SPE 112049

Reliable IT for Integrated Operations

Pieter J. den Hamer, DNV Research and Innovation, and Torbjørn Skramstad, DNV Research and Innovation and Norwegian University of Science and Technology, N-7094 Trondheim, Norway

This paper was prepared for presentation at the 2008 SPE Intelligent Energy Conference and Exhibition held in Amsterdam, The Netherlands, 25–27 February 2008.

Abstract

The oil & gas industry and especially integrated operations, depends heavily on reliable and robust information technology (IT). Systems and components are increasingly 'software intensive' and interconnected. However, at the moment IT is often not reliable enough, resulting in serious risks for production continuity and safety. To manage these risks, the oil & gas industry needs to mature its IT reliability, supported by guidelines that are developed in the 'GOICT' joint industry research project, initiated by DNV. So far, this project has identified a number of critical areas, summarized in this publication, that need to be addressed to improve IT reliability for integrated operations.

Introduction

Integrated operations and related initiatives like 'smartfields' and 'field of the future' depend heavily on the application of IT, with systems and components becoming ever more 'software intensive'. Moreover, as the name 'integrated operations' implies, there is a strong increase of integration and connectivity between systems and components in this area. Obviously, introducing integrated operations offers many advantages (OLF, 2005) in areas like production continuity and safety, reaping the benefits of real-time and remote monitoring and cross-discipline decision support. However, integrated operations may also lead to increased vulnerability, even more so at the potentially very large scale of integrated operations. In the nearby future integrated operation centres may exist onshore that control multiple offshore production facilities. Without proper measures to manage reliability, such integrated operation centres may become a 'single point of failure', of which malfunction or even shutdown will result in serious economical losses because of production interruption, not to mention the enormous safety and environmental risks involved.

Considering the benefits, vulnerability and risks of integrated operations, it is clear that the reliability of IT is of pivotal importance to anyone who is dealing with integrated operations. Unfortunately, recent studies and personal experience of many people show that today's reliability of IT is not as mature as we would like it to be, as demonstrated by these examples (Torstensen, 2007):

- In 2003, during operation, two GPS systems giving the position to the Dynamical Positioning system of a floating hydrocarbon production vessel suddenly changed position by 70 m. The software did not detect this failure, and consequently started to move the rig to the new position. This caused considerable economical losses since much equipment was broken and operation lost for several days. Moreover, an incident like this may have caused injury to personnel and severe pollution as well.
- In 2005, routine maintenance led to degradation of the ESD (emergency shutdown) system. The application software in the ESD controller was dependant upon higher level network functions. The ESD controller stopped because of maintenance at the higher level. One of the redundant controllers stopped, and no fault alarm was initiated. The other controller was (by luck) temporarily connected to an independent PC and did not stop for that reason. The consequences were minor, however, under normal situation the consequence would have been an uncontrolled total platform shutdown.
- In 2004, software faults and routine maintenance operation led to loss of Central Control Room (CCR) on a production

platform. Network servers in a 2oo3 (two-out-of-three) configuration got faults on two servers. Maintenance of the faulty servers also lead to that the one running also failed and the CCR was completely blacked out for one hour. If alarms or messages had occurred that needed attention from the operators, these would not have been shown.

In addition to these and other incidents, practical experience with software intensive systems in the oil & gas industry (and other industries) learns that there are many near-incidents and no doubt many unknown incidents that were caused by unreliable IT.

For safe and effective integrated operations it is a critical success factor that the oil & gas industry, together with IT suppliers, improves the reliability of IT. To enable this, the joint industry research project GOICT ('Gas & Oil ICT'), supported by the Norwegian research council, was initiated by DNV in 2007. The project consortium - with operators, technology suppliers (both oil & gas and IT) and research institutes - aims to develop guidelines to improve the reliability of 'software intensive systems' for integrated operations, with the objective to support the safety and continuity of hydrocarbon production processes.

