NORWEGIAN OIL AND GAS GUIDELINE No.112

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

PART 2 – Architecture and integration

THE NORWEGIAN OIL AND GAS ASSOCIATION

No: 112 Enter into force: Draft

PREFACE TO THE CURRENT UPDATE

The current update of Part 2 of guideline 112 is supported by Norwegian Oil and Gas Association´s (Norwegian Oil and Gas´) expert network IO RFID and by Norwegian Oil and Gas Committee for Operations. It has been approved by the general director.

The updates are primarily additions to the content, which has been restructured according to the Purdue Enterprise Reference Architecture (PERA). The PERA model illustrates how to integrate the architecture of RFID systems with enterprise applications.

The work group behind Part 2 has been composed of the following members: Magnar Gregersen, Statoil, Arne Kjetil Nilsen, Statoil, Thor Willy Skog, ConocoPhillips, Emil B. Andersen, ConocoPhillips, Thomas Røed, Talisman, Paul Hocking, BP, Spencer Roberts, BG, Tor Olav Schibevaag, Euro Offshore, Åsmund Krokstad, Swire, Vivienne Dyas, Swire, Kari Anne Haaland Thorsen, PCA, Nils Jacob Berland, Smart Management, Nils Sandsmark, PCA, Frank Wehus, Identec Solutions, Stephane Rousselet, Total, Knut Vala, GS1, Eivind Fredriksen, S3ID, Arne Thomas Haaland, Trac-ID, Astrid Merehte Karlsen, DNV, Thore Langeland, Norsk Oil and Gas.

The responsible manager in Norwegian Oil and Gas is Lars Petter Lundahl, who can be contacted via +47 51 84 65 00 (switchboard).

These guidelines document has been prepared with broad-based participation of interested parties in the Norwegian petroleum industry, and is owned by the Norwegian petroleum industry, represented by Norwegian Oil and Gas Association as responsible for administration and updates.

Norwegian Oil and Gas Association

Vassbotnen 1, 4313 Sandnes

P.O. Box 8065

4068 Stavanger, Norway

Tel.: + 47 51 84 65 00

Fax: + 47 51 84 65 01

Web site: www.norskoljeoggass.no

E-mail: firmapost@norog.no

Guideline title:

Deployment of Radio Frequency Identification (RFID) in the oil and gas industry
Part 2 Architecture and integration

Published by:
Norsk Olje og Gass
Vassbotnen 1
NO-4313 Sandnes

Entry into force: xx.xx.xx

Relevant committee: Operations Sanction date: xx.xx.xx

Norwegian Oil and Gas Guideline 112, Part 2 approved by:

Norwegian Oil and Gas's Director General Approval date: xx.xx.xx

Objective of the guideline:

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

Part 2 covers the area of RFID architecture and integration in the oil and gas industry, and the target group is mainly network architects and system administrators.

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 Norwegian Oil and Gas web site:
http://www.olf.no/retningslinjer/

Acknowledgements

The Norwegian Oil and Gas 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:
Tore R. Christiansen, POSC Caesar Association, NO
Nils Sandsmark, PCA, NO
Dr. Thore Langeland, OLF, NO
Dr. Ovidiu Vermesan, SINTEF, NO
Magnar Gregersen, Statoil, NO
Emil Andersen, Conoco Phillips, NO
Unni Ulland, IBM, NO
Roy Bahr, SINTEF, NO
Ian Glendinning, DNV, NO
Paul R. Carr, Capgemini, NO
Jan Robert Moen, Statoil, NO
August Nilssen, Standard Norge, NO
Dr. Asle K. Berger, Capgemini, NO
Jennifer Sampson, EPSIS, 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.

Spencer Roberts, BG Group, UK
Ken Douglas, BP, UK
Chris Geen, BP, UK
Paul Hocking, BP, UK
Tor Holm, Conoco Phillips, NO
Paul Chartier, Praxis Consultants, UK
Nils Sandsmark, DNV, NO
Magne Valen-Sendstad, DNV, NO
Gaute Barstad, GdF Suez E&P Norge AS, NO
Elin Kristin Sletten, GdF Suez E&P Norge AS, NO
John Bleka, Halliburton, NO
Lars Sandtorv, IBM, NO
Arild Nystad, Petromanagement, NO
Inge Krogstad, SAS Institute, NO
Halvor Hebnes, Shell, NO
Nils Jacob Berland, Smart Management, NO
Magnus 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
Kenneth D. Bever, Assetricity LLC, US
Alan John, Assetricity LLC, US

Contents

1. Introduction

Guideline 112 from Norwegian Oil and Gas Association (formerly known as OLF) addresses development, deployment and application of Radio Frequency Identification (RFID) equipment and systems in the offshore oil and gas industry.

The purpose of RFID is to get access to real time high quality location data that improve work processes and lead to safer, faster and better decisions. The objective of the Guideline is to secure cost effective deployment of RFID through common standards, technology adoption and operating practises that together bring about interoperability and collboration.

The Guideline is in line with Integrated Operations Generation 2 (IO G2) and addresses the main needs and requirements of the offshore industry for real time management and operational information. It consists of nine parts, including five deployment areas: Personnel – Health, Safety and Environment (HSE), Cargo carrying unit (CCU), Drill string component, Mobile equipment, and Fixed equipment, supported by four technical areas: General principles for deployment, Architecture and integration, RFID technology, and Unique identification number. The other eight Parts of the Guideline can be accessed here.

The current Part 2 addresses the Architecture of RFID Systems and their Integration with Enterprise Applications. The report has five chapters, excluding this introduction:

- Chapter 2 gives a summary of the purpose of architecture and integration, and an overview of requirements from a life-cycle cost perspective.
- Chapter 3 introduces the PERA Reference Architecture and presents an RFID Architecture Model (RAM), with Hardware, Control, Middleware and Application ***Layers***.
- Chapter 4 presents an RFID Integration Model (RIM) with Hardware, Middleware and Software ***Segments.***
- Chapter 5 discusses software and information system design principles and service orientation, and defines an RFID Software Engineering Model (REM), including system location and security, together with a brief look at system application and stakeholders.
- Chapter 6 introduces Enterprise Information Management and presents an RFID Information Utiilty Model (RUM), addressing the use of semantics, reference data libraries and the semantic technology stack. It also includes an initial RFID Ontology Model (ROM) with Reference Data about structure, content and usage of RFID systems.

A set of appendices give additional background information on topics discussed.

- Appendix A lists important references and relevant sections in other Parts of this Guideline.
- Appendix B gives a summary description and links to important standards for RFID systems.
- Appendix C contains a list of principles for planning and operating RFID systems.
- Appendix D shows examples of software system characteristics and mesaureable attributes.
- Appendix E shows and example of an Enterprise Information Management framework.
- Appendix F contains initial Reference Data classes related to RFID systems.
- Appendix G contains the initial model of RFID structure, content and usage.

2. Purpose and requirements

Successful expansion and adoption of RFID requires industry-wide agreement on system structure, content and operation. *The purpose of defining standards and references for Architecture and Integration of RFID in the Oil & Gas Industry* is to promote open and scalable deployment of RFID technology with plug and play ID methods for sensors/actuators and interfaces to enterprise system. Adhering to the references and standards proposed in this report is believed to address the above.

The required services from an RFID system include -

- RFID tag communication (active, passive, semi-passive),
- RFID tag management (deactivation, attach/detach to person/object),
- RFID signal sensing (handheld devices, antennas, portals),
- RFID data update (WRITE) and collection (READ), including data integrity checking,
- RFID event management (includes filtering, aggregation, management rules, routing of data),
- RFID information history (local and central storage) and application (integration and use),
- RFID application program interface between middleware control to enterprise applications.

From a design and development perspective important requirements include a *defined system structure with identified parts*, *agreed frequency choice* and bandwidth availability (avoiding conflicts, securing redundancy), *clearly defined tag/interrogator air interface data protocols*, *fault-tolerant storage of tag data* (hybrid use of both local and central storage), *holistic system security* (including equipment, transmission, processing, storage and application), *robustness, resilience and redundancy of safety critical equipment*, *agreed syntax and semantics for all RFID data*, and *mechanisms for flexible integration with legacy systems of various types and technologies*.

From an operational perspective required Quality of Service (QoS) attributes for RFID integration include *scalability, reliable message delivery, load balancing, error tolerance and security*.

From an overall life-cycle cost perspective it is also required that consistent choices are made with respect to *functionality* in defined operating and environmental conditions, *availability* of resources for material and manufacturing, *maintainability* of open and proprietary technologies, *adaptability* to changing development and interoperability needs, and *scalability* to future extension and enhancement.

3. System architecture and standards

In this chapter we define a reference model for RFID Architecture, and review the most important standards for RFID deployment and operation.

3.1 An Architecture Model for RFID Systems

In order to present a standardized enterprise view of the complete RFID system and infrastructure we adopt the Purdue Enterprise Reference Architecture (PERA) [1]. Figure 1 shows a simplified overview of the PERA the Decision-making and Control Hierarchy using standardized ***levels*** to partition the description of system physical components, control and application.

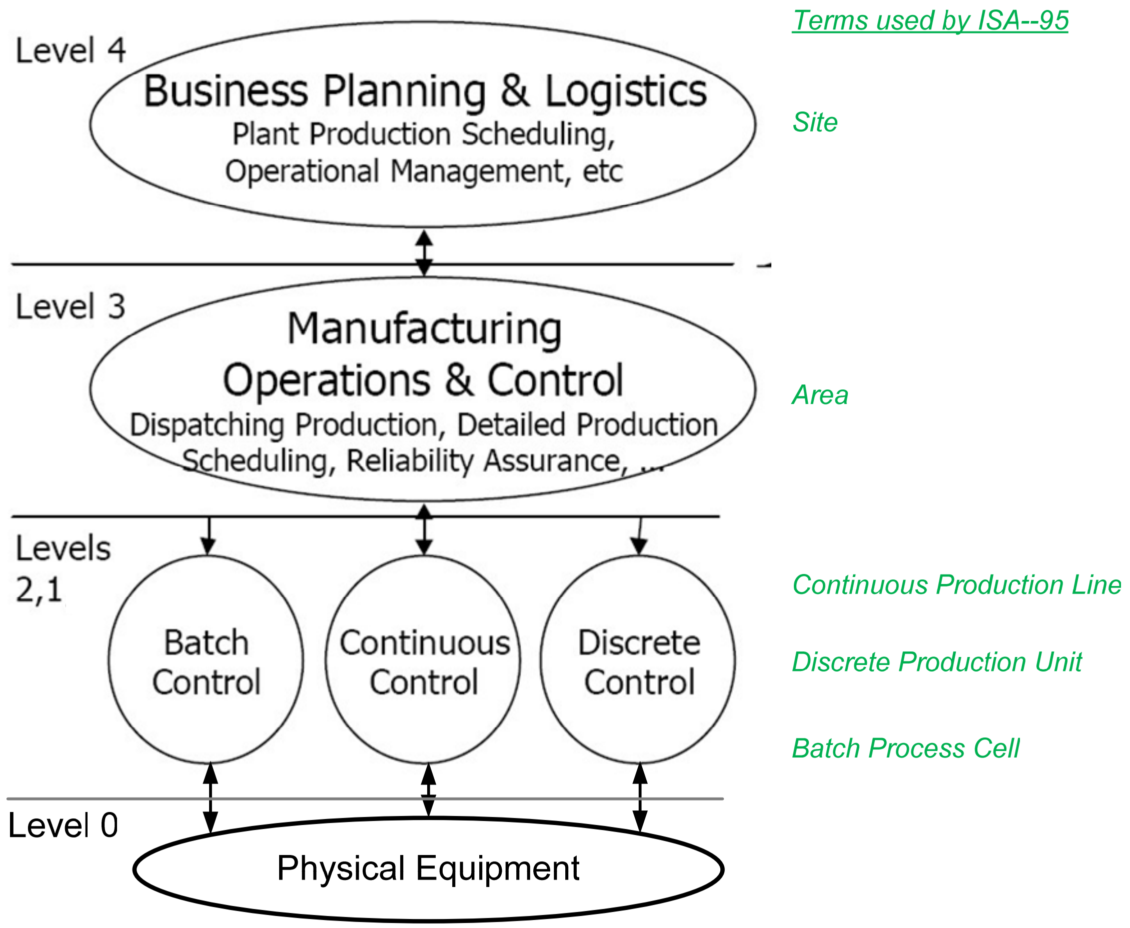

Terms used by ISA--95
Level 4
Business Planning & Logistics
Plant Production Scheduling, Operational Management, etc
Site
Level 3
Manufacturing Operations & Control
Dispatching Production, Detailed Production Scheduling, Reliability Assurance, ...
Area
Levels 2,1
Batch Control
Continuous Control
Discrete Control
Continuous Production Line
Discrete Production Unit
Batch Process Cell
Level 0
Physical Equipment

Figure 1: The PERA Architecture with physical process, device, operations and application levels

The figure illustrates how a complete manufacturing system can be described in terms of a set of defined levels for the physical process (machinery and equipment) at Level 0, basic control (devices and events) at level 1 and 2, manufacturing operations (production scheduling and dispatching) at level 3, and business applications (logistics, planning etc.) at level 4.

