I.D. FOS RESEARCH e.e.i.g.
(Fiber Optic Sensing Research Center)

DBE TECHNOLOGY GmbH

Operational Safety Monitoring with Fiber Optic Sensing Systems

Vol. III

- Standard and Qualification Document -

DBE TECHNOLOGY GmbH

June 2005

CONTENTS

SECTION 1: GENERAL

A. Introduction

A 100 Objectives

101 The objectives of this standard are to:

— provide an internationally acceptable standard for general requirements to control, fibre optical sensing systems by defining minimum requirements for design, materials, fabrication, installation, testing, commissioning, operation, maintenance, re-qualification and abandonment
— serve as a technical reference document in contractual matters between purchasers and contractor
— serve as a guideline for designers, purchasers and contractors.

A 200 Scope and application

201 The requirements of this standard shall apply to all fibre optical sensing systems used in nuclear waste repository sites.

A 300 Organisation of contents

301 Sec.1 to Sec.4 give common requirements which are considered applicable to all types of fibre optical sensing systems.

A 400 Alterations and additions

401 Alterations and additions to systems covered by this standard shall be carried out in accordance with the requirements of this standard.

A 500 Assumptions

501 The requirements of this standard are based on the assumptions that the personnel using the fiber optic equipment to be installed on board are familiar with the use of, and able to operate this fiber optic equipment.

B. References

B 100 Normative references

101 The standards listed below include provisions which, through reference in this text, constitute provisions of this standard. The latest issue of the references shall be used unless otherwise agreed. Other recognised standards may be used, provided it can be demonstrated that these meet or exceed the requirements of the standards referenced.

European Norm ***EN 10012***
Measurement management systems - Requirements for measurement processes and measuring equipment (ISO 10012:2003)

European Norm EN 60794-1-1/A1
Optical fibre cables - Part 1-1: Generic specification - general (IEC 60794-1-1/A1:2000-01)

European Norm EN 60794-1-1
Optical fibre cables - Part 1-1: Generic specification - general (IEC 60794-1-1: 2001)

European Norm EN 60794-1-2
Optical fibre cables - Part 1-2: Generic specification - Basic optical cable test procedures (IEC 60794-1-2: 1999)

European Norm EN 61757-1
Fibre optic sensors - Part 1: Generic specification (IEC 61757-1: 1998)
In addition: all European Norms and International Norms given as references within this norm.

European Norm EN 60793-1-44 (EN 188000)
Optical fibres (2001, 1992)

European Norm EN 186000-1
Generic specification: Connector sets for optical fibres and cables Part 1: Requirements, test methods and qualification approval procedures

European Norm EN 50014
Electrical apparatus for potentially explosive atmospheres, Part 1 - 20

International Standard CEI IEC 60874-1
Connectors for optical fibres and cables - Part 1: Generic specification

ITU-T Recommendations G.651
Series G: Transmission systems and media, digital systems and networks, transmission media characteristics - optical fibre cables: Characteristics of a 50/125 µm multimode graded index optical fibre cable.

ITU-T Recommendations G.652
Series G: Transmission systems and media, digital systems and networks, transmission media characteristics - optical fibre cables: Characteristics of a single-mode optical fibre cable.

The cover pages of the mentioned documents are given in the appendix for reference.

C. Definitions

C 100 Verbal forms

101 Shall: Indicates requirements strictly to be followed in order to conform to this standard and from which no deviation is permitted.

102 Should: Indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required. Other possibilities have to be agreed upon.

103 May: Verbal form used to indicate a course of action permissible within the limits of the standard.

104 Agreement, agreed or by agreement: Unless otherwise indicated, agreed in writing between contractor and purchaser.

C 200 General terms of fiber optic systems

200 Fiber optic sensor network: Physical network of passive components consisiting of fibre optical cables, couplers, connection boxes and the Fibre Optical (FO) sensors (Figure 1).

201 Control system: A system that is able to read out the FO sensor network, e.g. optical switch, spectrum analyser, process controller, etc.(Figure 1)

202 Monitoring system: A system that is able to monitor and issue alarms relating to the operation of the control system and FO sensor network. (Figure 1)

203 Safety system: A system able to perform safety shutdown of the FO sensing system. (Figure 1)

204 Telecommunication system: A system providing internal communication within the unit (e.g. telephones, public address, general alarm) or externally to the unit (e.g. radio). (see Figure 1)

212 Field instrumentation: All instrumentation that forms an integral part to maintain the FO sensor read-out function. The field instrumentation includes: control system, monitoring system and safety system.
Other equipment items do not, whether they are implemented locally or remotely, belong to the field instrumentation. This applies to data communication and facilities for data acquisition and pre-processing of information utilised by remote systems. (Figure 1)

208 FO sensing system: A system includes all components necessary for performing the fibre optical sensing: FO sensor network and field instrumentation. (Figure 1)

