

SCADA UPGRADE POTENTIALS

**JOCHEN FRINGS, ILF CONSULTING ENGINEERS,
GERMANY, SHOWS THE OPPORTUNITIES IN A
SCADA REVAMP AND HOW TO SEIZE THEM.**



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.

The decision for a revamp is often made due to equipment failures and the focus of the project hence becomes primarily on time- and cost-efficient replacement of the controllers, communication equipment, servers and workstations only. Due to years of operation, the software on the other side has typically been debugged, leaving only a few minor issues, working around which becomes routine for the operators. There is often the desire to minimise 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.

Although this approach might seem to be quite sufficient, in reality this often results in large and inefficient code, which in the end is difficult to maintain for the next 15 years – the average expected lifetime of most SCADA and control systems.¹

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 identifying and adapting 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 article.

As examples for changing regulatory requirements and state-of-the-art advancements, an overview on recent developments in SCADA operation safety and SCADA security will also be given.

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 system's 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 on between stakeholders.

The next phase, 'Requirements Elicitations', focuses on identification of the requirements for the new SCADA system. The term 'Requirements Elicitations' is referring to the fact that requirements are not "out there to be collected by simply

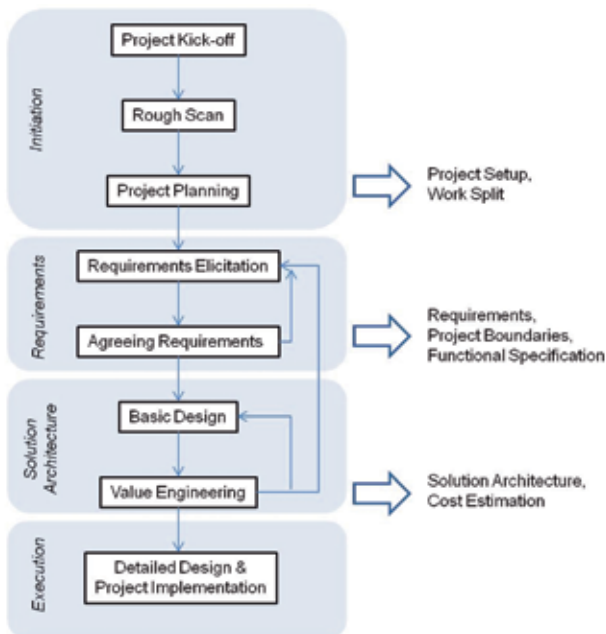


Figure 1. Systematic SCADA revamp method.

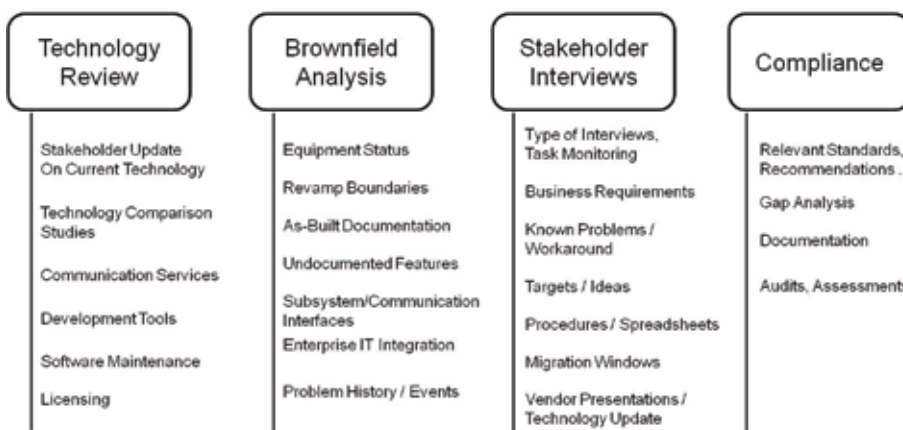


Figure 2. Requirements elicitations.

asking the right questions”, but that “the information gathered ... often has to be interpreted, analysed, modelled and validated” and last but not least all involved stakeholders have to agree on the final set of requirements.²

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, high level comparison studies can be executed – in order to identify the stakeholders' 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 workstations, 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 lifecycles typically some parts of the system can be reused, if their expected remaining useful lifetime is in a reasonable range.

To identify those parts that can be reused, the integrity status of all equipment needs to be analysed, 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, etc. have to be 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, utilisation 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 also includes any interfaces to the enterprise IT.

Optimisation 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 ageing pipeline system. These plans should be identified and considered throughout the revamp project where possible and can often be also used 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 requirements, based on which the project will be judged to be successful.