In conformance with PERA we define an ***RFID Architecture Model*** (RAM) for the Oil and Gas industry using the PERA levels adapted to RFID systems as shown in figure 2.

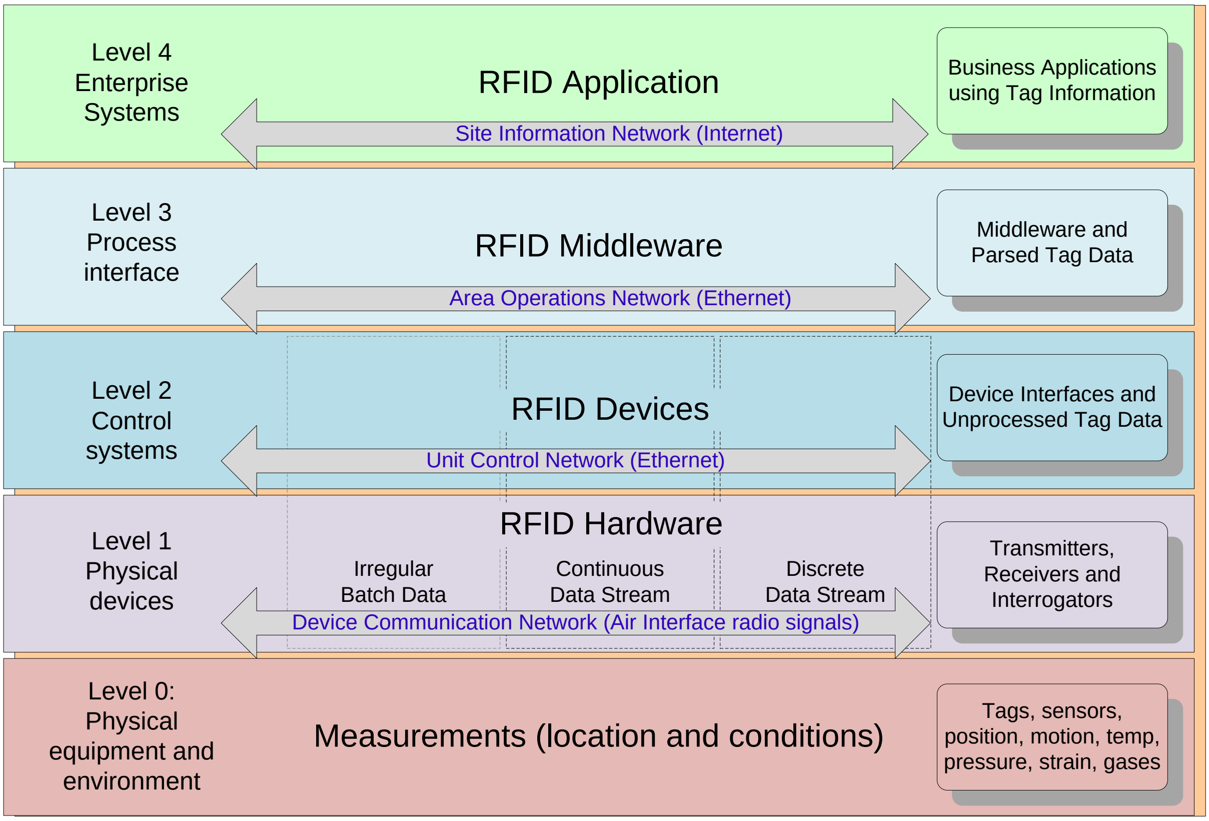

Level 4
Enterprise
Systems
RFID Application
Site Information Network (Internet)
Business Applications using Tag Information
Level 3
Process
interface
RFID Middleware
Area Operations Network (Ethernet)
Middleware and Parsed Tag Data
Level 2
Control
systems
RFID Devices
Unit Control Network (Ethernet)
Device Interfaces and Unprocessed Tag Data
Level 1
Physical
devices
RFID Hardware
Irregular Batch Data
Continuous Data Stream
Discrete Data Stream
Device Communication Network (Air Interface radio signals)
Transmitters, Receivers and Interrogators
Level 0:
Physical
equipment and
environment
Measurements (location and conditions)
Tags, sensors, position, motion, temp, pressure, strain, gases

*Figure 2: The RFID Architecture Model (**RAM**) for RFID Deployment in the Oil and Gas industry*

The figure illustrates how level 0 covers RFID hardware (tags, antennas and physical measurements), while levels 1 and 2 (sensors, devices and interfaces) can be set up to cover both continuous and intermittent data transfer of unprocessed data, using RFID tags that transmit (or are interrogated) in Batch, Continuously or at Discrete intervals.

Level 3 covers middleware and parsed data, while level 4 describes the various end user applications that utilize RFID data for monitoring, analysis and decision making. The figure also illustrates the communication networks involved at various levels, including the air interface between RFID Tags and readers, the control and operation of device and middleware, and the information exchange from, to and between various RFID applications.

The use of PERA makes the Reference Architecture for RFID conformant with ISA-95 Enterprise Control System Integration Standard [2], and the POSC CAESAR Information Technology Architecture for PCA MIMOSA integrated Engineering and Operations [3]. See [4] for further information about how enterprise level systems can be broken down into Enterprise Sites, Areas and Production Units/Cells/Lines; and described in terms of their conceptual, functional, logical and physical characteristics.

3.2 Standards for Data Transfer in RFID Hardware and Middleware

This section gives an overview of recommended standards for transfer of unprocessed data between RFID tags and interrogators (the air interface) and subsequent parsing and processing in device controllers and command units(the device interface). The most important standards include -

- *ISO 18000: Information technology – Radio frequency identification for item management – Air Interface* [5].
- *ISO 16962: Information technology – Radio frequency identification for item management – Air Interface – Data Protocol: Data encoding rules and logical memory functions* [6].
- *ISO 15961: Information technology – Radio frequency identification for item management – Air Interface – Data Protocol: Application Interface* [7].
- *ISO 24791: Information technology – Radio frequency identification (RFID) for item management –Software system infrastructure* [8].

The unprocessed data stream from tags to interrogators is encoded in binary format using standards such as BCD encoding (Binary Coded Decimals) [9], ASN.1 notation (Abstract Syntax Notation One) [10] with PER (Packed Encoding Rules) [11.

3.3 Standards for Information Exchange in RFID Applications

This section introduces the recommended standard for data integration, sharing, exchange, and hand-over between RFID Middleware and Applications (the Data Interface) -

- *ISO 15926: Industrial automation systems and integration—Integration of life-cycle data for process plants including oil and gas production facilities* [12].

It consists of several parts that are relevant to RFID System Architecture and Integration:

- *ISO 15926-2:2003*: *Part 2* [13] specifies a conceptual data model for computer representation of technical information about process plants.
- *ISO/TS 15926-4:2007*: *Part 4* [14] defines the initial set of reference data for use with the ISO 15926 and ISO 10303-221 [15] industrial data standards.
- *ISO 15926-7: 2011: Part 7* [16] defines a methodology for using reference data [14] in Templates that are adapted to industrial use.

The processed data is exchanged across the Data Management Interface according to ISO 15961 [7] and between Applications using POSC Caesar Reference Data Library [17]. The data stream should be encoded using XML [18], with semantics given by RDF/OWL [19], according to processing logic and rules defined in BPMN [20].

See chapter 5 for more on the use of ISO 15926 for defining the necessary RFID ontologies and reference data, and an overview of Semantic Technology for defining the syntax and semantics of the information exchange.

Additional information about these standards, with links to relevant references and resources, is given in Appendix B in Part 3: RFID Technology of this Guideline [21] contains an extensive list of the many standards that address various aspects of radio communication, device interfaces, data protocols, etc., etc.

4. System integration and technology

In this chapter we define an integration model for RFID Systems consisting of RFID Hardware, Middleware and Software segments, and review the content of each segment.

4.1 An Integration Model for RFID Systems

In order to present an integrated view of the complete end-to-end RFID system communication we have adopted the standard view from figure 1 of Part 1: General Principles of this Guideline [22], which divides the system into RFID, Database Middleware and Application layers, but have added additional details to display and discuss the integrated data flow and information processing.

A high-level overview of the RFID System Integration Model (RIM) is shown in Figure 3.

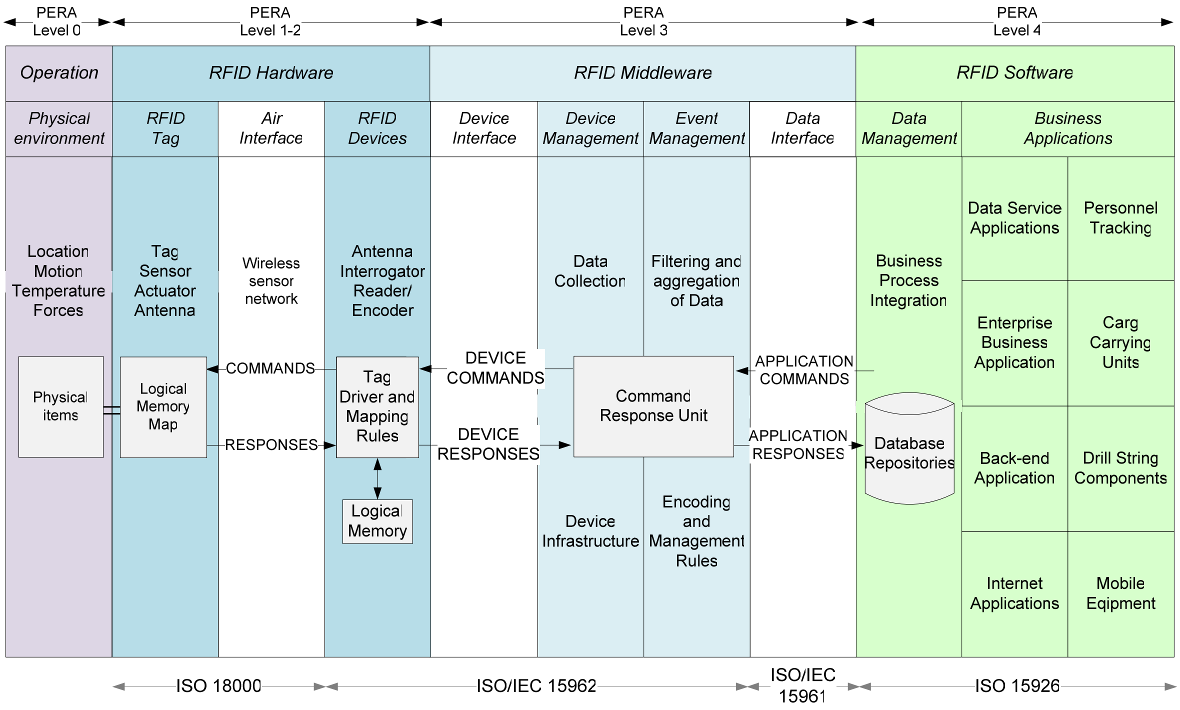


*Figure 3: The RFID Integration Model (**RIM**) for RFID Deployment in the Oil and Gas industry*

The figure illustrates the contents of, and information flow between, the RFID Hardware, Middleware and Software Application segments. Tags (with possible sensors) are attached to physical devices and communicate wirelessly to interrogators and readers, which pass unprocessed tag data on for collection, filtering and aggregation according to given encoding and management rules. The resulting processed tag information can then be passed on to data base repositories for use in a variety of local, central and networked applications.

The relationship between the Integration Model and Architecture Model from chapter 3 is shown by the arrows above the segments which map the Architecture Levels to Integration Segments (the integration model corresponds to the architecture model rotated 90 degrees clockwise). The Segments are shown in more detail in the following three sections.

4.2 The Hardware Segment

A detailed view of RFID layer is shown in Figure 4, illustrating that RFID Tags are attached to some defined physical item and placed in a given physical environment. The tags may operate (be placed) alone to report (only) the presence and location of the physical items, or together with sensors to report on a wide range of physical conditions at their given location.

Tags may use one (or more) of a series of frequencies for radio communication over the Air Interface. The radio commands, responses and data format are defined according to low level data languages such as BCD (Binary Coded Decimals) [10], ASN.1 (Abstract Syntax Notation One) [11] or PER (Packed Encoding Rules) [12].

The Interrogator (Tag Driver) and Reader uses Mapping Rules to encode the RFID signals into an unprocessed data stream that is passed onto the middleware further processing. Both the tags and reader may include various forms and amounts of storage capability for “local” data storage.

The RFID Hardware layer corresponds to Levels 1 and 2 of the (PERA—based) RFID Reference Architecture, and is specified by the ISO 18000 standards for the tags and air interface, and ISO/IEC 15962 for the data protocol and reader.

