

# EN50131 CORNER



DEALING WITH CLAIMS OF NON-COMPLIANCE



## Telephone Line Fault Timer must be zero seconds?

Technically, all faults come under the timing requirement of EN50131-1 clause 8.9; which requires that faults are processed within 10 seconds of the fault being reported – with 10 seconds being allowed for the actual processing before any system response is generated.

What this leaves open is how long the fault must be present before it is reported - this is left to be specified in the relevant product standards, but few are.

The simplest way of describing the sequence is to refer to BSIA Form 171 (attached). The timing diagram in clause 8.9.1 illustrates the "condition developing phase" and makes it clear that this could be different for each fault type.

**For a simple telephone line fault, this time is not specified anywhere.** Most SPTs (communicating devices - eg Red Care STUs) have a considerable filter period built into it, which can run into several minutes. This is the "condition developing phase" - with the CIE then having 10 seconds "recognition phase" before the further 10 second "processing phase" giving a total of another 20 seconds.

We default to a 20 second line fault filter in the panel – which is one of two things:  
a) for an SPT that does not have an internal filter – it is a combined “condition developing” and “recognition” phase totalling 20 seconds – and can legitimately be lengthened.  
b) for an SPT that has internal filter, it is an unofficial combining of the two 10 second periods (as processing is virtually instantaneous). The condition under which this theoretically comes unstuck is if the SPT removes its line fault condition between the 10 and 20 second points. With a 20 second filter on we would throw it away, whereas the standard would expect the condition to be latched internally at the CIE after 10 seconds, even if the processing delays the actual system response by another 10 seconds and appears after the fault clears.

This is the same at all grades. I have never before heard of an objection to the filtering (even with longer filtering times).

With our own SPTs (DigiModem), we are free to set the "condition developing phase" to suit ourselves (within reason).

The "transmission time" in the standards is the time allowed for an alarm event presented to the input of a communicator to reach the ARC, and is not related to the detection of a line fault.

The "reporting time" for an alarm transmission system is the time allowed for a fault to be reported to (or detected by) the ARC - not the CIE.

The max time allowed for an attempted transmission before considering a failure to communicate is reported as a fault has been defined elsewhere in BSIA Form 171 as 240 seconds.

## ANTI-MASKING (Grade 3) – 1

There is NO requirement in standards for a specific “masking” signal to be notified to the ARC.

The requirement is that a masking event is processed EITHER as a “Fault” OR as an “Intrusion.”

This means that if "FAULT" is selected, then a "fault" signal must be sent to the ARC. If on the other hand "INTRUSION" is selected, then an "intrusion" signal must be sent – but ONLY if the system is set (thus no signal is sent when unset). There is NO requirement to treat masking as "fault" when unset and "intrusion" when set.

To clarify (and this has been checked with NSI who are in full agreement with this summary):

prEN50131-1:2004 clause 8.4.5, clearly states:

*Masking signals or messages shall be processed as an intruder or fault signal or messages in accordance with Table 7.*

Note that this says "intruder OR fault" - leaving a choice available, but NOT permitting a "tamper" signal to be used.

BSIA Form 171 or - perhaps better still - the reprint of this document published by NSI (Bulletin 03/05), includes the following comment as item "e" under "Table 7:

*The table (ie table 7 of prEN50131-1:2004) does not show how a system will treat masking. Clause 8.4.5 specifies that it may be processed as a "fault" OR as an "intrusion." It is agreed that treating masking as an intrusion achieves all required responses.*

*NOTE: provision of the "masking" output when the IAS is set is NOT mandatory according to the requirements for detectors in TS50131-2-x, though is preferred by insurers.*

We have therefore followed this request of the insurers, and arranged for an "intrusion" response for masking events. In the UNSET state, it will prevent setting, in the SET state it will generate an intruder alarm - ie fully compliant with the standard.

Additionally, when unset, the panel will generate a local "alert" condition to warn the user of the condition so that it can be dealt with in advance of actually attempting to set the system.

The decision as to which option is used has been made by us in writing the system firmware, taking into account the industry-agreed interpretation of BSIA Form 171 and NSI Bulletin 03/05 – including the expressed preference of insurers for an "intrusion" response.

Castle Euro-MERiDIAN systems since firmware version 5.00 (September 2005) have fully complied with this. Any NSI (or other) inspector suggesting otherwise should be referred to the requirements of the standards, to the documents referred to above, or to Brian Harrington.

