Cyber security assessment process
for industrial control systems

Industry Information Sheet 2

EEMUA Industry Information Sheets are issued free of charge to ALL. Information Sheets are compiled by the EEMUA Technical Committees and the EEMUA Executive in good faith as a service to all across industry.
Cyber security assessment process for industrial control systems

Industry Information Sheet 2
Engineering Equipment and Materials Users Association

About EEMUA

The Engineering Equipment and Materials Users Association is usually known by its initials, EEMUA. EEMUA is an Association established by the owners and operators of industrial assets. Any organisation that is a substantial user or substantial purchaser of engineering products is eligible to apply to become a member of EEMUA. Membership is subject to the approval of Council.

EEMUA aims

EEMUA aims to improve the safety, environmental and operating performance of industrial facilities in the most cost-effective way, pursuing and promoting leadership in industrial asset management by sharing engineering experiences and expertise, and by the active, enlightened promotion of the distinct interests of users of engineering products. These aims are achieved by various means, including:

- Providing the organisation within which networking, information sharing and collaboration among users on non-competitive technical matters can take place.
- Influencing the way written regulations are interpreted and applied in practice.
- Promoting and presenting members’ views, and encouraging the application of good sound engineering practices.
- Developing user guides, specifications, training and competency schemes.
- Facilitating members’ participation in national and international standards making.
- Influencing relevant national and European legislation and regulation.

The income and resources of EEMUA are applied solely towards the promotion of the aims of the Association. No profit is transferred by way of dividend, bonus or otherwise to members. The work of the Association is mainly carried out by members’ representatives on EEMUA Technical Committees, Working Groups, and Forums, supported by EEMUA staff.

Incorporation, membership and other information

For the purposes of conducting its business, EEMUA is incorporated in England and Wales as a company, limited by guarantee, not having share capital. All usual aspects of company management and business administration are dealt with through the EEMUA Chief Executive, including policy implementation and leadership of the Executive team (the staff).

A list of EEMUA Publications for sale is given at the end of this Information Sheet. The full list is also on the Association’s website, including details of on-line shopping facilities.

To enquire about corporate Membership, write to ask@eemua.org or call +44 (0)20 7488 0801.
About this Publication

Legal aspects

All rights, title and interest in this Publication belong to EEMUA. All rights are reserved. No part of this Information Sheet may be reproduced, stored in a retrieval system, or transmitted in any form or by any means: electronic, mechanical, photocopying, recording or other, without the express prior written agreement of the EEMUA Chief Executive. Infringement of copyright is illegal and can reduce the Association’s income thereby jeopardising its ability to fund the production of future information sheets and publications.

It has been assumed in the preparation of this Information Sheet that: the user ensures selection of those parts of its contents appropriate to the intended application; and that such selection and application is correctly carried out by appropriately qualified and competent persons for whose guidance this Information Sheet has been prepared. EEMUA and the individual members of the Work Group that prepared this EEMUA Information Sheet do not, and indeed cannot, make any representation or give any warranty or guarantee in connection with material contained herein. EEMUA and the individual members of the Work Group that prepared this EEMUA Information Sheet expressly disclaim any liability or responsibility for damage or loss resulting from the use or reliance on this Information Sheet. Any recommendations contained herein are based on the most authoritative information available at the time of writing and on current good engineering practice, but it is essential for the user to take account of pertinent subsequent developments and/or legislation.

