The maximum current draw for the internal 8 ohm siren and any devices connected to J3 LAN + and - and the AUX power terminals is also 700mA.

Connections: – 5mm plug-on screw terminals

CLKOUT: J14 +12V DC Supply & Open collector OR data outputs; for connection to relay controllers. I.e. A single 4 Way Relay card OR 8 Way Relay and 16 Way Open Collector cards. TS0840 to TS0842 (V8 Relay cards) are connected with 10 way cable supplied. *(See V8 Prog. Guide Inst Menu Opt 7– Relay Controllers if 8 or 16 way cards used)*

Serial: J15

+12
RX
TX
0V

Interconnection facility for connection to Tecom Serial Securitel interface with cable supplied, OR other Serial Securitel interface via separate cable, OR to PC for temporary Upload/Download connection. *(See page 12 for wiring details, and V8 User Guide: User Menu Option 7– Service Menu).*

J17: Connection to Private or Exchange line via cable supplied. *(See LINE connection details on page 12)*

J18: Connection to optional Plug-on Printer interface (TS0094) or Computer & Printer interface (TS0091).

Links

TERM: The termination jumper link must be in if the panel is the first or last device on the LAN. If the system LAN is wired in a "star" configuration, the TERM link is only fitted on the devices at the end of the two longest LAN cable runs. I.e. In a Challenger system only two devices connected to the LAN can have the TERM link fitted. *(See: Diagrams on pages 5 & 6 & "LAN connection" details on page 7)*

WR & REQ: These links must not be fitted unless instructed to do so when installing certain interfaces.

TEST: 1 This link is used when resetting the Master installer code. Fit the link, press the "*" key on the master codepad, remove the link and press "Enter".

2 This link is for factory use only.

+12V Remove this link if relay card/s connected to J14 (CLKOUT) is powered from a separate 12 Volt power supply source.

Over-current protection

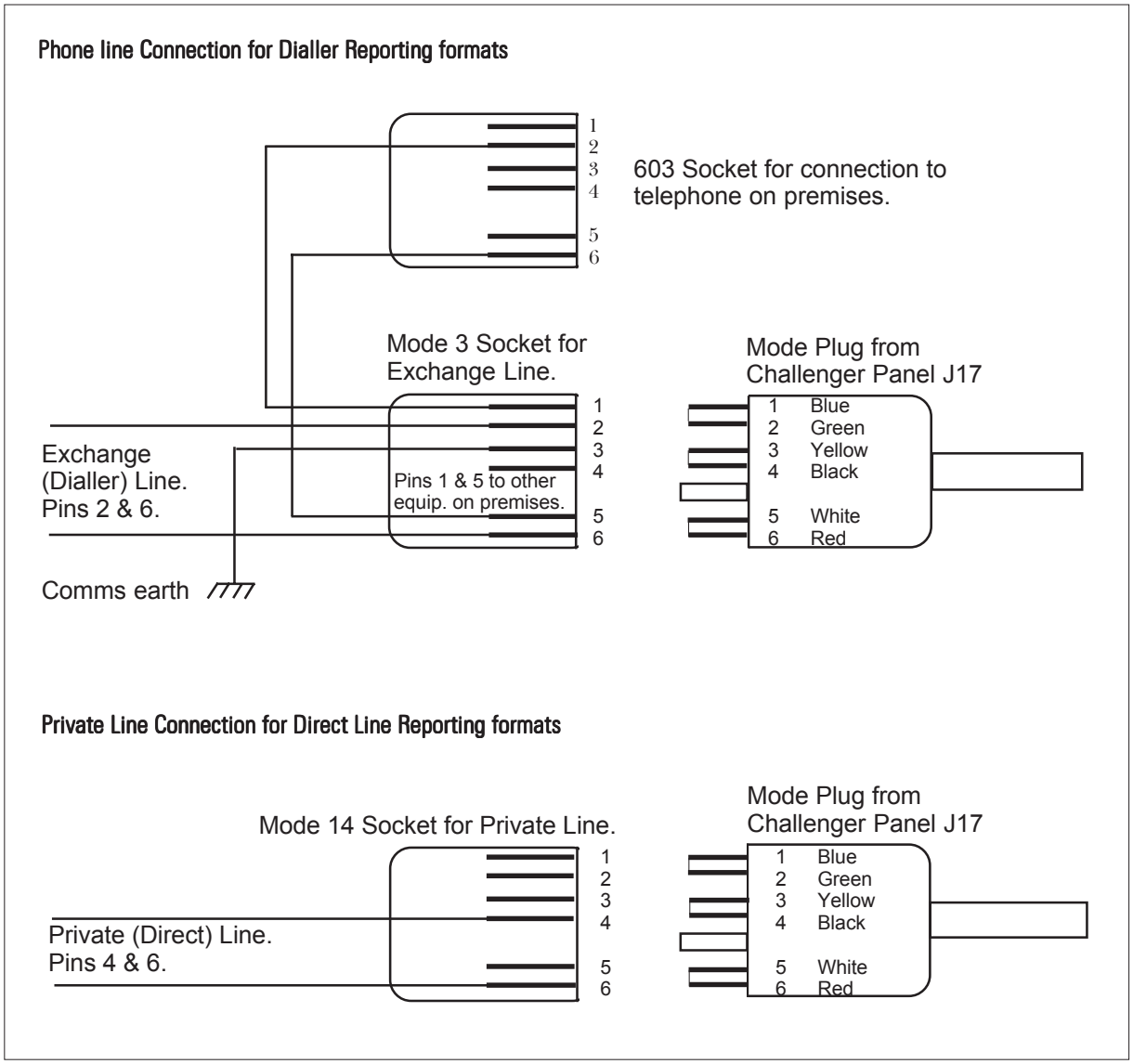
CAUTION! PTCs can become very hot when approaching their current limit. Avoid touching these devices.

