OFFSHORE NORGE

112 -OFFSHORE NORGE GUIDELINE

DEPLOYMENT OF RADIO FREQUENCYIDENTIFICATION (RFID) IN THE OIL AND GAS INDUSTRY

PART 1 – General principles for deployment

Guideline title:

Deployment of Radio Frequency Identification (RFID) in the oil and gas industry
Part 1 General principles for deployment

Offshore Norge
Hinna Park
Fjordpiren, Laberget 22, 4020 Stavanger
Postboks 8065, 4068 Stavanger

Entry into force: 01.07.2010

Relevant committee: Operations Sanction date: 03.02.2010

Offshore Norge Guideline 112 approved by:

Norwegian Oil and Gas's Director General Approval date: 22.03.2010

Objective of the guideline:

The objective of this guideline is to secure a cost effective deployment of Radio Frequency Identification (RFID) in the oil and gas industry through a common understanding, practice, and technology platform adoption to achieve data interoperability between RFID and corporate systems. The guideline is in line with Norwegian Oil and Gas's Integrated Operations (IO) and it consists of nine parts.

Part 1 covers the general principles for deployment of RFID in the oil and gas industry, and the target group is primarily management and decision-makers.

Status with the authorities:
This guideline has no formal relations to any authority.

Web site location:
This guideline can be downloaded for free from the Offshore Norge web site

Acknowledgements

The Offshore Norge Guideline No. 112 (part 1-9) was developed in a consensus oriented process with broad participation from major stakeholders within the Oil and Gas, ICT, Telecom manufacturing, and Service industries and in cooperation with the national standardization body, Standards Norway.

This project has based its work on voluntary participation in workgroups and plenary meetings, starting in June 2007 and was finalized December 2009. The guideline reflects the consensus of the individuals and their organizations that have participated in this work.

Authors and editor team:

Dr. Ovidiu Vermesan, SINTEF, NO
Magnar Gregersen, Statoil, NO
Emil Andersen, Conoco Phillips, NO
Dr. Thore Langeland, Offshore Norge, NO
Unni Ulland, IBM, NO
Roy Bahr, SINTEF, NO
Jan Robert Moen, Statoil, NO
August Nilssen, Standard Norge, NO
Dr. Asle K. Berger, Capgemini, NO
Tron Lund, IBM, NO

Many organizations and individuals have assisted with their views, comments and suggestions on this and previous issues of this guideline document. Their contributions are gratefully acknowledged.

Ken Douglas, BP, UK
Chris Geen, BP, UK
Paul Hocking, BP, UK
Tor Holm, Conoco Phillips, NO
Magne Valen-Sendstad, DNV, NO
Patrick Guillemin, ETSI, FR
Lars Sandtorv, IBM, NO
Paul Chartier, Praxis Consultants, UK
Manus Bakken, Telenor Objects, NO
Juan Carlos Calvet, Telenor Objects, NO
Arild Herstad, Telenor Objects, NO
Edvin Holsæter, Telenor Objects, NO
Eyvind Skaga, Telenor Objects, NO
Thor Steffensen, Telenor Objects, NO
Brede Fladen, Trac ID, NO

Table of contents

1 Introduction

This Offshore Norge Guideline No.112 for deployment of RFID in the oil and gas industry addresses the main needs and requirements of the offshore industry for real time data management and of operational information in five deployment areas. The overall integration of an RFID system with the enterprise applications is presented in Fig. 1.

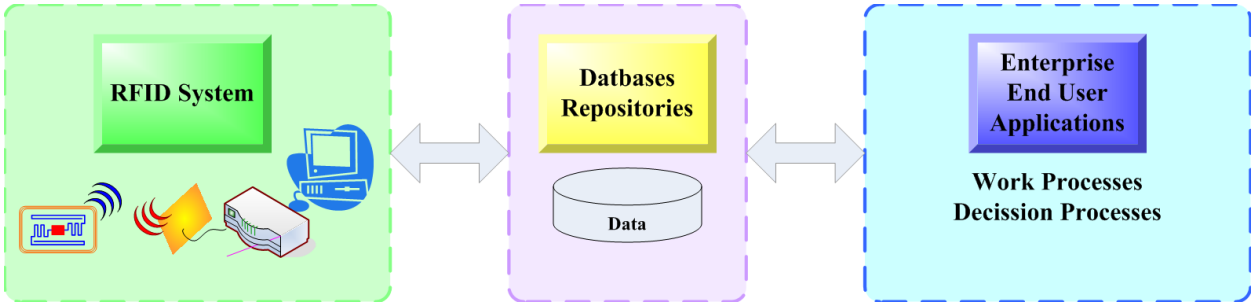

Fig. 1: End to end information workflow.

The four **technical parts** are addressing issues related to primarily management/decision-makers, network/system architects/administrators, and radio, computer and application engineers mainly.

- Part 1: General principles for deployment.
- Part 2: Architecture and integration.
- Part 3: RFID technology.
- Part 4: Unique identification number.

The five **deployment areas** are implementation specific and addressing issues related to application engineers and users within the special field:

- Part 5: Personnel (HSE)
- Part 6: Cargo carrying unit (CCU)
- Part 7: Drill string components
- Part 8: Mobile equipment
- Part 9: Fixed equipment

The organization of the guideline is illustrated in Fig. 2. Implementation of Norwegian Oil and Gas's Integrated Operations (IO) Generation 2, integration of operator and its suppliers in real time requires a common communication platform based on international standards. The key elements of this platform are a common terminology and a reference IT architecture.

In close collaboration with the global oil and gas industry, Offshore Norge encourages the development of an oil and gas ontology (that includes the terminology) and a common technology for exchanges data from application to another (common service bus). Any deployment of information technology in the oil and gas industry should be an integrated part of this communication platform.

This guideline will help the operators, the hardware and software providers, the system integrators, and the automatic data capture equipment suppliers to provide better products, services and to improve the deployment of RFID in the oil and gas industry. The goal of the

guideline is to define the requirements and needs of oil and gas industry for the deployment of RFID technology to successfully undertake the adoption and evaluation of the technology for petroleum personnel monitoring in critical situations, cargo carrying unit tracking, drill string component and tool tracking, and monitor and manage mobile and fixed equipment.

The guideline is recommending open and scalable architectures that consider possibility for plug and play new ID methods combined with sensing/actuating and being compatible with future internet solutions and Internet of Things infrastructure and required specifications.