Any person who encounters an inaccuracy or ambiguity when making use of this Information Sheet is asked to notify EEMUA without delay so that the matter may be investigated and appropriate action taken.
Contents

Cyber security assessment process ........................................................................................................1
  Process steps .................................................................................................................................. 1

Appendix A ...................................................................................................................................... 5
  References ...................................................................................................................................... 5
  Existing guidance ........................................................................................................................... 5

Appendix B ...................................................................................................................................... 6
  Good practice and possible easy wins ............................................................................................ 6
  What good looks like – how to make security work in the long term ........................................... 7

Appendix C ...................................................................................................................................... 8
  Risk assessment using the bow tie approach .................................................................................. 8

Appendix D ...................................................................................................................................... 10
  Special considerations for geographically remote sites ............................................................... 10
    Physical security ......................................................................................................................... 10
    Wireless point-to-point links ...................................................................................................... 10
    Remote access protocols ............................................................................................................ 10
    Dial-up (modem) access .............................................................................................................. 10
  Use of third parties ........................................................................................................................ 10

EEMUA Publication: feedback form .................................................................................................. 11
  EEMUA Publications Catalogue .................................................................................................... 12
  Asset and integrity management .................................................................................................... 12
  Automation and electrical equipment ........................................................................................... 12
  Pressure equipment ....................................................................................................................... 13
  Process pipework, valves and machinery ...................................................................................... 14
  Storage and containment systems ................................................................................................ 14
Glossary of terms

The following is a list of terms used throughout the information.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Havex</td>
<td>A type of remote access malware</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>CPNI</td>
<td>Centre for the Protection of National Infrastructure</td>
</tr>
<tr>
<td>P&amp;ID</td>
<td>Piping and Instrumentation Diagram</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control And Data Acquisition</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control Systems</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>Snort</td>
<td>A type of free and open source intrusion detection and protection system</td>
</tr>
<tr>
<td>ISA</td>
<td>International Society of Automation</td>
</tr>
<tr>
<td>VGB</td>
<td>Vereinigung der Grosskesselbesitzer (German power generators association)</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology (USA)</td>
</tr>
<tr>
<td>HSE</td>
<td>Health and Safety Executive (UK)</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>A wireless local area network based on IEEE standards.</td>
</tr>
</tbody>
</table>
Cyber security assessment process

This assessment process has been designed for use by an on-site engineer who has been tasked with making sure appropriate cyber security protection measures are in place. Written for those with limited prior knowledge, it should still be useful for others by providing a framework to maintain any existing protection measures and increase their confidence in a rapidly changing technical field.

It is predominately aimed at those working on physically contained sites but some further considerations for geographically distributed systems are given in Appendix D.

Process steps

Step 1. Define the roles and responsibilities.

Who has given you the task and are they ultimately the responsible person for the site’s cyber security and owner of the action plan? Are senior management aware of the responsibilities and potential risks and therefore prepared to provide necessary resource?

Conducting an initial audit can be a good way to raise both local and corporate management awareness. Useful examples such as the HAVEX incident can really help make the message relatable.

It is advisable to involve an I.T. representative at an early stage. Even though the systems are treated separately they will have (increasing) interactions and good co-operation is vital.

Step 2. Self-education

This should start with becoming very familiar with any relevant company policies and procedures, including those more focused on I.T. systems and the documentation for the system being assessed. Secondly, there is a need for general awareness training, for which particularly in terms of understanding current good practice, there is a considerable amount of existing guidance freely available, some of which is listed in Appendix A.

A number of third parties (including vendors) run various training courses. EEMUA would specifically recommend those run by the CPNI which includes a course designed for senior management.

Note: The main outcome required from this step is the ability to baseline the operations and systems being assessed.

Step 3. Documentation

There are two main activities within this step:

Step 3a. Firstly the identification of what inventory you have on site that could affect the control system. This is to include both hardware and software elements. Note: Make sure that the inventories themselves are managed and stored in a secure manner. It’s often interesting to ask colleagues about their awareness of document ‘classifications’ to make sure that they understand how certain documents are permitted to be handled and stored.
Step 3b. The second activity is to make sure you are confident of how the various pieces of equipment are connected. This activity is about knowing what you’ve got. A ‘P&ID’ diagram is not sufficient for this purpose as a detailed understanding of any system interconnections. Again, this is required for both hardware and software. How is the vendor’s system integrated into your plant? What protocols are used? What were their special needs and what were yours? You need to do a survey to document the site as built (including updates for any subsequent modifications).