Figure 3. A SCADA revamp can improve insight to process and operation.

Various interview methods have been described in requirements engineering literature.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 organisation 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 reorganisations such as the centralisation of control centres need to be identified. Only then can they 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 can often 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 optimisation 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 is typically regulated in various country specific laws, standards and regulations. Although often resulting in the same or very similar technical solutions, these regulations may differ considerably in detail.

In consequence, it is essential to analyse, 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 need 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 safety and security events.³

Compliance is not only technology oriented 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 in this way can it 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 is therefore not reusable.

Agreeing on requirements

In order to prepare the next step 'Agreeing on Requirements' (Figure 1), the list of requirements generated so far needs to be sorted, aggregated, any contradictions shown and missing items identified. Next, the requirements should initially be classified and prioritised in order to create starting points for discussion and the basis for stakeholders' decisions.

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 and maybe re-discussion of the of requirements.⁴

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.

SCADA safety

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

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

Subsequently, API published new recommendations for pipeline SCADA HMI design, alarm management and control room management, which are enforced in the US via PHMSA, so that regulated pipeline operators have to prove their compliance in audits.^{6,7,8}

As another example, the German technical rules for transmission pipelines extended its requirement for leak detection systems to nontransient operation scenarios.⁹

These are only a few examples for the ever evolving state-of-the-art upgrades in SCADA and control systems to be considered during the SCADA revamp.

SCADA security

A long time ago SCADA security was assumed to be provided simply by obscurity of proprietary communication protocols. Today, modern SCADA systems are based on off-the-shelf hardware 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 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.


The tragic events of 9/11, 2001 led to reconsideration of risk assessments for critical infrastructure and it became clear that SCADA systems might be targets for cyber attack. In consequence, various organisations developed security standards for SCADA systems such as API¹⁰; ISA¹¹; NERC CIP; AGA¹²; and these have been accompanied by government agencies recommendation in several countries (e.g. in the US¹³ and Germany¹⁴).

It is important to understand that none of these specifications require a specific security solution 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 rapidly evolving technology for attacks and countermeasures and a risk-based approach trying to balance risk versus cost of risk mitigation.

Of course, SCADA cyber security does not help without physical security – therefore during a SCADA revamp, prevention of unauthorised physical access should also be analysed.

Based on the above for any state-of-the-art SCADA revamp project it is a must to implement SCADA security, if the whole system shall not be at risk.

Conclusion

Even when a SCADA replacement actually has to be initiated due to spare parts' unavailability or increasing equipment failure rate, the focus should not be on equipment replacement. As shown, a SCADA revamp gives the opportunity to identify and satisfy current functional and nonfunctional requirements including efficiency, safety and security considerations. Seizing this opportunity means to improve the overall business case, as well as the operational safety and security of the entire plant. 

References

1. BURTON, M., 'The Ideal Migration Strategy', *ISA Automation Week* (2011).
2. NUSEIBEH, B. and EASTERBROOK, S., 'Requirements Engineering: A Roadmap', *Proceedings of the Conference on The Future of Software Engineering* (New York: ACM, 2000).
3. BODUNGEN, C., WHITNEY, J. and PAUL, C., 'SCADA Security, Compliance and Liability – A Survival Guide', *Pipeline and Gas Journal*, Bd. 236, 9 (2009).
4. WALK, T., 'Value Engineering Approach to increase Cost Efficiency', 7th Pipeline Technology Conference, Mainz : *EITEP - Euro Institute for Information and Technology Transfer in Environmental Protection* (2012).
5. National Transportation Safety Board, *Safety Study: Supervisory Control and Data Acquisition (SCADA) in Liquid Pipelines* (Washington D.C., 2005) NTSB/SS-05/02, PB2005-917005, Notation 7505A.
6. API 1165 – *Recommended Practice for Pipeline SCADA Displays*.
7. API 1167 – *Pipeline Alarm Management*.
8. API 1168 – *Pipeline Control Room Management*.
9. Technische Regeln für Rohrfernleitungen. s.l. : Bundesministerium für Umwelt, Natur-schutz und Reaktorsicherheit (2010).
10. API 1164 – *SCADA Security*.
11. ANSI/ISA-99, 'Security for Industrial Automation and Control Systems', *International Society of Automation* (2007).
12. AGA Report No. 12: *Cryptographic Protection of SCADA Communication* (2006).
13. Department of Energy, USA, *21 Steps to Improve Cyber Security of SCADA Network*.
14. Informationstechnik in der Prozessüberwachung und -steuerung: Grundsätzliche Anmerkungen. s.l. : Bundesamt für Sicherheit in der Informationstechnik (2008).