The terminology 'software intensive systems' is used to underline the fact that the subject of the project is not just about general purpose ICT (information and communication technology), or only about software engineering or only about system engineering. Instead, the terminology is chosen to underline the fact that to improve reliability - the ability to perform a required function under stated conditions for a specified period of time - the whole of systems and information technology, (software and hardware) should be considered in an integral way. The scope of the concept 'software intensive systems' is intentionally wide, and includes all systems that may be used for integrated operations. These may vary from all kinds of specialized systems, possibly with hardware embedded software, like pipeline sensors or drilling equipment to more generic systems like asset management or even personnel administration systems. In addition, systems for the actual connectivity and integration of all the other systems, or 'middleware', are explicitly part of the scope.

Improving reliability

Building on experience with software intensive systems in both the oil & gas and other sectors, a number of key areas for improvement of reliability, have been identified, as shown in figure 1. These areas represent different yet interdependent levels to address the reliability of software intensive systems, in an integral way. This means that paying attention to one level while ignoring another, will lead to lower reliability. For instance, in practice many reliability measures are only taken at a infrastructural (network, hardware) level, whereas information architecture aspects like data quality and semantic interoperability are not well understood or even ignored. As a consequence, data exchange between systems and components is error prone, resulting in software interaction errors and system failures, despite having reliable infrastructure.

The approach here is to have a multi-layered or stacked, integral approach to improve and manage reliability. At the lower level of 'base products / components', reliability is addressed by qualifying the technology that is used in the 'building blocks' of the system. However, having just reliable building blocks is no guarantee whatsoever that the building - or system - as a whole will be reliable. Therefore, reliability must also be addressed at the different interacting levels of architecture: infrastructure architecture (including network topologies), software architecture (including interaction between software components within and between different systems), information architecture (including data quality and semantics for information exchange) and process architecture (work processes, activities, actors).

Finally, it would not be sufficient to address reliability only during the design and building phase of a system. Hence, reliability should be an issue during the whole lifecycle of any system, from conception, design, building, commissioning and maintenance to decommissioning.

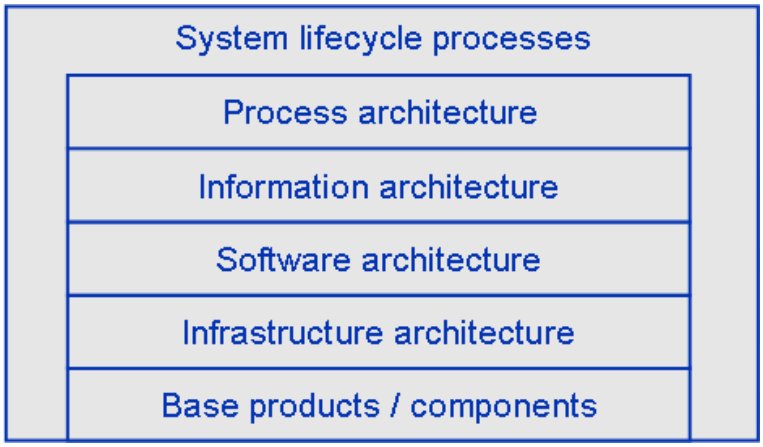

Figure 1: reliability needs to be addressed at different, interrelated levels, starting with base products or components, followed by several architectural levels to cope with the system and its environment as a whole, during all lifecycle processes (from conception to decommissioning and everything in between)

Base products / components

Systems for integrated operations and other production-critical systems are composed of base products or components that are increasingly software intensive. Different suppliers of components may have different ways of designing, developing, documenting and deploying software. Especially in integrated operations, there is often a diversity of suppliers and different software technologies and standards that somehow need to be combined.

To address reliability at the level of base products, it is necessary to qualify the software intensive components. If the component has significant and documented operating history in the same domain, it could be considered to be proven technology. If not, then some form of software verification and validation is required.

Today different approaches and standards exist to assess quality aspects, including reliability, of commercial off the shelf (COTS) and/or newly built software intensive components. These include approaches and standards like ISO 9126/Quint (Zeist, 1996), ISO 9001/TickIT (TickIT, 2007), IEC 61508 (IEC, 1998) or IEC 61511 (IEC, 2003), with typically the last two involving failure modes and effect analysis (FMEA) to calculate failure probabilities.