The purpose of step 3 is to facilitate the assessment of risk, so that distinct areas of high and low risk can be identified, as can the data flows between them. In IEC standards terms these areas and flows are referred to respectively as Zones and Conduits.

The identification of wireless links, networks and their connectivity is particularly difficult. Devices may make irregular connections, may be members of more than one network, may sometimes be switched off or be off-site. Added to this there may be some uncertainty about range and coverage.

Note: The following steps should be straightforward if this step is properly completed, so don’t be afraid of spending a significant amount of time getting it right.

Step 4. Risk assessment

This step is further subdivided into two process (Quantitative and Qualitative assessments) which do not have to be done sequentially although there may be some benefit from that. The CPNI Good Practice Guide: Process Control and SCADA Security - Understand the Business Risk! provides useful advice on the general process and an example.

Note: For both types of risk assessment it’s important to make sure you are assessing the right thing. As opposed to individual pieces of equipment, more logical ‘chunks’ of systems should be considered. Boundaries for the chunks could include protocol changes, firewalls or different IP networks.

In practice assessments are often carried out hierarchically, with some method to move from the assessment of larger ‘chunks’ down to their constituent parts. It can be useful to do a high level risk analysis first. This is particularly so when it isn’t clear at the outset where to set the boundaries for the detailed risk assessment. A well-structured environment on a large industrial site might be expected to contain at the minimum:

- A business tier
- A DMZ (demilitarized zone)
- A plant control tier
- A safety tier
- A set of inter-connection rules

The inter-connection rules would be applied by firewalls placed between tiers and/or logical chunks. Note that to enforce effective separation, firewalls must be specified to be capable of filtering all the protocols in use in the tiers that they interconnect. Firewalls suitable for ICS/SCADA protocols are available but are not common, therefore it is important to be aware of a specific firewall’s capabilities (and whether it is correctly configured).

Step 4a. Quantitative assessment

Most companies will already have internal risk assessment procedures or at least a standard way of carrying them out. These will involve some means of attributing a number to both the likelihood of the risk occurring and the severity of the potential impact. Consideration must be
given however to the method’s suitability for Cyber Security i.e. does it allow for non-standard design of control system infrastructure, and if it outlines priorities such as availability vs. confidentiality, do they still hold for control systems.

This process should result in a “score” which can be used as a benchmark against future assessments.

It is important to involve all stakeholders in this process. Don’t rely on site engineers for this information – a survey is required to ensure an accurate list. There will be illogical dependencies (such as an HMI screen feeding data to a central system) or timestamp times derived from a non-primary source (another system) due to historic projects. Where such instances of poor design are uncovered it may be appropriate to put in place a fix, if possible, before completing the assessment.

It is advised to include all systems and then decide on whether they are in or out of scope during the assessment phase. For example, an emissions monitoring system may have no physical or software connection to the control system, but if it was compromised and made to read erroneously high, the station (and therefore the control system) may have to cease production to comply with Environmental legislation. Similar considerations may be true for CCTV, site security and fire systems.

**Step 4b. Qualitative assessment**

EEMUA members have found that methods like a ‘bow tie’ assessment may be used although other equally suitable approaches are available. CAUTION: A rigorous application of bow tie assessment may not work but the general methodology is applicable. An example of such an analysis for a generic site is contained in Appendix C.

*Note: This form of assessment or ‘gap analysis’ is useful to help prioritise improvement opportunities.*

It is vital to do this analysis with a mixed team and to make sure Operations are suitably involved. The assessment work itself can act as a very useful way to raise their levels of education and awareness on the topic. Consider whether you can attribute a KPI to each control measure in order to better monitor performance. Control measures need to be defined which are relevant and should be grouped as ‘enhanced’ and ‘normal’.

