A Secure, Open and Non-Proprietary Standards-based Global Technical & Engineering Information Bus Enabling Collaborative Business Processes for Oil & Gas

Proposal to Enable Oil & Gas Organizations to Adopt a Secure, Open and Non-Proprietary Standards-based Global Technical & Engineering Information Bus enabling Collaborative Engineering, Procurement, Construction, Operations & Maintenance Business Processes

May 14, 2010

Oil & Gas companies continue to face on-going challenges in rapidly integrating and utilizing its vast amount of technical information to continuously improve operational efficiencies while operating in a safe and responsible manner. These challenges are shared with other capital-intensive multi-national corporations which must engineer, procure, construct, operate and maintain global assets in remote regions of the world. Outsourced EPC (Engineering, Procurement & Construction) often utilizes multiple international entities. This elevates the need for secure inter-enterprise collaboration to deliver assets and their associated technical information on time and within budget.

In this OpenO&M R&D proposal, Oil & Gas companies will work with other major capital asset owners to adopt the relevant non-proprietary **information content** standards from existing industrial information standards bodies including POSC CAESAR, MIMOSA, OpenO&M, and FIATECH in order to finalize tighter, non-proprietary information sharing linkages with EPC firms, capital equipment suppliers, and O&M service providers. These content standards must then be combined with secure **information on-ramp, off-ramp, and transport** standards to fully specify a **Secure, Standards-Based Global Technical & Engineering Information Bus** (hereon called "Information Bus") for broad-based exchange of industrial information. Through the use of the Information Bus, Oil & Gas organizations can significantly improve the availability, accuracy, and integrity of their engineering, procurement, construction, operations, and maintenance business processes.

Approaches to industrial information until recently have focused on providing a "document-oriented" approach. Printed or electronic "data sheet" documents embed all the specification information developed by an EPC firm for all the platform's assets, e.g. piping, control devices, instrumentation, and rotating equipment. These data sheets are either printed in hardcopy form for handover to Operations and Maintenance personnel or electronically delivered via formats such as Adobe's Portable Document Format (PDF). Unfortunately, the relevant fields on the data sheet, e.g. "Rated Discharge Pressure (bar g)" for a centrifugal pump, are not "machine-readable". For interpretation and entry into another system, these data sheet fields have to be manually read and re-keyed into an operation or maintenance system. This "document-oriented" approach to industrial information is costly, inefficient, and error-prone. Even with the adoption of document management systems, the inability for these documents to reveal their "hidden fields" in a standardized way, are highly inefficient and insufficient to sustain the EPC cycle or the Operations and Maintenance lifecycle.

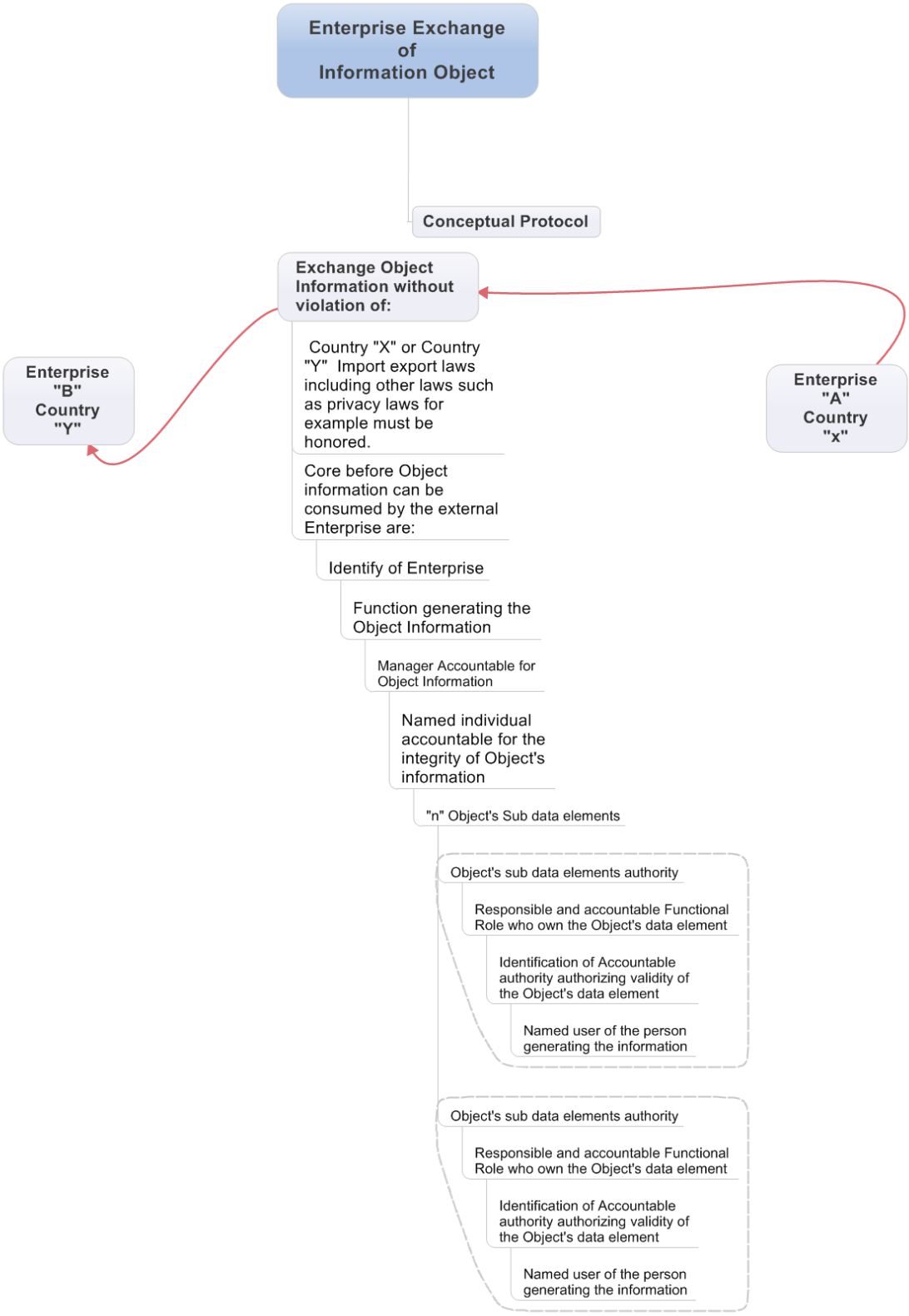
Next-generation "field-oriented" information standards such as ISO 15926 and MIMOSA now allow computer systems to recognize and understand key physical asset parameters on a data sheet and provide a standards-based method for moving granular information throughout compliant systems. These data sheet fields form the basic information "packets" which can flow across the standards-based global industrial information bus.