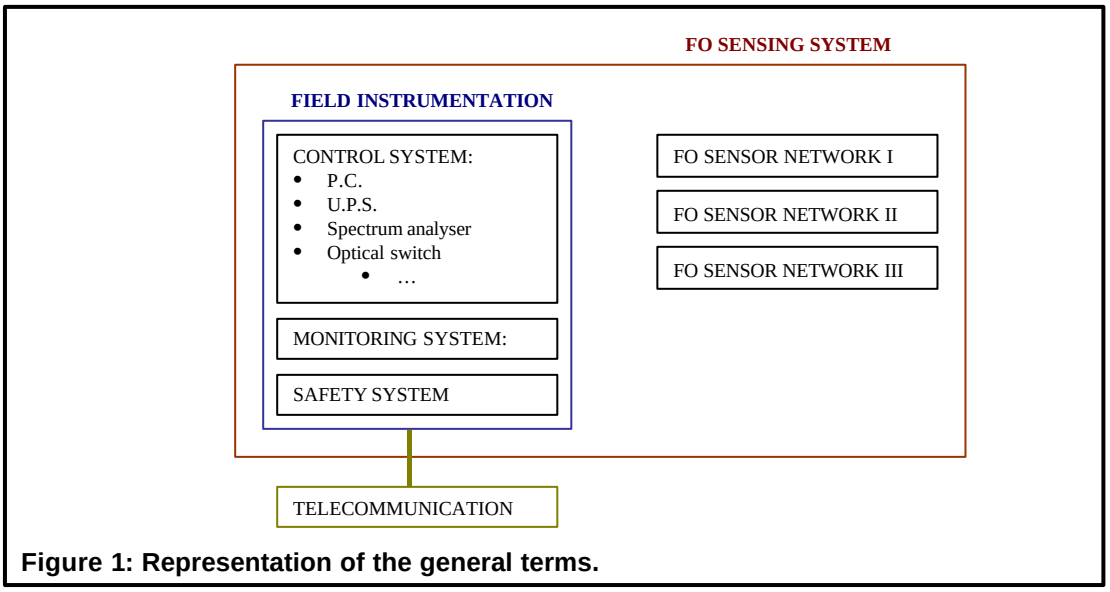

Figure 1: Representation of the general terms.

205 Alarm: A combined visual and audible signal for warning of an abnormal condition, where the audible part calls the attention of personnel, and the visual part serves to identify the abnormal condition.

206 Pre-warning: An indication of a FO system state that needs attention.

207 Safety shutdown: A safety action that will be initiated upon predefined events (e.g. power supply problems) and shall result in the shutting down of the control system in question.

209 An essential control, monitoring, safety or telecommunication system (hereafter called an essential system or essential function): A system supporting equipment, which needs to be in continuous operation for maintaining the safety conditions (e.g. hydrogen detection).

210 An important control, monitoring, safety or telecommunication system (hereafter called an important system or important function): A system supporting equipment, which need not necessarily be in continuous operation, but which is required by the this standard document.

211 Non-important control, monitoring, safety and telecommunication systems (hereafter called non-important systems or non-important function): Systems supporting functions that are not required by this standard document.

214 Integrated system: A combination of computer based systems which are interconnected in order to allow common access to the FO sensor information and/or command or control of the different FO sensing systems.

215 User: Any human being that will use a system or device, e.g. engineer.

216 Workstation: A position at which one or several functions constituting a particular activity are carried out.

217 Maximum unavailable time: The maximum duration of time the function is allowed to be unavailable, i.e. the maximum permissible time lag involved in restoring lost function upon failure.
220 Indications: The visual presentation of values for the FO sensors or system status to a user (LED's, lasers, displays,etc.).

221 Uninterruptible power supply (UPS): A device supplying output power in some limited time period after loss of input power with no interruption of the output power.

222 Independent systems: See Sec.2 A201.

223 Redundant systems: See Sec.2 A501.

224 Remote control system: comprises all hardware and software necessary to operate the FO sensing system from a location where the operator cannot directly have access to the corresponding control system of the FO sensing system.

225 Back-up control system: comprises all hardware and software necessary to maintain control when the main control systems have failed or malfunctioned.

C 300 Terms related to computer based system

301 Complex system: A system for which all functional and failure response properties for the completed system cannot be tested with reasonable efforts. Systems handling application software belonging to several functions, and software that includes simulation, calculation and decision support modules are normally considered as complex.

302 Computer: A computer includes any programmable electronic system, including main-frame, mini-computer or micro-computer.

303 Computer based system serving an essential or important function: The function can be in operation without support from the computer system, i.e. the computer is not part of the function.

304 Computer based system as part of an essential or important function: The function can not be in operation without support from the computer system, i.e. the computer is part of the function.

305 Visual display unit (VDU): Any area where information is displayed including indicator lamps or panels, instruments, mimic diagrams, light emitting diode (LED) display, cathode ray tube (CRT), and liquid crystal display (LCD).

306 User input device (UID): Any device from which a user may issue an input including handles, buttons, switches, keyboard, joystick, pointing device, voice sensor and other control actuators.

307 Software module: An assembly of code and data with a defined set of input and output, intended to accomplish a function and where verification of intended operation is possible through documentation and tests.

308 Basic software: The software necessary for the hardware to support the application software.
Guidance note:
Basic software normally includes the operating system and additional general software necessary to support the general application software and project application software.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

309 General application software: Computer software performing general tasks related to the control system, rather than to the functioning of the computer itself. (Example: drivers to controll the optical switch)

310 Project application software: Computer software performing tasks related to the actual FO sensing network for a specific project.

311 Computer task: In a multiprocessing environment, this means one or more sequences of instructions treated by a control program as an element of work to be accomplished by a computer.

312 Data communication links: This includes point to point links, instrument net and local area networks, normally used for inter-computer communication on board units. A data communication link includes all software and hardware necessary to support the data communication.

Guidance note:
For local area networks, this includes network controllers, network transducers, the cables and the network software on all nodes.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

313 Node: A process segment or a part of the system connected as part of the data communication link.

314 Point to point: Link used for data communication between two dedicated nodes.

315 Local area network: A network used for data communication between the field instrumentation and the other parts of a system, and between different systems.

316 Instrument net: A network used for data communication within the field instrumentation connecting instruments in a network. (Ex.: communication between optical switch and P.C.)