## **ANTI-MASKING (Grade 3) – 2**

We have now heard claims, again alleged to have originated with an NSI inspector, to the effect that in order to comply with the current standards, there must be a separate masking connection from a detector and that the Euro-MERiDIAN cannot therefore comply. It may equally have originated from a (desperate?) competing salesman – but wherever it came from it is **UTTER PIFFLE!**

Standards require that masking be PROCESSED, INDICATED and LOGGED separately. The standards do NOT state that there must be a dedicated connection from the detector. Indeed it is a fundamental principle that European Standards are not allowed to restrict any application of technology (including methods of connecting detectors to control equipment) that meets the specified requirements.

End of Line systems using several resistor values on a single "pair" for each detector are therefore fully compatible with current standards – as are iD systems using paired biscuits.

In fact TS50131-2-2 Table 1 specifically refers (as do the remaining specifications from the TS50131-2 series) to a detector providing the "masking" information in three different ways:

1. By means of 'bus' connection
2. As a dedicated "masking" signal or message
3. As a combination of "intrusion" and "fault" signals or messages.

Euro-MERiDIAN iD systems use method 1 with paired biscuits. End of Line systems can use method 2 or 3 (or indeed both, mixed on a single system).

Anyone suggesting otherwise should again be referred to the standards, and if necessary to us.

### **ANTI-MASKING (Grade 3) – 3**

One that we have not heard previously, but has now cropped up three times ... Allegedly some inspectors are claiming that an active beam type detector cannot be used in a grade 3 system because it has no anti-masking output. Whilst this query really should be referred to the manufacturer of the detector involved, the standards position is clear:

prEN50131-1:2004 clause 3.1.42 defines "masked" as:

*"condition whereby the field of view of a movement detector is blocked."*

An active beam detector is NOT a "movement detector" – so the requirement cannot be applied to this type of detector.

Note: The TS50131-2 series does not currently address this type of detector at all, thus a detector manufacturer is free to declare that a particular detector is "suitable for use with systems installed ... to grade 3" if it permits all the relevant requirements of prEN50131-1 at that grade to be met.

### **Level 3 Access**

We also continue to get comment about the fact that engineer access (level 3) is possible without being authorised every time by a level 2 user...

In a nutshell:

Once level 2 authorisation has been granted, it is permitted for this to remain in force UNTIL MANUALLY REMOVED by a level 2 user. It does NOT have to be renewed for each individual occasion – though the user can of course enforce this, should he/she wish.

BSIA Form 171 (NSI Bulletin 03/05) comments - 8.3.1.c(ii) - as follows:

*"prEN50131-1 does NOT require level 2 authorisation for level 3 access to be carried out individually every time such access is required, it may remain in force until manually removed at level 2 - eg permitting an engineer on site to have unlimited access during his visit following a single authorisation."*

The example quoted does not restrict the authorisation to a single visit - the operative term is that *"it may remain in force until manually removed at level 2"* - whether this be the same day or the next year...

The Euro "G" range implementation is that the "USER MENU" (ie press D key before entering code / tag) includes an option "Allow engineer menu?" This should be set to "NO" on commissioning the system (it is impractical to set it thus as a factory default in view of the

engineer's requirements prior to commissioning). The first time engineer (level 3) access is required, a user (level 2) enters this menu and selects YES. This permits engineer access until such time that a user (level 2) reverses this selection.

The operation is available to ALL users / managers.

This operation agrees with the industry agreed interpretation referred to above. It also complies with the more specific statement in TS50131-3:2003 (clause 8.2.1), which becomes mandatory for control equipment from 1st October 2006.

### **DD243-Clause 6.4.5.**

Yes, this also continues to give rise to difficulties ...

The most common problem is the concept of disabling confirmation during entry. Someone sees the option "**Disable confirmation on entry**" is not selected and declares that the system is not compliant with the requirement of clause 6.4.5 for confirmation to be disabled during entry time.

If you actually read DD243 – and please point this out to whoever raises the matter – clause 6.4.5 does not even mention "disabling" confirmation. It simply describes a procedure that does not permit a confirmed alarm to be generated during the entry procedure – which is how Euro-MERiDIAN works, by default.

On the other hand, clauses 6.4.3 and 6.4.4 both specifically refer to "disabling of all means of confirmation." When these options are used, confirmation must be completely disabled – permanently – on entry. It is for these options that the Euro-MERiDIAN option is designed. Hence the name of the option: "Disable confirmation on entry" – taken from the original DD243:2002 wording.