In practice, choosing the right approach and detail level of technology qualification, under pressure of project timing and economical feasibility, is often difficult. This is why in the current project guidelines will be developed, using a risk based approach to determine levels of criticality for base products and components, with corresponding levels of qualification rigorness.

Infrastructure architecture

Infrastructure like network facilities, application servers, data storage facilities and other ‘hardware’ are at the very core of IT reliability. Without infrastructure, there would be no (wireless or cabled) connectivity between components, no data flow between onshore and offshore facilities or other locations. Although many suppliers offer proven technology for infrastructure, the design and – most importantly – maintenance and management of infrastructure, should by no means taken for granted.

In practice, reliability measures in this area are often focused on introducing redundancy in network topology and server hardware to guarantee a minimal amount of availability, usually expressed as a percentage of time per year. However, this covers only part of the growing complexity and technological innovations in this area, not to mention the growing security demands. Also, service providers in this area are not always well aware of the differences between offshore networks for control systems and onshore networks for IT systems in an office environment. For instance, installing updates or replacing parts in the offshore context is much harder, also because of lack of offshore personnel with sufficient relevant skills.

Guidelines to improve reliability at the level of infrastructure architecture will build on existing practices, see for instance OLF 104 (OLF, 2006), but will also need to address challenging aspects of integrated operations, like connectivity with many distributed, possibly very remote and/or sub sea locations. Also, infrastructure reliability should be closely linked with the physical design of onshore integrated operation centres and their backup facilities.

Software architecture
Having a clear and complete overview of the software being used in integrated operations, and the assembly of (software) components or base products and their interactions is an absolute requirement to manage reliability. For instance, without software architecture it would be very hard to identify dependabilities between software components. Many reliability problems come from this, both during development and maintenance. For instance, when a malfunctioning system component is replaced, a new software version may have been introduced without warning of the supplier, causing unexpected problems in other components that assumed an older software version in the replaced component. Sometimes this (or other problems at local component level) may even lead to cascading effects, resulting in a complete failure of the system or indeed other connected systems as well.

A typical issue in this area is the introduction of so called service oriented architectures (SOA) and service bus middleware, providing – amongst others - less tightly or indirect couplings between applications or software intensive components. The bus middleware may even provide transformation and routing services, thus supporting connectivity between (embedded) software of different platforms and vendors, based on a variety of web service standards and industry standards like the unified architecture of OPC (OPC, 2006). Early experience in different industry sectors with SOA demonstrates the benefits of this approach, also with respect to reliability. For instance, some SOA implementations include failure detection and recovery services, building on the ability of monitoring application interactions through the intermediate bus structure (instead of 'hidden' direct 1-to-1 application interfaces). However, the same experience shows that successful application must go hand in hand with process modelling, information quality, standardisation efforts and organisational aspects like explicit roles and responsibilities for software architecture and integration, amongst others.

Information architecture
Another important area in the reliability of software intensive systems is the quality of information and the (real-time) integration of data from different (sub) systems. This is especially true in the context of integrated operations, which is characterised by a high degree of connectivity between work processes and systems to exchange and integrate data, typically for instance the integration of real-time acquired well data with geological and reservoir model data. This type of integration, often between systems of different origin and/or different suppliers can only be feasible and reliable if it is based on well defined data models and – preferably - industry standards like WITSML 1.3 (WITSML, 2005) and ISO 15926.

In addition, the quality of data and presented information to human operators has a direct impact on reliability. Lack of attention for information quality may result in incorrectness, incompleteness or for instance misinterpretation. Also, data quality issues like missing or exceptional values are quite often the cause of software malfunctions.

Process architecture
Effective attempts to improve reliability of IT should make a distinction between different levels of required reliability. Typically, primary production and/or safety processes or specific activities therein require the highest levels of reliability, whereas more supportive or processes that are not immediately critical to production continuity or safety, require less high reliability levels. These levels are then used to determine the effort that must go into the different ways to assess, improve and manage reliability. For instance to determine the needed type and detail in failure mode analysis, or the rigorness and extent of testing, or redundancy needs in hardware, etc.