317 Multifunction VDUs and UIDs: VDUs and UIDs that are used for more than one essential and / or important function for both control and monitoring, e.g. VDUs and UIDs used for integrated computer systems.

C 400 Abbreviations

401 The following abbreviations are used.

ATOS	Approval test of application software
CIBS	Classification information breakdown structure
CRT	Cathode ray tube
EMC	Electromagnetic compatibility
ESD	Emergency shutdown or Electrostatic discharge
FO	Fibre Optical
I/O	Input and/or output
IEC	International Electrotechnical Commission
LED	Light emitting diode
LCD	Liquid crystal display
MS	Manufacturing survey
OTDR	Optical time domain reflectometry
PROM	Programmable read only memory
UID	User input device
UPS	Uninterruptible power system
VDU	Visual display unit.

SECTION 2: DESIGN PRINCIPLES

A. System Configuration

A 100 General

101 Whenever possible, essential and important systems shall be so arranged that a single failure in one system cannot spread to another system (e.g. by use of selective fusing of electrical distribution systems).

A 200 Field instrumentation

201 The field instrumentations belonging to separate essential FO sensor networks shall be mutually independent.

Guidance note:
System B is independent of system A when any single system failure occurring in system A has no effect on the maintained operation of system B. A single system failure occurring in system B may affect the maintained operation of system A. Two systems are mutually independent when a single system failure occurring in either of the systems has no consequences for the maintained operation of the other system as described above.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

202 The alarm system, control system and safety shutdown system shall be designed mutually independent, unless any failure, which affects more than one of the systems initiates an alarm and does not change the operation mode.

203 When the field instrumentation of a process segment is common for several FO sensor networks, and any of these networks is essential, failures in any of the systems shall not affect this field instrumentation.

204 When manual emergency operation of an essential FO sensor network is required, the field instrumentation required for the manual emergency operation shall be independent of other parts of any system.

A 300 Fiber optic sensor network

301 When a FO sensing system contains more than one FO sensor network, a failure in one of the FO sensor networks may not cause a failure for the other ones.

A 400 Integrated systems

401 Essential FO sensing systems shall be independent of other FO sensing systems.

403 UIDs for control shall only be available at workstations from which control is permitted.

404 At least two interchangeable multifunction VDUs and UIDs shall be available at each control station.

Guidance note:
The number of VDUs and UIDs at control stations should be sufficient to ensure that all functions may be provided for with any one VDU or UID out of operation, taking into account any functions that shall be continuously available.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 500 Redundancy

501 Redundancy shall be built in to the extent necessary for maintaining the safe operation of the unit. Changeover to redundant systems shall be simple even in cases of failure of control and monitoring systems.

Guidance note:
Redundancy is defined as two mutually independent systems that can maintain a function. The two systems may be of a different type or have different functionality.
Due regard should be taken as to manning levels when considering the extent and availability of spare parts and the degree of redundancy to be employed. This is in order to ensure continuity of operation upon failure of the instrumentation equipment.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

502 Automatic switching between two systems shall not be dependent on only one of the systems.

B. Maximum Unavailable Time

B 100 General

101 The time needed to bring a FO system back in operation upon a failure condition, shall be adapted to the redundancy requirements imposed on the FO system served.

102 Typical maximum unavailable times for the different categories are given in Table B1.

System	Category	Time
Continuous availability	R0	None
High availability	R1	10 minutes
Manual system restoration	R2	4 hours
Repairable systems	R3	1 day

Table B1: Maximum unavailable time

103 The requirements in 200 to 500 only apply for systems of maximum unavailable time category R0, R1, R2 or R3.

B 200 Continuous availability (R0)

201 A system serving a function that shall be continuously available shall be designed to provide no interrupts of the function neither in normal operation modes nor in case of a single FO system failure.

202 Changeover between redundant systems shall take place automatically and with no disturbances for the continuous operation of the function in case of system failure. User requested changeovers shall be simple and easily initiated and take place with no unavailable time for the function.

203 User interfaces of redundant systems shall allow supervision of both systems from the same position.

B 300 High availability (R1)

301 A system serving a function that shall have high availability shall be designed to provide continuous availability in normal operation modes.

302 In case of system failures, changeover between redundant systems shall take place automatically if redundancy is required. User requested changeover in normal operation shall be simple and easily initiated and take place within the same maximum time.

303 User interfaces of redundant systems shall be located close to each other and changeover between the systems shall have no significant effect on the user's maintained execution of other tasks.

B 400 Manual system restoration (R2)

401 A system serving a function that requires manual FO system restoration shall be designed to provide restoration of the function within a maximum time specified for R2, in case of FO system failures.

Guidance note:
Restoring a function may involve a limited number of simple manual actions.
User interfaces of redundant systems may be designed for manning of normally unattended workstations when required, provided such manning is immediately available.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B 500 Repairable systems (R3)

501 A system serving a function of category R3 shall be designed to provide restoration of the function within a maximum time specified for R3 in case of system failures.

Guidance note:
Restoring a function may involve a number of manual operations, including minor replacements or repair of equipment.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

C. Response to Failures

C 100 Failure detection

101 Essential and important systems shall have facilities to detect the most probable failures that may cause reduced or erroneous system performance.

102 The self-check facilities are to at least, but not limited to, cover the following failure types:
— power failures
— FO sensor failures
and additionally for computer based systems:
— communication errors
— computer hardware failures
— software execution failures
— software logical failures
for essential computer based systems:
— input and output loop failures (at least broken connections and short circuit).

103 Adequate failure detection may be obtained by combining two mutually independent systems, which together provide the required failure detection properties, e.g. an automatic control system together with an independent alarm system.