TH1: 1.5A PTC (Thermistor) to limit current under fault conditions when unit is running on the battery. Will automatically reset when the fault condition is removed.

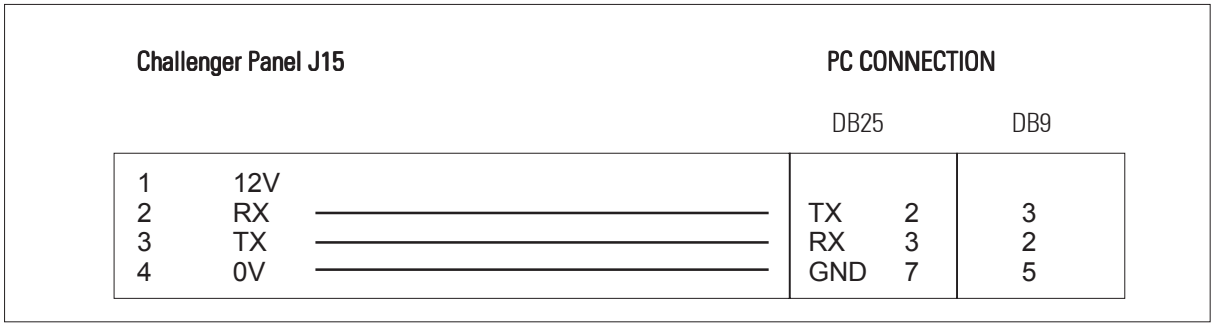
F2: 1A Fuse to limit current for Auxiliary O/P (J2), Comms+ (J3), and Internal Siren (S+, J4). Maximum power budget should not exceed 700mA.

F3: 1A Fuse to limit current for External Siren (S+, J4) and Strobe (STRB+, J4). Maximum power budget should not exceed 700mA.

Line Connections — Mode Plug & Socket (J17)



Temporary Service Connection – Serial Port (J15)



Power up

When installation is complete, power can be applied to the Challenger System. On initial power-up:

- The V8 Challenger Panel's LEDs should indicate as follows;
  - L1 – Slow Flashing.
  - L2 – Off.
  - Tx1 – Rapid Flashing
  - Rx1- – Rapid Flashing (If RAS 1 connected & functional)

- The Master LCD Arming Station (RAS 1) should have all area LEDs ON and the LCD should display the name "GE Interlogix" followed by details of the Arming Station software version. An 8 Area LCD RAS will also prompt you to Press the * key.
  Pressing the "*" key followed by <ENTER>, will bring up the normal alarm display shown below, unless there is a system condition which would be displayed on the top line.