Oil & Gas business processes which span the entire lifecycle of a platform require constant access to information sources. The lack of standardized information formats in the past have required complex, expensive, highly-customized integration data conversions. These integrations are fragile and expensive to maintain, since any software revision which results in a

change to an information input or output requires another integration engagement. With the emergence of the Information Bus, these information sources are now standardized and provide "pre-engineered" inputs to processes, which can trigger appropriate actions, and output standardized information feeds which can drive other intra- or inter-enterprise processes. The Business Process Execution Language (BPEL) http://en.wikipedia.org/wiki/Business_Process_Execution_Language and the Business Process Modeling Notation (BPMN) http://en.wikipedia.org/wiki/Business_Process_Modeling_Notation have emerged as a standardized way to uniformly represent the same semantic content of business processes.

Without adequate security, the Information Bus could present a host of new concerns. One concern is non-authorized data eavesdroppers. An even greater issue is "bad actors" interested in disrupting safe and secure operations who try to exploit vulnerabilities in the information systems. These attacks can be launched on individual corporations or as part of a coordinated attack on critical infrastructure. Industry and role-specific IT and automation Protection Profiles (PP) for the Information Bus are needed in compliance within a broader framework shared by critical infrastructure. The PP's enable the specification of the required levels of safe and secure sharing of knowledge, information and data for role-specific information exchanges. The basic elements in the profiles include policies, threats, assumptions (collectively called environmental considerations) that constrain the Information Bus environment.

The diagram below identifies an information object with data from a physical or virtual asset and the considerations which must be taken into account during the exchange of information between two business entities different countries. All the information exchanges must be traceable to authorities who are accountable and responsible for the creation or modification of the information exchange down to the datum. It must have full tractability to confirm integrity. This includes the exchange of information between the asset owner's IT and automaton spacers.


Enterprise Exchange of Information Object
Conceptual Protocol
Exchange Object Information without violation of:
Country "X" or Country "Y" Import export laws including other laws such as privacy laws for example must be honored.
Core before Object information can be consumed by the external Enterprise are:
Identify of Enterprise
Function generating the Object Information
Manager Accountable for Object Information
Named individual accountable for the integrity of Object's information
"n" Object's Sub data elements
Object's sub data elements authority
Responsible and accountable Functional Role who own the Object's data element
Identification of Accountable authority authorizing validity of the Object's data element
Named user of the person generating the information
Object's sub data elements authority
Responsible and accountable Functional Role who own the Object's data element
Identification of Accountable authority authorizing validity of the Object's data element
Named user of the person generating the information
Enterprise "B" Country "Y"
Enterprise "A" Country "x"

In addition to sophisticated, technology-based attacks, security reviews continue to indicate that most breaches of security still come through very traditional means, such as by losing proper control of printed material (including hand written notes with IDs and Passwords) or portable magnetic media. What is needed is a **holistic approach** to knowledge, information and data management where appropriate elements (whether in digital, printed or other form) are treated as an **asset** with unique identification, then traced and tracked in an auditable manner based on its value and sensitivity per defined policy and rules. Role-based relationships can then be defined between agents (human or systemic) and these information assets, just as with all other types of enterprise assets. This approach can be applied to simple documents (such as this one you are reading now) which may need to be reviewed and fully or partially cleared to be shared with other market participants as well as complex information and/or data exchanges related to topics such as project handover and or more granular exchanges such as might be required when seeking additional information and/or data about a particular asset (physical or informational). This information exchange is statefull and goes beyond simple transactional transactions common today.