104 Detection of failures in essential and important systems shall initiate an alarm.

C 200 Fail-to-safety

201 The most probable failures, for example loss of power or wire failure, shall result in the least critical of any possible new conditions.

D. Emergency Operation

D 100 Manual emergency operation

101 For functions where manual emergency operation is required, this shall be used to maintain a minimum functionality in case of major system failures.

102 This system shall be installed as an integral part of the mechanical equipment.

E. User Interface

E 100 General

101 When designing the layout of control and display devices, due consideration shall be given to the user interface. Attention shall be paid to the significance of human factors in the event that a critical failure or condition occurs. Graphic information systems shall contain all relevant functions for safe operation, shall be easy to understand and operate, and shall enable system overview.

102 For essential and important systems, deviations between a command action and expected result of the command action shall initiate an alarm.

F. Tests

F 100 General

101 All control, monitoring, safety and telecommunication systems required to be installed by applicable FO sensing standards shall be tested.

102 Testing according to 200, 300, and 400 shall be performed at the manufacturers' works.

103 The tests and visual examinations shall verify that all requirements given by the applicable FO sensing standards are met. The test procedures shall specify in detail how the various functions shall be tested and what is to be observed during the tests.

104 Failures shall be simulated as realistically as possible, preferably by letting the monitored parameters exceed the alarm and safety limits. Alarm and safety limits shall be checked.

105 It shall be verified that all automatic control functions are working satisfactorily during normal load changes.

F 200 Software module testing

201 Documentation of compliance with software module testing according to requirements for software manufacturing as described in Sec.4 B200 shall be available in conjunction with testing at the manufacturer's works.

F 300 Integration testing

301 Integration tests includes integration of hardware components and integration of software modules into the same hardware.

302 Integration tests shall be performed with the actual software and hardware to be used on board and shall include:

- Hardware tests; hardware failures.
- Basic software tests; basic software failures.
- Application software tests.
- Function tests of normal system operation in accordance with the requirements of Sec.2. Function tests are also to include a degree of performance testing outside of the normal operating parameters.
- User interface tests.

F 400 System testing

401 System tests includes the entire system, integrating all hardware and software. The test may also include several systems.

402 System tests shall be performed with the software installed on the actual systems to be used on board, interconnected to demonstrate the functions of the systems.

403 The tests shall include those tests which were not or could not be completed on hardware component or software module level.

F 500 On-board testing

501 The tests shall include:

- During installation the correct function of individual equipment packages, together with establishment of correct parameters for alarm, control and safety (time constants, set points, etc.).
- During installation, the correct function of systems and integration of systems, including the ability of the control systems to read-out the FO sensor network within the specified tolerances.
- The correct protection and capacity of power supplies.

SECTION 3: SYSTEM DESIGN

A. System Elements

A 100 General

101 A system consists of one or several system elements where each system element serves a specific function.

102 System elements belong to the categories:
— sensing control
— remote control
— alarm
— safety
— indications
— Reporting
— calculation, simulation and decision support.

A 200 Sensing control

201 Sensing control shall provide an accurate and stable read-out performance within the limits specified for the FO sensing system during normal working conditions. (e.g. self referencing system).

202 The sensing control system element shall be able to accomplish the function it shall serve.

A 300 Remote control

301 At the remote command location, the user shall receive continuous information on the effects of his or her orders.

302 One command location is to be designated as the main command location. The main command location is to be independent of other command locations.

303 When control is possible from several locations, only one shall be in control at a time.

304 Actual control shall not be transferred before acknowledged by the receiving command location unless the command locations are located close enough to allow direct visual and audible contact. Transfer of control shall give audible prewarning. The main command location shall be able to take control without acknowledgement.

Guidance note:
There may be several main command locations on different levels.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

305 Means shall be provided to prevent significant alteration of process equipment parameters when transferring control from one location to another.

306 On each alternative command location, it shall be indicated when this location is in control.

307 Control system elements shall include safety interlocks when the consequence of erroneous user actions may lead to major damages or loss of essential or important functions.

308 Safety interlocks in different parts of the systems shall not conflict with each other. Basic safety interlocks shall be hardwired and shall be active during remote and local operation.

Guidance note:
Hardwired safety interlocks should not be overridden by programmable interlocks.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 400 Safety

401 A safety system element shall be arranged to automatically take safety actions on occurrence of predefined abnormal states for the field instrumentation. The corresponding system element includes all resources required to execute these actions.

402 The safety system element shall be so designed that the most probable failures, for example loss of power supply or wire failure, result in the least critical of any possible new condition (fail to safety) taking into consideration the safety of the unit.

403 Automatic safety actions shall initiate alarm at predefined workstations.

404 When the safety system element stops the field instrumentation, the field instrumentation shall not start again automatically.

405 When a safety system element is made inoperative by a manual override, this shall be clearly indicated at predefined workstations.

406 When a safety system element has been activated, it shall be possible to trace the cause of the safety action by means of central or local indicators.

A 500 Alarm

501 Alarms shall be visual and audible and shall indicate abnormal conditions only. In areas where the audible signal may not be heard due to background noise, additional visual and audible display units shall be installed.

Guidance note:
Several suitably placed low volume audible alarm units should be used rather than a single unit for the whole area
A combination of audible signals and rotating light signals may be of advantage.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

502 Visual alarms shall be easily distinguishable from other indications by use of colour and special representation.

503 Audible alarms shall be readily distinguishable from signals indicating normal conditions, telephone signals, different alarm systems and noise.