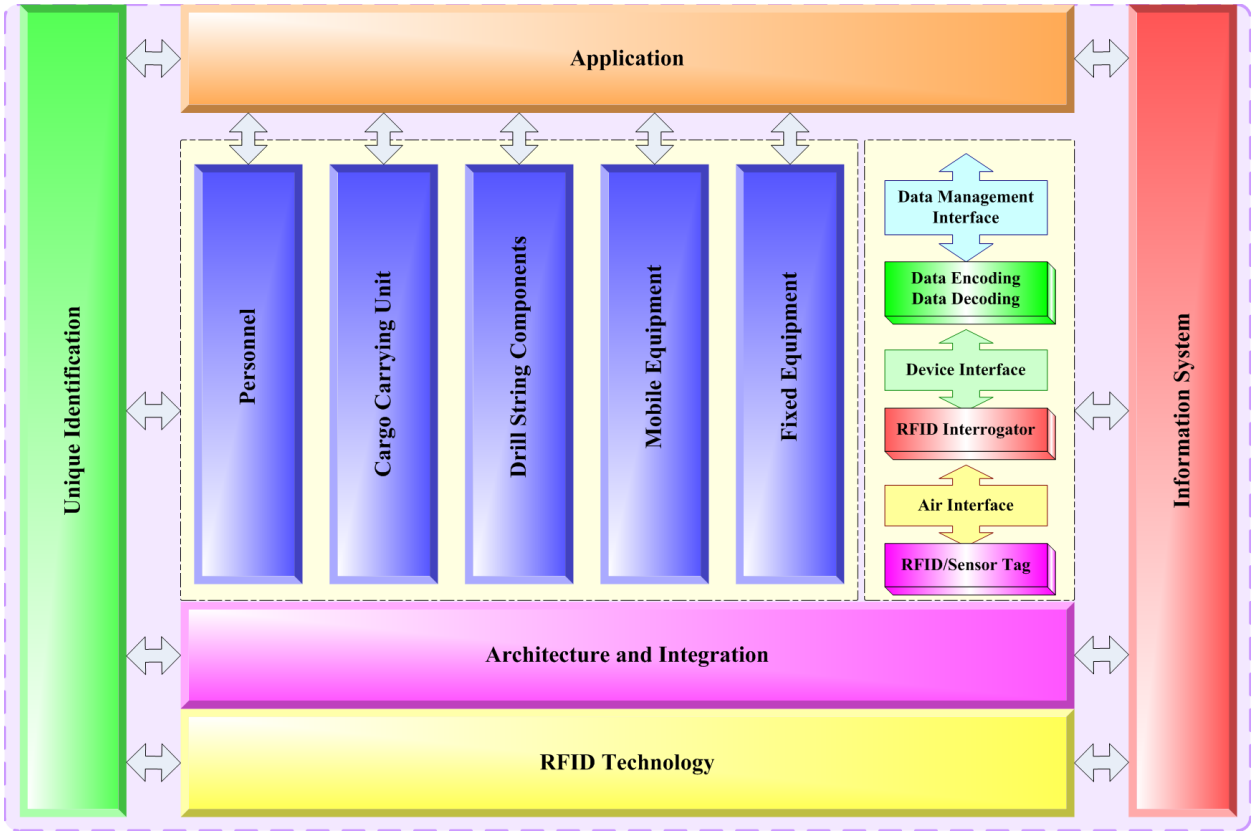

Fig. 2: RFID guideline documents organization.

Two key components in RFID systems are interrogators (readers) and transponders usually called tags. Fig. 3 represents an overview of the integration of RFID, sensor network nodes, real time location systems within the enterprise application layer.

The guideline documents present the requirements for RFID systems, tag and infrastructure Standards (based on OSI 7-layer Model to RFID), systems architectural considerations, in the context of the navigation from intra-enterprise to inter-supply chain RFID applications and considering the paradigm shift in e-business practices and the emergence of future Internet and Internet of Things and Services.

The documents will address the issues of tag and infrastructure ubiquity, in-enterprise RFID infrastructures based on systems architectures and business cases, and RFID infrastructures deployed across different enterprises within the same supply chain (i.e. container supply chain). The installation of these infrastructures has to be synchronized with the changes in e-business practices and work processes being implemented within the same supply chain.

At the end the success of an RFID deployment depends on the accuracy of the data reads, and on the analysis of the received data. Data management (analyzing data, filtering data) and deciding data's business relevance become increasingly critical in oil and gas industry.

This requires that an RFID system must provide a higher degree of real time business activity monitoring (the aggregation and analysis of relevant information to get accurate information) near the edge of the enterprise systems. At that level, the need for data analysis and integration is critical. The ultimate goal of deploying RFID in oil and gas industry is increasing the work process efficiency, increase revenues, operating income and capital efficiency.

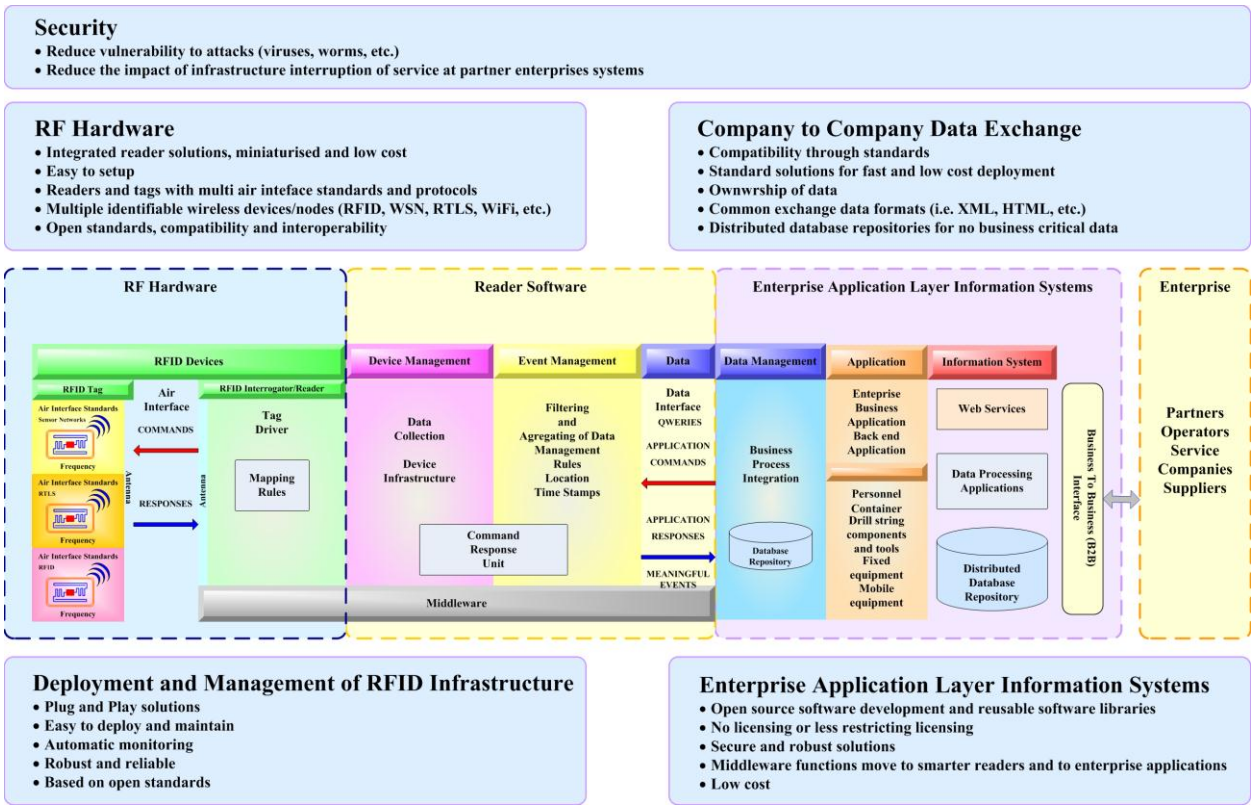

Fig. 3: RFID and sensor network nodes within the enterprise application layer information system.

2 RFID deployment preparation

The main purpose of deploying RFID is getting access to high quality real time data that improve both work processes and lead to safer, faster and better decisions. A successful deployment of RFID depends on a solid understanding of the technology and how it can improve work processes and decisions. The following preparation steps are recommended in the deployment of RFID in oil and gas industry. The steps should be carefully understood and applied for a successful implementation.

2.1 Define and create an RFID policy

The operators should define an RFID policy with focus on improved work processes and safer, faster and better decisions. The basis for improved work processes and better decisions is the availability of quality information. So the policy should focus on what RFID data is required for

improving work processes and decisions, which technology is most appropriate, how the data should is stored, and how it is distributed to different systems/work processes and how it is used by systems/end-users.

The RFID policy should to be reviewed every year to ensure that it is updated as implementation issues are resolved. Furthermore, the RFID policy should be inline with the Offshore Norge guideline to avoid different operators addressing the issues in their own ways. It is recommended to receive high level approval in the oil and gas operators management for the strategy and plan described in the RFID policy.

2.2 Document the reasons to consider RFID for adoption

For each planned deployment of RFID the arguments for RFID adoption should be documented. The document should describe and quantify the reasons for the implementing the technology. These could include improved HSE, improved regularity or reduced costs due to more and better quality on the information that leads to faster and better decisions, improved integrated work processes, better integration with suppliers or better services to the customers.

2.3 Define requirements, select RFID technology and candidate suppliers

Identify the high level conceptual framework in which the technology will be used. Identify key probable operating conditions and constraints e.g. temperature ranges (operating and survival), required read and write conditions (including probable read/write ranges), environmental conditions, data and data exchanges required, security, redundancy etc. Prepare a call for tender, compare offered solutions, and select one or more potential technology suppliers.

