Data Safety, Sources, and Data Flow in the Offshore Industry

T. Myklebust

SINTEF Digital, Trondheim, Norway. E-mail: thor.myklebust@sintef.no

T. Onshus

Cybernetics, NTNU, Norway. E-mail: tor.onshus@ntnu.no

S. Lindskog

SINTEF Digital, Trondheim, Norway. E-mail: stefan.lindskog@sintef.no

M. Vatshaug Ottermo

SINTEF Digital, Trondheim, Norway. E-mail: maria.v.ottermo@sintef.no

L. Bodsberg

SINTEF Digital, Trondheim, Norway. E-mail: lars.bodsberg@sintef.no

Digitization may provide increased access to and more efficient use of real-time and historical data, internally as well as externally in an organization. However, when information from industrial control systems (ICS) becomes more available in office IT systems and in the "cloud", ICS systems may become more vulnerable and attractive targets for cyberattacks. We have investigated data safety in ICS in the Norwegian offshore sector when data is processed from ICS to the office network. The work is mainly based on document review and nine interviews with selected oil companies, rig companies and service providers of operational data. The paper addresses strengths and threats related to data safety with emphasis on (1) Data sources and data flow, (2) Safety and security of data, (3) Data cleaning and processing, (4) Contextualization, (5) Validation, and (6) Quality assurance. We also discuss shortcomings for functional safety in current standards such as IEC 61508 and IEC 61511 and standard series for security, IEC 62443. It is a major challenge for the industry that there are no good international standards and guidelines that define the relevant terminology across IT systems and ICS. Future work should address data safety challenges when applying artificial intelligence and machine learning in ICS systems.

Keywords: Data, safety, data flow, data sources, security.

1. Introduction

This paper's primary goal is to give the industry a better understanding of the importance of data quality and data safety from the industrial ICT systems on the Norwegian shelf, with emphasis on data from the OT (Operational Technology) system to the office environment. The following two objectives are defined for the project:

1. Investigate which data and data sources are used in OT systems, and how data is addressed and processed before it is made available in the office environment.
2. Assess strengths and threats related to data quality and data safety in OT systems with special emphasis on the following topics:

   (a) Data sources and data flow
   (b) Safety and security of data
   (c) Data cleaning and processing
   (d) Contextualization
   (e) Validation
   (f) Quality assurance

In this paper, we use the term data quality to have access to the correct data when necessary. We focus on the availability and integrity of data and weaknesses in information and communications technology (ICT) systems that can directly affect data quality.

1.1. Methods

The work included document review, literature study including relevant standards and guidelines, interviews, and work sessions with the Petroleum Safety of Norway (PSA). An interdisciplinary project team has carried out the work with expertise in, among other things, industrial information and ICT systems and ICT security, as well as petroleum regulations and standards within these subject areas.

Interviews have been conducted with selected oil and rig companies and suppliers. A total of nine companies were included in the study. For reasons of anonymity, the names of the companies are not stated.

Proceedings of the 31st European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud, and Christophe Berenguer
Copyright © ESREL 2021.*Published by* Research Publishing, Singapore.
ISBN: 978-981-18-2016-8; doi:10.3850/978-981-18-2016-8_099-cd

1.2. Delimitations

The following delimitations apply:

- Confidentiality of data and securing data against intentional attacks by malicious individuals or groups is not an essential part of the paper.
- Today's solutions are emphasized rather than new technology trends.
- Challenges related to machine learning (ML) and artificial intelligence (AI) are not an essential part of the paper.

2. Background

2.1. The Oil & Gas industry and the Petroleum authority

Data is the new oil. There are several ongoing projects in the North Sea where the possibilities introduced by digitalization can result in improved and optimized processes as well as environmental benefits. To achieve these goals, improved data and dataflow is of crucial importance. These projects should involve experts both from the OT and information technology (IT) domains.

