123 - Norwegian Oil and Gas Association
Guideline
for
Classification of process control, safety and support ICT systems based on criticality

Guideline title: Classification of process control, safety and support ICT systems based on criticality

Norwegian Oil and Gas Guideline 123 approved by:
Operations Committee — Approval date: 05.01.2009

Entry into force: 15.01.2009

Revision no: 01 — Revision date: 01.02.2009

Norwegian Oil and Gas Guideline 104 approved by:
Steering Group Integrated Operations — Approval date: 08.12.2006

Objective of the guideline:
To contribute to the improvement of the overall information security of the offshore industry on the Norwegian Continental Shelf, specifically safety, regularity and integrity of operations. To ensure that information security is adequately addressed in all ICT systems installed in production control, safety and support networks.

Status with the authorities:
This guideline is a supplement to the Norwegian Oil and Gas Guideline 104. Similar to the Guideline 104 this document has no formal relations to the authorities. However, the Petroleum Safety Authority Norway (PSA) and the Norwegian Petroleum Directorate (NPD) have had one observer each in the Work Group Information Security (WG IS) who produced the Norwegian Oil and Gas Guideline 104 document.

Web site location:
This guideline and the Norwegian Oil and Gas Guideline 104 *Information Security Baseline Requirements for Process control, safety and support ICT Systems* can be downloaded for free from Norwegian Oil and Gas's web site:
http://www.norskoljeoggass.no/retningslinjer/category180.html

TABLE OF CONTENTS

Foreword

A prerequisite to implement effective and efficient information security controls and measures is to have a clear understanding of the business needs of each system and importance of the system in the production environment. To simplify the process of ensuring that all necessary safeguarding measures have been implemented and prevent systems having uneven security levels within the same domain a classification system is useful – and in larger installations considered a necessity.

The document "Information Security Baseline Requirements for Process Control, Safety and support ICT Systems" (ISBR) was first issued in June 2006 as Norwegian Oil and Gas Guideline no. 104. The guideline consists of 16 requirements to operators and suppliers within the oil and gas industry on the Norwegian Continental Shelf. The IBSR #2 requires that "Risk assessment shall be performed for process control, safety and support ICT systems and networks". To help focus the risk assessment on essential systems, a classification of the ICT systems in the process control environment may be needed. This document is a guideline on how to perform classification of Process Control, Safety and support ICT Systems based on the systems criticality.

Scope

This guideline applies to all ICT systems for Process Control, Safety and Support (PCSS) which are part of any type of production or drilling facility.

The guideline does not apply to ICT systems installed in the corporate office domain. However, if systems needed to sustain production are placed on the corporate office domain, they should be included in the classification system to evaluate any information security controls and measures needed. Typical systems in this category might be weather systems, telecommunication systems, simulators, engineering systems, integrated operations work places, plant production optimizers, information management systems and remote services.

The target audience for this document include personnel responsible for carrying out the criticality assessment:

- Plant/installation manager
- System Owners
- Data Owners
- Information Security Responsible for the PCSS domain

Furthermore the following groups should be acquainted with the document:

- Design Engineers
- Technical Managers
- Vendors and suppliers of PCSS/ICT systems and services
- Operation Support Managers
- Discipline Advisors

Terms and definitions

Within the scope of this document:

Criticality is an indicator of the importance of an ICT system given its purpose in the production environment.

Criticality Level is a ranking that signifies the importance of the equipment or ICT system for maintaining defined aspects of HSSE (Health, Safety, Security & Environment) as well as the production operations.

Classification is the assignment to a particular Criticality Level.

HSSE is an abbreviation for Health, Safety, Security & Environment.

ICT system is defined as the combination of computer hardware, firmware and software, i.e. computers, operating systems, networks, communication equipment and applications (Ref. ISO/IEC 27005). In the PCSS domain this will typically entail ICT systems such as systems for monitoring process variables in the production environment, controlling motors and actuators, remotely programmable devices, smart sensors, flow computers, and condition monitoring.

PCSS is an abbreviation for Process Control, Safety and Support.