This option should therefore **NOT** be selected when DD243 option 6.4.5 is used.

### **Does an Internal Warning Device need a tamper switch?**

prEN50131-1:2004 Table 12 identifies the system components that must be fitted with tamper detection. This shows that it is MANDATORY for WD at all grades.

Table 13 identifies that the only means of detection that is mandatory is "opening by normal means."

The final paragraph of PD6662:2004 C.3.1 identifies that EXTERNAL audible alarms must be fitted with means of detecting removal from mounting.

Other than this, there is **no** differentiation between Internal and External WDs, or between self-powered and remotely powered WDs.

There are also recommendations within TS50131-7 for tamper PROTECTION of connections to WDs. These relate solely to physical protection – not to tamper detection.

### **Does an internal loudspeaker need a tamper switch?**

A much more interesting question – which basically boils down to two sub-questions!

1. Is the loudspeaker a Warning Device?  
If so then it must be tampered, as above.
2. Is the loudspeaker an audible indicator of alarm events?  
If so, there is no stated requirement for an "indicator" (which may be audible or visual) to be fitted with tamper detection.

There is also another factor which is sometimes raised in this connection:

3. Does the loudspeaker also generate entry and exit tones?  
These are audible indications, for which there is no stated tamper detection requirement.

As to some degree these are system specification issues, we will leave it you to draw your conclusions on a site by site basis ....

### **iD Does not comply with Grade 3 Requirements?**

This is completely false. Subject of course to the detectors in use, iD systems meet ALL the requirements for grade 3 systems by a comfortable margin (though require two biscuits per detector to do so).

In fact reference to BSIA Form 171 (NSI Bulletin 03/05) clause 8.8 spells out very clearly that grade 3 can be achieved by:

*“double pole, end of line, etc – with individual tamper – iD or similar system.”*

We understand that problems have been experienced in obtaining suitable door contacts for use with iD systems, as most grade 3 contacts have integrated resistors that make them unsuitable. Having discussed this issue with detector manufacturers, we can confirm that there ARE contacts available that are suitable for use in grade 3 iD systems.

### **When carrying out Remote Servicing, you must include full details of the voltage and current of all peripherals to establish that it is within tolerance?**

The relevant requirement in PD6662:2004 is clause D.3, which includes:

- f) A check that all voltage and current levels are within acceptable tolerances.

Note that this specifically calls for a check that the items in question are “WITHIN TOLERANCE” – it is **NOT** a requirement to identify the actual values. The person best qualified to establish whether the values are “within tolerance” is not the installer viewing the information, but the manufacturer of the item in question.

This can be verified by reference to the product specifications in the EN50131 family (EN50131-6, TS50131-2-x and prTS50131-4), which state that system components are (or will be when the relevant TS is adopted in the UK) required to provide a “fault” output in the event of a problem – either internal to the device or with the supply. This is designed to provide a simple “go / no-go” indication to the CIE. These specifications establish exactly which conditions need to be separately identified and at which security grade.

The remote servicing requirements of PD6662 cannot require detail in addition to that specified within the standards for those components. Hence, even for Euro-MERiDIAN components from which diagnostic measurements may be obtained, the simple “pass/fail” statement in the ARM report meets all the requirements of the PD6662 scheme. From a practical point of view, to require that all this information is specifically included would effectively require all system components to originate with the same manufacturer – and make remote servicing impossible!

### **DD243 Does not permit the use of a “pre-alarm” time?**

DD243:2004 clause 6.4.5 includes the statement

*“If the entry time expires before the IAS is unset, an unconfirmed alarm should occur. Expiry of the entry time should not itself initiate a confirmed alarm”.*

It appears that this is being understood to mean that the intrusion signal must be sent to the ARC immediately on expiry of entry time. However, prEN50131-1 clause 8.3.8.2 states, in the context of an alarm resulting from an incorrect entry procedure:

*“When remote notification is included in the I&HAS, the intruder alarm condition shall not be remotely notified until the indicator or WD has operated for a minimum of 30 seconds.”*

It is a little vague as to whether this is intended to be applied solely to alarms triggered by a deviation from the entry route or whether it is applicable also to alarms caused by exceeding the entry time. The comment relating to this in BSIA Form 171 (NSI Bulletin 03/05) is clear:

*“The standard shows that at the end of entry time an alarm condition can be indicated or notified locally, remote notification is delayed for a further 30 seconds. If the system is unset during the 30 seconds then the notification can be cancelled.”*

It is therefore clear that compliance with the PD6662 scheme **REQUIRES** that there be such a delay. This is NOT over-riden by DD243.