506 Presentation and acknowledgement of alarms shall only be possible at the workstation(s) dedicated to respond to the alarm.
Guidance note:
Alarm lists may be available on any workstation.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

507 Alarms at workstations shall normally be manually acknowledged in two steps:

- Silencing audible signal and additional visual signal (for example rotating light signals) leaving the visual signal on the workstation unchanged. After acknowledgement, the audible signal shall operate for any new failure.
- Acknowledging the visual alarm. Alarms, including the detection of transient faults, shall be maintained until acknowledgement of the visual indication. The visual indications of individual alarms shall remain until no abnormal condition is being detected.
- Acknowledged alarms shall be clearly distinguishable from unacknowledged alarms.

Guidance note:
Unacknowledged alarms should be flashing.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

508 Acknowledgement of visual signals shall be separate for each signal or common for a limited group of signals. Acknowledgement shall only be possible when the user has visual information on the alarm condition for the signal or all signals in a group.

509 Local audible signal for an alarm included in a centralised alarm handling system shall be suppressed when localised in the same workplace as the centralised alarm handling system.

510 Permanent blocking of alarm units shall not be possible. Manual blocking of separate alarms is acceptable when this is clearly indicated.

511 Sufficient information shall be provided to ensure optimal alarm handling. Alarm text shall be easily understandable.

512 The more frequent failures within the alarm system, such as broken connections to measuring elements, shall initiate alarm.

513 Interlocking of alarms shall be arranged so that the most probable failures in the interlocking system, for example broken connection in external wiring, do not prevent alarms.

514 Blocking of alarm and safety functions in certain operating modes (for example during start-up) shall be automatically disabled in other modes.

515 It shall be possible to delay alarms to prevent false alarms due to normal transient conditions.

A 600 Pre-warning

601 Pre-warnings shall be acknowledged. Pre-warnings shall be distinguishable from alarms.

A 700 Indication

701 Indications sufficient to allow safe operation of essential and important functions shall be installed at all control locations from where the function shall be accomplished. Alarms or pre-warnings are not considered as substitutes for indications for this purpose.

Guidance note:
It is advised that indicating and recording instruments are centralised and arranged to facilitate watch-keeping, for example by standardising the scales, applying mimic diagrams, and similar.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 800 Reporting

801 Reporting system elements shall have no outputs for real-time process equipment control during planning mode.

Guidance note:
Planning and reporting functions are used to present a user with information to plan future actions.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 900 Calculation, simulation and decision support

901 Output from calculation, simulation or decision support modules shall not suppress basic information necessary to allow safe operation of essential and important functions.

Guidance note:
Output from calculation, simulation or decision support modules may be presented as additional information.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B. General Requirements

B 100 System operation and maintenance

101 Start-ups and restarts shall be possible without specialised system knowledge. On power-up and restoration after loss of power, the FO system shall be restored and resume operation automatically.

102 Testing of essential systems and alarm systems shall be possible during normal operation. The system shall not remain in test mode unintentionally.

Guidance note:
Automatic return to operation mode or alarm should be arranged.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B 200 Power distribution

201 Independent and redundant systems shall have separate supplies from the distribution system and separate circuit protection.

202 Redundant systems shall, if connected to the same distribution switchboard, be supplied from at least two power sources with independent supply to the distribution switchboard.

Guidance note:
The second source may be a battery.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

203 Power for local emergency operation shall be derived from the mechanical system or from a local dedicated source.

204 Systems that may be exposed to conducted electromagnetic interference exceeding their immunity level through their electrical power supplies shall have provision for adequate filtered power.

205 Essential and important systems shall be continuously powered and shall have an automatic change-over to a standby power supply in case of loss of normal power supply. The stand-by power supply shall be from an uninterruptible power supply (UPS). The UPS shall comprise continuously charged and dedicated accumulator batteries of an arrangement, location and endurance equivalent to that of the emergency source of electrical power.

SECTION 4: ADDITIONAL REQUIREMENTS FOR COMPUTER BASED SYSTEMS

A. General Requirements

A 100 System dependency

101 Where a computer based system is part of an essential system (see Sec.1 C), a secondary means of operation shall be provided by either non-computer based system or by an independent computer based system of appropriate diversity.

A 200 Storage devices

201 The on-line operation of essential functions shall not depend on the operation of rotating bulk storage devices.

Guidance note:
This does not exclude the use of such storage devices for maintenance and back-up purposes.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 300 Computer usage

301 Computers serving essential and important functions shall only be used for purposes relevant to unit operation.

A 400 System response and capacity

401 Systems used for control and monitoring shall provide response times compatible with the time constants of the related equipment.

402 System start-up and system restoration after power failures shall take place with sufficient speed to comply with the maximum unavailable time for the systems. The system shall revert to a pre-defined state providing an appropriate level of safety.

403 System capacities shall be sufficient to provide adequate response times for all functions, taking the maximum load and maximum number of simultaneous tasks under normal and abnormal conditions for the FO sensing network into consideration.

A 500 Temperature control

501 Wherever possible, computers shall not have forced ventilation. For systems where cooling or forced ventilation is required to keep the temperature at an acceptable level, alarm for high temperature or maloperation of the temperature control function shall be provided.

A 600 System maintenance

601 Integrated systems supporting one or more essential or important function shall be arranged to allow individual hardware and software entities to be tested, repaired and restarted without interference with the maintained operation of the remaining parts of the system.

602 Essential systems shall have diagnostic facilities to support finding and repair of failures.

A 700 System access

701 Access to system set-up or configuration functions for the FO sensing system shall be protected to avoid unauthorised modifications of the system performance. For screen based systems, tools shall be available to allow easy and unambiguous modification of configuration parameters allowed to be modified under normal operation.