2.4 Develop an implementation model

Develop an implementation model that defines the implementation strategy, covering such items as the proposed technology provider (ensure a second supplier in case the first can not deliver the required capability on time), safety issues associated with implementation, communication and agreements with the staff and unions, staff communication plan, testing processes etc.

2.5 Develop the deployment plan

Develop the deployment plan. Select the fastest implementation application where the company can see an immediate gain, and where the initial challenges will be manageable. Select first a pilot case using a small facility (platform/unit), where as many variables as possible can be controlled. Get the hardware implemented and properly tested and operated, and sort through the data, repository and software issues in this test environment.

2.6 Manage the stakeholders

At any time, ensure that the plan is fully supported at all levels - from the management level down to the platform floor. Those directly involved or influenced by the introduction, will then know what the aims are, and will be supportive of the changes done by introducing the RFID, wireless sensor technology and real time location systems (RTLS).

It is recommended that the RFID, RTLS and wireless sensor technology suppliers are involved in the plan, to maximise their support and have the ownership of the plan clearly understood. Inform about the progress and gains made, and confirm the results against the initial reasons for adoption.

3 Implementation projects

3.1 Initiation

The first step in the implementation project is to conduct a risk assessment to help shaping the final scope of the implementation and identify the most appropriate uses of the RFID technology and wireless sensors, as well as potential controls to mitigate the accompanying risk.

The risk assessment should be based on proposed changes in data flows and work processes by the deployment of RFID with respect to existing operations.

3.1.1 Site survey and connectivity

Conduct a site survey as part of your planning phase. A site survey will identify issues related to radio frequency (RF) communications and potential electromagnetic interference in your facility, so you can design your RFID system accordingly. A site survey will help to identify existing in-band RF sources that may present co-existence challenges, such as old wireless access points and wireless alarms or monitoring systems. A proper site survey is also instrumental in mapping out the antenna RF coverage, power and network architecture.

A site survey is vital to identify equipment requirements and as a vehicle to optimize component placement. Based upon the company objectives, the deployment team can determine the most appropriate programming and read zones. The site survey may also contribute to determine the amount and content of data that is needed in the tag. Some operators are comfortable with simply a short random number and a link to a central data base. Many operators need a fully programmed ID that has back-up both locally and to the network. A check of data needs locally and globally is required.

3.1.2 Acquisition and development

The acquisition and design phase of the project involved planning the RFID system. One design decision is to select the tag and interrogator types for each implementation site.

The various components of the system have to be integrated. When installing all the servers hosting wireless sensors, RFID management system software and databases, secure configuration guidelines have to be addressed considering the existing IT infrastructure. An important part of the installation is establishing data repositories that shall be shared between applications for end-users in and outside the company.

Once the interrogator limitations have been identified, then it will be better to determine the type and quantity of RFID components, including applicators, handheld interrogators, fixed conveyor interrogators, integrated interrogator/antenna assemblies, turntable interrogators, and portals.

3.1.3 Programming tags

Be cognizant of the tag commissioning (programming/application) location. Seek locations with inherent case isolation, such as the case erect/fill station, and if correctly deployed, you can take advantage of existing equipment, such as reject stations (where the cases are checked for case weight and proper tag ID, otherwise they are rejected). Be aware that some products may be imposed to further tag commissioning location restrictions if they are subjected to metal detection processes, as is often the case for such items as adhesive bandages.

3.2 Pilot

Best practices approach suggests different phases of an effective RFID project from the point of concept to implementation. The checklists combined with the deployment phases will allow a selection of a suitable business partner, and allow completion of a successful RFID implementation.

3.2.1 Deployment partner selection

Selecting partners is an intricate part of the RFID implementation since an emerging trend within the RFID industry is that several companies make partnership to provide a complete solution. One company provides the software, one company provides the hardware and one company handles the integration, or one partner fulfils all of the requirements. In other cases one partner provides the integration and hardware recommendation where another partner provides the software.

It is recommended that one supplier take the responsibility for the complete delivery. The other suppliers should be treated as subcontractors to avoid discussions about responsibility for system errors. The suppliers should also present the test procedures for the verification and validation of the complete system.

It is recommended that the operator validate the vendor claims by checking references for past installations, verify that deliverables were met, and verify the professionalism and ultimately the success of the implementations.

3.2.2 Test pilot environment and proof of concept

Assess future requirements by building a scalable pilot that should be a smaller version of the full system. The equipment, portals, antennas, interrogators, and the host should at least be the minimum components. The pilot will allow solving of problems that may occur in the deployed environment and be corrected before the full implementation.

The pilot will allow the operator to validate business processes, check validity of data, data storing, data distribution to different end-user applications, understand the physics and limitations of the technology, possible interrogator placement issues, tag placement, and very importantly provide lessons learned before going live. Factors to observe are problems related to signal strength, interrogator placement, noise issues, tag placement, and compatibility between the tag and the object.

3.2.3 Test and validation

RFID deployment is a challenging task and requires that experienced persons that understand the existing operations, systems, and work processes cooperate with the system suppliers.

The test procedures must be fully understood and agreed upon by the operator. The test results are used to validate the system. The question to be considered: Is it behaving as expected?

3.2.4 Data and system integration

When testing and evaluating, it is necessary to determine to what extent the capabilities are achieved, since the RFID systems minimize RF coverage and report precise readings in finite areas.

Today there are some multiple frequency devices and multiple protocol devices at a given frequency. Some standards and middleware systems above the interrogator have some way to go to support multiple protocols. But if possible, it is recommended to select systems that are multi protocol capable, and have an open data structure like XML between interrogators and the central system to facilitate integration for data exchange. The data from the interrogators are sorted and organised by the RFID middleware software. The integration with existing end-user systems through a data repository should consider the complexity of the data, how they are defined, and how the data management is working.

All RFID data should be well defined and stored in data repositories. The data should be distributed from the repositories to end-user systems in such a way that they do support the new work processes.

It is recommended to check the development of the interfaces between the RFID systems, data repository and the end-user applications. While monitoring the creation and definition of the interfaces, organizations should examine:

- Compatibility between databases used in all systems, and if they easily connect without additional programming.
- Interface definition and mappings of the interfaces between the systems.
- The language used for the data exchanged between systems.
- Who controls the data?
- Where are the data stored?

3.2.5 Work processes

Complete work process of the entire business domain should be documented such that there is a roadmap for the full installation. If these processes do not exist, be sure to allot additional time to the project plan to complete the process reengineering that is required.

3.2.6 Pilot implementation

The pilot implementation is actually the full system in the full working environment where RFID system will exist. The difference is that the operation and use of the system will be scaled back to manageable portions. Load testing should expose any further flaws in business processes, anomalies within the system and should allow full operational scale that is required to run the business.

The objective of the pilot program is to develop predictability and scalability in order to resolve as many possible scenarios that affect the business and the real scenarios. Achievement of precision, placement, output, and performance will need to be verified and recorded. The recording of the findings will provide a useful troubleshooting and training tool and can act as knowledge transfer document. Checklists for tasks that are completed during the pilot phase of the project are recommended.

3.3 Implementation

An implementation plan should be developed from the pilot implementation securing efficient deployment. This could include: a contingency plan, scheduling of resources both for hardware and software and IT resources etc.
Steps like validation, data capture, network and device management and scheduling will provide for the completion of the RFID implementation project.

3.4 Deployment

The complete system is rolled out. All relevant items are tagged, all reading points are established, and the data systems shall handle all data with minimum delay. The operators are familiar with the system responses.

3.4.1 Acceptance test

The acceptance testing process for every portal required passing a tagged object through the portal many times (enough to be statistically significant in relation to the expected usage levels) as defined in the requirements for the specific application. The acceptance test for RFID implementation has to address operations, reliability, certification, security and privacy before full acceptance. The acceptance test is carried out based on an agreed test procedures and criteria in order to verify completeness of project scope and formally signoff the project. The acceptance test gives the final verdict. From now on the system is up and running. Functional acceptance test on vendor site before the equipment is shipped offshore is also important.