For other terms and definitions refer to Appendix B in Norwegian Oil and Gas Guideline no. 104 - Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems.
(http://www.norskoljeoggass.no/retningslinjer/category180.html)

Introduction

Criticality Assessment is not equal to Risk Assessment, but the output of the Criticality Assessment will be an input to the Risk Assessment. When performing a Risk Assessment, both the *probability* of an information security incident can happen and the *consequence* should the incident occur, are considered. When performing a Criticality Assessment only the *consequence* is considered. The *probability* of loss, interrupts or irregularities in the function or service is not an element that needs to be considered – only the *consequence* of an event or an incident is relevant for a criticality assessment.

In Figure 1 a simplified Risk Management Process is shown. During the Criticality Assessment the organisation should consider the importance of the ICT assets in the production environment. The consequences related to HSE, production regularity and information security should be assessed and evaluated, related to possible relevant ICT incidents. The results should be documented and used as an input to the Risk Assessment, where the most critical ICT systems should be assessed first. The output of the Risk Assessment should be a Risk Treatment Plan, to ensure that necessary and adequate information security controls and measures are implemented. The concept of the barriers to improve safety and security (as defined in the Norwegian Facilities Regulations – The Management Regulations § 2) shall always be paramount when producing the plan.

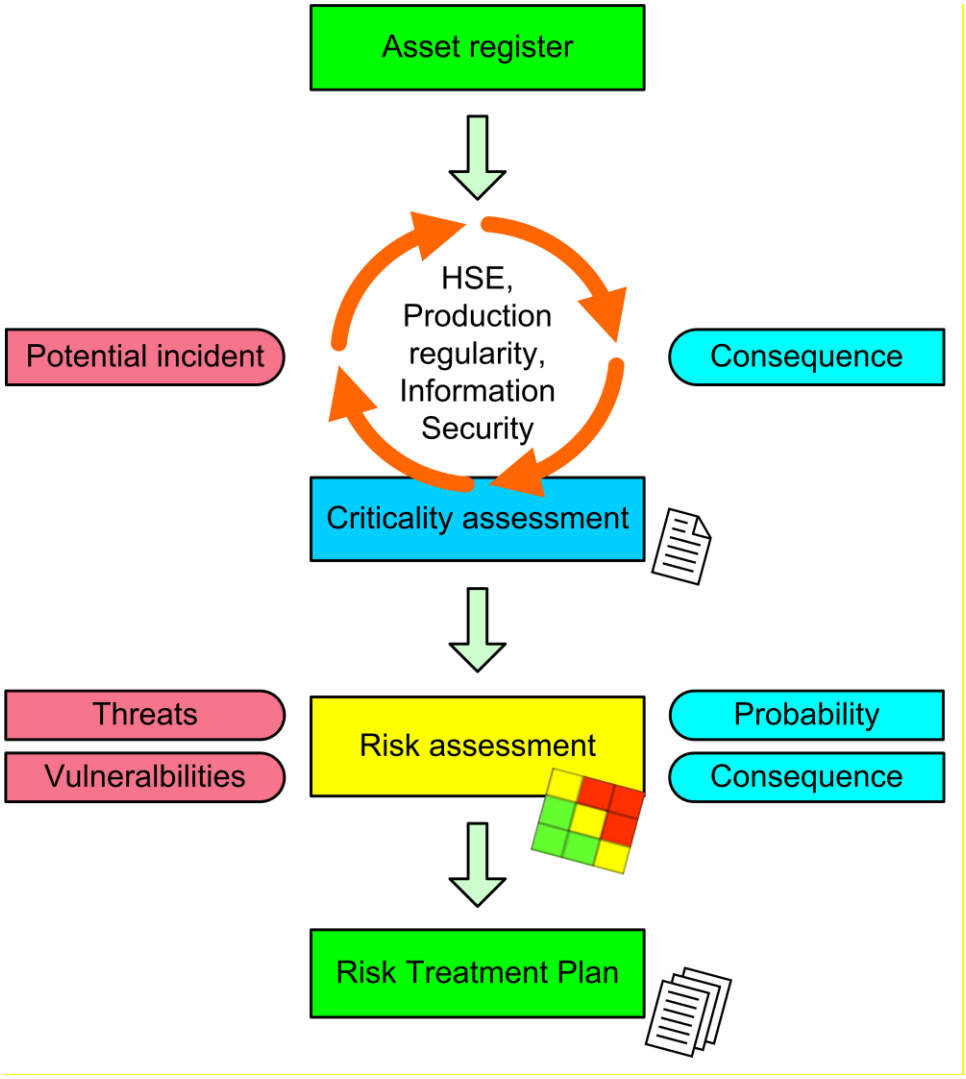


Figure 1: Risk management process

When evaluating the criticality of a function, the two following aspects should be considered:

- The consequences of interrupt or loss of the PCSS function
- The consequences of irregular functionality, malfunction or unexpected behaviour in the PCSS function

The criticality of a PCSS/ICT system depends on the context where it is used and may vary from installation to installation. It will also differ depending on where the system is used; is the system deployed in a production environment or in a drilling operation; is it on a platform or a floater; is it offshore or onshore? Furthermore, the criticality may change over time, depending on the character of the process' and the reservoir's nature, character and state, as well as other factors such as new or changed business objectives, new or updated regulations, major process modifications and tie-ins of other fields. The occurrence of such factors should trigger a repeat of the classification process. Furthermore, it is recommendable to re-evaluate to classification scheme periodically.

In the table below systems typically found in a production environment are listed, along with the typical possible consequences, should an incident occur.

System type	Possible consequences of an information security incident
Safety Systems	HSSE impact.
Process control systems Electrical control systems	HSSE and economical impact or impact on reputation.
Fiscal metering systems	Data integrity. Economical impact or impact on reputation.
Support systems (e.g. condition monitoring)	Economical impact.
Telecommunication infrastructure	Economical impact. Incidents may escalate to HSSE impact.
Telecom systems (e.g. PA, CCTV, UHF, VHF)	HSSE impact.

Table 1: System type and possible consequence of an information security incident

This guideline only focuses on the PCSS/ICT systems in the production environment, with the system's corresponding engineering tools. It is obvious that the criticality of the whole function has to be considered. In many instances the criticality level of the ICT system will be equal to the criticality level of the PCSS function. However, in some instances the ICT system will not be as critical as the PCSS function itself; hence it is important to evaluate the criticality of the ICT system after, or as a part of, the criticality assessment for the whole PCSS function, service or system.

Example:

The PCSS function depicted in Figure 2 is a vibration protection and monitoring function for a rotating machinery unit. The machinery is equipped with a number of transducers to monitor vibrations in all directions. In case of excessive vibrations during normal operation, the compressor will immediately be tripped by the protection system.

The embedded ICT system will monitor the vibrations of the rotating machinery for trending purposes, to enable the recognition of evolving failures. The criticality of the complete vibration monitoring function will be assessed and evaluated as part the organisation's maintenance strategy. However, in this guideline only the ICT system part of the function is covered.