  There Are No Alarms In This Area
  Code:

  If the Master RAS powers up with no LEDs ON and no LCD display then the RAS must not have power applied.
  If the Master RAS powers up with all LEDs flashing, the LCD reads "Your System Needs Service" and the Alarm Panel conditions as described above are correct, then the LAN cabling must be faulty, or the Arming Station address has been incorrectly set. (RAS 1 = All DIP switches OFF or All links bridged)

- The system must be disarmed before it is possible to use the Installer Menu.
- **To disarm the system**: **4 3 4 6** (Master PIN code) **<OFF>** followed by **0** (Select all areas) **<ENTER>**
- If you are unable to disarm the system using the Master Code and <OFF> key, then it may be necessary to Reset the Master Installer Code. Fit a jumper link to "TEST 1" on the Challenger panel, press the "*" (Menu) key on the master codepad, remove the link and press "Enter". This will reset the Master Installer Code and Arming Station 1 details to factory default. Details on how to access the Installer Menu are found on the following page.

Panel Programming Factory Defaults

The Challenger panel programming is set to factory defaults to make the initial setup easier:

- **Inputs 1 to 16** are set to Type 2 - Secure Alarm with the SIREN Event flag & Event flag 2 (Strobe) set to YES.
- All **Area Databases** have Exit time of 60 secs & Entry time of 30 secs, and the SIREN Event flag set to 1.
- **Arming Station 1** is programmed to be polled, and is assigned Alarm Group 2 (Master RAS or Door).
- There are 29 preprogrammed **Alarm Groups.** (See the Programming Guide for details)
- Most of the **Timers** have a default value programmed. (See the Programming Guide for details)
- In **Communication Options**, Area 1 is listed for Open Close reporting. (Reporting format is disabled)
- **Relay Mapping:** Relay 2 (Strobe O/P) is mapped to Event Flag 2.
  Relay 16 (Siren driver) is mapped to Event Flag 1.
  The 16th relay assigned to each DGP (DGP Siren drivers) are mapped to Event Flag 1, i.e. Relay 32, 48, 64, etc.

Installer Menu

Access the installer menu via the user menu, option 19.

The system **must be disarmed** before it is possible to use the installer menu.

To disarm the system:
4 3 4 6 (Master PIN code) **<**OFF**>**
0 (Select all areas) **<**ENTER**>**

To display menu option 19 on the user menu the alarm group of the user code must allow it.

- The *master installer* is user number 50
- The default *master PIN code* (user 50) = 4346
- The *master PIN code* should be changed.
- The alarm group assigned to *user 50* should never be changed.

Menu Options

The following pages provide a listing and brief description of the programming options available in the Version 8 Challenger installer menu.

Complete programming details and blank programming sheets are available in the Challenger Version 8 Programming Guide.

User Menu Options

The following user menu options may also need to be used when programming your Challenger system.

Test Input	User Menu Option 12
Program Users	User Menu Option 14
Program Time & Date	User Menu Option 15
Door & Floor Groups	User Menu Option 20
Holidays	User Menu Option 21

The programming details for all user menu options are available in the Challenger Version 8 User Guide supplied with every Version 8 Challenger Panel.

To access the installer menu:

1. The display will show:

```
There Are No Alarms In This Area
Code :
```

Menu * ~ Press

2. The display will show:

```
To Access Menu Enter Code
Code:
```

4346 Enter ~ Enter Master code.

3. The display will show:

```
"0"-Exit, "ENTER"-Down "*"-Up
0-Exit, Menu:
```

19 Enter ~ Enter Installer menu option number.

4. The display will show:

```
Install Menu
0-Exit, Menu:
```

Enter ~ Scroll forwards through the menu options.

or ***** ~ Scroll backwards through the menu options.

or **0 Enter** ~ Return to the User Menu.

or **? Enter** ~ Select a menu option.