3.4.2 Operations and maintenance

The operations phase also includes the management of the wireless sensor network and RFID system. Unexpected situations will occur, like malfunctioning tags, reflections causing interference, and overloaded data systems, etc. The operators should have routines and procedures for handling of such events.

In addition, the establishment of an information security management system, that regularly analysis and audits the security and privacy infrastructure is necessary to protect information, and gain revenue from infrastructure investments into RFID (ref. section 4).

3.5 Update and upgrading

The RFID industry is under a rapid development, and new features and equipment are presented. It will be important to follow up and evaluate new tags and solutions to see if they are compatible with the existing system, and if new features will be of value for the participating companies.

If network infrastructure upgrades are required, it may impact the timeline for implementation as some network hardware lead times and installation of additional power requirements can be lengthy. The lead times to order some network equipment can impact on the time line of the project. Any further power requirements that need to be added will also further push out the timeline for the RFID implementation.

4 Security and privacy

These subjects are depending on the given RFID solution and the level of pertinence and importance will vary. For instance, is the protection of privacy important when it comes to Personnel (HSE) and less relevant when it comes to Drill string components and tools, but the security issues are important within both areas. The detailed security and privacy issues are presented for each deployment area and have to be specifically addressed by each implementation project.

4.1 Security

As RFID systems are deployed, security issues must be addressed, not only for the new technology, but also for the technology’s interaction with existing/legacy products and services.

The operator needs to highlight security challenges and solutions in the engineering and operation of new technologies related to RFID, RTLS and wireless sensor networks as well as significant security concerns in existing technologies and applications.

Related to RFID, the tag can contain information about the object or an object ID only. Security issues are reduced when tags contain only an identifier, rather than information about the object they are attached to. But the security issue is still presence, for example through its tracing abilities that can be exploited by a competitor or environmental organization.

RFID engineering is an intense process involving stakeholder analysis, consensus building, economic constraints, and multilateral security. To design, engineer, implement, and optimize a complex RFID system will depend on the type of application and on the user's requirements. Some applications will require higher power demands and a lower tolerance for latency, so the RFID system's available power, amount of onboard data storage, radio frequency, and security requirements will vary.

4.2 Protection of privacy

Protection of privacy involves privacy management principles, awareness programs, policy enforcement mechanisms and audits. Privacy is recommended to be designed into IT systems and infrastructure. The IT solutions have to comply with law and legal principles, and the privacy and trust are very important issues in a networked world using wireless identifiable devices as RFID, RTLS and sensor networks. It is recommended that the deployment of RFID includes informing individuals of the presence of RFID tags, RTLS and wireless sensor networks that are placed on or embedded in equipment, products and/or used by employees constitute a likely threat to privacy or the protection of personal data. It is as well recommended that the industry informs and raise awareness of potential benefits and risks associated with the use of RFID technology; apply risk minimization techniques; and stimulate and support the introduction of "security and privacy by design" principle at an early stage in the development of RFID applications.

5 Appendices

Appendix A – Terminology and definitions

Terms	Definitions
6LoWPAN:	Specification for high-level communication protocols using radios based on the IEEE 802.15.4 standard for wireless sensor networks. Supports IPv6 address.
A:	
Active tag:	An RFID tag that uses a transmitter to return information as opposed to reflecting a signal back from the reader as a passive tags do. Most active tags are battery powered, though they may gather energy from other sources. Typical, active tags can be read from up to 100 meters.
ADC:	Analogue to digital converter.
Agile Reader:	An RFID reader that reads tags operating at different frequencies or using different methods of communication between RFID tag and reader.
AIDC:	Automatic identification and data capture. A broad term that covers methods of identifying objects, capturing information about them and entering it directly into computer systems without human involvement. Technologies normally considered part of auto-ID include bar codes, biometrics, RFID and voice recognition.
AIM:	1) Automatic identification manufacturers. 2) Association for Automatic Identification and Mobility. Global trade association that provides products and services related to data collection, automatic identification, and information management systems.
Air Interface Protocol:	Rules that govern how RFID tags and RFID readers communicate.
ANSI Variant:	The American National Standards Institute. A non-government organization responsible for the coordination of voluntary national (United States) standards. Object type derived from a basic (general) object type. Variants are intended to exist at the same time and require simultaneous management, while versions follow each other sequentially in time. Versions can exist at the same time, depending on how older versions are phased out.

Antenna gain:	The power ratio at the input of a loss-free reference antenna to that supplied to the input of the given antenna to produce, in a given direction, the same field strength at the same distance. Expressed in decibels. The higher the gain the more energy output. Higher gain antennas can read RFID tags from farther away.
Antenna:	The conductive element to send and receive tag data. Passive low- frequency tags (135 kHz) and high-frequency tags (13.56 MHz) use a coiled antenna that couples with the coiled antenna of the reader to form a magnetic field. Readers have antennas that are used to emit radio waves. The RF energy from the reader antenna is "harvested" by the tag antenna and used to power the tag microchip to reflect back its signal back to the reader.
Anti-collision:	A general term used to cover methods of preventing radio waves from one device from interfering with radio waves from another. Anti-collision algorithms are also used to read more than one tag in the same reader's field.
API:	Application Programming Interface.
Applicator:	A label-printing device to print and apply pressure-sensitive labels to RFID tags. Pressure sensitive labels consist of a substrate and an adhesive. Used for shipping, content, graphic images or complying with standards such as UPC or GS1.
ASCII:	American Standard Code for Information Interchange. The code is used in the transmission of data. It consists of eight data-bits used to code each alphanumeric character and other symbols.
ASIC:	Application Specific Integrated Circuit.
Asset tracking:	The most common RFID tag application. RFID asset tagging increases asset utilization, identifies the last known asset user, reduces lost items and automates maintenance routines.
ATA:	Aircraft Transportation Association
ATEX:	The EU ATEX (ATmosphere EXplosible) directives provide the technical requirements to be applied to equipment intended for use in potentially explosive atmospheres.

Authentication:	In RFID, identify verification or authentication is used in two ways. In non-contact smart cards or other payment systems the RFID reader must ensure the transponder is a valid device and is not being used with the intent to commit fraud.
Auto-ID center and labs:	A non-profit collaboration between private enterprise and researchers for the development of a global tracking network using RFID tags carrying Electronic Product Codes (EPCs). The center closed in Sep. 2003. The center's research continues at Auto-ID Labs in universities around the world, and is headquartered at the Massachusetts Institute of Technology.
Automatic identification:	Methods to collect data and enter into computer systems without human involvement. Technologies normally considered part of auto-ID include bar codes, biometrics, RFID and voice recognition.
B:	
Backscatter:	A method of communication between passive (or semi-passive) RFID tags and the readers. The tag reflects back a signal from the reader, usually modulated and at the same carrier frequency.
Bar code:	A patterned series of vertical bars of varying widths used by a computerized scanner for inventory, pricing, etc.
Base station:	An RFID tag reader that is connected to a host system.
Battery-assisted tag:	These RFID tags incorporate batteries and use the battery power to run the tag circuitry and sometimes an onboard sensor. They communicate with the tag reader using the same backscatter technique as passive tags though they have a longer read range because all of the energy gathered from the reader is reflected back to it. Also known as "semi-passive RFID tags."
Beacon:	Active or semi-active RFID tags programmed to broadcast a signal at set intervals.
BI:	Business Intelligence.
Binary value:	A mark on the substrate surface indicates the binary of one. The absence of a mark or a smooth surface surrounding a cell centre point indicates the binary value of zero.