Guidance note:
As a minimum this should cover:
- calibration data
- alarm limit modification
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

702 Unauthorised access to essential and important systems from a position outside the unit shall not be possible.

B. System Software

B 100 Software requirements

101 Basic software on processor systems running application software belonging to different functions shall have facilities for:
— running several modules under allocated priorities
— detection of execution failures of individual modules
— discrimination of faulty modules to ensure maintained operation at least of modules of same or higher priority.

102 Individual application software modules allocated as tasks under an operating system as specified in 101 shall not perform operations related to more than one function. These modules shall be allocated priorities in accordance with the relative priority between the functions they serve.

103 When hardware belonging to input, output, communication links and user interface is configured to minimise the consequences of failures, the related software shall be separated in different computer tasks to secure the same degree of separation.

104 When calculation, simulation or decision support elements are used to serve essential functions, and a basic functionality can be maintained without these elements, the application software shall be designed to allow such simplified operation.

105 System set-up, configuration of the FO network and the setting of parameters for the FO network onboard shall take place without modification of program code or recompilation.

106 Means shall be provided to identify the version(s) of the software in use.

Guidance note:
When the setting of parameters is equivalent to programming then version identification of these settings shall be available. Version identification may be a check sum. For integrated systems, identification shall be available in the system overview. For any screen based system, identification shall be readily available on the VDU during normal operation. PROMs shall be labelled.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B 200 Software manufacturing

201 All relevant actions shall be taken during manufacturing of software for a complex system to ensure that the probability of errors to occur in the program code is reduced to an acceptable level.

202 Relevant actions shall at least include actions to:
— ensure that the programming of applications is based on complete and valid specifications
— ensure that software purchased from other parties has an acceptable track record and is subject to adequate testing
— impose a full control of software releases and versions during manufacturing, installation onboard and during the operational phase
— ensure that program modules are subject to syntax and function testing as part of the anufacturing process
— minimise the probability of execution failures.

Guidance note:
Typical execution failures are:
- deadlocks
- infinite loops
- division by zero
- inadvertent overwriting of memory areas
- erroneous input data.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

203 The actions taken to comply with 201 shall be documented and implemented, and the execution of these actions shall be retraceable. The documentation shall include a brief description of all tests that apply to the system (hardware and software), with a description of the tests that are intended to be made by sub-vendors, those to be carried out at the manufacturer's works and those to remain until installation onboard.

C. User Interface

C 100 General

101 The status of the information displayed shall be clearly indicated.

Guidance note:
E.g. this applies to indications not being updated or indication of blocked alarms.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

102 Alarms and alarm messages for alarms shall, when initiated, be given priority over any other information presented on the VDU. Such alarms shall be easily distinguishable from other alarms. The entire list of alarm messages shall be easily available.

103 Alarms shall be time tagged.

104 Time tagging for all alarms shall be consistent throughout the system.

Guidance note:
This is required to handle inconsistency of time tagging when the same alarm is available at several positions on the unit.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

105 Full redundancy shall be provided for VDUs receiving and displaying alarm presentations of essential screen based systems.

Guidance note:
A printer or other equivalent means may provide the necessary redundancy.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

106 UIDs shall be designed and arranged to avoid inadverted operation. For essentional and important systems, dedicated function keyboards shall be used.

107 Symbols and their associated information in a mimic diagram shall have a logical relationship.

108 Means shall be provided to ensure that only correct use of numbers and letters and only values within reasonable limits will be accepted when data is entered manually into the system. If the user provides the system with insufficient input, the system shall request the continuation of the dialogue by means of clarifying questions. Under no circumstances shall the system end the dialogue incomplete without user request.

C 200 Illumination

201 Means shall be provided for adjustment of illumination of all VDUs and UIDs to a level suitable for all applicable light conditions. However, it shall not be possible to make adjustments down to a level which makes information belonging to essential and important functions unreadable.

Guidance note:
Adjustments may be arranged by use of different sets of colours suited for the applicable light conditions.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

C 300 Colour screens

301 For cathode ray tubes (CRTs), colours used for essential information shall not depend on a single source of light.

D. Data Communication Links

D 100 General

101 Failure in a node shall not have any effect on the remaining part of the data communication link and vice versa.

102 Data communication links shall be automatically initialised on power on. After a power interruption, the links shall regain normal operation without manual intervention.

103 The capacity of the data communication link shall be sufficient to prevent overload at any time.

104 The data communication link shall be self-checking, detecting failures on the link itself and data communication failures on nodes connected to the link. Detected failures shall initiate an alarm on dedicated workstations.

105 For essential and important functions, means shall be provided to prevent the acceptance of corrupted data at the receiving node.

106 When two or more essential functions are using the same data communication link, this link shall be redundant.

107 Redundant data communication links shall be routed with as much separation as practical.

D 200 Local area networks

201 Means shall be provided to monitor the usage and status of the network.

202 It shall be possible to remove and insert nodes without interrupting normal network operation.

203 When serving essential or important functions, facilities shall be provided to ensure that a message is received within a predefined time.

D 300 Redundant local area networks

301 The requirements of 200 shall be complied with.

302 Switching between the networks shall be automatic when serving functions with category R0 and R1. Otherwise switching may be manual as long as the switching is simple and unambiguous.

D 400 Instrument net

401 Instrument nets shall meet the requirements of local area networks.

D 500 Interconnection of networks

501 Networks interconnected shall be mutually independent.

Guidance note:
Means of interconnections may be routers, bridges or gateways.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

SECTION 5: COMPONENT DESIGN AND INSTALLATION

A. General

A 100 Environmental strains

101 FO sensing equipment shall be suitable for mining use, and shall be designed to operate under the environmental conditions as described in B.

102 Data sheets, which are sufficiently detailed to ensure proper application of the instrumentation equipment shall be available.

