SCADA Revamp: The Opportunity

Jochen Frings, ILF Consulting Engineers, Germany

Abstract
When a pipeline’s SCADA and control system shows increasing hardware failure rates and it gets harder to find spare parts, software updates and skilled people for maintenance or engineering, it is high time to execute a SCADA and control system revamp.

Therefore the focus of a SCADA revamp project often is primarily on time and cost efficient replacement of the controllers, communication equipment, servers and work stations with the target to reuse as much equipment and to change as little functionality as possible.

Unfortunately, this focus on equipment replacement frequently hinders making optimum use of the inherent opportunities contained in each SCADA Revamp project: to increase the system’s value by resolving all known issues, integration of work around procedures, removal of unnecessary functions, consideration of changing business needs as well as by improving efficiency, safety, security and compliance to the state of the art.

In order to overcome this problem a systematic SCADA Revamp approach for a new functional specification will be proposed that focuses on a complete requirement engineering, considering the existing SCADA solution for existing locations and potential equipment or wiring reuse only.

As examples for the many requirements that evolved during the recent 15 years an overview on operational safety and SCADA security will be presented.

1. Introduction

When a pipeline’s SCADA and control system shows increasing hardware failure rates and it gets harder to find spare parts, software updates and skilled people for maintenance or engineering, it is high time to execute a SCADA and control system revamp.

In consequence the decision for a revamp often is made due to equipment failures and the focus of the project hence is primarily on time and cost efficient replacement of the controllers, communication equipment, servers and work stations only. Due to years of operation the software on the other side had been debugged leaving only a few minor issues for which work arounds became routine for the operators. Hence there is the desire to minimize engineering efforts and to transfer the software functionality and screens to new hardware, if possible automatically with the help of
reverse engineering tools. These are available for several combinations of old and new SCADA and control systems with several SCADA vendors.

**Figure 1: Systematic SCADA Revamp Approach**

Although this approach might seem to be quite comfortable, in reality this results often into large and inefficient code (1) - which in the end is hard to be maintained for the next 15 years.

Unfortunately, this focus on equipment replacement hinders making optimum use of the inherent opportunities contained in each SCADA Revamp project: to increase the system’s value by resolving known issues, integration of work around procedures, removal of unnecessary functions, consideration of changing business needs as well as improving efficiency, safety, security and compliance. Using this opportunity basically means identify and to adapt the system to the requirements that may have evolved or appeared during the last 15 years.

In order to ensure that all relevant requirements are properly reflected in the new SCADA and control system design, a systematic SCADA Revamp approach to create a new functional specification will be outlined in the following section.
As examples for changing regulatory requirements and advancement of the state of art an overview on recent developments SCADA operation safety and SCADA security will be given.

2. Systematic SCADA Revamp Method

To use the opportunities in a SCADA revamp project means to improve the overall system value and project business case by designing a state of the art SCADA system under consideration of the existing systems reusable specifications, software and equipment and special focus on the experience of operators and maintenance teams.

As shown in Figure 1 following to the project kick-off a rough scan of existing documentation and installations as well as a first round of interviews should be executed in order to get a feeling for the project and to identify the relevant stakeholders. Based on this information a detailed project approach and project plan should be developed and agreed between stakeholders.

**Figure 2: Requirements Elicitation**

<table>
<thead>
<tr>
<th>Technology Review</th>
<th>Brownfield Analysis</th>
<th>Stakeholder Interviews</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholder Update</td>
<td>Equipment Status</td>
<td>Type of Interviews, Task Monitoring</td>
<td>Relevant Standards, Recommendations …</td>
</tr>
<tr>
<td>On Current Technology</td>
<td>Revamp Boundaries</td>
<td>Business Requirements</td>
<td>Gap Analysis</td>
</tr>
<tr>
<td>Technology Comparison Studies</td>
<td>As-Built Documentation</td>
<td>Known Problems / Workaround</td>
<td>Documentation</td>
</tr>
<tr>
<td>Communication Services</td>
<td>Undocumented Features</td>
<td>Targets / Ideas</td>
<td>Audits, Assessments</td>
</tr>
<tr>
<td>Development Tools</td>
<td>Subsystem/Communication Interfaces</td>
<td>Procedures / Spreadsheets</td>
<td></td>
</tr>
<tr>
<td>Software Maintenance</td>
<td>Enterprise IT Integration</td>
<td>Migration Windows</td>
<td></td>
</tr>
<tr>
<td>Licensing</td>
<td>Problem History / Events</td>
<td>Vendor Presentations / Technology Update</td>
<td></td>
</tr>
</tbody>
</table>

The next phase “Requirements Elicitations” focuses on identification of the requirements for the new SCADA system. The term requirements elicitation referring to the fact that requirements are not “out there to be collected by simply asking the right questions”, but that “the information gathered … often has to be interpreted, analysed, modelled and validated” (2) and last but not least all involved stakeholders have to agree on the final set of requirements.