Biometrics:	Techniques designed to recognize and authenticate the identity of people based upon one or more intrinsic physical or behavioral traits (e.g., fingerprints and retinal patterns). Because biometric traits cannot be lost or forgotten like passwords and are impossible to copy or distribute they make very effective identifiers if they can be read accurately.
Bistatic:	A bistatic RFID interrogator or reader uses a one antenna to transmit energy to the RFID tag and a different antenna to receive reflected energy back from the tag.
Bit:	Binary Digit. The basic unit of information in a binary numbering system. 1's and 0's are used in a binary system.
BPMN:	Business Process Modelling Notation.
C:	
CAGE code:	Commercial and Government Entity Code
Card operating system:	Software in a smart card that manages the basic functions of the card, such as terminal communication, security management and data management.
Character set:	That character available for encoding in a particular automated identification technology.
Character:	Data character. A letter, digit or other member of the ASCII character set.
Checksum:	Code added to a data block on an RFID chip that is checked before and after data transmission from tag to reader to evaluate whether data has been corrupted or lost.
Circular-polarized antenna:	A UHF reader antenna that produces radio waves in a circular pattern. As the waves move in a circular pattern, they have a better chance of being received, though circular polarized antennas have a shorter read range than linear-polarized antennas. Used in situations where the orientation of the tag to the reader cannot be controlled.
Closed-loop systems:	RFID tracking systems where the tracked item never leaves the company's control and the system does not have to use open standards.
CMMS:	Computerized Maintenance Management system.
CMOS:	Complementary Metal Oxide Semiconductor

COB:	Chip On Board.
Commissioning:	The process of writing a serial number to a tag and associating that number with the tagged product in a database.
Compatibility:	RFID systems are compatible if they employ the same protocols, frequencies and voltage levels and are able to operate together within the same overall application.
Compliance label:	A label that indicates conformance to industry standards for data content and format. Compliance labelling standards ensure a similar labelling approach that clearly defines the label format, usage, and the information to include on the label. There are no RFID compliance labelling standards yet but some consider bar-code labels with embedded UHF EPC tags as compliance labels.
Concentrator:	A device that communicates with several RFID readers for the purpose of gathering data, which it then filters and passes on the information to a host computer.
Conducted power:	The RF power supplied by an RFID system to the antenna. It is measured at the cable to antenna connection. In the U.S., Federal Communication Commission regulations limit maximum conducted power to 1 watt.
Contact less smart card:	A credit card or other card incorporating an RFID chip to transmit information to a reader without having to be swiped.
CRC:	Cyclic Redundancy Code/Check. The CRC-16 is used as error detection code for the backscattering operation of the tag. If errors are detected, the tag will retransmit the involved data to the reader.
CRM:	Customer Relationship Management.
D:	
Data carrier:	A medium for storing machine-readable data, such as bar codes and RFID tags. May also refer to the carrier frequency for data transmission.

Data field:	RFID chip memory assigned to a particular data type. Data fields may be protected or written over. For example, a data field might contain information about where an item should be sent, and when the destination changes the new information is written to the field. A protected data field could be used to store an Electronic Product Code, which doesn't change during the life of the product it's associated with.
Data retention:	RFID tags can retain data for over 10 years depending on temperature, humidity and other factors.
Data transfer rate:	Number of characters that can be transferred from RFID tag to reader over a specified time. Baud rate defines how quickly readers can read information on a RFID tag, and is different from read rate, which refers to how many tags can be read over a specified time.
DaWinci:	Personnel on board (POB) application used by operators in the oil and gas industry. The DaWinci system is a future oriented and comprehensive POB system, facilitating resource sharing and cost reduction with respect to personnel movements. The system has high focus on safety and security, and integrates offshore contingency planning, as well as handling of emergency situations. Furthermore, DaWinci ensures follow-up governmental and company specific requirements regarding work periods, training requirements, etc
DCA:	Direct On Chip.
Dead tag:	An RFID tag that cannot be read by a reader.
De-tune:	When a UHF antenna is placed close to metal or metallic material, the antenna can be detuned to better receive RFID waves of a certain length from a reader so that the RFID tag can be read, but results in poor performance. OMNI-ID tags do not need to be de-tuned.
Dipole:	Antenna consisting of two straight electrical conductors or "poles". The antenna is typically ½ wavelength from end to end. In an RFID transponder the antenna is connected to a microchip.
DNS:	Domain Name Service.
DoD:	Department of Defence (US).

Domain identification number:	String of characters representing the value of the identifier assigned to a domain.
Domain:	Distinguished part of an abstract or physical space where something exists.
DPM:	Direct Part Marking.
Dual dipole:	An antenna that contains has two dipoles. The goal of the dual dipole design is to reduce the tag's orientation sensitivity.
Dual interface smart card:	A card containing a microchip that can be read either when in contact with a reader or read remotely using radio waves.
Dumb reader:	A tag reader with limited computing power that converts radio waves from a tag into a binary number, passing it to a host computer with little or no filtering.
Duty cycle:	Length of time a tag reader is set to emit energy. European Union regulations permit tag readers to be on no more than 10 percent of the time.
E:	
ECC:	Error Checking and Correction. Mathematical techniques used to identify symbol damage and reconstruct the original information, based upon the remaining data in a damaged or poorly printed code.
EEPROM:	Electrically Erasable Programmable Read-Only Memory. A method of storing data on microchips where bytes can be individually erased and reprogrammed. More expensive than factory programmed RFID tags where the number is written into the chip silicon during manufacture, but offers more flexibility because the end user can write an ID number to the tag at the time the tag is going to be used.
EHF:	Extremely high frequency, (frequency range 30GHz – 300GHz).
EIRP:	Effective Isotropic Radiated Power. A measurement of RFID tag reader antenna output which is used in the United States and elsewhere, usually expressed in watts.

Electronic seal:	A method of sealing a digital document in a manner similar to that used for electronic signatures. Electronic seals enable computers to authenticate that document or electronic messages have not been altered, providing a level of security in digital communications.
Electroplating:	The process of using electrical current to coat an electrically conductive object with a thin layer of metal. The primary application of electroplating deposits a layer of a metal with a desired property onto a surface lacking such a trait. Electroplating can also be used to build up the thickness of undersized parts.
EMC:	Electromagnetic compatibility.
EMI:	ElectroMagnetic Interference. This occurs when the radio waves of one device alter the waves of another device. Cells phones and wireless computers may produce radio waves that interfere with RFID tags.
EMMS:	Enterprise Material Management System.
EMR:	EMergency Response.
Encryption:	Altering data so that it cannot be read by those for whom it is not intended. In RFID systems encryption is used to protect stored information or to prevent the interception of communications between RFID tag and reader.
ENOB:	Effective Number Of Bits.
EPC Discovery Service:	An EPCglobal Network service that allows companies to search for every reader that has read a particular EPC tag.
EPC Gen 2:	EPC Generation 2. The RFID standard ratified by EPCglobal for the air-interface protocol for the second generation of EPC technologies.
EPC global:	An organization which objective is world-wide adoption and standardization of EPC technology in an ethical and responsible way.
EPC Information Service:	A network infrastructure that enables companies to store data associated with EPCs in secure online databases with different levels of access.

EPC:	Electronic Product Code. A serial number created by the Auto-ID Center that will complement barcodes. The EPC identifies the manufacturer, product category and individual item.
EPCglobal:	A non-profit organization set up by the Uniform Code Council and EAN International, the two organizations that maintain barcode standards, to commercialize EPC technology.
EPCIS:	Electronic product code information service.
EPROM:	Erasable Programmable Read-Only Memory. Non-volatile memory in an RFID tag that can be erased by exposure to intense ultraviolet light and then reprogrammed.
ERP system:	Enterprise Resource Planning system.
ERP:	Effective Radiated Power. A measurement of the output of RFID tag reader antennas used in Europe, usually expressed in watts.
Error correcting mode:	A mode of data transmission between RFID tag and tag reader so that errors or missing data is automatically corrected.
Error correcting protocol:	A set of rules used by tag readers to interpret data from the RFID tag correctly.
Error detection code:	Code stored on an RFID tag to enable the reader to determine the value of lost or scrambled data, see CRC (cyclic redundancy code).
ESB:	Enterprise Service Bus.
ESD:	Emergency Shut down.
ETL:	Extract, Transform and Load.
ETSI:	European Telecommunications Standards Institute. An independent, non-profit organization that defines telecommunications standards for Europe. Responsible for standardization of broadcasting and related areas, such as intelligent transportation, medical electronics and RFID.
Event data:	Information related to a significant business transaction or event, such as products leaving a manufacturing facility or equipment leaving a construction site.