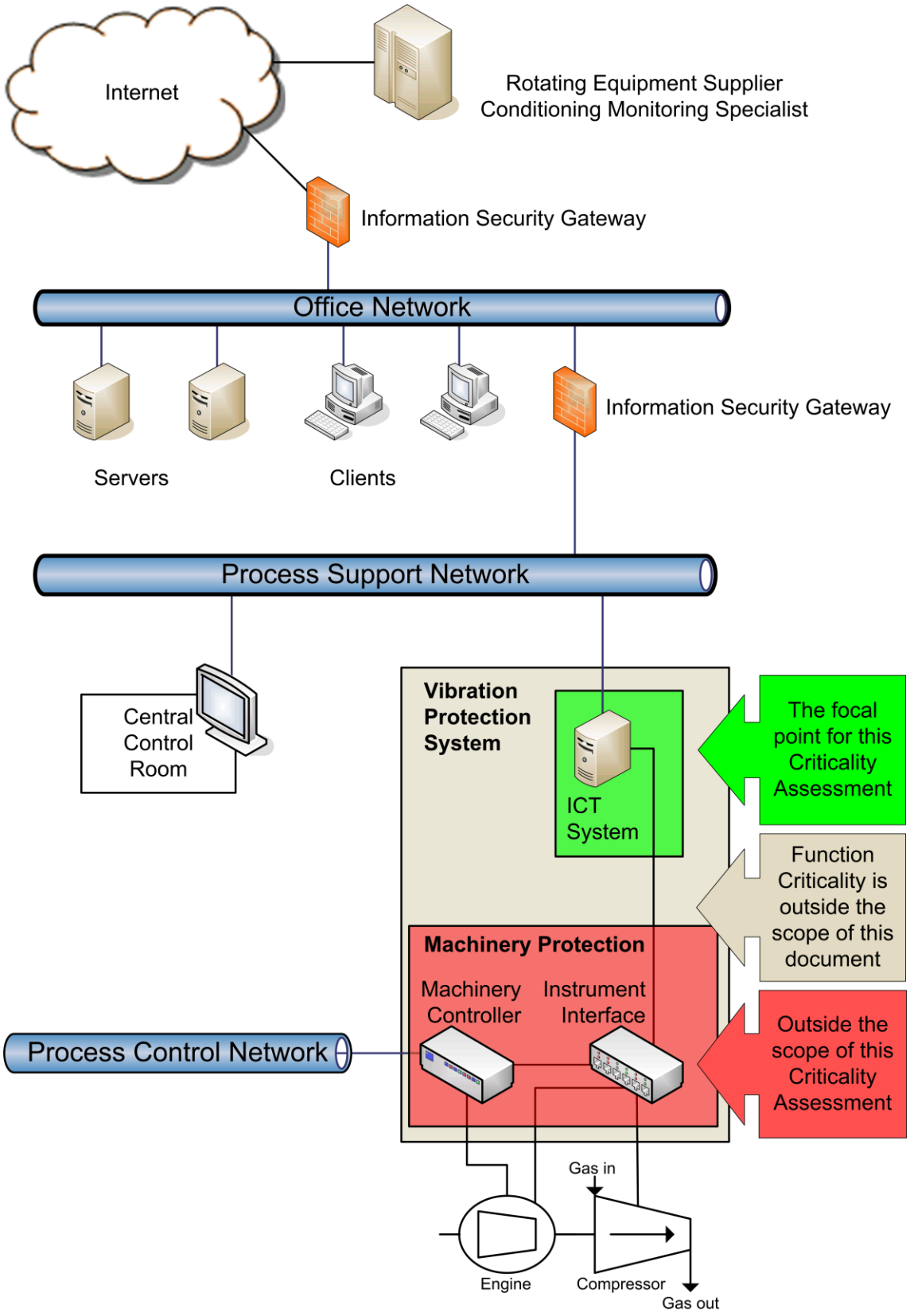


Figure 2: Focal point for Criticality Assessment

The classification scheme

ICT systems supporting, monitoring and controlling equipment for process control, safety and support are typically real-time systems where the requirements for availability and integrity are high. With today's level of connectivity, "all" systems are connected to networks running TCP/IP and hence the need for information security measures and controls are essential. As the companies have to invest in the security measures and controls and there are costs associated with the maintenance of the safeguards to have them perform efficiently and effective, the need of protection should be assessed for all the PCSS/ICT systems in the production domain. The ICT systems should be classified based on their criticality in the production chain. To prevent the assessment from being subjective and imprecise a methodology is needed. Furthermore, to ensure consistent information security levels through-out the production environment a classification scheme with defined criticality levels is required.

The classification scheme should be based on HSSE – where Security in this context is Information Security and primarily focuses on Availability and Integrity of the PCSS/ICT systems, but also to some extent on Confidentiality – and on production regularity.

More detailed, the classification scheme for the ICT systems in the PCSS domain should consist of four categories:

I. Health and Safety, including SIL rating (IEC 61511 & Norwegian Oil and Gas 070)
II. Environment
III. Production regularity and the Availability and Integrity aspects of Information Security
IV. Confidentiality aspects of Information Security

The number of criticality levels should be defined and documented. The number of levels should be aligned with the company's existing assessment system, and preferably be 4 or 5. It may be recommended to label each level to prevent any confusion whether a 1 is the highest or lowest level. Good practice for naming four levels is *Low*, *Medium*, *High* and *Very High*. If five levels are used, then *Very Low* may also be used. Colour coding each level is also useful, to make it easier to quickly find the critical ICT systems in a list of systems. In the office domain the colours of the traffic light is used. As the colour green often is associated with "no risk" and "no need to implement any security measures", the use of this colour should be avoided in the production environment, where there "always" will be a need for safeguards, controls and security measures. The colour pallet used may instead be blue, orange, light red and dark red.

The criteria for selecting a particular criticality level, i.e. the attributes of each criticality level, should be documented for each of the four categories above (I–IV). Furthermore, for each criticality level the company or operating unit should specify which information security controls and measures should be implemented as a minimum. These minimum information security measures constitute the Information Security Baseline for that particular criticality level.