**Step 5. Time-bound Action plan**

There are a number of items which might be included in the Action Plan but the following are representative:

- Maintenance plan/activities – including patching
- Training / Education
- Re-engineering of networks
- Device hardening
- Password and media controls
- Authentication
- Physical security upgrade
- Encryption where possible
- Procedure writing
- Formal change procedures
- Configuration controls (including firewall configurations)
- Security incident response planning
- Disaster recovery/mitigation planning
- End-to-end testing
- Implementing quick wins
- Implementing good practice
- Walking the job
- Use of hardware and software discovery and inventory management tools

To which could be added:

- Implementation of extra good practice measures
Risk assessment 4b should have helped identify the ‘quick wins’. Typically they would be things like physical access control, USB and network port physical blockers, disabling of unused network switch ports, changing of default passwords and enforcement of password policies. Whitelisting can also be very effective, although it can be seen as onerous to implement and maintain (but possibly less onerous than frequent patching).

Extra good practice measures could include:

- Intrusion detection – use of tools such as SNORT
- Penetration testing
- Deployment of ICS/SCADA honeypots.

Extra good practice measures generally require a high level of specialist expertise but will provide potential benefits in identifying soft or attractive targets, the sources of attacks and the methods used.

The cyber security action plan should be included in the overall action plan for each site and assigned an appropriate priority consistent with business risk, so that there is high level ownership of risk with a hierarchy of ownership of each mitigation task and sub-task.

**Step 6. Continuous Improvement**

It is advised that at appropriate periodic intervals based on perceived risk the process is repeated by returning to Step 2. Re-evaluation may also be needed as a result of upgrades and changes. There is a quickly changing threat landscape, emerging technologies and cyber security responses should be used to define a shorter periodic interval than might otherwise be assumed. Continuous improvement should be used in refining the action plan implementation and risk assessment. It may be useful to note that many

EEMUA members are starting to assign permanent human resource to the ICS/SCADA cyber security role to make sure it doesn’t suffer from falling in between role responsibilities.
Appendix A

References


Existing guidance

Useful guidance is available on cyber security topics from the following sources:

- ISA 99 / IEC 62433 – in preparation
- CPNI – extensive web site with many guides on various topics: http://www.cpni.gov.uk/
- VGB175 – particularly relevant to generating plant: http://www.vgb.org/
- NIST800: – various parts on particular topics: http://www.nist.gov/
- Future learn – Introduction to cyber security – a free on-line course: https://www.futurelearn.com/courses/introduction-to-cyber-security
- Manufacturer-led training courses
- Security company websites, eg ICS/SCADA specific:
- General:
  - Secunia: http://secunia.com/
  - Symantec: http://www.symantec.com/
  - Bluecoat: https://www.bluecoat.com/
  - Greycastle security: http://www.greycastlesecurity.com/
  - Vectra networks: http://www.vectranetworks.com/
Appendix B

Good practice and possible easy wins

What is listed here may not be applicable or even possible in every case, and in any case should be considered on its merits for the risk environment. For example, extra locks for increased physical security might also carry a risk of not being able to access certain parts of the site sufficiently promptly to complete some time-critical operation.