As shown in

Figure 2 four major fields for elicitation of requirements can be identified:
Technology Review

It is of high importance for the project’s success to gain a common understanding of typically available features of current SCADA systems, as well as of limitations in order to get a common understanding of the solution space. To this end stakeholders update their technology know how e.g. via vendor or integrator presentations, focus presentations or similar.

In case multiple comparable technologies are available on the market already now high level comparison studies can be executed - in order to identify the stake holders real requirements, which may diverge from the requirements as stated before the study.

When the pipeline does not have its own communication facilities, the market for reliable data communication services available at the various pipeline sites should be scanned.

Special focus should be given to typical features of development tools or engineering work stations, software maintenance and licensing approaches, as these concepts can influence the total lifetime cost considerably depending on system extensions or changes.

Brownfield Analysis

Since the various parts of SCADA and control systems have different life cycles typically some parts of the system can be reused, if their expected remaining useful life time is in a reasonable range.

To identify those parts that can be reused the integrity status of all equipment needs to be analyzed including failure rates, typical problems, spare part availability, software maintenance and development tool availability as well as spare capacity for potential new features. Besides other aspects this will be important information for specification of the Revamp boundary that separates those systems which have to be replaced from those that have to be interfaced.

Next the as-built documentation including operation and control philosophy for the main system and all subsystems, functional design specification, interface descriptions, operation manuals and etc. have to verified and updated in order to reflect any undocumented functional and procedural changes.

The latest status of actual operation including roles, command power handling, operation mode, utilization and deficits of automatic procedures, maintenance procedures and work order handling, reporting and planning should be documented and reflected with task monitoring and interviews. Of course this includes also any interfaces to the enterprise IT.
Optimization potential can often be identified easily, when the functionality of the existing system and procedures are translated to the new solutions becoming available with new SCADA and control technology.

The SCADA and control system most likely is not the only equipment that needs revamp or undergoes modification or extension in an aging pipeline system. These plans should be identified and considered throughout the revamp project where possible and often can be used also to identify potential SCADA migration windows.

All of these works will include site visits and these should be used intensively to interview the operation and maintenance staff at the equipment they operate or maintain and the documentation they use and notes at hand - independently of their management.

*Stakeholder Interviews*

As with any software oriented project it is of high importance to identify all stakeholders from management, accounting, purchase department, company strategy, operation, maintenance etc. and to involve them in the project, where suitable.

While during a revamp project most actual control requirements can be derived during the Brownfield analysis, stakeholders need to be involved in order to identify the current needs, targets and business requirement based on which the project will be judged to be successful.

Various interview methods have been described in requirements engineering literature (e.g. (2)). Methods for structured and unstructured interviews with individual persons or in groups have been proposed and tested in different configurations. It depends on the individual company’s communication culture, its organization and focus on strategy, which of those methods or which combination should be applied.

Of course any current and foreseeable changes regarding the controlled pipeline process, batch planning, operation and maintenance procedures, reporting, enterprise software integration and other reorganizations such as the centralization of control centres need to be identified. Only then they can be considered in addition to the existing SCADA system’s configuration.

Known problems or deficits of the SCADA and control system should be identified as well as any workarounds, which often can be resolved easily in a new system. The same is true for updated operation procedures or for the integration of spreadsheets that have been developed for reporting and planning purposes.

All optimization potential identified during the Brownfield analysis should be verified during these interviews in order to identify those items that need to be kept as is due to stakeholder request.
Finally any innovative features or requirements proposed by consultants need to be verified with the stakeholders.

**Compliance**

Compliance for pipeline systems transporting hazardous liquids or gases typically is regulated in various country specific laws, standards and regulations. Although resulting often into the same or very similar technical solutions these regulations may differ considerably in detail.

In consequence it is essential to analyze, by how far the SCADA revamp might influence the operation permit, which additional requirements will have to be fulfilled or if any authorities have to be involved or re-tests and re-certifications to be considered.