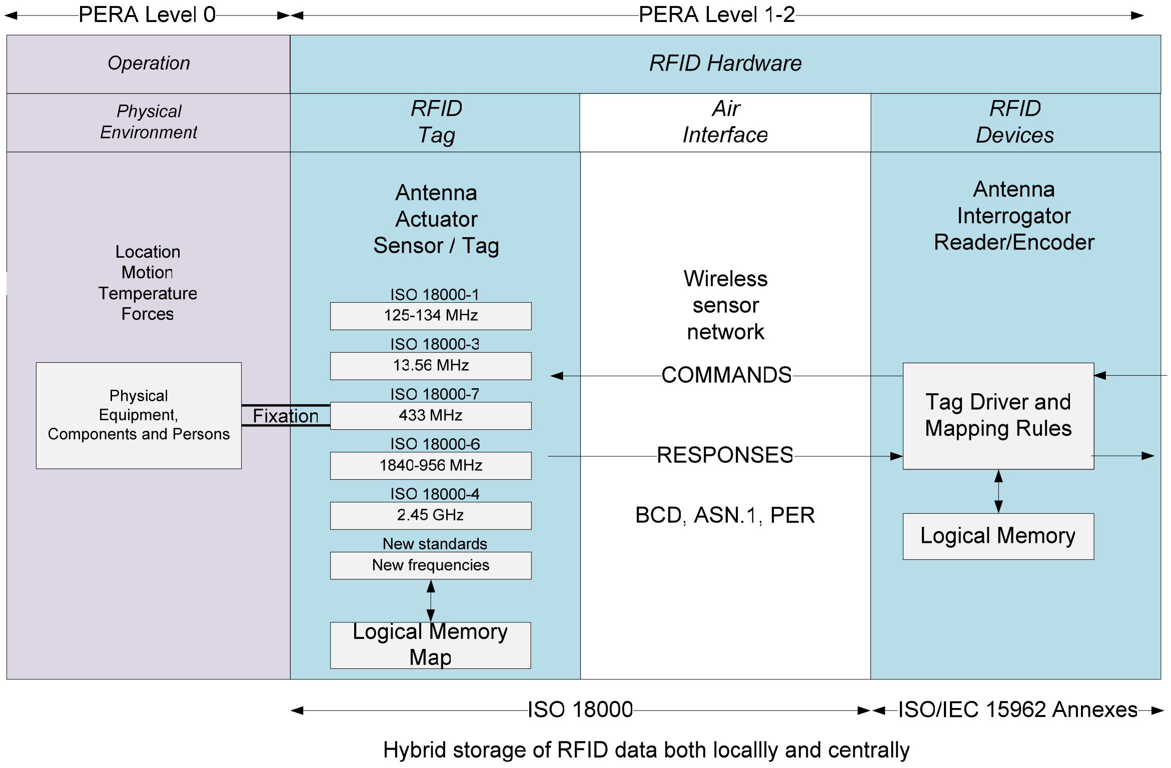


Figure 4: A detailed view of the Environment (location) and RFID Hardware Segment

4.3 The Middleware Segment

A detailed view of the Middleware Layer is shown in Figure 5, illustrating the device interface (to the previously discussed Hardware layer), device and event management and communication via the data interface to the application layer.

The unprocessed data from the Hardware layer is handled by the data protocol processor according to ISO 15962 encoding rules, collected, formatted and stored, before being passed on for filtering, aggregation and further reasoning by the event manager.

Finally the parsed data (typically in XML form, including tag ID and timestamp) can be passed onto various user applications.

The Middleware Data layer corresponds with level 3 of PERA and the Reference Architecture for RFID deployment in the Oil and Gas industry, and is specified in ISI 15962 [6] (for device and event management) and ISO 15961 [7] for the Data interface with user applications.

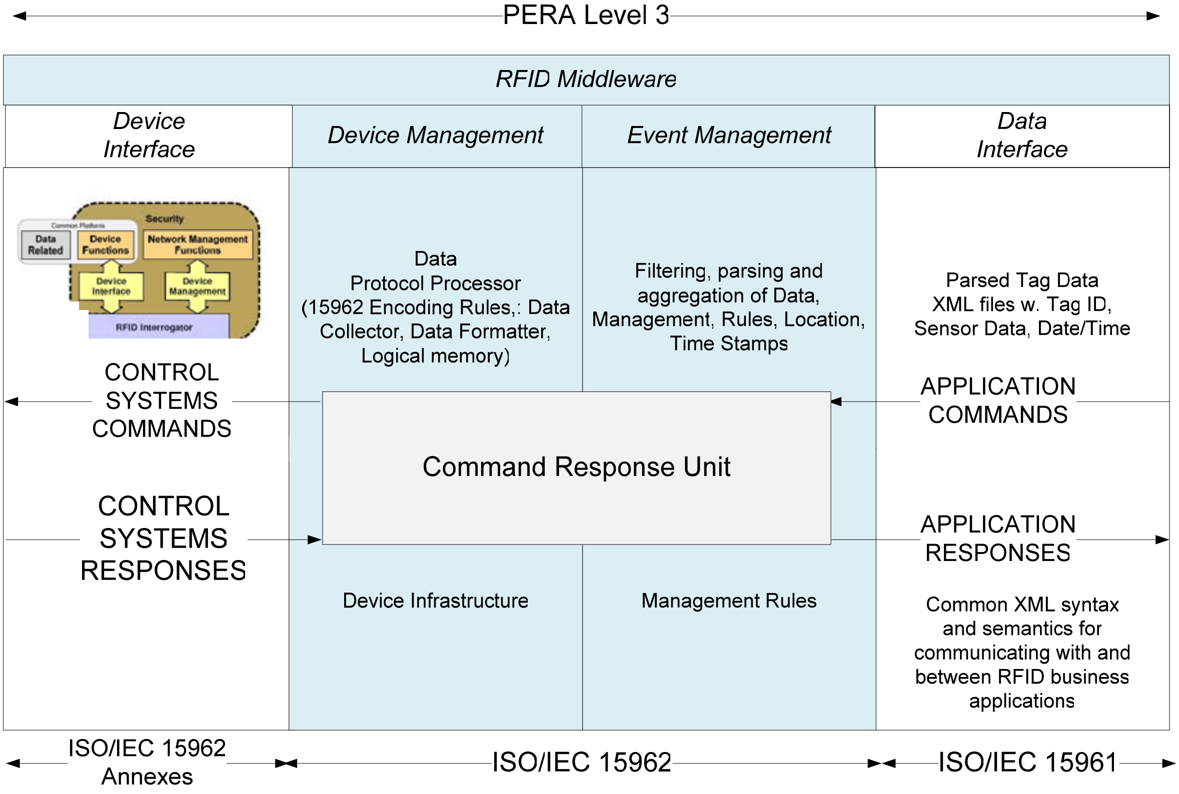

PERA Level 3
RFID Middleware
Device Interface
Device Management
Event Management
Data Interface
Security
Common Platform
Data Related
Device Functions
Network Management Functions
Device Interface
Device Management
RFID Interrogator
CONTROL SYSTEMS COMMANDS
CONTROL SYSTEMS RESPONSES
Data Protocol Processor (15962 Encoding Rules,: Data Collector, Data Formatter, Logical memory)
Filtering, parsing and aggregation of Data, Management, Rules, Location, Time Stamps
Parsed Tag Data XML files w. Tag ID, Sensor Data, Date/Time
APPLICATION COMMANDS
Command Response Unit
APPLICATION RESPONSES
Device Infrastructure
Management Rules
Common XML syntax and semantics for communicating with and between RFID business applications
ISO/IEC 15962 Annexes
ISO/IEC 15962
ISO/IEC 15961

Figure 5: A detailed view of the RFID Middleware Segment

4.4 The Application Segment

A detailed view of the Application Layer is shown in Figure 6, illustrating how a series of databases are used for storing both the RFID data/information (the RFID Historian), and information about the various tagged objects (the Asset Object Mapping Registry), operations (Configuration Management Events), and logic (Business Rules).

Note that the Application Layer corresponds to level 4 of the RFID Reference Architecture, and that the exchange of information between all RFID applications should (ideally) take place according to the semantics of ISO 15926.

In order to achieve the required functionality, in a reliable and maintainable manner, both the Data Management and Application software must be designed, developed, deployed and operated in a well-defined and documented manner. This is discussed in chapter 5 below.

In order to secure relevant, meaningful and unambiguous information processing between end-user applications the system must allow (only) syntactically and semantically well-defined data exchange. This is addressed by using agreed ontologies with standard Reference Data as defined in ISO 15926-4. There are already such ontologies available or under development, covering both the RFID system and the many possible application areas. This is discussed in chapter 6 below.

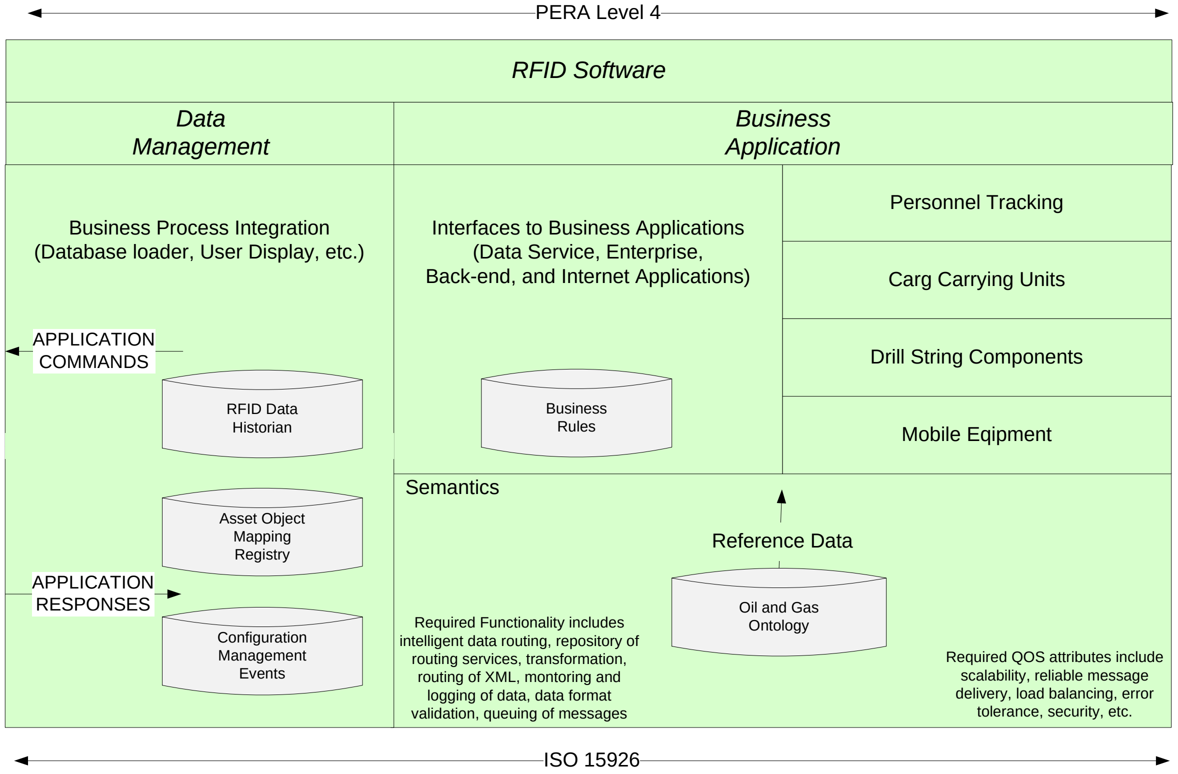

PERA Level 4
RFID Software
Data Management
Business Application
Business Process Integration (Database loader, User Display, etc.)
Interfaces to Business Applications (Data Service, Enterprise, Back-end, and Internet Applications)
Personnel Tracking
Carg Carrying Units
Drill String Components
Mobile Eqipment
APPLICATION COMMANDS
RFID Data Historian
Business Rules
Semantics
Asset Object Mapping Registry
Reference Data
APPLICATION RESPONSES
Oil and Gas Ontology
Configuration Management Events
Required Functionality includes intelligent data routing, repository of routing services, transformation, routing of XML, montoring and logging of data, data format validation, queuing of messages
Required QOS attributes include scalability, reliable message delivery, load balancing, error tolerance, security, etc.
ISO 15926

Figure 6: A detailed view of the RFID Application Segment

5. System design, development and operation

In this chapter we discuss various topics and issues related to design, development and operation of the RFID hardware, software and applications, including required principles and qualities, the use of an Enterprise Service Bus for information exchange between applications, classification of system location and security, and a brief overview of stakeholder interests.

5.1 Solution Principles and System Qualities

When planning (and operating) any application involving RFID tags and technology, it is important to start with a sound understanding of the fundamental principles of system design [24]. A list of design principles, adapted to and relevant for RFID solutions is given in Appendix C.

When discussing system quality it is useful to distinguish between two related but distinct notions -

- *Functional quality* reflects how well the system complies with or conforms to a given design, based on functional requirements or specifications. That attribute can also be described as the fitness for purpose and is typically enforced and measured through testing.
- *Structural quality* refers to how the system meets non-functional requirements that support the delivery of the functional requirements, such as robustness or maintainability, the degree to which the system was produced correctly. For a both hardware and software systems structural quality is evaluated through analysis of the inner structure, such as its circuitry or source code - in effect how the system architecture adheres to sound systems principles.