2.2. Terminology

A comprehensive and agreed terminology for data quality in OT systems has not been established. Even standards such as the ISO 8000 series for data quality and the SCSC guide (2021) lack definitions for several key words and expressions used by the industry. Nor does the PSA have specific definitions related to data in their list of "words and expressions" (2021). Relevant IEC standards for functional safety and ICT security do not include all the relevant definitions for data quality, but IEC 61508 will refer to the SCSC guide in the next edition of the standard (2020). Through our interviews, we experienced that OT and IT personnel in the various companies used different words and expressions for data quality. The professional environments within OT and IT are based on different standards and guidelines that do not use the same definitions. It is also a challenge that data terminology is relevant for at least four professions:

1. Functional safety
2. Cybersecurity
3. IT
4. Operator

The most used terms in connection with the interviews are defined below:

1. Data cleaning is defined by ISO 5127:2017 "*Information and documentation — Foundation and vocabulary*" but a more complete definition has been added as part of this project: Data cleaning is the process of preparing data for analysis by removing or modifying data that is incorrect, incomplete, irrelevant, duplicated, or incorrectly formatted. Data lineage has been defined by this project as: Data lineage is a data life cycle that includes the data's origins and where the data moves over time. Note 1: Data lineage can describe what happens to data as it goes through diverse processes. Note 2: Data lineage can help with efforts to analyse how information is used and to track key bits of information that serve a particular purpose.
2. Data ingestion has been defined by this project as: Data ingestion is the process of collecting and importing data from databases or files for immediate use, integrating it into a data lake or storage in a database.

3. Data Sources and Data Flow

We have focused on describing typical SAS solutions and how data flow takes place from sensors to the cloud and all the way down to a handheld device as one example. Historically, there has been a distinction in the industry between administrative computer systems (office support systems) that process data and information (IT and ICT systems) and computer systems that control and monitors operations (OT systems) on drilling and production facilities. The PSA's regulations use the term ICT systems for systems that take care of the need for collection, processing and dissemination of data and information. Industrial ICT systems are generally used for OT systems that involve changes in physical equipment and processes such as control and monitoring systems and security systems. The PSA's area of authority in relation to ICT systems is mainly aimed at industrial ICT systems (OT systems), and especially systems that have a barrier function (safety systems). OT systems on a facility that was previously separated from the outside world are being modernized and are becoming increasingly complex and interconnected with IT systems. This opens up for more comprehensive solutions, including management and monitoring from onshore where OT systems have more connection points to the company's IT systems and extensions to external networks such as cloud solutions via the Internet. This means that the traditional distinction between IT systems and OT systems is being challenged. IT equipment is increasingly also used to take care of OT functions. Examples are monitoring, maintenance and configuration systems for field instruments that have traditionally been regarded as IT systems since they do not directly affect production. In the following, an overall description of OT systems which, in accordance with the PSA's regulations, perform safety functions, i.e., control and monitoring systems and instrumented safety systems (SIS). Then a typical example of both logical and physical data flow between IT and OT systems according to the Purdue model is given. Note that there may be several variants of the figures for specific facilities.

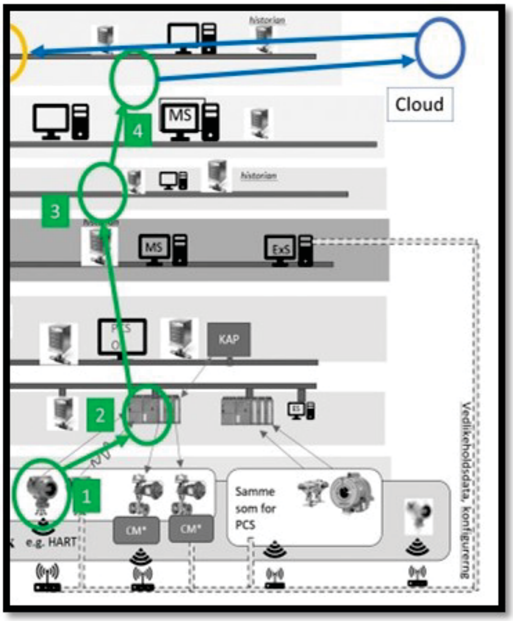


Fig. 1. The green parts illustrate the flow of data from sensors to the cloud. The blue part represents the cloud.