103 If sufficient data sheets are not available, performance and environmental testing should be performed in order to ascertain the suitability of the equipment.

A 200 Materials

201 Explosive materials and materials, which may develop toxic gases shall not be used. Covers, termination boards, printed circuit cards, constructive elements and other parts that may contribute to spreading fire shall be of flame-retardant materials.

A 300 Component design and installation

301 Component design and installation shall facilitate operation, adjustment, repair and replacement. As far as practicable, screw connections shall be secured.

302 Mechanical resonance with amplification greater than 10 shall not occur.

303 Electric cables and components shall be effectively separated from all equipment, which, in case of leakage, could cause damage to the electrical equipment. In desks, consoles and switchboards, which contain electrical equipment, shall pipes and equipment conveying water or other fluids or steam under pressure be built into a separate section with drainage.

304 Means shall be provided for preventing moisture (condensation) accumulating inside the equipment during operation and when the plant is shut down.

308 Clamps used to secure capillary tubes shall be made of a material that is softer than the tubing.

A 400 Maintenance, checking

401 Maintenance, repair and performance tests of systems and components shall as far as practicable be possible without affecting the operation of other systems or components.

Guidance note:
The installation should, as far as possible, be built up from easily replaceable components and designed for easy troubleshooting, checking and maintenance. When a spare component is mounted, only minor adjustments or calibrations of the component should be necessary. Faulty replacements should not be possible.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 500 Marking

501 All equipment and test points shall be clearly and permanently marked.

Guidance note:
The marking of system identification should preferably not be placed on the equipment itself, but adjacent to it.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 600 Standardisation

601 Guidance related to standardisation:
Guidance note:
Systems, components and signals should be standardised as far as practicable.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B. Environmental Conditions, Instrumentation

B 100 General

101 The environmental parameters specified in 200 to 1200, including any of their combinations, represent «average adverse » conditions to be fulfilled, which will cover the majority of applications Where the environmental strains will exceed those specified in 200 to 1200, the corresponding requirements shall be modified accordingly.

B 200 Electric power supply

201 Power supply failure with successive power breaks with full power between breaks:
— 3 interruptions during 5 minutes
— switching-off time 30 s each case.

202 Power supply variations for equipment connected to A.C. systems:
— combination of permanent frequency variations of ± 5% and permanent voltage variations of + 6 / - 10% of nominal
— combination of frequency transients (5 s duration) ± 10% of nominal and voltage transients (1.5 s duration) ±20% of nominal.

203 Power supply variations for equipment connected to D.C. systems:
— voltage tolerance continuous ± 10% of nominal
— voltage transients cyclic variation 5% of nominal
— voltage ripple 10%.

204 Power supply variations for equipment connected to battery power sources:
— + 30% to - 25% for equipment connected to battery during charging
— + 20% to - 25% for equipment connected to battery not being charged
— voltage transients (up to 2 s duration) ± 25% of nominal.

B 400 Temperature

401 Class A: Ambient temperatures + 5 °C to + 55 °C.

402 Class B: Ambient temperatures + 5 °C to + 70 °C.

403 Class C: Ambient temperatures – 25 °C to + 55 °C.

404 Class D: Ambient temperatures – 25 °C to + 70 °C.

B 500 Humidity

501 Class A: Relative humidity up to 96% at all relevant temperatures, no condensation.

502 Class B: Relative humidity up to 100% at all relevant temperatures.

B 600 Salt contamination

601 Salt-contaminated atmosphere up to 1 mg salt per m3 of air, at all relevant temperatures and humidity conditions.

B 900 Vibrations

901 Class A
— frequency range 3 to 100 Hz
— amplitude 1 mm (peak value) below 13.2 Hz
— acceleration amplitude 0.7 g above 13.2 Hz.

902 Class B
— frequency range 3 to 100 Hz
— amplitude 1.6 mm (peak value) below 25 Hz
— acceleration amplitude 4.0 g above 25 Hz.

903 Class C
— frequency range 3 to 50 Hz
— amplitude 3 mm (peak value) below 13.2 Hz
— acceleration amplitude 2.1 g above 13.2 Hz.

B 1100 Electromagnetic interference

1101 Minimum immunity to electromagnetic interference with regard to the state of the art of technology is required.

Guidance note:
Electrical and electronic equipment should be designed to function without degradation or malfunction in their intended electromagnetic environment. The equipment should not adversely affect the operation of, or be adversely affected by any other equipment or systems used on board or in the vicinity of the unit.
Upon installation, it may be required to take adequate measures to minimise the electromagnetic noise signals. Such measures may be in form of a list of electromagnetic noise generating and sensitive equipment, and an estimate on required noise reduction, i.e. an EMC management plan. Testing may also be required to demonstrate electromagnetic compatibility.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B 1200 Miscellaneous

1201 In particular applications other environmental parameters may influence the equipment, such as:

- fire
- explosive atmosphere
- temperature shock

— wind, rain, snow, ice, dust
— audible noise
— mechanical shock or bump forces equivalent to 20 g of 10 ms duration
— splash and drops of liquid
— corrosive atmospheres.

C. Electrical and Electronic Equipment

C 100 General

101 Fused isolating transformers shall be fitted between the main power supply and the different equipment or systems.

102 Switching of the power supply on and off shall not cause excessive voltage or other strains that may damage internal or external components.

103 Equipment requiring insulating resistance in cables and wiring higher than 200 k? shall normally not be used. Exceptions can be made for special cable arrangements.

104 Key components of computer based systems necessary for maintaining essential and important functions shall be subjected to burn-in for 72 hours at 70 °C (temperature in environment) or an equivalent screening procedure. Power shall be supplied to the devices during burn-in.