For the third category; *Production regularity and the Availability and Integrity aspects of Information Security,* it may be useful to evaluate the time frame for each criticality level. Should an ICT system go offline, the process may still continue to work unobstructed for a period of time. Some processes or systems will then gradually become more and more vulnerable and hence, compensating measures may be needed, or the whole or parts of the production may have to be shut down. As an example; An ICT system may be considered having a Medium Level of Criticality for the first fifteen minutes it is not available. From then on the Criticality Level is rated as High for the next two hours and finally, if the system is still unavailable, the level rises to Very High.

The classification process

A premise for implementing and maintaining the required information security level with effective and efficient controls is a complete register of all ICT systems and communication devices installed in the production network, as well as all operational applications. This asset register may be a paper based list, but preferably it is a database used to register and manage all the information about the systems and applications – CMDB – Configuration Management DataBase,

All types of PCSS/ICT systems and equipment including the installed applications should be evaluated and rated against each of the four categories (I–IV). The criticality level may be given by the system's function within the production environment, as well as the criticality level of the other dependant systems, before or after the assessed PCSS/ICT system, in the production chain.

The classification of each PCSS/ICT system should be performed against the organisation's defined criteria (see Appendix B for an example of classification questionnaire). The justification for the evaluation and rating of each PCSS/ICT systems should be documented. The rationale and possible additional comments should be specific and precise.

A pragmatic approach to define the criticality level for each particular system is suggested. It is not recommended to differentiate between and weight each of the categories. In stead, aggregate the highest criticality level from the four categories and make this applicable for the system.

The information security measures and controls required for all ICT systems within each criticality level should be documented. Examples of information security measures are anti-virus software, local firewall, intrusion detection/prevention system, system monitoring software, single sign-on (SSO) and use of virtual private networks (VPN).

For each system the required or acceptable access method should also be documented, e.g. local access (i.e. physical presence is required), remote login is accepted, VPN connection is required, remote login via terminal server.

The types of system activities should also be documented. Examples of such are; if access is limited to read-only, if changes to system configurations are prohibited, if remote installation of applications is restricted and if back-up and restore may be executed remotely.

If these baseline security measures and controls are not sufficient for particular ICT systems, then additional necessary safeguards should be evaluated. The concluding solutions should be implemented, tested and documented.

Should the baseline security controls and measures be impossible to implement or unfeasible due to technical or system restraints, then compensating security measures should be evaluated and documented.

Appendix A

Examples of criticality classification

This appendix gives examples of classification of PCSS/ICT systems. The examples do not reflect a complete evaluation and are not necessarily set answers to the criticality for the systems described.

In these examples, four criticality levels have been chosen. Each organisation should choose the number of levels it finds suitable.

System		Aggregated result
PCS System		**Very high**
Category	**Criticality level**	**Rationale and comments**
Health and Safety	Low	The system does not perform functions directly related to health and safety.
Environment	Medium	The system affects the quality of products and waste in normal operations.
Regularity, Availability and Integrity	Very high	The system has direct impact on the production.
Confidentiality	Medium	Production data and parameters handled by the system may be sensitive.

Other systems that typically may be classified similarly:

- PIMS (Production Information Management Systems). The systems may have lower rating on Regularity, Availability and Integrity.
- Subsea Control Systems (PCS functions).
- Power management and electrical distribution control systems.

NOTE: The criticality level of the Health and Safety category in this example is considered to be Low. However, the barrier concept given in the Norwegian Facilities Regulations may in other installations necessitate a higher criticality level.

System		Aggregated result
ESD/F&G System		Very high
Category	**Criticality level**	**Rationale and comments**
Health and Safety	Very high	The system handles health and safety related situations.
Environment	High	The system has impact on reducing spillages and emissions.
Regularity, Availability and Integrity	Medium	The fail safe nature of the system (e.g. automatic shutdown) can cause reduced production regularity.
Confidentiality	Low	The system does not handle production sensitive data.

Other systems that typically may be classified similarly:

- HIPPS (High Integrity Pipeline Protection System).
- Subsea Control Systems (PSD functions).
- PSD (Production Shutdown System). The rating on H&S and Environment may be lower and higher on Regularity, Availability and Integrity.
- Positioning and ballast system. The rating on Environment may be lower and higher on Regularity, Availability and Integrity.