Programming Sequence

When setting up a basic system, program the records in this order:

1. Fill-out the programming sheets (rear of the V8 Challenger Programming Guide)

2. **Defaults –** Installer menu option 14, default to STD All (**99 Enter)**.

3. **Communication Options –** Installer menu option 9.

4. **System Options –** Installer menu option 7

5. If any words required for the names of inputs, areas etc. are not recorded in the Word Library:
   Text Words – Installer menu option 10.

6. If functions available to users are to be restricted by time:
   Time Zones – Installer menu option 13.
   Holidays – *User menu* option 21.
   Also see **Time Zone to Follow Relay –** Installer menu option 22.

7. **Area Database –** Installer menu option 2 for all areas in the system.

8. **Alarm Groups –** Installer menu option 5. To specify the security requirements (area/s, level of control and menu options available) for groups of users and for arming stations.

9. **Input Database –** Installer menu option 1 for all inputs in the system.

10. If the system has more than 16 inputs :
    Data Panels – Installer menu option 4.

11. If the system has more than one arming station :
    Arming Stations – Installer menu option 3.

12. **Times –** Installer menu option 6.

13. **Map Relay –** Installer menu option 16.

Installer Programming Options Summary

1. Input Database

Records parameters of inputs

Inputs 1 to 16 are defaulted to Type 2 - Secure alarm. All other inputs have no default type programmed.

Input Number	–	1 to 256 (Depends on the number of DGPs in the system)
Input Name	–	Name/description of input.
Input Type	–	Number and name for a pre-defined input type which determines the input function.
Reporting	–	Method of reporting to the monitoring company. (Contact ID Type)
Area Assignment	–	List of areas assigned to the input. (Or Alarm Group on Area Control input types)
Test Option	–	Determines testing procedure.
Event Flags	–	Records the event flags which can be activated by the input.

Selected Event Flag Secure	Alarm x 8 Camera
Siren	Access Alarm x 3
Console Warning	24 Hour Alarm

Make all Events 24 Hr	–	Determines active period of event flags assigned to the input-Access/Secure.
Print I/P when unsealed	–	Allows printout of input condition to be enabled/disabled.

2. Area Database

Records parameters of areas

Area Number	–	1 to 16.
Area Name	–	Programmable text for easy area recognition.
Exit Time	–	Time allowed between exit and area arm before an alarm is activated.
Entry Time	–	Time allowed between entry and area disarm before an alarm is activated.
Event Flags	–	Records event flags which can be activated by conditions in the area or condition of inputs with this area assigned to them.

Siren	*Secure Alarm*	*Entry Timer*
Accessed	*Access Alarm*	*Warning (User Cat expiry)*
Unsealed	*Local Alarm*	*Camera*
Isolate	*Exit Timer*	*Pre-Alarm*

Out of Hour Timezone	–	Timezone which will cause an alarm if area is accessed out of specified hours.
Area Disarm Time	–	Records the Timed Disarm period for individual areas. (Overrides User Category timers)

3. Arming Stations

Records details of arming stations.

Arming Station number 1 is programmed to be polled by default and is assigned
Alarm Group 2 – Master RAS or DGP.

RASs to be polled	–	Records the number of each arming station to be polled by the main control panel.
Area Alarm Group	–	Alarm group to determine the areas which can be controlled by the arming station.
Menu Alarm Group (Optional)	–	Alarm group to determine the areas which can be accessed via the arming station when using menu options.
Door Function	–	Assign event flag to allow arming station to be used to open a door.
Relay Group assigned	–	Assign relay group to enable Output on RAS.
LCD Arming Station	–	Defines type of arming station.