For hardware components structural quality is typically defined in terms of reliability by measurable terms such as Mean time between failures (MTBF), the predicted arithmetic mean (average) time between inherent failures of a system during operation.[25] . The MTBF is typically part of a model that assumes the failed component is immediately repaired or replaced (MTTR), as a part of a renewal process. This is in contrast to the mean time to failure (MTTF), which measures average time to failures with the modeling assumption that the failed system is not repaired. For an RFID system consisting of a variety of hardware components (tags, sensors, antennas, controllers, etc.) it is essential to define acceptable criteria for MTBF and MTTR/MTTF. The expected MTBF is dependent on the environmental/physical conditions to which the component is exposed – determined in turn by the *location* of the various parts of the RFID system.

For software systems the structure, classification and terminology of attributes and metrics applicable to quality management have been derived or extracted from the ISO 9126-3 standard and subsequent ISO 25000:2005 [26] quality model. Based on these models, the Consortium for IT Software Quality (CISQ) has defined 5 major desirable structural characteristics needed for a piece of software to provide business value: *Reliability*, *Efficiency*, *Security*, *Maintainability* and (adequate) *Size*. In addition we propose to add *Extendibility* to characterize how easy/hard it is to reconfigure, extend and apply the software in new functions/applications. An overview of the relationship between desirable characteristics and measurable attributes is shown in Appendix D. Since any RFID system includes (a large or small amount of) software it is important to identify structural characteristics, establish desired qualities, and define measurable criteria. In order to maintain acceptable quality over the lifetime of system, it is essential that active quality management [27] is in place for hardware and control systems [28], software systems [29], data and info systems [30].

5.2 Enterprise Service Bus

In order to promote extendibility of the RFID System we promote a Service Oriented Architecture (SOA) design paradigm [31], with loose coupling between diverse applications connected and communicating via an Enterprise Service Bus (ESB) [32]. Figure 8 illustrates an ESB approach with

Service Oriented Integration of RFID (and other Enterprise) Applications (services), and a common repository for Reference Data used in various ontologies for RFID in the Oil and Gas industry (see chapter 6 below for details).

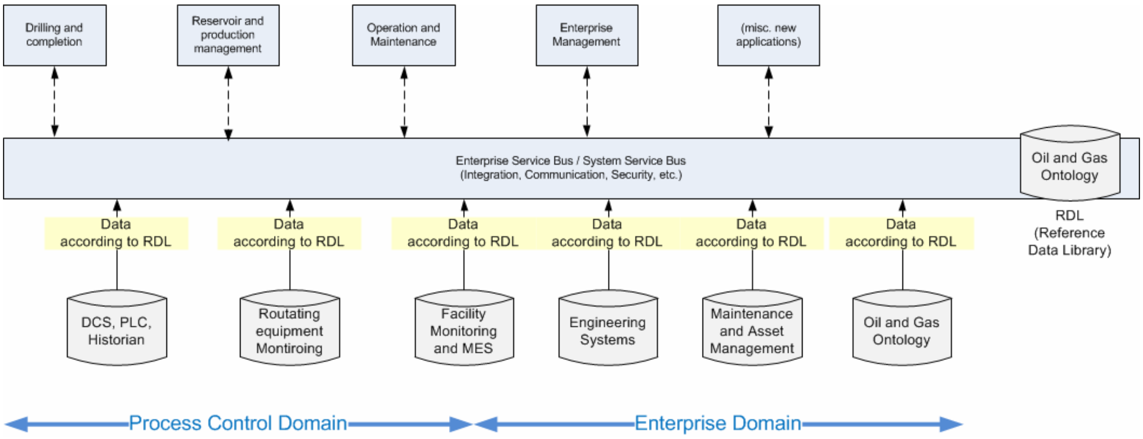


Figure 7: RFID Software Engineering Model (REM) with Enterprise Service Bus integration

The ESB solution must be able to handle RFID integration with other systems, including a wide variety of services that utilise RFID (note that this integration is between applications at Level 4 of the Reference Architecture, and does not apply to communication between devices, interrogators and tags at lover levels).

The ESB may also be used for other integration requirements for the operator, and should include the following functionality:

- Intelligent routing of data (rules based routing / preferably also content based).
- Address repository of services for routing purposes / service mapping.
- Queuing of messages when services are not available.
- Transformation between data formats and protocol.
- Routing of XML format data as standard.
- Validation of data format integrity.
- Monitoring and logging of traffic.

The ESB is key for the RFID event management service (and may be used for event management instead of a separate event management service). Event management is responsible for end to end handling of an event – from capture through to completion. Open standards like the Business Process Execution Language (BPEL) [32] should be used for defining *orchestrations* of event management into higher level business process services.

5.3 System Location

Location of RFID equipment and system components should be where it is most effective with respect to constraints imposed by the environment, processing of information and physical security requirements. RFID services and applications may be divided in four groups, based mainly on their requirement for physical location:

Group 1: Services and equipment that must be on location, mainly because of technical limitations. Thus "on location" means the location where the RFID solution is placed, e.g. on equipment, person, rig, container, port, onshore warehouse. This group includes the following: RFID tag communication, RFID sensing, Data collection, Local data storage and (possibly also) tag management.

Group 2: Services which use RFID for data capture may be placed at different locations. The group includes the following: Event management, Data storage, Tag management.

Group 3: Data integration services need to be available at the right time at the right place to meet application needs and therefore has to be integrated into the system. A first step towards integration of data is to take data from its point of capture and deposit in an RFID data repository (historian). Information to be exchanged should be represented in a logical structured language that is application independent. This suggests building of an oil and gas ontology based on ISO 15926, as discussed further in chapter 6 below.

Group 4: Other services that need to integrate with data captured by RFID. This group may include services such as: Personnel movement (tracking, access control systems, monitoring), Logistics and inventory (CCU tracking, content, locations, etc.), Movement of equipment/parts/goods (drill string components, drilling pipes, etc.), Tracking mobile equipment/parts (operations, maintenance, etc.), and Fixed equipment monitoring (operations, maintenance). Note that several of these services may be provided on location. They should never the less be treated as separate from the RFID local group.

RFID systems may use different types of data management methods: central or local data management, and a third hybrid model.

- Central data management only transfers the tagged object's identification number to the tag.

  All other data associated with the object (class etc.) is stored in central databases.

- Local data management, stores data directly on the tag in order to optimize the process runtime. The database connection is necessary only to verify the data.

- Hybrid data management, uses the central data management model as a primary solution, but has local data for those times and locations where there is no access to the central database.

For all of these groups, the location of the tagged item (and tag) must be kept in mind. If for example, the tag is on the right item, but the item is placed at the wrong location, the received RFID information may be incorrect or even misleading.

5.4 System Security

System security can be defined in terms of *availability*, *integrity* and confidentiality of relevant assets. For RFID systems this includes everything from the physical infrastructure and applications to people and organizations, and needs to be defined and designed with a wide range of requirements in mind.

For information assets the integrity and availability of information must be considered for wired and wireless transmission of information: Machine to Machine interfaces (M2M), Human to Machine interfaces (H2M) and Human to Human interfaces (H2H). Likewise, the availability (denied access) of information to authorized (non-authorized) personnel must be secured. In order to ensure a holisitc perspective, technical measures must be supported by seurity risk management and procedures.

Implementation of information security should be based on Norwegian Oil and Gas Association Guideline no.104 - "Information security baseline requirements for process control, safety and support ICT systems" [33]. This Guidelne is a subset of ISO/IEC 27001 Information Security Management Systems [34] and 27002 Code of Practise for Information Security Management [35] and describes a minimum set of requirements. In addition, ISO/IEC 15408 Evaluation criteria for IT Security [36] and ISO/IEC 18045 Methodology for IT Security Evaluation [37] may be used for evaluating the security level of the RFID solutions themselves.

Group 1 requirements:

Confidentiality measures are needed on location for personnel information, onshore locations, data storage on shared systems, and sensitive personnel information, which must be encrypted to ensure confidentiality. For this group -

- *Authentication* is always required, and may be delivered by any industry standard method. It is recommended to use the operators own standard system (and aim at single sign on).

- *Data integrity* checks must be included to ensure correct data whenever it is received by a system. It is also recommended to include integrity check when data is sent from a system.

- *Physical access control* is required for all computer room equipment and services.

- *Logical access control* is required for all systems, so that only authenticated people or systems may access data. Access control should ideally be based on defined roles for specific assets.

- *Availability* is required when the site is operational. Availability (% uptime) must be specified.

- *Reliability* must be high to avoid lengthy periods of downtime. Redundant (duplicate) equipment must be available to ensure operation after loss of equipment - with automatic or semi-automatic fail-over. Response time requirements must be specified.

Group 2 and 3 requirements:

The requirements are the same as for group 1, with the following additions –

- *Confidentiality* measures must be in place in all cases, ideally in the form of encryption.
- *Physical access control* is generally required for access to all IT equipment or systems.
- *Reliability* must be high, but the need for on-site duplicate equipment may be relaxed if equipment can be replaced within a reasonable time.

Group 4 requirements:

The requirements are defined by the each application or service - and thus not described here.

These four groups may be merged into fewer groups. If that is done, the highest quality and security requirements of any of the individual groups must apply to the whole group.

5.5 System Applications and Stakeholders

Deployment and application of RFID Systems in the Oil and Gas Industry involves a number of stakeholders, including both users, service providers, suppliers and integrators. A simplified overview of this is shown in figure 8.

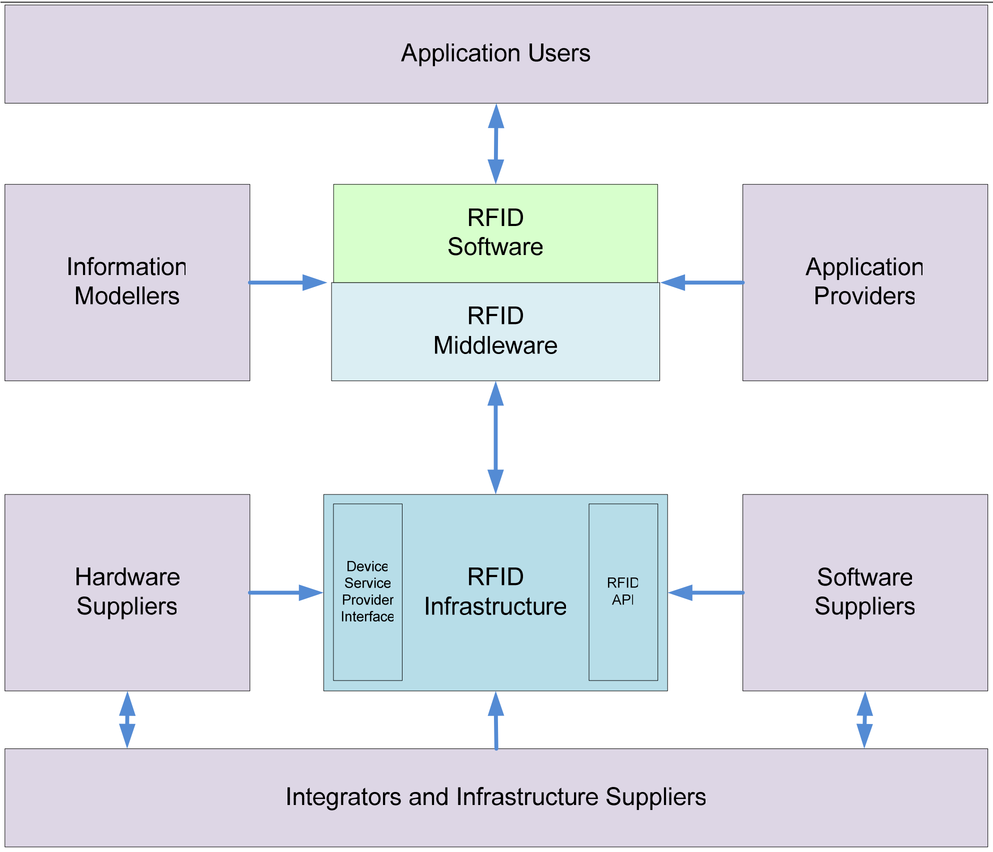


Figure 8: Typical Stakeholders involved in Deployment of RFID applications

The figure illustrates how the RFID infrastructure is dependent on both Infrastructure (network), hardware and software suppliers. For both the Data Middleware and Application Software there is a need for involving the services of (information) modellers and (software) developers. The last (but not least) stakeholder is the appplication user, who may belong to the same or a different organization than the RFID System owner.

Parts five through nine of this Guideline address application of RFID Systems to tracking of Personnel, Cargo Container Units, Drill String Components, Mobile equipment and Fixed Equipment. These and other applications should be integrated with the RFID system by means of the above mentioned ESB.