EX:	Regulations for equipment in explosive areas.
Excite:	Tag readers "excite" a passive tag when the reader transmits RF energy to activate the tag and cause it to transmit data back to the reader.
F:	
Factory programming:	Some read-only RFID tags must have their identification number written into the microchip at the time of manufacture. This is known as factory programming. That data cannot be over-written or modified.
False read:	When a tag reader reports the presence of an RFID tag that does not exist. Also called a phantom transaction or false read.
Far-field communication:	RFID tags farther then one full wavelength away from the tag reader are said to be "far field", within one full wavelength away is "near field." Far field signals decay as the square of the distance from the antenna, while the near field signals decay as the cube of distance. Passive RFID tags that use far field communications (UHF and microwave systems) have a longer range than tags using near field communications (low- and high-frequency systems).
FDIS:	Final draft international standard, (Ref. ISO).
Field programming:	RDIF tags with non-volatile EEPROM memory can be programmed after they are shipped from the factory so that users can write data to the tag once it is placed.
Fixed reader:	An RFID interrogator mounted to a permanent or non-mobile structure enabling users to read RFID tag numbers attached to movable items.
Folded dipole:	A dipole antenna in which the two poles are connected to each other, as well as to the microchip.
Form factor:	The transponder packaging type; thermal transfer labels, plastic cards, key fobs, etc.
Forward channel:	Energy path from the tag reader to the RFID tag.
Free air:	Reading an RFID tag that is not attached to anything.
FSM:	Finite State Machine.
G:	

GDS:	Global Data Synchronization. The process of matching a manufacturer's master files with retailer's product information. GDS is a prerequisite to deploying RFID in open supply chains to ensure that RFID serial numbers refer to the correct database product information.
GIS software:	Geographical Information System software. For recording, analyzing and managing geospatial data (data referenced to a fixed location). With GIS software users can run queries, analyze spatial information, and create maps.
GLN:	Global Location Number. A numbering system developed by EAN International and the Uniform Code Council as a way to identify legal entities, trading parties and locations to support electronic commerce. GLNs can identify functional entities (e.g., a purchasing department), physical entities (e.g., a particular warehouse) and legal entities or trading partners (e.g. buyers or sellers).
Global commerce initiative:	Founded by manufacturers, retailers and trade industry associations to improve international supply chains for consumer goods through collaborative development and EAN International/Uniform Code Council standards and best practices, including use of EPC.
GTIN:	Global Trade Item Number; GS1 Global trade item number, (see also SGTIN). Standardized system of identifying products and services created by the Uniform Code Council and EAN International. Product identification numbers, such as EAN/UCC -14, are based on the GTIN.
GUID:	Global Unique Identifier
H:	
Hardness:	A measure of the resistance of a material to surface indentation or abrasion; may be thought of as a function of the stress required to produce some specified type of surface deformation. There is no absolute scale for hardness; therefore, to express hardness quantitatively, each type of test has its own scale of arbitrarily defined hardness. Indentation hardness can be measured by Brinell, Rockwell, Vickers, Knoop, and Scleroscope hardness tests.
Harvesting:	The way passive RFID tags gather energy from RFID reader antennas.

HF:	High Frequency. This is generally considered to be from 3 MHz to 30 MHz. HF RFID tags typically operate at 13.56 MHz. Typical, can be read from less than 1 meter away and transmit data faster than low frequency tags but consume more power.
HSE:	Health, safety and environment.
Hub:	Repeater for wireless or cable bounded data traffic.
Human readable identification:	The letters, digits or other characters associated with specific symbol characters that are incorporated into linear bar code or two-dimensional symbols.
Hybrid card:	A smart card that has both a no-contact IC and a contact IC, so that a hybrid card acts as two separate cards.
I/O port:	Input/Output port. Connections on an RFID reader for external devices. An output device could be a panel that opens when a tag is read. An input device could be a photoelectric eye to turn on the reader when an object breaks the beam.
I:	
ICS:	International classification for standards, (ref. ISO).
ID:	Identification number (unique). String of characters representing the value of the identifier
Identification scheme:	Definition and description of the structure of identifiers
Identification system:	Set of formal rules for objects to be identified in a given domain
Identification:	Act of associating identification numbers to an object
Identifier:	Attribute associated with an object to unambiguously identify it in a specified domain
Identity:	Established relation between an object and an identification number
IEC:	International electro-technical commission. An international standards organization dealing with electrical, electronic and related technologies.
Induction loop:	A coil-wire transceiver used when doing RFID reads in the presence of metal.

Inductive coupling:	The transfer of energy from one circuit to another through mutual inductance. In RFID systems using inductive coupling, the tag reader antenna and the RFID tag antenna each have a coil which together forms a magnetic field so that the tag draws energy from the field to change the electrical load on the tag antenna. The change is picked up by the tag reader and read as a unique serial number.
Inlay:	Inlays can be considered "unfinished" RFID labels, as they are a chip attached to an antenna and mounted on a substrate. Usually sold to label converters who turn them into smart labels. Also known as inlets.
Intelligent reader:	A reader that can filter data, execute commands and perform functions similar to a personal computer.
Intentional radiator:	A device that produces a RF signal for the purpose of data communications. Examples are cordless phones and door openers.
Interoperability:	The ability for RFID tags and readers from different vendors to communicate. Interoperability testing assesses the ability different systems to exchange information and use the data that has been exchanged.
Interposer:	A device connecting an RFID microchip to an antenna to create an RFID transponder.
Interrogation zone:	Area in which a tag reader can provide enough energy to power up a passive tag and receive back information. Also known as the read field or reader field. RFID tags located outside the interrogation zone do not receive enough energy from the reader to produce a signal.
Interrogator:	See Reader.
IO:	Integrated Operations.
IoM:	Internet of Media.
IoS:	Internet of Services. A software based component that is delivered via different networks and Internet. The Internet of Services based on RFID applications has to address the privacy issues. IoS is not just about technology, but also about usage, community building, deployment, business models, public policy, security and privacy.

IoT:	Internet of Things. A dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network. "Things" are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information "sensed" about the environment, while reacting autonomously to the "real/physical world" events and influencing it by running processes that trigger actions and create services with or without direct human intervention. Interfaces in the form of services facilitate interactions with these "smart things" over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues.
IS:	Intrinsically safe.
ISA100:	Specification for high-level communication protocols using radios based on the IEEE 802.15.4 standard for industrial applications.
ISM frequency bands:	Industrial, scientific, and medical frequency bands.
ISO:	International Standards Organization, (see the guideline's part 3 for an overview of ISO RFID related standards).
Isotropic:	Isotropic antennas radiate energy equally in all directions.
Issuing organization/issuing agency:	Organization being entrusted by a registration authority to assign identification numbers in a given domain.
IT:	Information technology.
Item-level:	The tagging of individual products, as opposed to case-level and pallet-level tagging.
J:	
K:	
KU-tag:	An RFID tag that reads objects containing metal or liquid. At just 1.5 millimetres in thickness it as one of the thinnest RFID tags designed to operate under such conditions.
L:	

Label applicator:	A device for applying labels. Some label applicators can print bar codes and encode RFID transponders in labels before application.
LEL:	Lower explosive limit.
LF:	Low frequency. This is generally considered to be from 30kHz to 300kHz. Low frequency tags typically operate at 125 kHz or 134 kHz. Disadvantages of such tags are they have to be read from within 1 meter typically and data transfer rates are slow, though they are less subject to interference than UHF tags.
License plate:	A simple RFID tag that contains a serial number associated with database information as a way to simplify the tag and reduce cost.
License tag number:	The information contained with the symbol character set to uniquely identify the component. As a minimum the information shall contain the manufacturers CAGE code followed by an asterisk (ASCII separator) and trace code (lot, member or serial number).
Linear-polarized antenna:	An antenna designed to focus radio energy from the reader in one orientation or polarity, thereby increasing the read distance and providing increased penetration through dense materials. In order to be read accurately, RFID tags designed to be used with a linear polarized antenna must be aligned with the reader antenna.
LLRP standard:	A standard to foster RFID reader interoperability and create a foundation for technology providers to offer capabilities that meet industry-specific requirements.
Lot number/batch number:	String of characters representing the value of the identifier assigned to a group of specimens considered as one object to identify the specimens that are manufactured together under assumed identical conditions and in a limited time interval
Low-level reader protocol standard:	A standard to promote RFID reader interoperability and improve capabilities to meet industry-specific requirements.
M:	
Manufacturer:	Producer or fabricator of component or the supplier in a transaction if the supplier is the warrantor of the component.
MCM:	Multi Chip Module.