The basic dimensions of the problem are illustrated in Figure 1 (below).

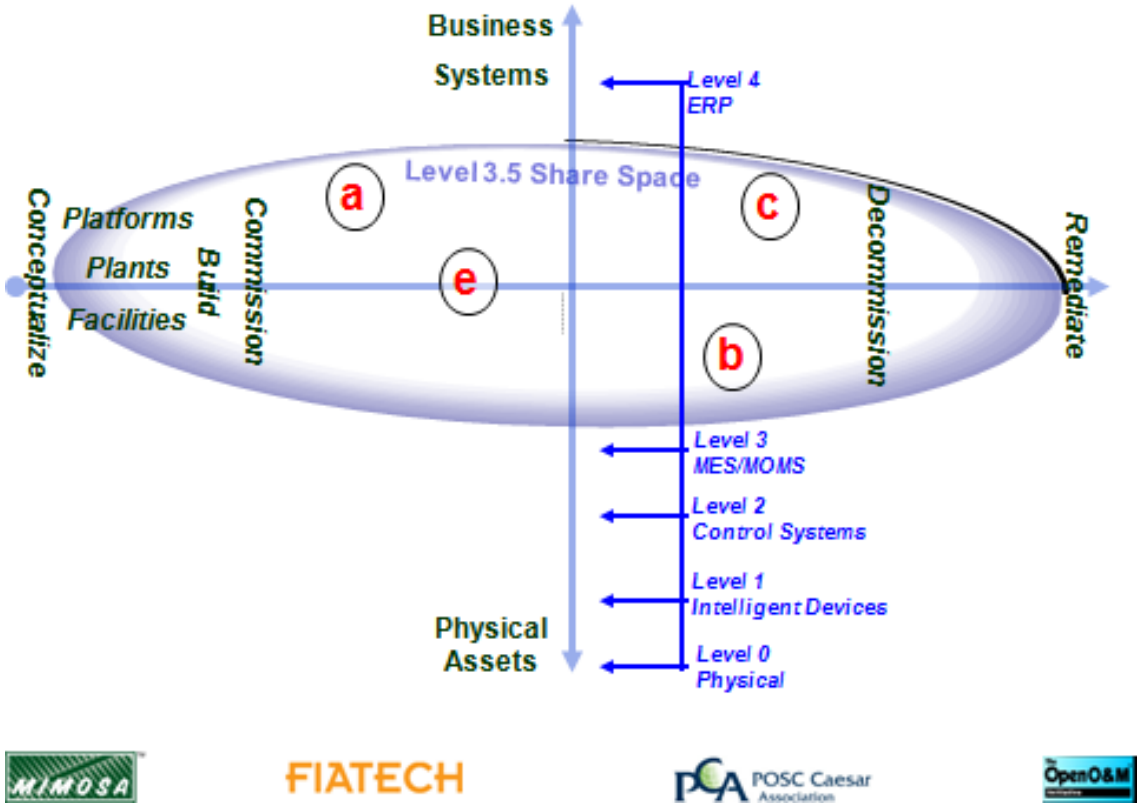


Figure 1

The vertical y axis of Figure A depicts the traditional layers as defined by the Purdue model, where Layer 4 (L4) is defined as the Enterprise Business Systems Layer (shown as ERP), which is typically under the control of corporate IT. Layer 3 (L3) and below are the environments which are directly responsible for the safe and efficient Operation of the facility, plant or platform and they are normally under the control of an operations group. The horizontal x axis depicts the life-cycle of the entire facility, plant or platform beginning with the concept, continuing through the Operations & Maintenance phase and running through end-of life to remediation. The layer between L4 and L3 is identified as Layer 3.5 and depicted as a flattened sphere in the (x,z) plane. It represents the shared space which must be well-defined to support safe and secure information exchange between systems typically located in L3 and L4 as well as with internal engineering systems (e) and with external partners (a, b and c) with which Asset Owners wished to share technical and engineering oriented information. As with most such efforts to represent complex systems of systems in a single figure, this is a dramatic oversimplification, but it is illustrative of the problem. Alternative and more comprehensive views of elements of the problem space and the related solutions architecture can be found in deliverables B and E.

OpenO&M specifications and best practices documents will need to be developed in a way that is consistent with the basic requirements identified above. Individual elements of the related architecture can continue to be developed through specifically identified, scoped and prioritized activities, but there will remain an overarching architecture development process to tie all of the elements together through a process that will ensure the needed levels of security. Such a process is both incremental and continuous as business requirements and the elements of the architecture continue to evolve along with Information Technology.