The concept of “supply chain visibility” is an example of “simple RFID enabling” of existing applications that need little or no modification to work in an RFID system.

Cost effecticve application of RFID technology, wireless networks and network infrastructure depends on the overall usage and evolution of software and systems technology -

- Evolution of the network from Internet of computing devices to Internet of Things (IoT) [38].
- Intelligence movement into the network - knowledge, and information value.
- Establishment of intelligent network foundation for RFID, WSNs and IoT.
- Enhancements in Quality of Service (QoS) and security considerations.

- New network architectural frameworks for passive, active RFIDs, WSNs and IoT including information flows and data management for oil and gas industry applications.

As these developments allow increasing numbers of physical assets to communicate about their operational status and performance, both the volume and content of data in machine to machine (M2M) communication will grow dramatically. So also will the size and complexity of sensor networks, control devices and communication systems. RFID systems, connected to a large list of sensors and monitors will be an (the) important part of this, and it is critcally important for all stakeholders that systems are built on a solid understanding of functional and operational requirements, design principles, systems engineering, software development and hardware manufacturing.

6. Information management and usage

In this chapter we define an enterprise information management framework, and present ISO 15926 as the choice for representing and structuring reference data for RFID systems deployment. We discuss reference data and ontologies (with an initial reference data and ontology for describing RFID system structure), and the use of the semantic technology stack for implementation.

6.1 An RFID Enterprise Information Model

Enterprise Information Management specializes in finding solutions for optimal use of information within organizations by combining business intelligence (BI) and enterprise content management (ECM). Enterprise information management takes these two approaches to managing information one step further, in that it approaches information management from an enterprise perspective.

Where BI and ECM respectively manage structured and unstructured information, Enterprise Information Management does not make this “technical” distinction. It approaches the management of information from the perspective of enterprise information strategy, based on the needs of information workers. For an RFID system this translates to the ability of the system to manage both structured commands and predefined data streams, and interpret and use information from unstructured auxiliary sources.

In order to enhance the value out of RFID information throughout its lifecycle we define an RFID Enterprise Information Model (REIM), as a framework for designing and describing important information aspects and activities. The REIM model is shown in figure 9.

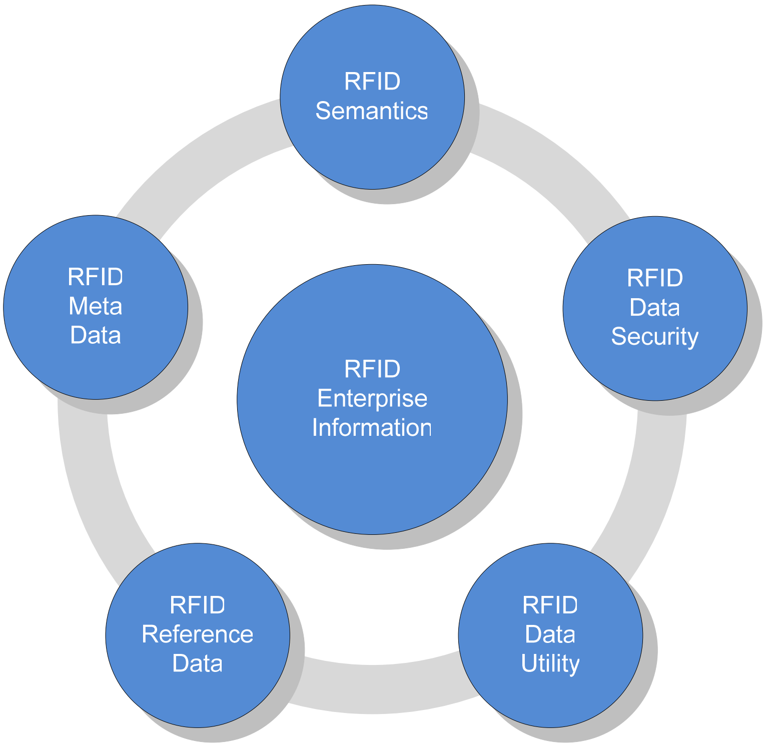


Figure 9: The RFID Information Utility Model (RUM) for Deployment in the Oil and Gas industry

Figure 9 illustrates how the value (quality) of RFID information depends on data security (discussed in chapter 5 above), data utility (discussed below), metadata (discussed in section 6.2 below), reference data (discussed below) and semantics (discussed below). Examples of other information management models can be found in Appendix E.

Data utility is often used as a collective terms for data that has the following qualities Stages of Data Utility & Value **[39] -**

- **Recorded, i**n some sharable, objective medium and not just in some human brain.
- **Accessible,** with the right resources and technology.
- **Navigable,** easy to find.
- **Understandable** in terms of language, culture, technology, etc.
- **Of sufficient quality** for the intended use.
- **Topically relevant to** (perceived and unknown) needs.

As defined in the RFID Integration Model (RIM) in chapter 4 all RFID data should be stored at the application level in a data repository (also called an RFID Historian). The mapping of data to and from

the RFID Historian should be based on XML schemas. All the data concepts and associated logistics information (metadata) in the XML schemas should be included in the overall oil and gas ontology.

As mentioned in the dicussion about location in chapter 5 above, it is important to also store enough data locally to be able to perform basic functions when access to the server is unavailable. Thus it should be possible to store data in the RFID components also.

A number of international standards exist for specifying the RFID data protocol. This Guideline recommends using ISO/IEC 15961 [7] to interface between the application and data protocol processor, and ISO/IEC 15962 [6] for encoding of transfer syntax according to application commands defined in ISO 15961.

In addition to the syntax defined in ISO/IEC 15961 and ISO/IEC 15962, the semantic part of the RFID data has to be well defined and aligned with the terminology in use in the offshore industry in order to secure effective data sharing across disciplines and organizations. The ISO 15926 standard for "Integration of lifecycle data for process plants including oil and gas production facilities" define an abstract data model for classifying data, and a reference data library (RDL) of (currently) over 45,000 standard items and activities (classes). Based on this the POSC Caesar Association (PCA) has developed a set of PCA Reference Data Services (RDS) [40].

In order to enable effective (efficient and error-free) exchange of information (data) between all parts (levels or segments) of the complete RFID System it may be necessary to carry out several development activities, including analysis of current and anticipated usage, (possible) extension of data and commands in the air and device interfaces, development of new of XML schemas for data transfer, and extension of Reference Data for information exchange in and between applications. These development activities and results are illustrated in figure 10.

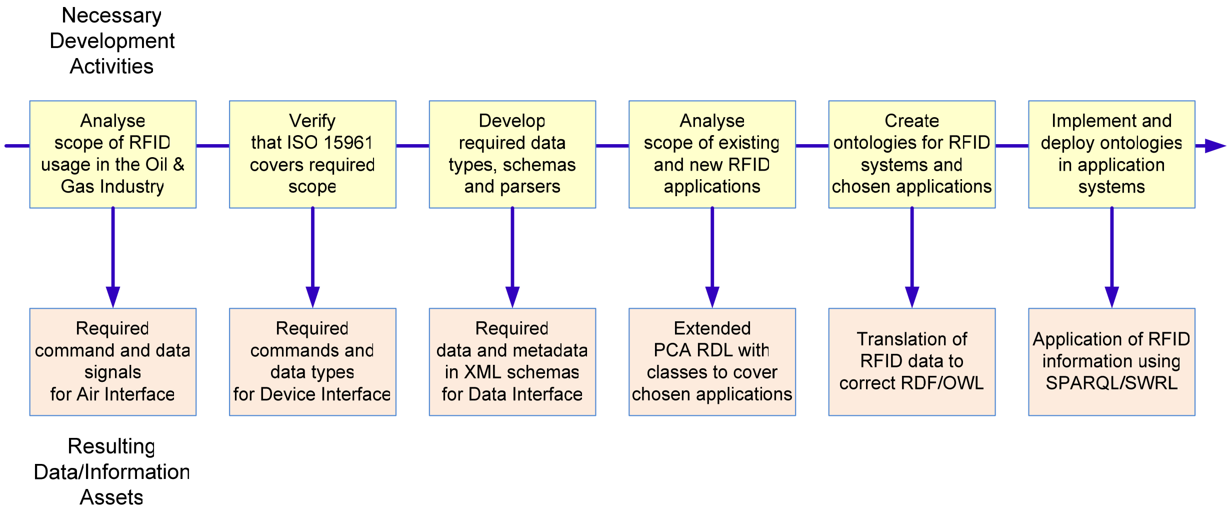

Necessary Development Activities
Analyse scope of RFID usage in the Oil & Gas Industry
Verify that ISO 15961 covers required scope
Develop required data types, schemas and parsers
Analyse scope of existing and new RFID applications
Create ontologies for RFID systems and chosen applications
Implement and deploy ontologies in application systems
Required command and data signals for Air Interface
Required commands and data types for Device Interface
Required data and metadata in XML schemas for Data Interface
Extended PCA RDL with classes to cover chosen applications
Translation of RFID data to correct RDF/OWL
Application of RFID information using SPARQL/SWRL
Resulting Data/Information Assets

Figure 10: Development Activities for data transfer, mapping and interpretation in RFID Systems

6.2 Semantics for Lifecycle Management

ISO 15926 [12] is the only available ISO standard for data integration across time, disciplines and functional domains is ISO 15926. ISO 15926 contains several parts that are relevant for deployment of RFID technology:

- Part 2, the data model, defines the syntax that is used to define the semantics, i.e., terminologies, taxonomies and ontologies.
- Part 4 contains the core reference data, which holds the semantics for key concepts.
- Part 7 describes how to implement ISO 15926 to achieve integration of distributed systems.

Figure 11 shows the structure of ISO 15926 and illustrates how the abstract data model Part 2 on the top of the pyramid is used to define the core reference data library (RDL) of (fairly) general products, items and activities, which in turn can be extended by specialization into an (essentially infinite) number of reference data classes, which then can be instantiated as individuals (project data that represent actual physical items that are specified, or which already exist in the real world).

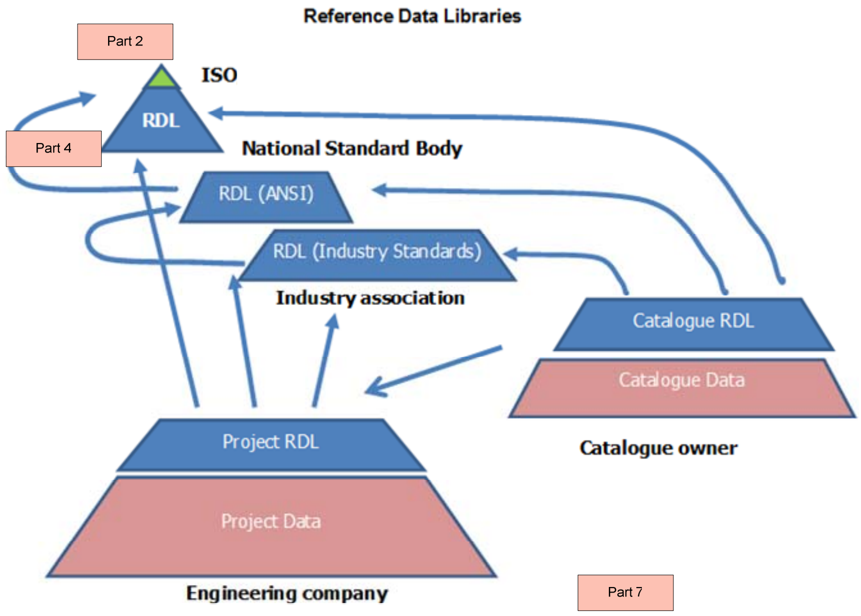


Figure 11: The ISO 15926 data model (Parts 2), reference data (Part 4) and templates (Part 7)

Using the ISO 15926 standard as basis for defining interfaces between applications means that information exchange can take place between different external applications that use similar data, independent of format and without loss of meaning.

The standard is developed and operated (made available) by POSC Caesar Association (PCA) [40], and maintained by a series of Special Interest Groups (SIG) within PCA. The Norwegian Oil and Gas Association has chosen to use ISO 15926 for data integration across the exploration and production

(E&P) sector, and an oil and gas ontology has been developed covering parts of HSE, drilling, production, and operation and maintenance.

6.3 Reference Data Libraries and Ontologies

Over the years a series of ontologies have been developed to describe different disciplines and applications within the oil and gas industry, and a large set of associated Reference Data Classes is part of the associated Reference Data Library (RDL), made available for browsing or downloading by the Reference Data Service (RDS) on PCA's web site: http://www.posccaesar.org/.

The data model and initial reference data in the ISO 15926 are useful as reference classifiers for defining and relating new terms in shared databases and data warehouses. The system structure, components and data elements in RFID systems must all be defined as (new) reference data classes, and connected to existing reference data classes in the RDL.

Important advantages of using the ISO 15926 Reference Data include:

- Dictionary alignment allows application of a common terminology
- Taxonomy/ontology alignment allows discovery of additional knowledge
- Data quality gives content from various databases a standard classification
- Integration makes ISO 15926/reference data content is suitable for exchange
- Application of OWL/RDF makes content available for other semantic tools and applications.
- XML documents can be annotated with content from the ISO 15926 reference data library.