3. Arming Stations *cont'd*

Toggle Keyboard Control	–	Disables use of OFF or ON control when arming/disarming at the arming station.
ENTER key Opens Door Only	–	Prevents ENTER key from being used for Alarm functions. (Toggle Keyboard Control must be set to NO)
Door Event Flag on Alarm Codes	–	Determines if Alarm Codes can be used for door function.
Display Shunt on LCD	–	Allows Shunt functions to be displayed on LCD RAS.
Disarm/Arm using one key	–	Option for use of special 16 Area Membrane RAS.
Cards Auto Disarm	–	Allows Cards to Disarm without using OFF key.
Card Always Disarm/Arm	–	Allows Cards to Arm and Disarm without using ON/OFF keys.
Reset without Code	–	Allows user to reset alarms without PIN.
Restrict User Categories to Disarm	–	Restricts User Category functions to disarm only.

4. Data Panels

Records details of Data Gathering Panels.

To be Polled	–	Records the number of each DGP to be polled by the main control panel.
DGP Type	–	Records the type of DGP being polled. (Standard, Door Controller or Lift Controller)

5. Alarm Groups

Records parameters of each alarm group.

Alarm Group Number	–	1–128 (1–10 hardcoded, 11–29 preprogrammed).
Alarm Group Name	–	Name of the alarm group.
Areas Assigned	–	Areas where the alarm group can control functions.
User Alarm Group	–	Indication of whether alarm group can be assigned to a user.
Alarm System Control	–	Allow alarm system control functions.
List Areas	–	User is prompted with List of areas on LCD during arm/disarm.
Keyboard Duress	–	Allows duress facility to be activated by a code.
Reset System Alarms	–	Allows the alarm group to reset latching system alarms.
Disable Auto De-isolate	–	Disables Auto De-isolate function.
Arm and Reset Only	–	Restrict alarm system control to arm and alarm reset only.
Disarm Only	–	Restrict alarm system control to disarm only.
Alarm Reset Only	–	Restrict alarm system control to alarm reset only.
Auto Isolate Unsealed Inputs	–	Isolate unsealed inputs when arming.
Forced Arming when Inputs Unsealed	–	Arm with unsealed inputs.
Prevent Forced Disarming	–	Prevent disarming with unsealed inputs.
Modem Access	–	Allows access to Challenger Panel via dial-up modem.
User Category 1	–	Link User to Category 1.
User Category 2	–	Link User to Category 2.
User Category 3	–	Link User to Category 3.
User Category 4	–	Link User to Category 4.
User Category 5	–	Link User to Category 5.
User Category 6	–	Link User to Category 6.
User Category 7	–	Link User to Category 7. (Dead Man Alarm)
User Category 8	–	Link User to Category 8. (Counter)
No Arming if User Category not Timing	–	Prevent user category timer if area disarmed without timer running.
User Menu Options	–	Allow access to user menu options – individually.
Time Zone	–	Allocate timezone to control when alarm group is enabled.
Alternate Alarm Group	–	Allocate alarm group to apply when timezone for this one is not valid.

6. Times

Records time values applicable to some timed system functions.

User Category 1 to 7	–	Individual times for user categories 1 to 7 function of Time Disarm.
User Category 8	–	Time for user category 8 function of Time Disarm. (Category 8 time must not be programmed if used for Counter option.)
Access Test	–	Time that an access test runs.
Secure Test	–	Time that a secure test runs.
Warning Time	–	Time provided as a warning before group timer expires or before test procedure expires.
Delayed Holdup	–	Time between delayed type input being activated and an alarm being reported.
Suspicion Time	–	Time that a camera continues to operate after a suspicion input seals.
Service Isolate	–	Time applicable to enable service.
Local Alarm Reminder	–	Time between alarm and re-alarm for local alarms.
Individual Input Test	–	Time that a test on an individual input runs.
Door/s Unlock Time	–	Time that door locks activate.
Tester Event Flag	–	Time that tester event flag activates for during secure test.
Siren Time	–	Time that the internal siren drivers operate.
Mains Fail Time	–	Time allowed before the Panel reports Mains Fail to the Remote Monitoring company.

7. System Options

Records system options.