- Don’t overlook physical security – door locks, alarms, CCTV.
- Devices should be password protected wherever technically feasible. Password strength should be enforced. Periodic password changes should be enforced as appropriate.
- Change default passwords. It can be most enlightening to do a Google search on the phrase “default password”. Hackers do it regularly.
- Change admin passwords. Try a Google search for “default admin password”. You should now be in no doubt that changing default passwords is necessary!
- Perform actions with the lowest feasible level of account privilege – the admin account should not be used for everything.
- Patch up-to-date where feasible.
- Secure network ports. This might be done, for example by use of software which implements the IEEE 802.1x standard to prevent devices connecting to the network without first authenticating. Be aware that this may still permit a determined attacker at least to gather information by listening on a network port. Physically preventing access to the ports with a lockable access plate or placing the device in a lockable cabinet are other possibilities.
- Secure device USB ports wherever technically feasible. This may be done using software which denies access to devices which aren’t recognised. However there may be technical limitations on this policy due to use of legacy hardware or software or incompatibility with the method of applying patches. Lockable port blockers to insert into USB sockets are also available, but many do not provide high security.
- Consider using encryption on storage media – hard disks (especially if removable or in laptops), USB devices, CDs and DVDs. This may not be feasible for backup and recovery media.
- Ensure that any on-site backup and recovery media are securely stored, for example in a data safe, with one or more recent copies also securely held off-site.
- Where remote access is permitted or on sites where physical security may be difficult to maintain, it may be appropriate to consider use of one or more of:
  - Link encryption.
  - Virtual Private Network (VPN).
  - IP tunnelling (SSL/TLS).
  - Two part authentication.
  - Failed authentication lockout timer.
  - Time-limited connection.
- Disable Wi-Fi if it isn’t needed. If it is, ensure that access is password protected with encryption on, and of the most secure level that the equipment supports. Better still, if the equipment only supports older security protocols, consider a wireless modem upgrade or replacement to support higher security. Remember that wireless networks are intrinsically insecure and even with the best encryption are vulnerable to an attack, given sufficient interception and analysis time.
- Disable Bluetooth and infra-red if they are not needed.
- Document site inventory and configuration and carry out periodic audits of both.


- Keep a record of logins and physical site access times, and identify any discrepancies.
- Remove the access credentials of those people (staff, contractors, vendors) who no longer need access.
- Ensure that access provided, physical or IT, is appropriate to role and work area.
- People who are entrusted with access to critical systems should be vetted to an appropriate level.

**What good looks like – how to make security work in the long term.**

The items listed above are a good basis for improvements, but inevitably will fall into disuse unless business structures are put in place which are supportive of them. At a minimum there should be:

**Procedures:**

- Business as usual – including backups, testing and periodic security reviews;
- Change and configuration management – including patching and rule changes;
- Security incident and emergency procedures.

**Architectural standards:**

- System rules - build and configuration – physical and logical;
- Connectivity rules – physical and logical – including firewalls and whitelisting.

The definition of these is beyond the scope of this information sheet.
Appendix C

Risk assessment using the bow tie approach

In the bow tie approach there is a top event (manifestation of a hazard—an adverse event) which can be triggered by one or several threats. Barriers are provided to protect the system from these threats. The operation of the barriers may be impaired by various decay modes for which decay control measures need to be put in place. Further barriers need to be erected to prevent the hazard resulting in one or several adverse consequences.

The bow tie method has the advantage that for a particular hazard the possible preventive measures and the results of their erosion can be clearly seen. Likewise, given that a hazard has manifested itself, the barriers to its consequential impacts can be clearly seen. The following bow tie diagram is a simplified fragment of a bow tie assessment of the IT infrastructure of an industrial site. The principles used for this are outlined in Research Report RR 637 - Optimising hazard management by workforce engagement and supervision, published by the UK HSE.
Appendix D

Special considerations for geographically remote sites

Physical security

For remote sites physical security is likely to be harder to maintain than for core sites. Even if a physical intrusion is detected it may be difficult to provide a prompt and adequate response. Therefore it is important that an intruder should encounter layers of security, which make mounting an attack a time-consuming business.

Wireless point-to-point links

These may be old technology, possibly analogue or possibly digital without encryption. A risk assessment should be done and mitigations identified, e.g. encryption applied to the end-to-end data flow. Link availability might be degraded through jamming. What impacts might that have? On links which have poor or non-existent security, man-in-the-middle attacks are a real possibility. What might be the consequences of missing, extra or altered messages and how might they be mitigated?

Remote access protocols

These should be disabled if not essential. Telnet in particular is an easy target for attackers. If at all possible it should be replaced with an end-to-end encrypted protocol such as SSL. If that isn’t possible then link encryption should be used.