An initial set of Reference Data for RFID Systems is presented in Appendix F.

An ontology is a "knowledge model" of some specific domain, with specified scope and viewpoints. Shared understanding is built by developing new, or aligning existing ontologies, which then act as building blocks for organisational interoperability. They can also be the basis for integrating separate domains through the identification of logical connections and constraints between schemas.

Figure 12 illustrates how domain specific terms are included in the ISO 15926 Reference Data Library, and can then be used in a variety of ontologies.

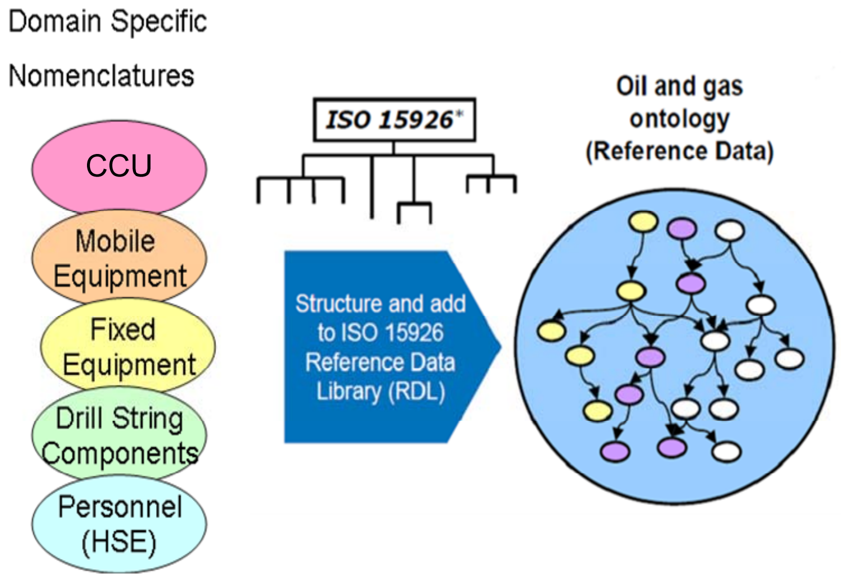


Figure 12: Adding domain specific terms to the RDL make them available for use in ontologies

An initial RFID Ontology Model (*ROM*) with reference classes and relationships describing structure, content and operation of RFID Systems is given in Appendix G. A set of ontologies for the various RFID application areas, such as CCUs, will be added as separate reports.

6.4 The Semantic Technology Stack

The technologies selected for implementing reference data and ontologies are represented in the well-known Semantic Technology Stack from the World Wide Web Consortium (W3C) [41] shown in figure 13.

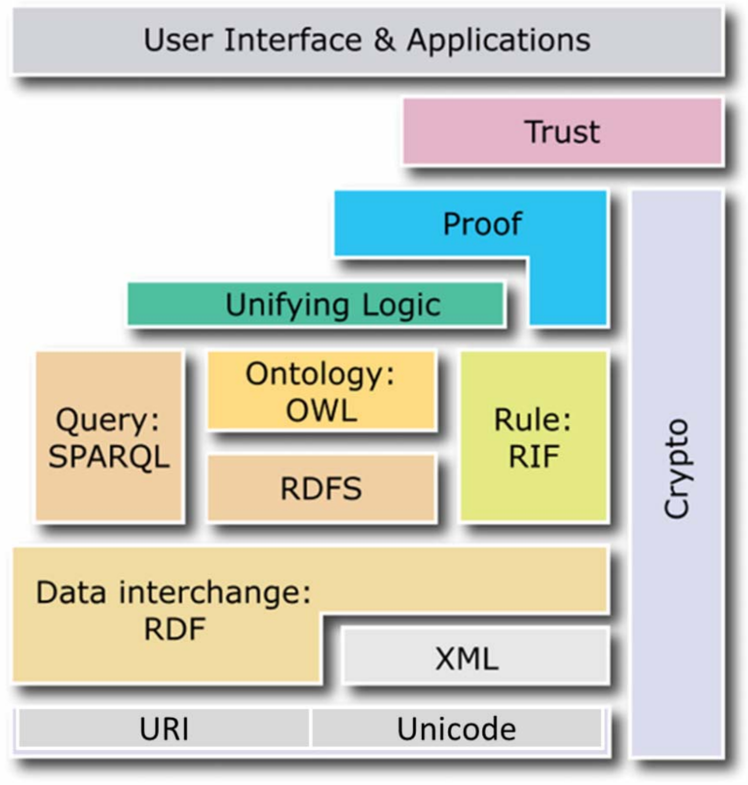


Figure 13: Semantic Technologies defined by W3C

The figure illustrates how different technologies are based on each other, from basic definitions of addresses and character sets, through mark-up languages and resources descriptions (RDF) and taxonomies to languages for defining, querying and reasoning about ontologies and logic constructs.

XML should be used for data exchange when sending data, supporting multiple RFID tag formats within and between applications. This means that all applications should have a standard XML interface to the Enterprise Service Bus (ESB) discussed earlier.

As noted above, ontologies are logic based data models which define concepts and relations in a domain of interest. These concepts and relations have instantiations in a particular instance model, and the ontology can be used to infer interesting logical facts about the instances. One powerful feature of ontology based models is the ability to perform automatic classification.

By unambiguously defining core concepts in selected deployment areas we can express our domain knowledge in the Web Ontology Language (OWL) [19], which is a cornerstone technology of the Semantic Web as coined by Tim Berners-Lee and colleagues [42].

Figure 14 illustrates a “Semantic ISO 15926 stack” using ISO 15926 Templates [16] (composite data structures) as a methodology for facilitating data integration.

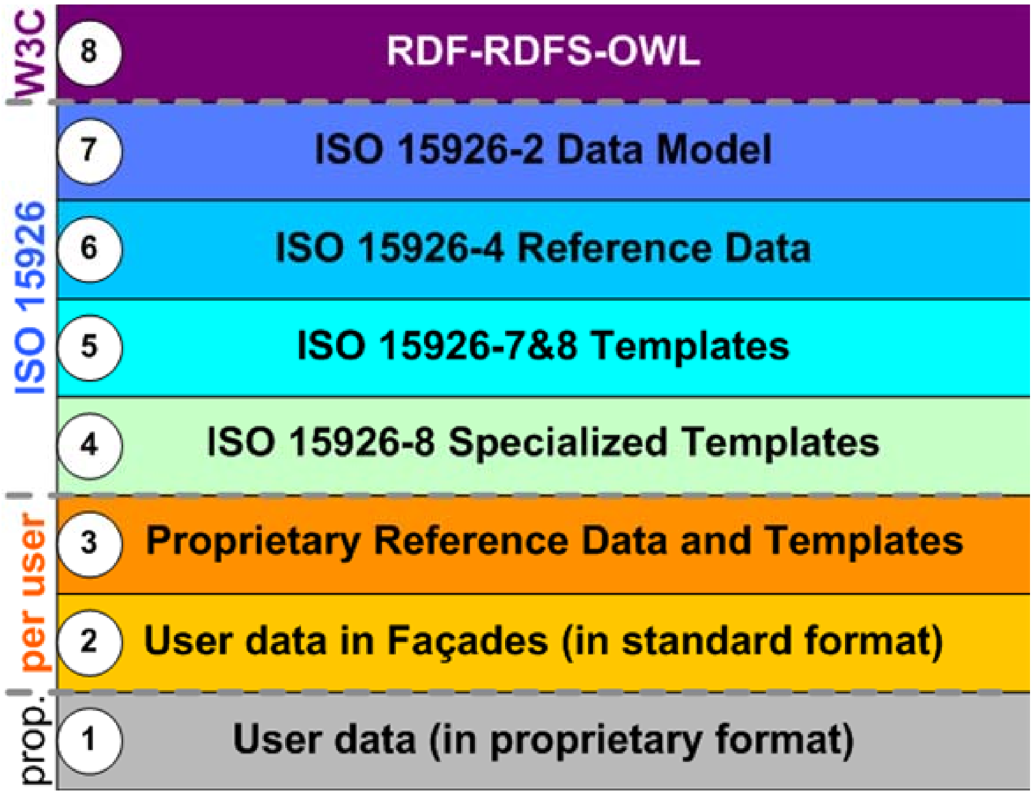

W3C
8 RDF-RDFS-OWL
7 ISO 15926-2 Data Model
ISO 15926
6 ISO 15926-4 Reference Data
5 ISO 15926-7&8 Templates
4 ISO 15926-8 Specialized Templates
per user
3 Proprietary Reference Data and Templates
2 User data in Façades (in standard format)
prop.
1 User data (in proprietary format)

Figure 14: ISO 15926 and the Semantic Technology Stack

The figure illustrates how proprietary user data is represented in standard format in (data storage) Facades, which are then combined and expressed in proprietary reference data templates. These proprietary templates can reference specialized (15926-8) and generic (15926-7) templates [16]. The templates are built up using the PCA Reference Data Library [17] and ISO 15926-4 Reference Data [14], which are instances of the abstract (15926-2) data model [13], which is formally represented in OWL and encoded in XML syntax.

Appendix A: List of references

[1] Purdue Enterprise Reference Architecture (PERA),
http://www.pera.net/

[2] ISA-95 Enterprise Control System Integration Standard,
http://www.isa.org/MSTemplate.cfm?MicrositeID=285&CommitteeID=4747

[3] POSC CAESAR Information Technology Architecture for PCA MIMOSA integrated Engineering & Operation,

https://www.posccaesar.org/svn/pub/PCA/MemberMeeting/201202/Presentations/01_Monday/120227_FrodeMyren.pdf

[4] ISA-95 and B2MML presentation
www.futuristix.co.za/content/S95_Tutorial.pdf

[5] ISO 18000: Information technology – Radio frequency identification for item management – Air Interface
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=040&ics3=&csnumber=46145

[6] ISO 15962: Information technology – Radio frequency identification for item management – Air Interface – Data Protocol: Data encoding rules and logical memory functions
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30529

[7] ISO 15961: Information technology – Radio frequency identification for item management – Air Interface – Data Protocol: Application Interface
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30528

[8] ISO 24791: Information technology – Radio frequency identification (RFID) for item management –Software system infrastructure
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46137

[9] BCD encoding (Binary Coded Decimals
http://en.wikipedia.org/wiki/Binary-coded_decimal

[10] ASN.1 notation (Abstract Syntax Notation One)
http://en.wikipedia.org/wiki/Abstract_Syntax_Notation_One

[11] PER (Packed Encoding Rules)
http://en.wikipedia.org/wiki/Packed_Encoding_Rules

[12] ISO 15926: Industrial automation systems and integration—Integration of life-cycle data for process plants including oil and gas production facilities
http://en.wikipedia.org/wiki/ISO_15926

[13] ISO 15926-2:2003: Part 2 specifies a conceptual data model for computer representation of technical information about process plants
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=29557

[14] ISO/TS 15926-4:2007: Part 4 defines the initial set of reference data for use with the ISO 15926 and ISO 10303-221 industrial data standards
http://www.iso.org/iso/catalogue_detail.htm?csnumber=41329

[15] ISO 10303 Part 221
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=36771

[16] ISO 15926-7: 2011: Part 7 defines a methodology for using reference data in Templates that are adapted to industrial use
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52455

[17] PCA Reference Data Library
https://www.posccaesar.org/wiki/ISO15926

[18] XML (Extensible Markup Language)
http://en.wikipedia.org/wiki/XML

[19] RDF/OWL (Resource Description Framework/Web Ontology Language)
http://no.wikipedia.org/wiki/Resource_Description_Framework
http://en.wikipedia.org/wiki/Web_Ontology_Language

[20] BPMN (Business Process Model and Notation)
http://en.wikipedia.org/wiki/Business_Process_Model_and_Notation

[21] Norwegian Oil and Gas Guideline 112 – Deployment of RFID in the Oil and Gas Industry - Part 3: RFID Technology
http://www.norskoljeoggass.no/Documents/Retningslinjer/100-127/112%20-%20Deployment%20of%20radio%20frequency%20identification%20in%20the%20oil%20and%20gas%20industry%20Part%203.pdf?epslanguage=no

[22] Norwegian Oil and Gas Guideline 112 – Deployment of RFID in the Oil and Gas Industry - Part 1: General Principles for Deployment
http://www.norskoljeoggass.no/Documents/Retningslinjer/100-127/112%20-%20Deployment%20of%20radio%20frequency%20identification%20in%20the%20oil%20and%20gas%20industry%20Part%201.pdf?epslanguage=no

[24] Fundamental Principles of Good System Design
Vol. 20 No. 4. Engineering Management Journal, Fundamental Principles of Good System Design. A. Terry Bahill, PE, University of Arizona

[25] Jones, James V., Integrated Logistics Support Handbook, McGraw–Hill Professional, 3rd edition (June 8, 2006), ISBN 0-07-147168-5

[26] ISO 25000:2005
ISO/IEC 25000:2005 – Software Engineering – Software Quality Requirements and Evaluation (SqarRE)
http://www.iso.org/iso/catalogue_detail.htm?csnumber=35683

[27] Adams, Cary W.; Gupta, Praveen; Charles E. Wilson (2003). Six Sigma Deployment, Burlington, MA: Butterworth-Heinemann, ISBN 0-7506-7523-3.