On an offshore platform, there are mainly three separate instrumented safety systems (SIS) in addition to the control system. These are commonly known as SAS (Safety and Automation system):

- Process Control System (PCS),
- Process Shut Down (PSD),
- Fire and Gas (F&G), and
- Emergency Shut Down (ESD).

The safety systems must handle dangerous incidents on the facility. This includes detecting abnormal conditions, preventing abnormal conditions from escalating into dangerous situations and limiting damage in the event of accidents (cf. section 8 of the Facilities Regulations (2020). Examples of dangerous events can be process control system failure, a gas leak or fire, or other incidents where operators consider it safest to shut down. In addition, there is a requirement that the ESD and PSD systems are fail-safe, i.e., that they must go to or remain in a safe state if an error occurs (in the ESD or PSD system) that can prevent the system from functioning (cf. chapters 33 and 34 of the Facility Regulations). There are further requirements for the safety systems (ESD, PSD and F&G) to be able to perform their intended functions independently of other systems. Figure 1 shows how the individual systems in SAS are connected on a production facility.

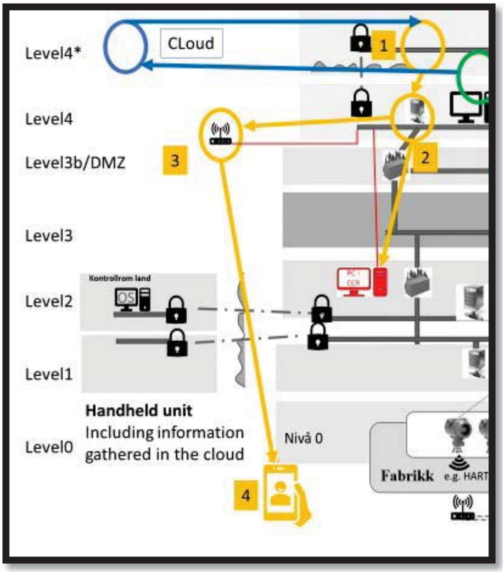


Fig. 2. The yellow parts illustrate the flow of data from the cloud to a handheld device. The blue part represents the cloud solution.

Common to all the systems in SAS is that they consist of three subsystems:

- Sensors that convert physical values/states to a measurement signal,
- Controllers or logic devices (also called PLCs - Programmable Logic Control), and
- Final elements (usually valves and switches) that intervenes to handle the dangerous event.

Figure 2 identifies 7 levels (levels 0, 1, 2, 3, 3b, 4 and 4*). These are taken from Purdue reference architecture for OT/IT systems (also referred to as ISA-95 reference model), with associated detailing in DNV-GL RP G108 (2017) and ISA 84.00.009:2017. Note that a distinction is made between equipment that is placed in IT networks and equipment that is placed in OT networks, and within each of these networks there will be different sub-networks. We also notice that there should be a clear separation between OT and IT with firewall(s).

4. Functional Safety Standards and Guidelines

The evaluations and analysis of functional safety standards have been limited the IEC 61508:2010 series and the IEC 61511:2016 series as they are the main standards for the offshore industry. Both standards state in their definitions of software that software comprises data. In addition, we have evaluated the IEC 62443 series.

4.1. IEC 61508 series

The IEC 61508:2010 series is the generic standard series that defines SIL (Safety Integrity Level). IEC

61508 uses SIL 1-4 (Safety Integrity Level) to describe the risk reduction a function can provide. There are quantitative requirements for the hardware and requirements for both the working methods and methods for software development. In this standard, data is often associated with configuration and test data, and with requirements for interfaces between software and external systems. The IEC 61508 series is weak when it comes to data safety. The standards include several data-related requirements, but most of them are related to data quality, data configuration, and V&V. In the next edition of IEC 61508, it is expected that the standard will include a reference to the SCSC data safety guide (2021).