MCU:	Micro Controller Unit.
MEMS:	Micro-Electro-Mechanical Systems. Systems made up of components between 1 to 100 micrometers in size (0.001 to 0.1 mm). An RFID MEMS tag with micromechanical components is designed to withstand wide temperature ranges as well as gamma radiation and may be used on medical devices.
MES:	Manufacturing Execution System. A system that allows companies to control critical production activities and improve traceability, productivity and quality.
Metadata/meta information:	Information (irrespective of its form) used to describe a real or abstract object
MF:	Medium frequency, (frequency range 300kHz – 3MHz).
Microwave:	Microwave frequencies are generally considered to be from 300MHz to 300GHz. RFID tags that operate at 5.8 GHz (or above 415 MHz) have very high transfer rates and typically can be read up to 10 meters but are costly and use a lot of power and are expensive.
Middleware:	RFID software that resides on a server between readers and enterprise applications and used to filter data or manage readers across a network.
MIPS:	Material management system, (ERP system).
Mobile reader:	An RFID interrogator that is easily transported, allowing employees to read RFID tags attached to items in a warehouse or other setting along the supply chain.
Monostatic:	An RFID reader that uses the same antenna to transmit RF energy to and receive RF energy from an RFID tag.
Multimode:	RFID transponders that can be programmed to operate and comply with multiple standards.
Multiple access schemes:	Techniques to increase the amount of data that can be wirelessly transmitted within the same frequency spectrum. RFID readers may use Time Division Multiple Access (TDMA) so that they read tags at different times to avoid interference.

Multiplexer:	A technique that allows a reader to have more than one antenna and reduces the number of readers needed to cover a given area while preventing the antennas from interfering with each other.
N:	
NCS:	The Norwegian Continental Shelf.
NFC:	Near-Field Communication. RFID tags closer then one full wavelength away from the tag reader are said to be "near field", while more than one full wavelength away is "far field." Near field signals decay as the cube of the distance from the antenna, while far field signals decay as the square of distance. Passive RFID tags that use far field communications (UHF and microwave systems) have a longer range than tags using near field communications (low- and high-frequency systems).
Noise:	Random or ambient electromagnetic energy found in the operating environment of RFID equipment. Other RF devices such as robots, electric motors and other machines may cause noise.
Nominal range:	The read range at which at which an RFID tag can reliably be read.
Null spot:	An area in the RFID tag reader field that does not receive radio waves. This is a common issue with UHF systems.
O:	
Object identification number:	String of characters representing the value of the identifier assigned to an object (synonyms used; product number, item number, part number, article number, product identifying number, traceability number (serial or batch))
Object:	A physical or non-physical "thing", i.e. anything that might exist, exists or did exist and is considered as an entity treated in a process of development, implementation, usage and disposal
Offshore Norge: One-time	The Norwegian Oil Industry Association.
programmable tag:	Also known as a field-programmable tag, it is RFID tag memory that can be programmed once and is then write-protected. After the memory is written to it is considered read only memory.

ONS:	Object Name Service. A system for looking up unique Electronic Product Codes (EPCs) and information about the item associated with the code.
Ontology:	Ontology in the Semantic Web define the concepts and relationships used to describe and represent an area of knowledge and are used to classify the terms used in a particular application, characterize possible relationships, and define possible constraints on using those relationships.
Organization identification number:	String of characters representing the value of the identifier assigned to an organization.
Organization:	Company, corporation, firm, enterprise, authority or institution, or part or combination thereof, whether incorporated or not, public or private, that has its own functions and administration.
Orientation:	Position of a reader antenna in reference to a tag antenna. In UHF systems reader antennas can be linear- or circular-polarized. When using a linear polarized antenna the tag and reader must be in alignment to achieve the maximal reading distance.
P	
Part identification data:	Markings used to relate parts to their design, manufacturing, test, and operational histories.
Passive tag:	RFID tag without an internal battery or power source. The energy is gathered from the reader, these radio waves are converted by the tag antenna into current. The tag reflecting back the signal (modulated) from the reader.
Patch antenna:	A square reader antenna made from metal or foil.
PDA:	Personal Data Assistant.
Phantom read:	When a reader reports the presence of a tag that doesn't exist. Also called a false read or phantom transaction.
PIFA:	Planar Inverted F Antenna.
PML:	Product Markup Language.
POB:	Personnel on board.
Portal:	An RFID interrogator gateway where tagged items are moved through a portal reader to collect RFID tag data.

POS:	Point of Sale.
Power level:	The amount of RF energy emitted from an RFID tag reader. The higher the power output the longer the read range. Many countries regulate power levels to avoid interference with other devices.
PPE:	Personal protective equipment.
Printer:	An RFID printer, or printer/encoder, prints a label with an embedded RFID transponder and encodes item information in the chip within the transponder.
Programming a tag:	The act of writing data to an RFID tag. When a serial number is first written to a tag it is called "commissioning".
PSD:	Process shut down.
PT:	Personnel tracking system.
Q:	
Quiet tag:	RFID tags that are only readable with reader output at full power, or which can be read only at very close range.
R/W:	Read/Write.
R:	
RDF:	The Resource Description Framework is a standard model for data interchange on the Web. RDF has features that facilitate data merging even if the underlying schemas differ, and it specifically supports the evolution of schemas over time without requiring all the data consumers to be changed.
Read range:	The distance from which tag readers can accurately and reliably communicate with RFID tags. Active tags have longer read ranges than passive tags because they have their own power source for signal transmission. In passive tags the read range is controlled by frequency, reader output power, antenna design, and the method used to power up the tag. Low-frequency tags use inductive coupling which requires the tag to be close to the reader.
Read rate:	A specification describing how many tags can be read within a given period or the number of times a single tag can be read within a given period. Alternatively, the maximum rate that data can be read from a tag expressed in bits or bytes per second.

Read:	The process of retrieving RFID tag data by broadcasting radio waves at the tag and converting the waves the tag returns to the tag reader into data.
Reader field:	The area a tag reader can cover. Tags outside the field do not receive radio waves emitted by the tag reader and cannot be read.
Reader module:	Reader electronics (digital signal processor and circuit board) can be placed in a dedicated device or an RFID label printer, for example.
Reader talks first:	A passive UHF reader initially communicates with RFID tags in its read field by sending energy to the tags. The tags do not transmit until the reader requests them to do so. The reader finds tags with specific serial numbers by asking all tags with a serial number that starts with either 1 or 0 to respond. If more than one responds, the reader might ask for all tags with a serial number that starts with 01 to respond, and then 010. Also known as "walking" a binary tree, "tree walking", or "singulation".
Reader:	A device used to communicate with RFID tags via radio waves, it has one or more antennas that emit radio waves and receive a signal back from the tag. Tag readers are also sometimes called interrogators.
Read-only:	RFID tag memory that cannot be altered unless the microchip is reprogrammed.
Read-write:	RFID tags that can store new data, often used on reusable containers and other storage assets. When the contents of the container are changed, new information is written to the tag.
Registration authority:	Organization responsible to receive and acknowledge applications from organizations wishing to become an issuing organization in a given domain.
Reverse channel:	The path energy travels from the RFID tag to the interrogator, or reader. It is also sometimes called the back channel.
RF:	Radio Frequency.
RFFE:	Radio Frequency Front End.
RFID tag:	See Tag.