Areas Selected to total Disarm	–	Allow Access Local/Secure Alarm inputs to be totally disarmed.
Film Low Level	–	Frame count number used to indicate low film.
Film Out Level	–	Frame count number used to indicate no film.
Test Mode	–	Determines if/when secure and access tests run automatically.
Relay Controllers	–	Number of relay controllers fitted to the main panel.
Event Text	–	Text shown on LCD when event text inputs activated.
Alarm Prefix	–	Number of Alarm Prefix digits for defining Door and Alarm codes.
Time Before LCD Text Rotation	–	Option to allow the period before LCD Text begins to rotate, to be altered.
LCD Text Rotation Speed	–	Option to allow the rotation speed of LCD text to be altered.
Input Tamper Monitoring	–	Indicate if input alarm is tamper alarm.
Automatic De–Isolate	–	De-isolate input when area accessed.
Input Display	–	Display one input at a time for user functions.
Name File	–	User PIN to have a record of user name.
System Alarms set Siren/Strobe	–	System alarms on Panel & DGP (Tamper, Mains fail etc.) activate Siren & Strobe.
System Alarms Latch	–	System Alarms are latching and need to be reset with code.
Siren Testing	–	Sirens operate when secure test is started.
Disable "0 Enter" for Camera Reset	–	"0 Enter" disabled for use to stop cameras operating.
Disable Auto Insert of User Categories	–	Disables the ability to treat areas as vaults.
Disable Area LEDs that don't Report	–	Disables LEDs for areas not reported on.
Disable Code from Displaying	–	Disables codes from being displayed when being programmed. (In User Menu Opt. 14)
Disable Flashing Area LEDs	–	Disables the flashing of area LEDs when an alarm condition occurs.
Dual Custody	–	Two users are required to enter their PIN to enable user programming.
Display Alarm Instant	–	Enables alarms to be displayed instantly on the LCD Arming Station/s
Sirens Only after Report Fail	–	Enables Sirens to be disabled unless Panel fails to report.
Financial Institution Options	–	Enables three special options specific to financial institutions.
Display User Flags	–	Enables the special User Flags to be displayed when programming Users. (User Menu Opt. 14)

9. Communication Options

Records the details of the communications link between the Challenger panel and the remote monitoring company.

PABX access code	–	Number/s (if required) for access to PABX.
Telephone Numbers	–	Numbers used for Dialler reporting formats, "Dial for Service", "Callback" and "Computer via dialler".
Account Numbers	–	Unique number/s to identify the system to the monitoring company. (Dialler formats)
Format	–	Reporting format type. E.g. Direct Line, Dialler formats, Securitel etc.
Direct Line Address	–	System identification number when communicating via a direct line.
Computer Address	–	System identification number when connected to a Central Management System.
Areas to Report On	–	Areas where arm/disarm reported to monitoring company.
Securitel Hard ID	–	Address of Securitel Interface Unit.
Encryption Key	–	Enables Data encryption key to be programmed for Tecom Direct Line format.
Number of Rings	–	Number of rings in Callback request call.
No. of Calls before answer	–	Number of calls before panel answers Callback request .
Dialler Test mode	–	Determines testing procedure for communications.
Test Call Time	–	Records time of day when test call will be activated.
Buffer Size	–	Defines Transmission Buffer size for Ademco format diallers.
Alarm Reporting	–	Report multi break alarms.
Alarm Restoral	–	Report multi alarm restorals.
Always Terminate Direct Line	–	Allows Direct Line connection to be permanently loaded (direct line only).
Remote System Control	–	Allow system control via remote monitoring company (direct line only).
Open/Close Reporting	–	Defines condition required to report armed/disarmed.
Tone/Decadic dialling	–	Defines the panel's dialling format.
Disable Isolates triggering Dialler	–	Disables Isolates from triggering the dialler to report. (Isolates will be reported to the monitoring company with the next report)
Answering machine defeat	–	Enables the Challenger Panel to connect instantly when being accessed via dial-up modem.
Enable PSTN Line Fault Monitor	–	Enables the Challenger Panel to monitor the integrity of the dialler line.
Computer Port connected via Modem	–	Allows Challenger Computer I/face to be linked to System management computer via modem.
Dial Alarm Events to Computer instantly	–	Enables the Challenger Panel to dial through Alarm Events to the computer instantly.
Dial Access Events to Computer instantly	–	Enables the Challenger Panel to dial through Access Events to the computer instantly.
Dial Events via Computer Port	–	The Challenger Panel is reporting to the computer via the Dial-up modem on the Computer Port
Dial Events via On-board modem	–	The Challenger Panel is reporting to the computer via the On-board modem.