4.2. IEC 61511 series

IEC 61511:2016 is a domain standard for the process industry based on the generic IEC 61508 standard and uses SIL in the same way. The IEC 61511 is weak related to data sources, while NOROG 070 (2020) presents the relevant SIS (Safety Instrumented Systems) for the offshore industry. Data cleaning is not explicitly mentioned in the standard but is necessary for the SAS system to function as intended. Processing of data is only weakly described in the standard. The standard includes requirements for validation and quality assurance of data but improvements due to modern data solutions could preferably be included. In addition, the next edition of this standard could also refer to the SCSC data safety guide (2021).

4.3. IEC 62443 series

IEC 62443 is an international standard for ICT security in ICS. In IEC 62443-2-4:2015, it is specified that sensitive data (Requirements related to data requiring safeguarding) must be protected regarding confidentiality and integrity. This applies to both stored data and data in transit. The standard does not specify how this should be done, but it states that cryptography must be supported. Keyed-Hash Message Authentication Code (HMAC) may be used to protect against unauthorized modifications and fabrication of data, and data encryption may be used to meet the requirement of data confidentiality.

4.4. Data safety guide

The SCSC Data Safety Initiative Group has developed a guide (2021) that aims to:

- Describe the data safety problem,
- Provide methods for identifying and analysing risk levels, and
- Recommend methods and approaches to evaluate and address these risks.

This guide was used as a basis when performing this work. The guide is developed for several safety domains and is therefore in many ways too generic and must be adapted to the individual domain, context, and projects. The target audience for the guide covers all those who have an interest in, or responsibility for, safety-related data within systems, including managers, developers, security engineers, insurers (including independent safety assessors), authorities and operators. The guideline includes a description of a Data safety Management Plan (DSMP) with proposed content that can complement companies' safety plan, Myklebust et al. (2016). They propose that the DSMP include the following main sections:

- Introduction,
- impact assessment of specific DSAL (Data Safety Assurance Level) and ODR (Organizational Data Risk),
- the scope of categories of safety data,
- analysis of data requirements,
- data risk management,
- arguments for data use,
- necessary analyses and verifications, and
- documents which must be prepared.

As part of the interviews, there were some discussions regarding verification and validation. V&V is defined differently in international standards, so a clarification is presented below.

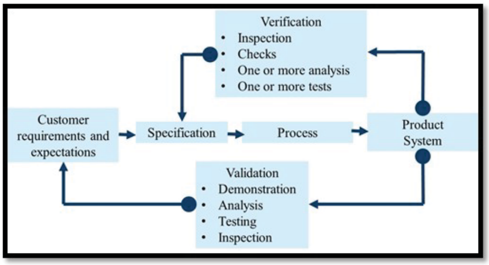
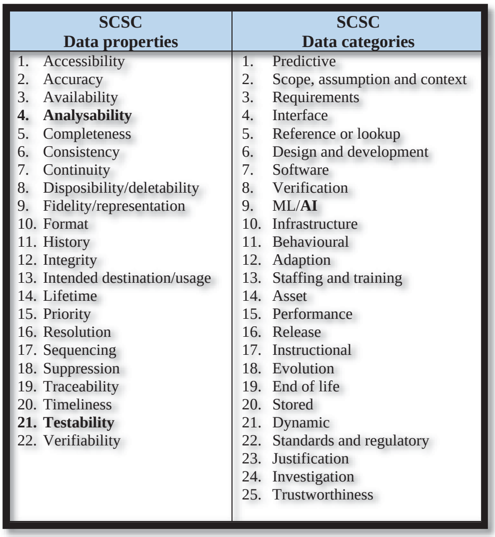


Fig. 3. The relationship between verification and validation together with different V&V aspects.