System		Aggregated result
PA System		Very high
Category	**Criticality level**	**Rationale and comments**
Health and Safety	Very high	The PA System is a critical part of the incident management system.
Environment	Low	The functionality of the system does not affect the environment.
Regularity, Availability and Integrity	Low	The system has no direct impact on the production.
Confidentiality	Low	The system does not handle production sensitive data.

The PA System has traditionally been an analogue system and hence not been considered being a part of the PCSS domain. The state-of-the-art PA Systems are digital and integrated into the PCSS domain, where the system configuration is done through TCP/IP communication.

Other systems that typically may be classified similarly:

- Personal Tracking System. The rating on Confidentiality will typically be higher and lower on the H&S. (The system is generally not considered being a part of the PCN.)
- Phone Exchange System. (The system is generally not considered being a part of the PCN.)

System		Aggregated result
Fiscal Metering System		**Very high**
Category	**Criticality level**	**Rationale and comments**
Health and Safety	Low	The system does not perform functions related to health and safety.
Environment	Low	The functionality of the system does not affect the environment.
Regularity, Availability and Integrity	Very high	The system is the basis for the income and taxation.
Confidentiality	Medium	Production data and parameters handled by the system may be sensitive.

Other systems that typically may be classified similarly:

- Gas Chromatograph.
- Environment Monitoring System. The rating on Regularity, Availability and Integrity may be lower. (The system is generally not considered being a part of the PCN.)
- Marine Surveillance System. (The system is generally not considered being a part of the PCN.)

System		Aggregated result
Conditioning Monitoring System		**High**
Category	**Criticality level**	**Rationale and comments**
Health and Safety	Low	The system does not perform functions related to health and safety.
Environment	Low	The functionality of the system does not affect the environment.
Regularity, Availability and Integrity	High	The system warns of evolving failures which enables preventive maintenance.
Confidentiality	Low	The system does not handle production sensitive data.

Other systems that typically may be classified similarly:

- Systems installed to monitor equipment performance. The rating on Regularity, Availability and Integrity may be lower, based on the criticality of the monitored equipment as well as the repair cost and time.
- Valve Monitoring System.

System		Aggregated result
Corrosion Monitoring System		**Medium**
Category	**Criticality level**	**Rationale and comments**
Health and Safety	Low	The system does not perform functions related to health and safety.
Environment	Medium	Good control of corrosion rates may reduce the use of chemicals that not are environmentally friendly.
Regularity, Availability and Integrity	Medium	The system does not directly affect platform performance, unless the system is out of service for a longer period.
Confidentiality	Low	The system does not handle production sensitive data.

Other systems that typically may be classified similarly:

- Structure Monitoring System.
- Sand Monitoring System. The rating on Regularity, Availability and Integrity may be higher.

System		Aggregated result
Oil in Water Analyser		**Low**
Category	**Criticality level**	**Rationale and comments**
Health and Safety	Low	The system does not perform functions related to health and safety.
Environment	Low	The functionality of the system does not directly affect the environment. (Lack of timely analyzer results may influence the quality of produced water to sea.)
Regularity, Availability and Integrity	Low	The functionality of the system does not directly affect the regularity of the production. (Lack of timely analyzer results may influence the production performance.)
Confidentiality	Low	The system does not handle production sensitive data.

Other systems that typically may be classified similarly:

- Lubricants Monitoring System.
- Stock Inventory System. (The system is generally not considered being a part of the PCN.)

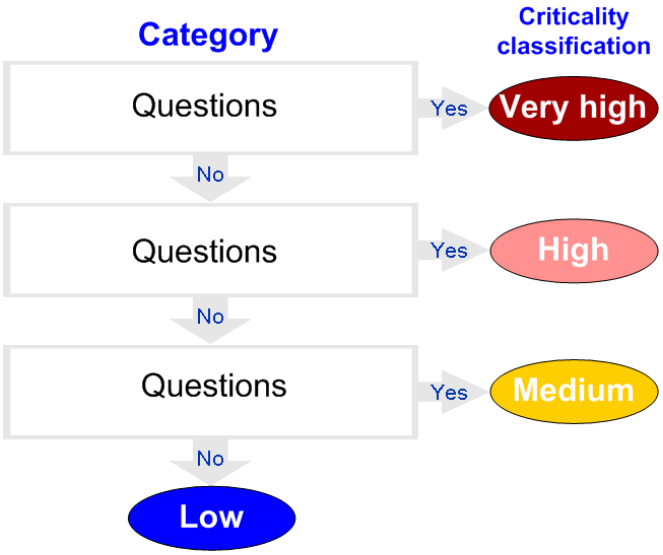
Appendix B

Example of criticality classification questionnaire

This appendix gives examples of valuable questions for use during the criticality assessment process for the PCSS/ICT systems.