Identifying requirements for reliability is preferably done at the functional level, in the context of work processes and operational modes, preferably including usage quantification and frequency of demand. This way, any measure that is taken to manage reliability at more technical levels can always be related to the level of work processes, activities and functionality, which is critical for business-level understanding, validation and justification. Unfortunately, in practice, work processes and activities are often implicit or poorly described. This is one of the reasons that IT failures occur during critical production processes that weren't explicitly identified as critical a priori, and hence were never explicitly supported in terms of reliability measures. Instead, in today's practice many reliability measures, if at all, are taken more or less undirected or in a generic way at the level of network topology or server hardware, resulting for instance in servers that are used simultaneously by systems for real-time drilling monitoring and salary administration (an exceptional, yet real life example).

To support reliability, models that describe work processes, activities and supporting system functionalities must be improved or developed, and maintained. Of course, in the context of integrated operations this is necessary anyway, considering the desired integration and optimisation of work processes (OLF, 2005) that underpin the investments in integrated operations. In order for integrated operations to be effective, work process models are necessary anyway, not just to identify IT reliability requirements, but also to optimize work processes, to coordinate closer collaboration with suppliers and for instance to manage competences of people who will have to work in new positions and roles.

System lifecycle processes

In general, experience in the oil & gas and other industries shows that reliability and other aspects directly relate to the quality of system engineering processes. Ideally, these processes cover the whole life cycle of a system, including design, development, commissioning, maintenance and decommissioning. GOICT will deliver guidelines for the processes (including roles, competences and activities) that are needed to develop and maintain reliable systems. To prevent reinventing the wheel, standards and models from other industries like the aerospace and automotive industries will be sought. This is especially the case for CMMI, a well known capability maturity model, adopted in many industries, originally in software engineering but nowadays also for system engineering (Gibson, 2006).

In the GOICT project, special emphasis will lie on system integration, being the process where typically most complexity arises, both in technological and organisational terms. Currently, integration at the system level (or higher) is typically a late phase activity, often resulting in problems that could have been avoided if integration would have been part of the system engineering process at an earlier stage.

Next steps

Having identified the most important areas that must be addressed together to improve reliability of software intensive systems, this joint industry research initiative will go on, in the coming three years, by further deepening and understanding these areas, combining scientific findings with practical experience and applicability. Importantly, this will also be done by looking at other industry sectors, specifically aerospace, automotive, nuclear and railway industries. In addition, relevant existing industry standards of amongst others IEC, OLF and Energistics and other related work will be taken into account. This will result in guidelines that can be used by operators, technology suppliers and other industry parties in their cooperation in developing and maintaining integrated operations.

The consortium that is involved in this project will be the first to evaluate the guidelines in real world situations - several partners have ongoing and new initiatives for integrated operations. After evaluation and improvement, the goal is to disseminate the resulting guidelines internationally.

References

IEC: *IEC 61508 Functional safety of electrical /electronic/programmable electronic safety related systems* – Part 1-7. (1998)

IEC: *IEC 61511 Functional Safety Instrumented Systems for the Process Industry Sector,* Part 1-3. (2003)

Gibson, D. L., Goldenson, D. R., Kost, K.: *Performance Results of CMMI®-Based Process Improvement*, http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06tr004.pdf (2006)

OLF: *OLF Guideline 104: Information security baseline requirements for process control, safety, and support ICT systems* (2006)

OLF Workgroup Integrated Work Processes: *Integrated Work Processes: Future work processes on the Norwegian Continental Shelf* (2005)

OPC: *OPC Foundation Unified Architecture*, available on www.opcfoundation.org/ua (2006)

TickIT: *TickIT International Journal*, BSI/Firmfocus (2007)

Torstensen, A., Bratthall, L., Skramstad, T., Johansen, E.O.: *Achieving system quality in software intensive maritime systems,* EuroSPI 2007 (2007)

WITSML: *Wellsite Information Transfer Standard Markup Language*, available on www.witsml.org (2005)

Zeist, R.H.J. van, Hendriks, P.R.H.: *Specifying software quality with the extended ISO 9126 model*, Software Quality Journal, volume 5, nr 4, Springer (1996)