Dial-up (modem) access

Dial-up (modem) access should be curtailed if possible. If not, then it should be permitted only with extra security measures in place such as those recommended for remote access, plus called number ring back to whitelisted numbers only. Access should be password controlled. Be aware that calling number identification can be spoofed and should not be relied upon.

Use of third parties

Whilst it may be economically attractive to use third parties (‘contractors’) to carry out operations at remote sites, there should be a mechanism for regular validation and audit of their activities. Non-disclosure agreements and penalty clauses are no substitute for consistent and demonstrable trustworthiness.
# EEMUA Publication: feedback form

An electronic version of this form is available at www.eemua.org

<table>
<thead>
<tr>
<th>Date feedback provided: (dd/mm/yyyy)</th>
<th>EEMUA Industry Information Sheet 2 Cyber security assessment process for industrial control systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feedback provided by:</td>
<td>Feedback provided on behalf of which organisation?</td>
</tr>
<tr>
<td>Contact name:</td>
<td>Organisation name:</td>
</tr>
<tr>
<td>Phone:</td>
<td>Location:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EEMUA ref (EEMUA use only)</th>
<th>Page no.</th>
<th>Paragraph Figure/Table concerned</th>
<th>Type of comment (General/Technical/Editorial)</th>
<th>COMMENTS</th>
<th>Proposed change (Please provide alternative wording, or propose removal of, or addition to, existing wording.)</th>
<th>OBSERVATIONS OF THE EXECUTIVE (EEMUA use only) on each comment submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Fig 2</td>
<td>E</td>
<td>This is an example only</td>
<td>No change to wording required</td>
<td>Example only</td>
<td></td>
</tr>
</tbody>
</table>

When you have completed this form with all your comments, please save and e-mail to info@eemua.org or post a paper copy to: Publications Department, EEMUA, 63 Mark Lane, London EC3R 7NQ.
EEMUA Publications Catalogue

All EEMUA Publications can be purchased on-line. To order a Publication, please contact EEMUA at www.eemua.org, telephone: +44 (0)20 7488 0801, fax: +44 (0)20 7488 3499 or e-mail: sales@eemua.org. List complete at time of print. Check EEMUA website for most up to date publication list.

Asset and integrity management

232 Specifying, procuring & managing 3rd party inspection service
231 The Mechanical Integrity of Plant Containing Hazardous Substances: A Guide to Periodic Examination and Testing
206 Risk Based Inspection: A Guide to Effective Use of the RBI Process
193 Recommendations for the Training, Development and Competency Assessment of Inspection Personnel
181 A Guide to Risk Based Assessments of In-situ Large Ex ‘e’ and Ex ‘N’ Machines
161 Guide to the Selection and Assessment of Silencers and Acoustic Enclosures
159 Users’ Guide to the Inspection, Maintenance and Repair of Above-ground Vertical Cylindrical Steel Storage Tanks
148 Reliability Specification - Model clauses for inclusion in purchasing Specifications for equipment items and packages

Automation and electrical equipment

226 Design and installation of on-line analyser systems - a guide to technical enquiry and bid evaluation
222 Guide to the Application of IEC 61511 to Safety Instrumented Systems in the UK Process Industries
214 Toolbox Guide - Electrical Installation, Inspection and Maintenance in Potentially Explosive Atmospheres
201 Process Plant Control Desks Utilising Human-Computer Interfaces - A Guide to Design, Operational and Human Interface Issues
189 A Guide to Fieldbus Application for the Process Industry
186 A Practitioner’s Handbook - Electrical Installation, Inspection and Maintenance in Potentially Explosive Atmospheres
178 A Design Guide for the Electrical Safety of Instruments, Instrument/Control Panels and Control Systems
175 Code of Practice for Calibration and Validation of Process Analysers
155 Standard Test Method for Comparative Performance of Flammable Gas Detectors against Poisoning
138 Design and Installation of On-Line Analyser Systems