All of the four areas should be covered, i.e. Health and Safety, Environment, Production Regularity and the Availability and Integrity aspects of Information Security, as well as Confidentiality.

In the example, four criticality levels have been chosen. Each organisation should choose the number of levels it finds suitable.



When a **Yes** is given to a question, the corresponding Classification Level should be noted and the next category of questions should be reviewed. There is no need to answer the remaining questions within the same category.

The examples given on the next pages are typical questions that may be asked. The organisation should develop its own portfolio of relevant questions. Questions related to financial loss and reputation may also be considered.

Health and Safety

Question	Example Classification Level
Is the system a part of a SIL rated functions?	Very high
Is the system part of barriers defined in the Norwegian Facilities Regulations (Innretningsforskriften)?	Very high
Can a system stop or a degradation in performance cause death?	Very high
Company specific questions inserted here	Very high
Does the system support barriers defined in the Norwegian Facilities Regulations (Innretningsforskriften)?	High
Can a system stop or performance degradation cause permanent disabilities?	High
Company specific questions inserted here	High
Can a system stop or performance degradation cause minor injuries?	Medium
Does the system have a direct impact on the company's HSSE performance goals?	Medium
Company specific questions inserted here	Medium

Environment

Question	Example Classification Level
Is the system part of barriers defined in the Norwegian Facilities Regulations (Innretningsforskriften)?	Very high
Is the system part of barriers defined by the company?	Very high
Can an unintentional system halt result in a major hydrocarbon leakage?	Very high
Company specific questions inserted here	Very high
Does the system support barriers defined in the Norwegian Facilities Regulations (Innretningsforskriften)?	High
Does the system support barriers defined by the company?	High
Can an unintentional system halt result in a moderate hydrocarbon leakage?	High
Company specific questions inserted here	High
Can the system indirectly influence other systems part of the environmental barriers?	Medium
Can an unintentional system halt result in a minor hydrocarbon leakage?	Medium
Company specific questions inserted here	Medium

Production Regularity and the Availability and Integrity aspects of Information Security

Question	Example Classification Level
Will the production process halt if the system is unavailable for ten minuttes?	Very high
Will the production process halt if the system produces erroneous data?	Very high
Can a system stop or a degradation in performance cause physical damage to equipment in the production process within ten minutes?	Very high
Company specific questions inserted here	Very high
Will the production process halt if the system is unavailable for one day?	High
Will the production process (volume/quality) immediately be affected if the system is unavailable or the system's performance is degraded?	High
Will the production process (volume/quality) be severely affected if the system produces incorrect data?	High
Can a system stop or a degradation in performance cause physical damage to equipment in the production process within one hour?	High
Company specific questions inserted here	High
Will the production process (volume/quality) be affected over time if the system is unavailable or the system's performance is degraded?	Medium
Will the production process (volume/quality) be affected if the system produces incorrect data?	Medium
Will a delay in the mandatory reporting to authorities of statistics from the system result in penalties or additional activities?	Medium
Can a system stop or a degradation in performance cause physical damage to equipment in the production process within one day?	Medium
Company specific questions inserted here	Medium

Confidentiality

Question	Example Classification Level
Does the system produce/handle data that is considered sensitive as defined by the Norwegian Privacy Laws (Personopplysningsloven)?	Very high
Company specific questions inserted here	Very high
Does the system produce/handle data that may affect the company's reputation or competitiveness should the data be disclosed?	High
Does the system store data that may reduce the information security level should they be disclosed?	High
Company specific questions inserted here	High
Does the system produce/handle data that may affect the company's reputation or competitiveness locally should the data be disclosed?	Medium
Company specific questions inserted here	Medium