[28] Industrial control systems
http://en.wikipedia.org/wiki/Industrial_control_systems

[29] Software systems
http://en.wikipedia.org/wiki/Software_system

[30] Data and information systems
http://en.wikipedia.org/wiki/Data_system
http://en.wikipedia.org/wiki/Information_systems

[31] Service Oriented Architecture
http://en.wikipedia.org/wiki/Information_systems

[32] ESB

[33] Norwegian Oil and Gas Association Guideline no.104 - "Information security baseline requirements for process control, safety and support ICT systems"
http://www.norskoljeoggass.no/no/Publikasjoner/Retningslinjer/Integrerte-operasjonerIntegrated-operations/104/?guidelineLanguage=1

[34] ISO/IEC 27001 Information Security Management Systems
http://en.wikipedia.org/wiki/ISO/IEC_27001
http://www.iso27001security.com/html/27001.html

[35] 27002 Code of Practise for Information Security Management
http://en.wikipedia.org/wiki/ISO/IEC_27002
http://www.iso27001security.com/html/27002.html

[36] ISO/IEC 15408 Evaluation criteria for IT Security
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341
http://en.wikipedia.org/wiki/Common_Criteria

[37] ISO/IEC 18045 Methodology for IT Security Evaluation
http://www.iso.org/iso/catalogue_detail.htm?csnumber=30830
http://en.wikipedia.org/wiki/IT_risk

[38] Internet of Things (IoT)
http://en.wikipedia.org/wiki/Internet_of_Things

[39] Michael Scofield, October 2005, referenced in Stages Of Data Utility & Value, TDAN.com - November 2012 (http://www.tdan.com/)

[40] POSC Caesar Association Reference Data Services (RDS)
https://www.posccaesar.org/wiki/Rds

[41] World Wide Web Consortium (W3C)
http://www.w3.org/

[42] Berners-Lee T., Hendler J., and Lassila O. The Semantic Web, Scientific American, May 2001.

Appendix B: Relevant Standards for RFID Systems

ISO/IEC 18000-1:2008 defines the generic architecture concepts in which item identification may commonly be required within the logistics and supply chain and defines the parameters that need to be determined in any standardized air interface definition in the subsequent parts of ISO/IEC 18000. The subsequent parts of ISO/IEC 18000 provide the specific values for definition of the air interface parameters for a particular frequency/type of air interface from which compliance (or non-compliance) with ISO/IEC 18000-1:2008 can be established. ISO/IEC 18000-1:2008 also provides a description of example conceptual architectures in which these air interfaces are often to be utilized.

This standard limits its scope to transactions and data exchanges across the air interface at reference point delta. The means of generating and managing such transactions, other than a requirement to achieve the transactional performance determined within ISO/IEC 18000-1:2008 are outside the scope of ISO/IEC 18000-1:2008, as is the definition or specification of any supporting hardware, firmware, software or associated equipment.

ISO/IEC 15961:2004 focuses on the interface between the application and the data protocol processor, and includes the specification of the transfer syntax and definition of application commands and responses. It allows data and commands to be specified in a standardized way, independent of the particular air interface of ISO/IEC 18000.

ISO/IEC 15962:2004 focuses on encoding the transfer syntax, as defined in ISO/IEC 15961:2004 according to application commands defined in that International Standard. Encoding is in a Logical Memory as a software analogue of the physical memory of the RF tag addressed by the interrogator

ISO/IEC 24791 defines a Software System Infrastructure that enables radio frequency identification (RFID) system operations between business applications and RFID interrogators. RFID software systems are composed of RFID interrogators, intermediate software systems, and applications that provide control and coordination of air interface operation, tag and sensor information exchange, and health and performance management of system components

ISO/IEC 24791-1:2010 provides the following:

- An overview of the Software System Infrastructure
- Relationship of Software System Infrastructure to existing ISO components, e.g. ISO/IEC 15962.
- A basic description of each Software System Infrastructure component and the services that it provides (The detailed description of a particular component can be found in other parts of ISO/IEC 24791).
- Illustrative (informative) deployment models of the components of the Software System Infrastructure.

This standard addresses Device Management (Part 1), Data Management (Part 2), Application Management (Part 3), Application Interface (Part 4), Device Interface (Part 5) and Security (Part 6).

ISO 15926-1:2003 specifies a representation of information associated with engineering, construction and operation of process plants. This representation supports the information requirements of the process industries in all phases of a plant's life-cycle and the sharing and integration of information amongst all parties involved in the plant's life cycle.

Appendix C: Principles for planning and operating RFID solutions

Below is a prioritized table showing the principles to be used when planning or operating RFID solutions, together with some descriptive comments.

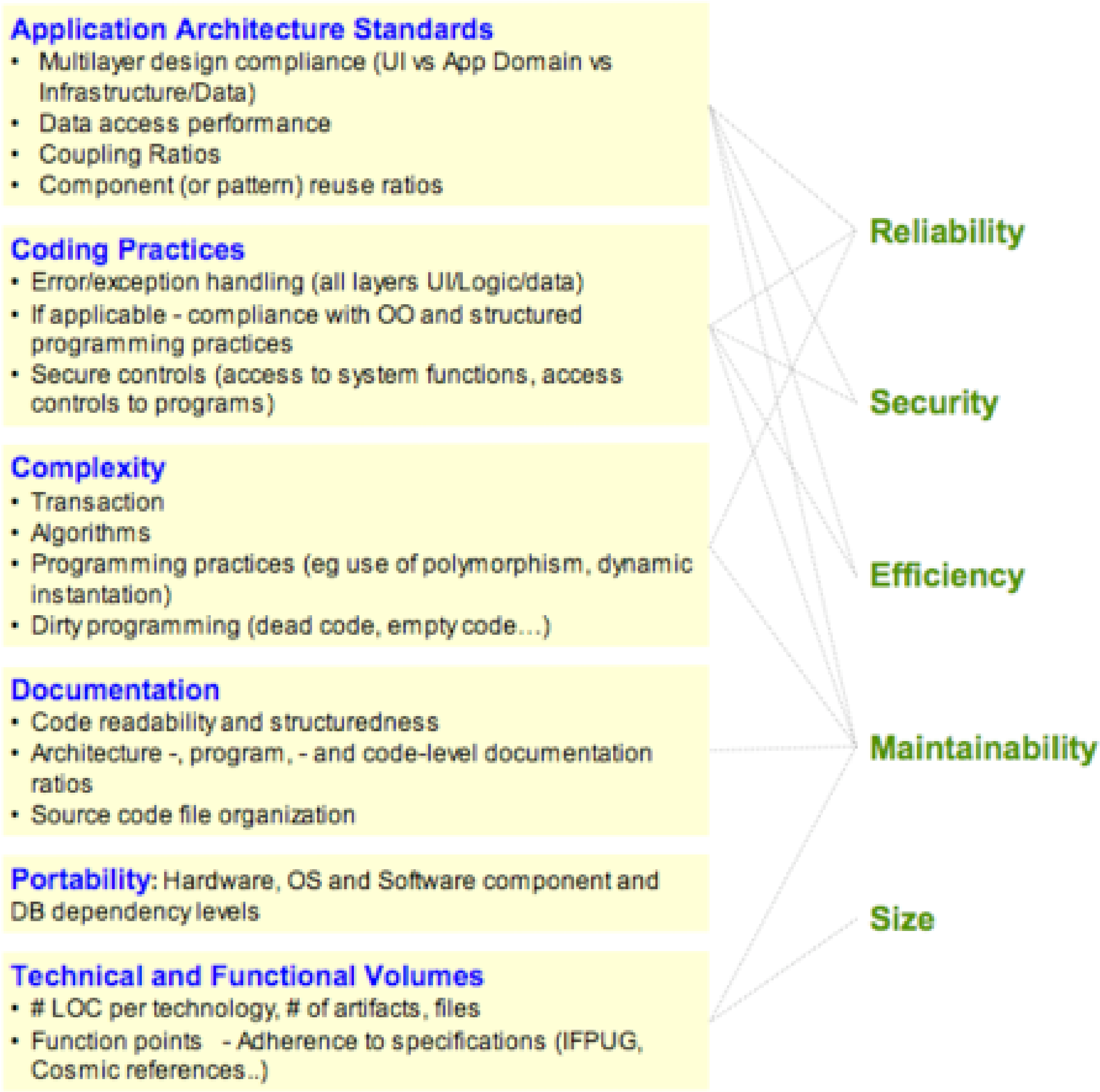
Priority ***(1-5, 5 is highest)***	***Name***	***Comments***
5	Loose coupling between systems	**Systems should be independent of changes in other systems**
5	Formats of data interchange should be standard	**E.g. Web services**
5	All data should have a clear owner	**An appointed owner decides on security and quality requirements for the data.**
5	A service provider and a service consumer must be able to interact with each other	**Reach ability is an essential pre-requisite for service interaction.**
5	A service should be self-contained	**Independent and autonomous. Limit the number of external services that a service is dependent on**
4	Semantics should be defined for all relevant data types	**All data types should be described so that the meaning of the data type is clearly understood.**
4	All data should have audit and quality attributes	**E.g. availability, version updated by, preliminary version…**
4	Conform to open standards	**The standards should be listed as part of this project**
4	Any service should have a well defined interface	**Describe data, formats, timing…**

4	A service description should include sufficient data to enable a service consumer and service provider to interact with each other.	**This may include metadata such as the location of the service and what information protocols it supports and requires. It may also include dynamic information about the service, such as whether it is currently available. The description should be according to the formalized agreement between the service provider and the service consumer.**
4	Roles and corresponding responsibilities must be defined	**Roles and responsibilities must be described to see who needs what in the patterns**
4	Physical location of a service provider should be transparent for any service consumer	**The availability, quality and performance of a service should be independent of the physical location of the service provider.**
3	Use service lookup mechanisms for finding services	**A mechanism is needed (e.g. a kind of directory) to find the name and location of a service.**
3	Data formats should implement agreed semantics	**E.g. Daily drilling report is an example where a format has been defined, The format represents the whole report, and each element, e.g. drillBit has a semantic meaning and therefore also a data type.**
3	Access should be role and asset based	**Users need to be allocated a role for an asset (e.g. an oil field) so that it is possible to see what access is allowed against that asset for that person.**
3	Authentication should be at the local company	**Authenticated at one"s own company, for use anywhere.**
3	There should be no vendor or platform lock-in	**Solutions should be available from several vendors and should be replaceable.**
3	Build on existing infrastructure	**E.g. SOIL**
3	Any standard should be qualified by inclusion in the standards catalogue prior to use	**Implication of the role of the standards catalogue as a qualifying entity.**
3	A service should be stateless	**Results/effects don"t depend on previous calls.**

3	Asynchronous handling of interaction requests must be possible (e.g. by queuing of requests for later consideration)	
2	Use event driven data exchange	**Data should (when relevant) be exchanged automatically when an event happens, e.g. at a specific time**
2	Data exchange should have guaranteed quality of service	**How fast, what volumes, availability, etc**
2	A service description should unambiguously express the function(s) of the service and the real world effects that result from it being invoked.	**Describe the functionality of the service (not how it does it, but what it provides) and what data or other effect it produces. Hence, any service should be encapsulated.**
2	A service should be reusable	**Designed to be used by multiple customers, and also to be used in different contexts (within the scope if its intended use)**
2	Any solution should be qualified with technical readiness level	**Not ready, not in mass production, early production, mature, or legacy.**
1	Actions should be traceable in real-time	**All actions performed should be traceable so that it is possible to see the status at any time**
1	Any service interactions should be based on an intentional act to initiate and to participate in a service interaction. Such intention should be formalized by a contract (e.g. a Service Level Agreement) between the actors. A service definition should be based on such an agreement.	**The extent of a service participant”s willingness to engage in service interactions may be the subject of policies.**

Appendix D: Software System Characteristics and Attributes

The figure below illustrates (an example of) relationships between typical software system characteristics (right) and measurable characteristics (left).



Application Architecture Standards
- Multilayer design compliance (UI vs App Domain vs Infrastructure/Data)
- Data access performance
- Coupling Ratios
- Component (or pattern) reuse ratios

Coding Practices
- Error/exception handling (all layers UI/Logic/data)
- If applicable - compliance with OO and structured programming practices
- Secure controls (access to system functions, access controls to programs)

Complexity
- Transaction
- Algorithms
- Programming practices (eg use of polymorphism, dynamic instantation)
- Dirty programming (dead code, empty code...)

Documentation
- Code readability and structuredness
- Architecture -, program, - and code-level documentation ratios
- Source code file organization

Portability: Hardware, OS and Software component and DB dependency levels

Technical and Functional Volumes
- # LOC per technology, # of artifacts, files
- Function points - Adherence to specifications (IFPUG, Cosmic references..)