RFID:	Radio Frequency IDentification. A technique for identifying unique items using radio waves. Typically a tag reader communicates with an RFID tag, which contains digital information. There are also "chipless" forms of RFID tags that use material to reflect back radio waves beamed at them.
ROI:	Return of investment.
RSD:	Redundant Signed Digit.
RSSI:	Received signal strength indication is a measurement of the power present in the received radio signal, (IEEE 802.11 protocol).
RTLS:	Real-Time Locating System. A technique for finding the position of assets using active RFID tags. Three reader antennas are positioned to receive signals from tags in their common read field. Triangulation is used to calculate the asset location.
Rules:	Rules in the Semantic Web refer to elements of logic programming and rule based systems bound to the data. Rules offer a way to express e.g. constraints on relationships defined by RDF or may be used to discover new implicit relationships.
S:	
SAP:	ERP system used by most of the operators.
SAR:	Successive Approximation Register.
SAW:	A technology for automatic identification using low power microwave radio frequency signals that are converted to ultrasonic acoustic signals by a piezoelectric crystalline material in the transponder. Variations in the reflected signal can be used to identify an object.
Scanner:	An electronic device, such as an RFID tag reader, that sends and receives radio waves. When combined with a digital signal processor that turns the waves into data, the scanner is called a reader or interrogator.
SCM:	Supply Chain Management.

Semantic web:	It is a Web of data that provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries. It is a collaborative effort led by W3C with participation from a large number of research and industrial partners.
Semi-active tag:	Sometimes used for semi-passive tag, (see semi-passive tag).
Semi-passive tag:	RFID tag with an internal battery. The battery is used to power the microchip's circuitry, but not used to send a signal to the reader. Some semi-passive tags sleep until they are woken up by a signal from the reader to conserve battery life. These tags are sometimes called semi-active tag or battery assisted tags. The names are used rather interchangeably to describe this type of tag.
Serial number:	String of characters representing the value of the identifier assigned to an individual specimen of objects or an object type
SGTIN:	GS1 Serialized Global Trade Item Number, (see also GTIN).
SHF:	Super high frequency, (frequency range 3GHz – 30GHz).
Shielding:	The use of a Faraday cage, Mylar sheet or metal barrier to prevent radio frequency noise from interfering with tag readers or to prevent readers from interfering with other devices.
Signal attenuation:	The drop in RF energy from an RFID tag or tag reader as a function of distance is proportional to the inverse square of the distance. Attenuation can be increased by external factors as well such as the presence of liquids or metal..
Singulation:	A passive UHF reader initially communicates with RFID tags in its read field by sending energy to the tags. The tags do not transmit until the reader requests them to do so. The reader finds tags with specific serial numbers by asking all tags with a serial number that starts with either 1 or 0 to respond. If more than one responds, the reader might ask for all tags with a serial number that starts with 01 to respond, and then 010. Also known as "walking" a binary tree, "tree walking", or "reader talks first".
Skimming:	Reading an RFID tag covertly.
Slap and ship:	The act of putting an RFID label on a case or pallet just before it is shipped from a supplier to a retailer.

Slotted antenna:	An antenna designed as a slot cut into an electrical conductor connected to the transponder. Slotted antennas have the same orientation sensitivity as dipole antennas.
Smart card:	Any payment card that contains an embedded microchip. A contact less smart card uses RFID technology to send and receive data.
Smart label:	A bar code label that contains an RFID transponder is considered "smart" because it can store information and communicate with a reader.
Smart reader:	A reader that can filter data, execute commands and perform functions similar to a personal computer.
SOIL:	Secure Oil Information Network.
Structure:	The order of data elements in a message.
Substrate:	The material (paper, plastic, metal, etc.) upon which a RFID tag is placed.
Supplier:	The trading partner in a transaction that provides the component (e.g., manufacturer, distributor, reseller, etc.).
Switch:	A more advanced hub.
Synchronization:	Controlling the timing of tag readers that are close together so they don't interfere with one another during the read process.
T:	
TAB:	Tape Automatic Bonding.
Tag talks first:	How tag readers in a passive UHF system identify tags in their field. When RFID tags enter the reader's field they immediately announce their presence by reflecting back a signal, which is useful in an environment where items are moving quickly.
Tag:	A microchip attached to an antenna capable of reflecting/ transmitting data. Some tags also receive and store data. They are packaged so that it can be attached to or into an object, animal or person, programmed with a unique serial number. Some tags are also managing additional information. A RFID tag receives signals from a tag reader and sends signals back to the reader and can be active, passive or semi-passive. RFID tags are also sometimes called transponders.

Tamper-evident tag:	An RFID tag that signals a reader when a container has been opened without authorization.
TBD:	To be done.
TC:	Technical committee, (ref. ISO).
TDS:	Tag data standard.
Traceability:	Ability to trace (identify and measure) the stages that lead to a particular point in a process
Traceability:	For purposes of this document, traceability is defined as the ability to relate historical documentation to parts using part identification numbers.
Track and trace:	The process of gathering information about the movement and location of items.
Transceiver:	A device that both transmits and receives radio waves.
Transponder:	A combination of a transmitter and a receiver, (TRANSmitter /resPONDER). RFID tags are sometimes referred to as transponders because they can be activated when they receive a predetermined signal. RFID transponders come in many forms, including smart labels, simple tags, and smart cards. See also Tag.
U:	
UCC:	Uniform Code Council. The non-profit organization that oversees the Universal Product Code (UPC), the North American bar code standard.
UHF:	Ultra high frequency. The frequency band from 300 MHz to 3 GHz. RFID tags typically operates between 840 MHz to 960 MHz so they can send information faster and farther than high- and low frequency tags.
UII:	Unique Item Identifier is the code that identifies any item in an RFID tag, (e.g. the EPC codes are a subset).
UPC:	Universal Product Code. The 12 digit data format encoded in UCC bar codes.
UPS:	Uninterruptible power supply.
UWB:	Ultra Wide Band.
V:	

Value chain:	All companies involved in any business process.
Variant:	Object type derived from a basic (general) object type. Variants are intended to exist at the same time and require simultaneous management, while versions follow each other sequentially in time. Versions can exist at the same time, depending on how older versions are phased out.
Version number:	String of characters representing the value of the identifier assigned to a version
Version:	Identified state of an object to indicate changes in its life cycle, related to a given object identification number for the type of object
VHF:	Very high frequency, (frequency range 30MHz – 300MHz).
W:	
W3C:	The World Wide Web Consortium develops interoperable technologies (specifications, guidelines, software, and tools) to lead the Web to its full potential and is a forum for information, commerce, communication, and collective understanding.
Wi-Fi:	Wireless network according to IEEE 802.11.xx standard.
WirelessHart:	Specification for high-level communication protocols using radios based on the IEEE 802.15.4 standard for industrial applications.
WMS:	Warehouse Management System. A methodology to control the movement and storage of materials within a warehouse and process the associated transactions, including shipping, receiving, put away and picking. WMSs may use bar-code scanners, mobile computers, wireless LANs and RFID.
Work-in-process tracking:	The use of RFID to track manufacturing changes reduces manual data collection and ensures that the right processes are preformed at the proper time on the correct product.
Workmate:	ERP system used by some operators.
WORM:	Write Once, Read Many. An RFID tag that can be written to once and thereafter can only be read.
Write range:	The maximum distance over which data can be written to an RFID tag.

Write rate:	The rate at which information is written to a tag and then verified as being correct.
X:	
X12 EDI:	The American National Standards Institute electronic data interchange standard developed for inter-industry electronic exchange of business transaction data.
XML:	eXtensible Markup Language.
Y:	
Z:	
ZigBee:	Specification for high-level communication protocols using low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs). Used in RF applications requiring low data rate, long battery life and secure networking.
Zone number:	Defines the presence of hazardous atmospheres, (Ref. ATEX).