The SCSC guide (2021) has listed relevant data properties and different data categories. We see several properties and categories from the table in figure 4, and far more than many safety engineers and software developers are aware of. The two properties in bold are added as part of this project. Also, we have added AI (Artificial Intelligence) together with ML as a category. A standard for functional safety and AI will be issued (ISO/IEC TR 5469) in the near future.

Measuring the level of awareness of processes and concepts in an organization is challenging, and the safety standards IEC 61508 and IEC 61511 are silent regarding safety culture. The guideline has included a questionnaire that has been developed to explore the specific area of measuring the data safety culture for a particular activity. The questionnaire could be for the organization as a whole or a particular project, service, or activity.



SCSC Data properties	SCSC Data categories
1. Accessibility	1. Predictive
2. Accuracy	2. Scope, assumption and context
3. Availability	3. Requirements
4. Analysability	4. Interface
5. Completeness	5. Reference or lookup
6. Consistency	6. Design and development
7. Continuity	7. Software
8. Disposibility/deletability	8. Verification
9. Fidelity/representation	9. ML/**AI**
10. Format	10. Infrastructure
11. History	11. Behavioural
12. Integrity	12. Adaption
13. Intended destination/usage	13. Staffing and training
14. Lifetime	14. Asset
15. Priority	15. Performance
16. Resolution	16. Release
17. Sequencing	17. Instructional
18. Suppression	18. Evolution
19. Traceability	19. End of life
20. Timeliness	20. Stored
21. Testability	21. Dynamic
22. Verifiability	22. Standards and regulatory
	23. Justification
	24. Investigation
	25. Trustworthiness

Fig. 4. Relevant data properties and data categories copied from the SCSC guide (2021).

5. Strengths and Threats Related to Data Quality and Data Security in OT Systems

This section assesses strengths and threats related to data quality and securing data in OT systems and is mainly based on views that have emerged in interviews with nine companies. The section is based on the overall description of data sources and data flow in OT as mentioned above and requirements for data quality and security of data in OT systems in standards and guidelines. Vulnerabilities in OT systems can contribute to personnel making wrong decisions. Vulnerabilities include both data and software and there will be an interdependence between data and software. Key questions are:

- Can data affect the software so that the safe operation of OT systems is compromised? An example might be a system that is fed with data outside the expected range.
- Can the software affect data so that the safe operation of OT systems is compromised? An example might be the delay of critical data due to buffering.

Challenges that were highlighted during the interview were mainly related to time stamping, old systems and in general that there has not been much focus on data related to functional safety.

5.1. Processing of data

Our interviews indicate that operating companies have not emphasized their follow-up of processing data in their OT systems. They have primarily relied on the OT suppliers to take care of this. Most of the addressing and processing of data from and to field devices is performed before reaching the IMF (Information management system) system. Some OT systems have quality flags that provide information about e.g., the data source and alarm status (acknowledged or unacknowledged alarm). The conversion of measuring units into a standard unit such as pressure (Pascal, bara and barg) has been part of data processing in OT systems. This is a challenge as there are many ways to present e.g., the pressure, see figure 5. One informant said that for temperature they had had 19 different systems of naming!

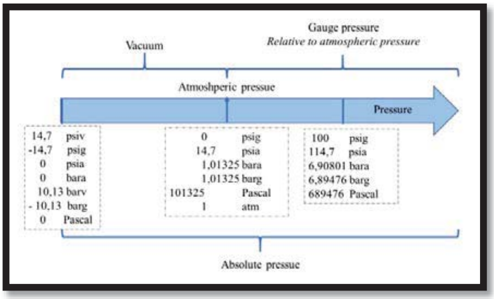


Fig. 5. This figure shows that pressure can be presented in several different ways.