10. Text Words

Used to program additional words unique to this system and in addition to existing word library.

Word Number
Word

11. Version Number

Records software version and database revision numbers.

12. Lamp Test

Turns LEDs on or off to enable testing.

13. Time Zones

Records parameters of time zones.

Timezone Number	–	1 to 24
Times	–	Start and end time.
Days	–	Days of week/holiday that timezone is valid.

14. Reset Defaults

Resets system to various default settings and allows history to be cleared.

15. User Category Data

Records user category parameters.

User Category Number	–	1 to 8.
User Category Name	–	Name of the User Category.
Areas to Time On	–	Areas programmed for Time Disarm.
Areas to Arm/Reset	–	Areas programmed for Arm/Reset.
Alternates	–	Alternate areas to time on/arm/reset for alternate alarm groups.

16. Relay Mapping

Records details of settings which control the activity of relays.

Relay Number		
Event Flag Number	–	Number of the event flag which will activate the relay.
Timezone	–	Controls times that relay is active/inactive.
Active/Inactive during Timezone	–	Determines the effect of the timezone.
Relay is Inverted	–	Reverses the logic to the relay.

17. Arm/Disarm Timers

Relates a timezone to an access level to facilitate arm/disarm in accordance with a timezone.

Program Number	–	Number for each record.
Timezone	–	Number of timezone.
Alarm Group	–	Number of the alarm group.

18. Areas Assign to Vaults

Assign areas to be treated as vaults.

By using a special programming procedure a user category timer will start when all the vault areas are armed. When the timer expires, a non-vault area linked to the vault areas will automatically arm. *(See V8 Prog. Guide)*

19. Area Linking

Links an area to other areas to enable common control.

20. Site Number

Records up to two site identification numbers ("Site Codes" or "Facility Codes") and provides the option of programming two card offset values used in access card codes for readers connected to the Challenger LAN.

21. Input Shunts

Records details of a shunt procedure.

Shunt Timer Number	–	Number of the shunt timer. 1 to 16
Input Number	–	Number of the input which is shunted.
Relay Number	–	Number of the relay connected to the shunt timer.
Shunt Time	–	Time that the input will be shunted.
Shunt Warning Time	–	Time that the Shunt Warning will be activated before Shunt timer expires.
Shunt Event Flag	–	Event Flag number that will be activated during the Shunt time.
Shunt Warning Event Flag	–	Event Flag number that will be activated during the Shunt warning time.
Door Open Command	–	Determines how the shunt timer will be activated.
Door Shunted in Access	–	Allows the shunt to operate in access.
Door Shunted in Secure	–	Allows the shunt to operate in secure.
Cancel Door Event Flag	–	Door event flag will be cancelled when shunt timer seals.
Input Holds Event Flag at 2 Seconds	–	Allows delay in cancelling door event flag – for magnetic locks and drop bolts.
Entry/Exit Shunting	–	Allows Shunted input to be treated as Entry/Exit point.
Report Door Open/Close	–	Allows input unsealed/sealed to be logged on printer as door open/close.

22. Timezone to Follow Relays

Used to program a timezone to be active only when a relay is active.

Timezone Number
Relay Number

23. Poll Errors

Displays errors in communication between Challenger and units connected to it.

24. Download

Allows User, Door/Lift Group, Timezone, and Holiday data to be downloaded to Intelligent DGPs, i.e. Door Controllers and Lift Controllers.

Display Status	–	Displays status of Download operation.
Down Load All	–	Provides options for downloading of specific databases .

25. Display Card

Displays the Site Code and Card I.D. Number of the last card read by a reader connected to the Challenger LAN, i.e. Doors 1 to 16.