## Understanding Table 10

It is clear from discussions at the Seminars we recently presented that Table 10 in prEN50131-1:2004 is surrounded by confusion.

The table, with the addition of PD6662:2004 clause E.1.1 added, appears as follows:

**TABLE 10 – NOTIFICATION REQUIREMENTS:**

Option	GRADE 1			GRADE 2					GRADE 3				GRADE 4				
	A	B	C	X	A	B	C	D	A	B	C	D	A	B	C	D	
Remotely powered WD	2				2					2				2			
Self-powered WD		1		1		1				1				1			
Main ATS			ATS 1		ATS 2	ATS 2	ATS 2	ATS 3	ATS 4	ATS 4	ATS 4	ATS 5	ATS 5	ATS 5	ATS 5	ATS 6	
Additional ATS							ATS 1				ATS 3					ATS 4	

NOTE: These are MINIMUM requirements. Blanks are OPTIONAL and may be added as desired.

“ATS” values refer to the performance criteria specified by prEN50131-1:2004 Table 11. In practice, you will obtain these from the manufacturer’s compliance statement, and will not need to work them out for yourselves.

These numbers refer to the number of devices that may be fitted.

### What does it mean?

Basically it is very simple ...

Firstly, establish (from your risk assessment) which grade the system you are about to install should be.

Secondly, use this table to choose which combinations of WDs (Warning devices) and ATS (Alarm Transmission Systems) that you wish to use to meet the required security requirement.

For example, at **GRADE 2**, you have a CHOICE of applying option **X OR A OR B OR C OR D**; ANY of these may be used within the context of a grade 2 system, to suit what you (or the insurance company!) believe offers the best solution to your client’s security needs.

Taking these choices one at a time:

**X:** is a simple “Bells Only” system, requiring simply one “self powered” WD.  
A “self-powered” WD is one that contains a power source – in every day terms, an SAB *or* an SCB (either is acceptable).

**A:** is a system including an ATS meeting at least ATS2, plus TWO “remotely powered” WDs. “Remotely powered” WDs are those that do NOT include a power source – ie a simple siren or bell incapable of sounding except when driven from the panel.

**B:** is similar, but requires just one “self-powered” WD.

**C:** requires two ATS – or a “dual path” system – meeting the minimum of ATS2 (main path) + ATS1 (secondary path).

**D:** requires only a single ATS, but to the higher ATS3.

At **GRADE 3** (and 4 for that matter), the A,B,C,D options follow exactly the same pattern, but with higher graded WDs and ATS.

Note that C and D do NOT require a WD at all to meet the standards. However, a WD may be added to the system as required (and will likely be mandatory if an insurer is involved in the specification).

#### **SYSTEM COMPLIANCE STATEMENT**

For all systems there should be a simple statement that the system is installed to comply with the requirements of PD6662:2004 at grade “x” **and using notification option “y”**.

NOTE: Whilst there may be a requirement to state the fact that a wireless (or hybrid) system is installed, this has no bearing on the use of Table 10, or on the compliance statement required by the standards – and should not be confused with it.

#### **NOTES:**

Final selection will need to take into account any insurance requirements.

Option **2X** (bells only) option is specific to the UK and is not permitted elsewhere in Europe.

Not all grades of ATS will be manufactured, so you will simply need to use the next grade up from the MINIMUM requirement stated in table 10.

Typical ratings are something like:

Digicom	ATS 2	
RedCare	ATS 5	
RedCare GSM	ATS 5 + ATS 4	
DualCom Plus	ATS 5 + ATS 4	
DualCom GPRSATS 4	+ ATS 3	
DualCom GSM	ATS 4 + ATS 3	
DualCom IP	ATS 3	(additional path for DualCom GPRS)
WebWayOne 2424	ATS 5 + ATS 4	

- but make sure you confirm these from manufacturers declarations!

Whatever grade of system is specified / installed, additional items can be added without compromising the system. For example a smoke-generating system can be added. Indeed a speech dialler (although not meeting any of the ATS requirements) can be added to a system of any grade – provided that it is not a replacement for the mandatory signalling equipment.