As part of SINTEF's assessment, it is a strength that OT data has so far been processed as much as possible in the OT system, especially since the SIS systems have been developed based on their own standards in functional safety that place extra high demands on reliability. The PCS systems will also ensure that data are processed to a large extent as it must be ensured that HMI requirements are followed and that this must be consistent, understandable, and user-friendly for the operators. Relevant ICT security standards, such as the IEC 62443 series, were immature when the current OT systems were developed.

5.2. Timestamp

Time stamping means that a timestamp is attached to each operation in the OT system so that operations in and between OT systems are carried out in the correct sequence. Systems that run WinX at the bottom often use Network Time Protocol (NTP) to distribute time information between nodes from a server that serves as or is a dedicated time server. The time server receives time from either GPS clock, or other reliable sources. Exchange of date and time information is standardized in ISO 8601-1: 2019. In some interviews, informants said that time stamping is a challenge in, for example, decision support. Some challenges that were highlighted:

- The production process requires high time resolution,
- The data is not always synchronized,
- Some people use their own clock,
- Time stamping in connection with old systems,
- Time stamp operation, it can take several seconds,
- Queue on data transfer,
- The sequence of events,
- Synchronization in general,

- Strict requirements for response time in NORSOK, and
  > "*The maximum response time of a process safety function to reach safe state on demand in actual operation shall be defined according to process dynamic behaviour. Typical response times that shall be complied with unless faster responses are required from dynamic analysis: Time from signal from sensor to start of PSD execution, e.g., de-energised solenoid valve, should be less than 2 seconds.*"
- Summertime.

One of the frequently used standards used for industrial communication, OPC UA, includes time and quality, but the system does not become better than the application itself. This is one of the reasons that some companies want direct access to the sensors since that will provide access to e.g., better time data, but as a result, this can lead to e.g., challenges in ICT security. Also, when monitoring and assessing ICT security, accurate time stamping across systems is very important, as it is essential to have information about correct time sequences both before and after an incident or attack.

5.3 Data cleaning

Data-cleaning is the process of improving data quality. Data-cleaning can be done by removing or modifying data that is incorrect, incomplete, irrelevant, duplicate, or data that has invalid values, unhandy variable names, number formatted as text, impractical structure, or incorrect format. Although cleaning is not explicitly mentioned in the safety standards IEC 61508 and IEC 61511, in practice, the usual requirements for data quality will be included when designing OT systems.

Most of the operating companies interviewed expect that the SAS systems suppliers have carried out adequate data-cleaning. This means that information from Historian/IMS or similar systems have already been cleaned. In addition, operating companies can perform some of their own checks in relation to, e.g., special values and contextualization of the information.

5.4. Contextualization

For information to have value, it must be interpreted, given meaning, and placed in a given context (the context in which data is used). Contextualization includes several factors such as:

- System context (context) and how the system (e.g., OT system) is to be used,
- Current stakeholders. For example. operators, suppliers, etc.,
- Identification of current data objects (artefacts). For example, sensor data, monitoring data, etc.,
- Interfaces, e.g., from a transmitter to PLC, or from OT to IT system.

In the petroleum business, tag hierarchies and P&ID (piping and instrumentation diagram) are used. To describe equipment and understand tasks in OT systems. This information is often also linked to the 3D model and technical documentation if you have a digital twin. The different companies develop different systems that are often based on Python software. Power BI is often? used for analysis and visualization of context and information flow. Tools for understanding and visualizing data are essential for data analysts and technically oriented business users. These tools' focus is not primarily reporting and monitoring but instead ad hoc analysis of several data sources. These tools give data analysts an intuitive way to filter through large amounts of data to reveal patterns and discrepancies hidden in the data. They are increasingly replacing the traditional rows and columns and data presentations with graphic images and diagrams. Concerning ICT security, it is important to have good context information both before and after e.g., an ICT security incident. Early or instant information is essential to ensure a good picture of how the incident has been. This is the information that analysts use when assessing what has happened and what needs to be done to improve ICT security.