26. Edit

Do not use. Diagnostic Facility.

27. Tecom Address Mapping

Displays the Physical Address and Reporting Address of Tecom Direct Line Panels.

28. Remote Controllers

Allows access to Intelligent Door and Lift Controller DGP Programming. Refer to Separate "V7/V8 4 Door Controller" or "V7/V8 Lift Controller" Programming Guides.

29. Security Password

Records the Security Password required to access the Challenger Panel via any Computer Protocol, e.g. Challenger Management software.

30. Printer

Records parameters of printer output, i.e. "Port B" on the TS0091 or TS0094 interface module if fitted.

Enable Real-time Printer	–	Enables printer output to print in real-time. (If set to NO, "Print History" must be used)
Print Alarm Events	–	All alarm system events will be printed.
Print Access Control Events	–	All Access Control events will be printed.
Dump Print Data Outside	–	Option for Printer to operate outside the timezone instead of during Timezone the timezone.
Print During Timezone	–	Timezone during which printer will be active.
Printer Options	–	Printer Baud rate and Data format options.

31. Battery Testing

Records parameters of Auto Battery Test options and allows manual testing of battery.

Test mode selection	–	Enables Auto Battery Test and selects frequency.
Start Battery Test	–	Specifies time of day when battery test will start.
Battery Test time	–	Specifies how long battery test is to run for.
Manual Battery Test	–	Allows manual testing of Challenger Panel and DGP batteries.

32. Custom Message

Records 32 Characters of customised Text which will be displayed on the LCD Arming Station/s in place of the message "There are no Alarms in this Area"

33. Program Next Service

Records the date on which the next routine service call is due and the message to be displayed. The client will be prompted with programmable text to call the Security Company, via the LCD Arming Station/s.

34. Program Summary Event Flags

Records Event Flags assigned to system functions and system alarms.

Summary Event Flags – Records event flags which can be activated by conditions or faults in the system.

Mains Fail	DGP Isolate	Film Out
Low Battery	DGP Offline	Report Fail
Fuse Fail	RAS Offline	Testmode
Tamper	Duress	All Secured
Siren Fail		Console Trigger

35. Program Macro Logic

Records details of high level Relay and Event Flag logic programming.

Macro Logic Program Number	–	Number of the Macro logic program. 1 to 24.
Function	–	Selects the way in which the logic output will function.
Time	–	Records the period that the function will time for. (If a timed function selected)
Activate Event Flag or Input Number	–	Records the number of the Input or Event Flag that will be activated.
Logic Equation	–	Records up to 4 Logic Inputs (Event Flag or Relay Numbers) and whether each of those inputs performs an AND, OR, NAND or NOR function in the logic.

36. Radio Communications

Records details of the reporting parameters when the Challenger is communicating to the remote monitoring station via the Radio Interface.

47. Ethernet Interface (TS0898)

Set up options for the Challenger Ethernet Interface (TS0898).

Please note, this product conforms to the standards set by Standards Australia on behalf of the Australian Communications Authority (ACA). GE Interlogix recommends enclosure covers remain fitted to comply with C-Tick.

GE Interlogix recommend enclosure covers remain fitted to maintain C-Tick compliance.

WARNING:
This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Disclaimer

The customer is responsible for testing and determining the suitability of this product for specific applications. In no event is GE Interlogix Pty Limited responsible or liable for any damages incurred by the buyer or any third party arising from its use, or their inability to use the product.

Due to ongoing product development, the contents of this manual can change without notice. We make every effort to ensure the accuracy of this manual. However, GE Interlogix Pty Limited assumes no responsibility for errors or omissions in this manual or their consequences. Please notify us if you find errors or omissions.

Technical Support

GE Interlogix Pty Limited
646 Whitehorse Road, Mitcham, Victoria, 3132, Australia
Phone: +61 3 9259 4700
Fax: +61 3 9259 4799
Email: techsupport@indsys.ge.com

Technical Support hours are from 9:00 AM to 5:30 PM, Monday to Friday. (EST)

Part number: MAINST-TS0816