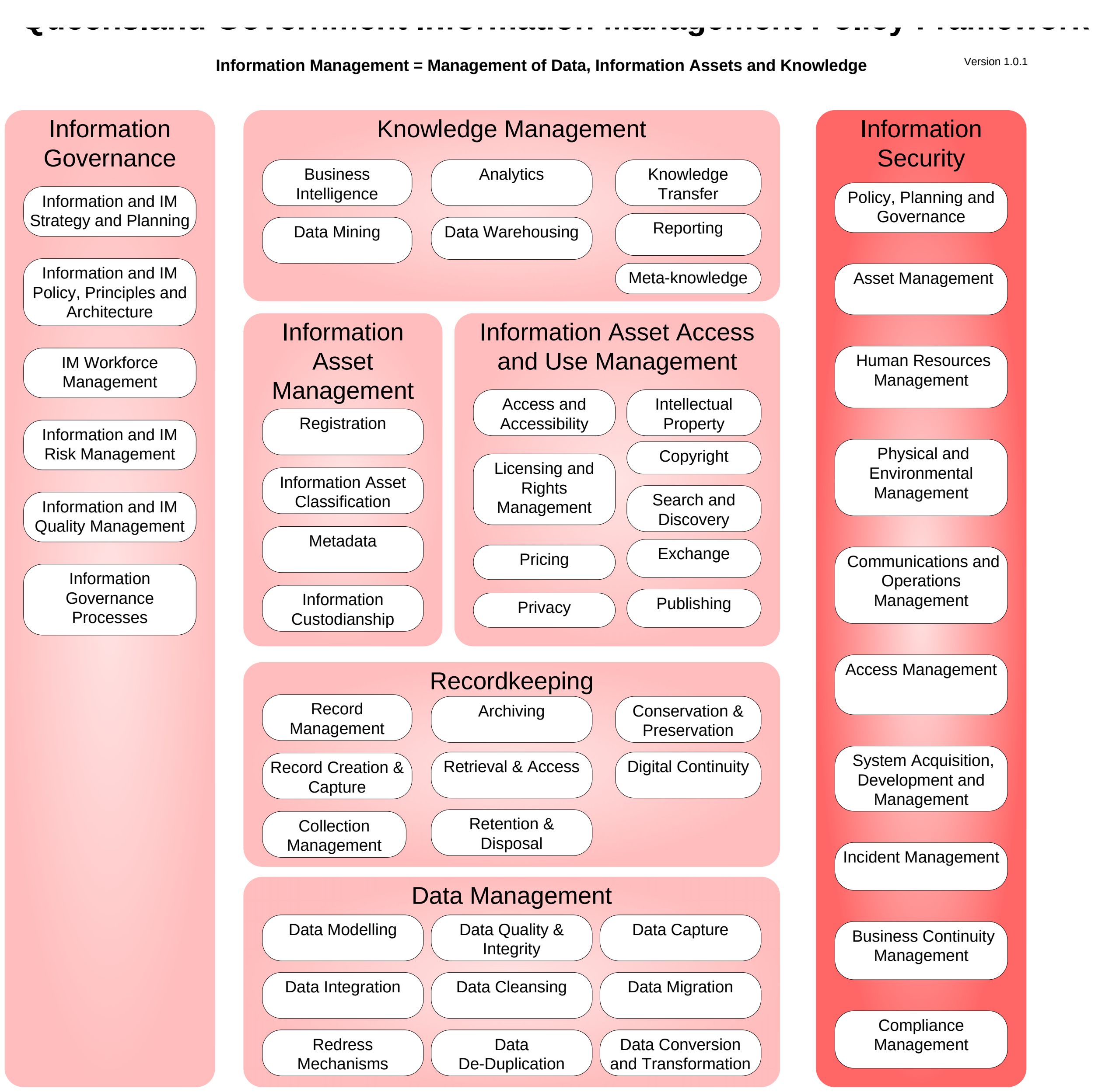
Software Quality Characteristic Attribute Relationship

(http://en.wikipedia.org/wiki/File:SoftwareQualityCharacteristicAttributeRelationship.png)

Appendix E: Enterprise Information System examples

The figure below illustrates (an example of) a taxonomy of information management tasks.

N



Queensland Government Information Management Policy Framework

Information Management = Management of Data, Information Assets and Knowledge

Version 1.0.1

Information Governance
- Information and IM Strategy and Planning
- Information and IM Policy, Principles and Architecture
- IM Workforce Management
- Information and IM Risk Management
- Information and IM Quality Management
- Information Governance Processes

Knowledge Management
- Business Intelligence
- Analytics
- Knowledge Transfer
- Data Mining
- Data Warehousing
- Reporting
- Meta-knowledge

Information Asset Management
- Registration
- Information Asset Classification
- Metadata
- Information Custodianship

Information Asset Access and Use Management
- Access and Accessibility
- Intellectual Property
- Copyright
- Licensing and Rights Management
- Search and Discovery
- Pricing
- Exchange
- Privacy
- Publishing

Recordkeeping
- Record Management
- Archiving
- Conservation & Preservation
- Record Creation & Capture
- Retrieval & Access
- Digital Continuity
- Collection Management
- Retention & Disposal

Data Management
- Data Modelling
- Data Quality & Integrity
- Data Capture
- Data Integration
- Data Cleansing
- Data Migration
- Redress Mechanisms
- Data De-Duplication
- Data Conversion and Transformation

Information Security
- Policy, Planning and Governance
- Asset Management
- Human Resources Management
- Physical and Environmental Management
- Communications and Operations Management
- Access Management
- System Acquisition, Development and Management
- Incident Management
- Business Continuity Management
- Compliance Management

An example implementation of an Enterprise Information Management Framework

(The Queensland Government Information Management Policy Framework http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/qgea2.0/Pages/index.aspx)

Appendix F: Initial Reference Data for RFID Systems

An (incomplete and preliminary) example of reference data classes related to RFID system structure, components and operation is listed below. Only classes and their definitions have been defined so far. The various classes must be defined as instances of appropriate ISO 15926-2 entity types, and the required relations must be defined in order to relate classes into an ontology about RFID systems (see Appendix G below for an illustration of a preliminary RFID ontology). Also, the various classes must be checked against the PCA RDL [17] to see if the class already exists, and to determine the appropriate superclass for the RFID classes.

Active tag

An RFID tag that has a transmitter to send back information, rather than reflecting back a signal from the reader, as a passive tag does. Active tags use a battery to transmit a signal to a reader or can gather energy from other sources. Active tags can be read from 100 meters or more. They are used for tracking expensive objects over long ranges.

AIDC

Automatic Identification and Data Capture and Data Collection include a broad category of technologies that includes Radio Frequency Identification (RFID) plus bar coding, smart cards, biometrics and other forms of automated data capture.

Automatic Identification

Term which encompasses bar coding, RFID, and other electronic technologies that electronically identify and track things/goods/objects.

Contact less smart card

Contact less smart card refers to identification cards (for example, some credit cards) that do not need to make contact with the reader to be read, or swiped in a special slot. This capability is implemented using a RFID tag in the card; the intent is to provide the user with greater convenience by speeding checkout or authentication processes.

Data repository

Also called RFID Historian. Aggregates data from real time locating systems and provides the history, from enterprise information to single events, for reporting.

Discovery Service A service that allows companies to search for every reader that has read a particular RFID tag.

Domain Distinguished part of an abstract or physical space where something exists.

Enterprise A company (or business).

Far Field Far Field is far range (usually more than 1 meter) RFID reading. In far field communication backscatter is used. Backscatter is the reflection of the radio frequency wave when it hits a conductive surface.

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.

Levels A division of the RFID System Architecture Model to describe Hardware, Software and Infoware that realize the functionality covered by the appropriate part of the Architecture Model

Meta data

Information, irrespective of its form, used to describe a real or abstract object.

Near Field

Near Field is close range reading of RFID tags, up to say 1 meter. In near field communication the tag communicates with the reader by electromagnetic inductance.

Object

A physical or non-physical “entity”, 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.

Operator

The oil and gas company (either proprietor or lessee) which runs the business, i.e. actually operating the well or engage subcontractors.

Passive tag

An RFID tag without its own power source and transmitter. When radio waves from the reader reach the chip’s antenna, the energy is converted by the antenna into electricity that can power up the microchip in the tag. The tag is able to send back information stored on the chip.

Portal

An RFID interrogator gateway used in RFID applications. Forklifts or other methods are used to transport tagged items through a portal reader to collect RFID tag data.

Reader

Also called interrogator. A device that communicates with the RFID tag via radio waves.

Real time locating system

A system of finding the position of objects/things, using active RFID tags. The tags broadcast a signal, which is received by three reader antennas. The time each signal is received is passed on to a software system that uses triangulation to calculate the location of the object.

Segments

A division of RFID System Integration Model to describe details of data communication and information processing for the appropriate part of the Integration Model.

Semi passive tag

Similar to active tags, but the battery is used to run the microchips circuitry but not to broadcast a signal to the reader. Some semi passive tags sleep until they are woken up by a signal from the reader, which conserves battery life. These tags are sometimes called battery assisted tags.

Tag

Also called transponder. Identification device capable of transmitting/reflecting data. Some tags also receive and store data. The tag could be active, passive or semi-passive.

XML

eXtensible Markup Language**.**

Appendix G: An example Ontology for RFID Systems

The figure below gives an (incomplete and preliminary) illustration of how the Reference Data classes from Appendix F (red boxes with round corners) can be related in an ontology to describe the structure, content and behaviour of RFID system. Only a few relation of the (many) required relations are shown. The assignment of the reference Data classes to ISO 15926-2 entity types (grey boxes with sharp cornets) has been suggested for illustration purposes only.

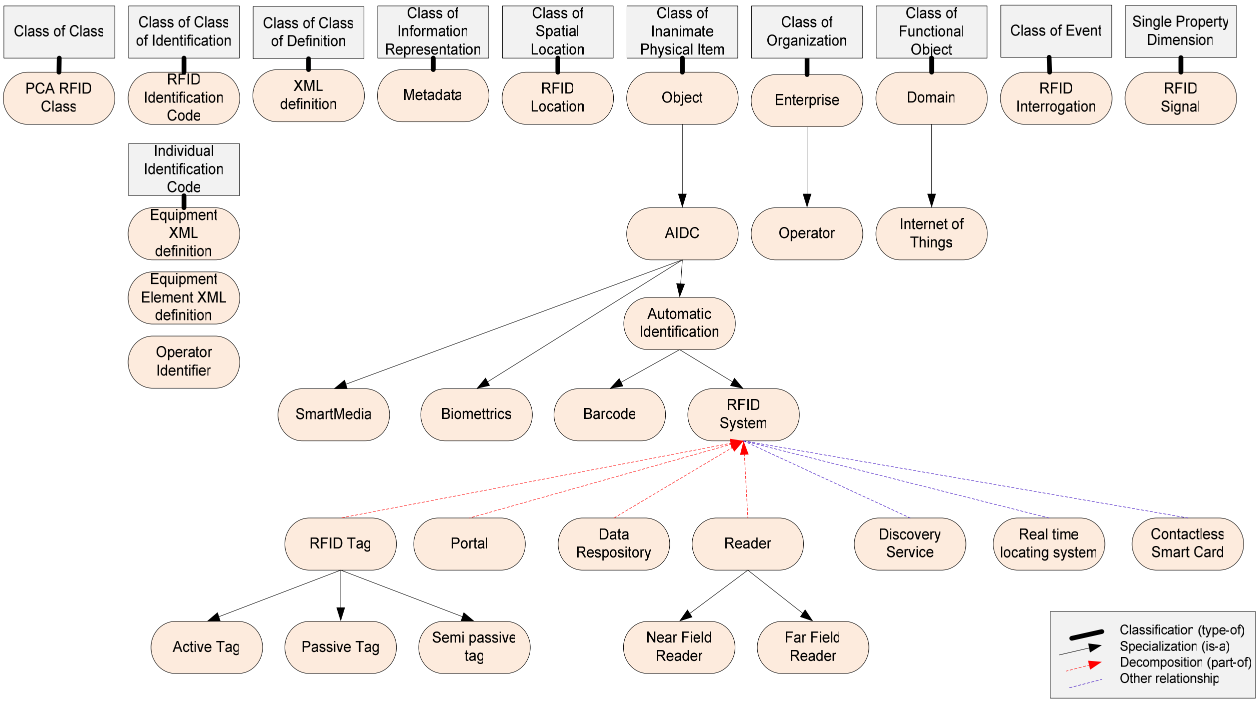


Figure 14: The RFID Ontology Model (ROM) with reference classes and relationships

Parts 5 through 9 of this guideline describe different application areas. An example ontology has been developed for CCU, and will be added in separate documents. Similar ontologies must be developed for the other applications (mobile and fixed equipment, etc.), using existing Reference Data classes and defining new classes and relations to properly describe the application logic.