Guidance note:
Examples of equivalent screening procedure:
- use of components subjected to burn-in by the manufacturer
- operation for 1000 hours at 20 °C.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

C 200 Mechanical design, installation

201 The components shall be effectively secured to avoid mechanical stressing of wires and soldered joints through vibrations and mechanical shock.

Guidance note:
Components weighing more than 10 g should not be fastened by their connecting wires only.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

Guidance note:
Circuits should be designed to prevent damage of the equipment or adjacent elements by internal or external failures. No damage should occur when the signal transmission lines between measuring elements and other components are short-circuited, grounded or broken. Such failures should lead to a comparatively safe condition (fail to safety).
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

Guidance note:
The equipment should preferably function without forced cooling. Where such cooling is necessary, precautions should be taken to prevent the equipment from being damaged in case of failure of the cooling equipment.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

C 300 Protection provided by enclosure

301 Enclosures for the equipment shall be made of steel or other flame retardant material capable of providing EMC protection. The required degree of protection is defined in IEC 60529.

Guidance note:
Equipment of class A and B that shall be in operation during emergency situations, located in areas exposed to wash down, should have IP 55 protection.
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

C 400 Cables and wires

401 Cables and wires shall comply with the requirements of the mine operators standard and norms for electrical systems and equipment.

C 500 Cable installation

501 Cable installations shall comply with the requirements of the mine operators standard and norms for electrical systems and equipment.

C 600 Power supply

601 When using low voltage battery supply, the charging equipment, batteries and cables shall keep the voltage at equipment terminals within + 25% to - 20% of the nominal voltage during charging and discharging. Provisions shall be made for preventing reverse current from the battery through the charging device.

602 Systems including a standby battery connected for continuous charging shall not be disturbed in any way by disconnection of the battery.

603 Battery installations shall be in accordance with the mine operators standard for electrical systems and equipment.

604 Regulated rectifiers shall be designed for the variations in voltage and frequency stated in B.

605 Different system voltages shall be supplied through different cables.

606 Terminal lists shall be clearly marked. Various system voltages shall be distinguished.

607 Uninterruptable power supplies shall comply with the requirements of the mine operators standard for electrical systems and equipment with respect to electromagnetic noise and interference and with respect to voltage variations.

D. Fibre optical equipment

D100 General

104 Fibre optic systems using standard single and multimode fibres to be used for intrinsically safe circuits in hazardous areas shall have a power level below 10 mW.

D200 Mechanical design and installation

201 The safety of personnel and operations shall be considered in the installation procedures. Warningsigns and labels giving information to the operators shall be placed where hazard exists. Care must be taken to prevent fibres from penetrating eyes or skin.
It is advised to use equipment with 'built-in' safety, e.g. interlock the power to the light sources with the covers, possible to disconnect or lock parts of the system under service, screen laser beams.

Guidance note:
The safe distance between the light source or fibre end and the eye of the operator shall be given and applied
---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

202 Power budget calculation shall be used to:
— determine the length between I/O components
— select components to obtain a safe reliable transmission system
— demonstrate that adequate power reserve has been provided.
After installation, optical power measurements for each fibre shall be used to correct and re-evaluate the power budget calculations.

D300 Protection provided by enclosures

301 Enclosures for the fibre optical equipment shall be made of steel or other flame retardant material capable of providing EMC protection. The required degree of protection is defined in IEC 60529.

D500 Minimum standards

All fibre optical and electro-optical componenets that will be used in the FO sensing system have at least to to meet the Telcodia and ITU standards listed in Table D1.

Component	**Standard**
Network Interface Devices	GR-49-CORE
Network Equipment-Building System Requirements (NEBS): Physical Protection	GR-63-CORE
Singlemode Optical Connectors and Jumper Assemblies (Fiber Optics)	GR-326-CORE
Optoelectronic Devices	GR-468-CORE
Fiber Optic Branching Components	GR-1209-CORE
Optical fibres	G. 651 / G.652
Passive Optical Components	GR-1221-CORE

Table D1: Telcordia standards defined for different components

APPENDIX

Normative References

European Norm EN 10012
Measurement management systems - Requirements for measurement processes and measuring equipment (ISO 10012:2003)

European Norm EN 60794-1-1/A1
Optical fibre cables - Part 1-1: Generic specification - general (IEC 60794-1-1/A1:2000-01)

European Norm EN 60794-1-1
Optical fibre cables - Part 1-1: Generic specification - general (IEC 60794-1-1: 2001)

European Norm EN 60794-1-2
Optical fibre cables - Part 1-2: Generic specification - Basic optical cable test procedures (IEC 60794-1-2: 1999)

European Norm EN 61757-1
Fibre optic sensors - Part 1: Generic specification (IEC 61757-1: 1998)
In addition: all European Norms and International Norms given as references within this norm.

European Norm EN 60793-1-44 (EN 188000)
Optical fibres (2001, 1992)

European Norm EN 186000-1
Generic specification: Connector sets for optical fibres and cables Part 1: Requirements, test methods and qualification approval procedures

European Norm EN 50014
Electrical apparatus for potentially explosive atmospheres, Part 1 - 20

International Standard CEI IEC 60874-1
Connectors for optical fibres and cables - Part 1: Generic specification

ITU-T Recommendations G.651
Series G: Transmission systems and media, digital systems and networks, transmission media characteristics - optical fibre cables: Characteristics of a 50/125 µm multimode graded index optical fibre cable.

ITU-T Recommendations G.652
Series G: Transmission systems and media, digital systems and networks, transmission media characteristics - optical fibre cables: Characteristics of a single-mode optical fibre cable.