5.5. Data validation

According to the interviews, data for SAS systems are validated mainly based on the functional safety standards IEC 61508 and IEC 61511. Complying to standards is a strength, especially for the systems that have been developed in accordance with the latest edition of IEC 61511, which was published in 2016. The IEC standards focus more on validation of design than on validation carried out during operation. Validation also has a solid connection to context. See also figure 3 to clarify what is meant by validation ("getting the right system and the right data"). It is worth noting that the system requirement specification (SRS), in connection with the IEC safety standards, has mainly been developed to ensure that SIS and SAS systems follow strict requirements and not been developed in relation to the current use of IT personnel such as data analysts. Thus, it may be relevant to assess whether SRS should be adapted to IT personnel's intended use. The SCSC guide (2021) is somewhat weak in terms of validation and does not include validation as a separate topic. Actors who are not involved in developing products and systems (SIS and SAS) by following these standards do not perform validation of data to any great extent. Examples of validation given in the interviews are:

- Check new data against old data and trends, and
- Maintenance data is manually validated by process personnel and technical personnel.

There may be vulnerabilities here since ICT security standards were immature when today's OT systems were developed.

5.6. Quality assurance

By quality assurance of data, we mean the level of trust that the data delivered meets the user's requirements. These requirements may include levels of accuracy, resolution, traceability, timeliness, completeness, and format. As part of the interviews, most of the companies stated: "This is mainly satisfied by the fact that the OT equipment satisfies standards such as IEC 61508 and IEC 61511". Both standards include "data" in the software definition. An application programming interface (API) is a set of subroutine definitions, communication protocols and is a tool for developing software. In general, the API is a set of clearly defined communication methods between different components. A good API makes it easier to develop a computer program by offering the relevant building blocks, which the programmer then assembles. When creating API specifications, the companies also include quality assurance. An API specification can take many forms but often includes specifications for, among other things, routines, data structures, object classes, and variables. Some informants believe that too many mappings are performed. This process should be simplified and harmonized. In addition, they wanted simplified models, and that these are put in the proper context for the users. It was also noted that mapping takes too long. The interviewed companies envisage that AI may be relevant to create a better solution for this, by feeding a mapping template into e.g., an API specification, which then builds up the model. The model that is then established is quality assured. There is a separate IEC OPC UA standard for mapping: IEC 62541-6:2020. OPC UA's strength is that it includes its own standard for ICT security IEC TR 62541-2: 2020, while OPC UA does not contain its own IEC standard for safety.

5.7. Security and vulnerabilities

Within the OT systems, access to the correct data is central to maintaining production and shutting down production in a secure manner when an unwanted event occurs. Requirements for high availability and integrity are thus more important than the requirement for confidentiality. Securing data in the OT systems can be implemented physically (through, e.g., access control) and/or logically (through, e.g., firewalls that separate OT systems from the IT systems and the cloud). When data is sent out to the IT systems and possibly further out in the cloud, there are further security challenges.

A significant vulnerability in today's OT systems is that they often contain older equipment that does not have built-in support for cryptography. This means that data integrity rely on a good shell protection. HMACs, which can verify that data is authentic and has not been altered, are typically not used in OT systems. However, DNVGL-RP-G108 (2017) contains the following recommendation:

- Symmetric encryption: AES 128 or stronger,
- Asymmetric encryption: RSA 2048 or stronger, and
- Hash: SHA-224 or stronger.

IEC 62443 includes encryption requirements and OPC UA may also include encryption. There are also disadvantages to using encrypted messages within OT since signature-based intrusion detection systems (IDSs), such as Snort, Suricata, and Bro, will not be able to detect forced entry attempts. Network monitoring then also becomes more difficult. Another challenge is that encryption/decryption requires resources and will be at the expense of response time and the possibilities for exchanging information between the individual systems. The operator interface can also be slower. Hence shell protection in the form of zones and tunnels, according to IEC 62443, might be a better solution for OT systems. There are SIL 4 certified hardware security systems in accordance with IEC 61508, where the logic cannot be influenced via ICT systems. The logic is then not vulnerable to ICT threats and information and status can, for example, be retrieved with OPC-UA (but the OPC part has not yet been certified in accordance with current IEC 62443 standards). This means that the logic does not need protection against ICT threats, while the information on OPC has the same challenge as other software-based infrastructure.