Due to the high number of relevant standards, which in several cases do not provide clear instructions, it is of high importance to document the design and decision process for individual items for later auditing or investigations in case of any accidents (3).

Compliance is not technology only and requires in many cases creation of plans for specific situations or periodic management of certain features. Where possible it should be considered to support these procedures, checks etc. with SCADA or enterprise software appropriately.

During Brownfield analysis the Revamp boundary between equipment that has to be replaced or modified and equipment that has to be interfaced was drawn a first time. Now, in case new compliance requirements become applicable due to the SCADA Revamp, a gap analysis of the existing system has to be executed. Only that way it can be ensured that the boundary is correct or if additional equipment has to be considered part of the SCADA revamp project since it does not fulfil the new requirements and thus is not reusable.

**Agreeing on Requirements**

In order to prepare the next step “Agreeing on Requirements” the list of requirements generated so far needs to be sorted, to be aggregated, any contradictions to be shown and missing items to be identified. Next the requirements should be initially classified and prioritized in order to create starting points for discussion and the basis for decisions of the stakeholders.

For several requirements it may not be possible to decide, if they should be included, since side effects are expected or financial aspects need to be clarified.
In these cases basic engineering of the revamped solution is required, together with a value engineering approach (4) and maybe re-discussion of the of requirements.

From the beginning this approach shifts focus from replacement of equipment towards identification of additional requirements that might improve the SCADA revamp business case and thus the value of the resulting system for its owner.

3. SCADA Safety

When the National Transportation and Safety Board published its Safety Study on involvement of SCADA and controllers in liquid pipeline accidents (5) in 2005 it became clear that in various cases SCADA systems and controller interaction contributed to the evolution of the accidents or increased caused by the pipeline accidents.

To overcome these problems NTSB recommended improvements in the areas of display graphics, alarm management, controller training, controller fatigue and leak detection systems.

Subsequently API published new recommendations for pipeline SCADA HMI design (6), alarm management (7) and control room management (8) which are enforced in the U.S. via PHMSA, so that regulated pipeline operators have to proof their compliance in audits.

As another example the German technical rules for transmission pipelines (9) extended its requirement for Leak Detection Systems to nontransient operation scenarios.

4. SCADA Security

It was a long time ago, when SCADA security could be provided simply by obscurity of proprietary communication protocols. On contrary modern SCADA systems are based on of the shelf hard- and software with standard compatible Ethernet/IP-communication equipment and thus are susceptible to cyber attacks, just as any other networked computer system.

Even a completely isolated SCADA system thus needs protection against attacks from insiders. The danger increases, when the SCADA system is connected to enterprise networks (e.g. to interface any enterprise business applications). Due to the flexibility and connectivity needed in enterprise networks more insiders may become active, more different software packages and computer equipment are interconnected and usually there are connections to the internet.
However, while the compatibility to the internet technology creates parts of the problem, basically the same security mechanisms as developed for the internet and IT world can be applied for SCADA - with a few deviations for consideration of availability and real time requirements.

When 9/11 made it clear that SCADA systems of critical infrastructure might be targets for cyber attack various organisations developed security standards for SCADA systems such as API (10), ISA (11), NERC CIP, AGA (12) and these have been accompanied by government agencies recommendation in several countries (e.g. (13), (14)).

It is important to understand that these specifications do not specify one specific security solution that has to be implemented, but provide guidance and requirements for assessing security risks, designing security solutions and security procedures including necessary training. This is due to the risk based approach that tries to identify risks and to find protection mechanisms against these risks in order to balance cost of a solution versus the actual risk.

Of course SCADA cyber security does not help without physical security - thus during a SCADA revamp also prevention of unauthorized physical access should be analyzed.

Based on the above clarifications it becomes clear, that any state of the art SCADA revamp projects needs to implement SCADA security, if whole system shall not be at risk.

5. Conclusion

Even when a SCADA revamp is originally caused by spare parts unavailability and increasing equipment failure rate, the project focus should not be on equipment replacement. The focus should always be on identification of the current stake holder requirements and targets, on optimization potential identified during the Brownfield analysis and fulfilment of any compliance requirements. A systematic SCADA revamp approach has been described in order to achieve this goal.

Literature


6. API 1165 - Recommended Practice for Pipeline SCADA Displays.

7. API 1167 - Pipeline Alarm Management.

8. API 1168 - Pipeline Control Room Management.


13. 21 Steps to Improve Cyber Security of SCADA Network. s.l. : Department of Energy, USA.