Materials selection, plant design and construction

234 90/10 copper nickel alloy piping for offshore applications (incorporating EEMUA 144,145 and 146)
Quality assurance of safety-critical engineering equipment and materials: A guide to risk-based procurement

Quality requirements for the manufacture/supply of duplex stainless steels

Specification for the Fabrication of Non-Primary Structural Steelwork for Offshore Installations

Guidelines for Materials Selection and Corrosion Control for Subsea Oil and Gas Production Equipment

Guide for Hot Tapping on Piping and other Equipment

Specification for Integral Block and Bleed Valve Manifolds for Direct Connection to Pipework

A Working Guide for Carbon Steel Equipment in Wet H2S Service

Specification for Structural Castings for Use Offshore

Construction Specification for Fixed Offshore Structures in the North Sea

Guidance to Owners on Demolition of Vertical Cylindrical Steel Storage Tanks and Spheres

Code of Practice for the Identification and Checking of Materials of Construction in Pressure Systems in Process Plants

Recommendations for the Design and Construction of Refrigerated Liquefied Gas Storage Tanks

Guide to the Use of Noise Procedure Specification

Noise Procedure Specification

Specification for Underground Armoured Cable Protected against Solvent Penetration and Corrosive Attack

Factory Stairways, Ladders and Handrails (incl: Access Platforms/Ramps)

Noise: A Guide to Information required from Equipment Vendors

Lifting Points - A Design Guide

Pressure equipment

Pressure equipment testing after repair, modifications or re-rating: a guide to the pressure test waiver

Guidance on the Specification of pressure vessels

Guide to life-cycle management of Pressure

Piping and the European Pressure Equipment Directive: Guidance for Plant Owners/Operators

Valve Purchasers’ Guide to the European Pressure Equipment Directive

Guide to the Isolation of Pressure Relieving Devices


A Guide to the Pressure Testing of In-Service Pressurised Equipment

Code of Practice for the Identification and Checking of Materials of Construction in Pressure Systems in Process Plants
Process pipework, valves and machinery

230 Ageing rotating equipment: Guide for maintenance and operation
205 Guide to the Production Testing of Valves for the Energy, Process, Oil and Gas Industries
204 Piping and the European Pressure Equipment Directive: Guidance for Plant Owners/Operators
200 Guide to the Specification, Installation and Maintenance of Spring Supports for Piping
199 On-Line Leak Sealing of Piping - Guide to Safety Considerations
196 Valve Purchasers’ Guide to the European Pressure Equipment Directive
192 Guide for the Procurement of Valves for Low Temperature (non-cryogenic) Service
188 Guide for Establishing Operating Periods of Safety Valves
185 Guide for Hot Tapping on Piping and other Equipment
182 Specification for Integral Block and Bleed Valve Manifolds for Direct Connection to Pipework
164 Seal-less Centrifugal Pumps: Class 1
151 Liquid Ring Vacuum Pumps and Compressors

Storage and containment systems

217 Safe and effective operation of storage tanks for oil movements
213 Emission reduction from oil storage tanks and loading operations
207 Double Concrete Tanks for Liquefied Gas: Guidelines on design, construction and operation
190 Guide for the Design, Construction and Use of Mounded Horizontal Cylindrical Bulk Storage Vessels for Pressurised LPG at Ambient Temperatures
183 Guide for the Prevention of Bottom Leakage from Vertical Cylindrical Steel Storage Tanks
180 Frangible Roof Joints for Fixed Roof Storage Tanks: Guide for Designers and Users
159 Users’ Guide to the Inspection, Maintenance and Repair of Above ground Vertical Cylindrical Steel Storage Tanks
154 Guidance to Owners on Demolition of Vertical Cylindrical Steel Storage Tanks and Storage Spheres
147 Recommendations for the Design and Construction of Refrigerated Liquefied Gas Storage Tank