6. Conclusion and Recommendations

Data is the new oil, and both safety and security have to be taken into account as new technology, and work processes are implemented. Below we have listed several relevant improvements as recommendations. Most of these recommendations apply to other similar domains too.

6.1. IEC 61508 and IEC 61511 related recommendations

The next edition of the standard series should include relevant data definitions and generally improve the data safety requirements. An alternative minimum approach is to refer to the SCSC guide (2021). In addition, both standards should include requirements related to safety culture.

6.1.2. SCSC Guide recommendations

The next edition of the guide should include more definitions, see Section 2.3 above. In addition, the data properties should add analysability and testability. The ML category should be extended with AI.

6.1.3. IEC 62443 recommendations

All parts of the standard need to be finalized, and some parts need to be updated to be useful in todays and future OT systems.

6.2. Recommendations for the industry

1. Establish a template, including guidance, for a data plan for data used in safety related systems.
2. Perform data HAZOP-analyses and emphasise awareness and culture for follow-up of data

quality (ref. SCSC-127E and DNVGL-RP-0497). This applies to both OT and IT systems.

3. Establish terminology for data quality for improved communication between IT and OT personnel.
4. Improve relevant guidelines (e.g., NOROG 070) based on international standards and adapt use of the SCSC-127E.
5. Emphasize increased understanding of ICT vulnerabilities, including those regarding read access in lower zones of OT systems.

6.3. Recommendations for PSA

1. Strengthen the surveillance of operator's quality assurance of IT suppliers, including requirements for data flow from the cloud to OT systems (see-to-it duty).
2. Strengthen the PSA role to share knowledge and experience regarding safety and security among small suppliers.
3. Strengthen the PSA role in surveillance of competence requirements to IT and OT personnel.
4. Strengthen surveillance of ICT safety and security during design.
5. When possible, refer to international standards instead of national standards in guidelines.

6.4. The necessity of improved knowledge

In a future scenario, the information presented on, e.g., handheld devices could be used as a basis for intervention in process equipment, for example, to check the pressure and conditions in part of the process before a "manhole" is opened for internal inspection and work. There is a need for increased knowledge about data quality and strengths and threats associated with handheld devices in the field. Wireless field equipment presents the same challenges as for handheld devices. How to perform remote configuration of SIS and ensure adequate protection of zones and tunnels in such configurations. There is a need for increased knowledge about appropriate risk assessments to protect OT systems in petroleum activities.

Acknowledgement

This work was funded and carried out in 2020 and 2021 by commission by the Norwegian Petroleum Safety Authority (PSA) and the SINTEF SEP project "Secure Safety 2.0".

References

SCSC-127E Data Safety Guidance version 3.3, DSIWG 2021.

NORSOK S001:2018 Technical Safety.

NOROG 070 Norwegian Oil & Gas: Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry. (Recommended SIL requirements), fourth edition 2020.

ISA-TR84.00.09-2017 Cybersecurity Related to the Functional Safety Lifecycle.

PSA, Facilities regulations (2020).

ISA/IEC-62443-2-4:2017 – Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers.

T. Myklebust, T. Stålhane and N. Lyngby. The Agile Safety Plan. PSAM13, 2016 Seoul.

PSA 2020-11-10: www.ptil.no/fagstoff/ord-og-uttrykk/, seen 2021-03.

DNVGL-RP-G108:2017, Cyber security in the oil and gas industry based on IEC 62443, September 2017. http://rules.dnvgl.com/docs/pdf/dnvgl/rp/2017-09/dnvgl-rp-g108.pdf.

IP "Data safety" IEC 61508 proposal 2020.