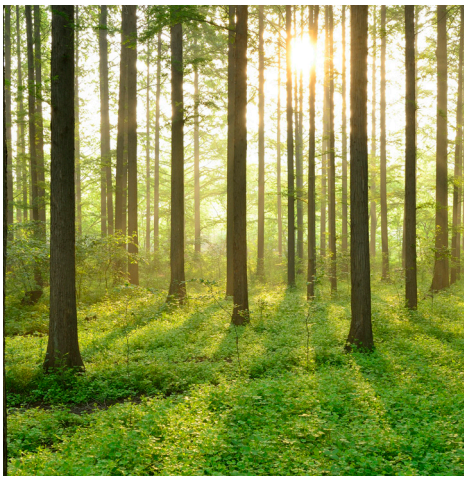
UPGRADE STRATEGIES FOR DIGITAL I&C SYSTEMS

REPORT 2019:622



NUCLEAR

ENERGIFORSK NUCLEAR SAFETY RELATED I&C – ENSRIC

Energiforsk

Upgrade Strategies for Digital I&C Systems

FREDRIK BENGTSSON AND JOHAN SLOTTE

ISBN 978-91-7673-622-7 | © Energiforsk October 2018 | Cover photo: Annika Adler Örnborg

Energiforsk AB | Phone: 08-677 25 30 | E-mail: kontakt@energiforsk.se | www.energiforsk.se

Foreword

Computerized I&C systems often require upgrades or new software versions regularly, for example due to software components that no longer can be supported, safety threats etc. This means that the utilities can be forced to make modernizations or system upgrades even though the actual system and its implemented plant function itself is working well.

Facilitating these upgrades at the plant will mean spending both money and labor and will eventually drive cost for the utilities. Therefore, it is important to find the optimal way and frequency to do these upgrades, taking into account both production cost and plant safety.

In hits study, we have investigated different strategies to cope with these types of upgrades within the Nordic nuclear industry and compared with how other nuclear countries and other types of industries are managing the situation.

The project was carried out by ÅF with the following participants: Mikael Esberg, Sebastian Blom, Rikard Andersson, Johan Slotte and Fredrik Bengtsson. The activity is included in the Energiforsk Nuclear Safety Related Instrumentation and Control program – ENSRIC. The project is financed by Vattenfall, Sydkraft Nuclear/Uniper, Teollisuuden Voima Oy (TVO), Fortum, Skellefteå Kraft, Karlstads Energi and the Swedish Radiation Safety Authority.

Sammanfattning

Moderna I&C system har ofta digitala komponenter och/eller mjukvara som innehåller applikationer som måste uppgraderas. Detta innebär att industrin tvingas till uppgraderingar även om systemet och dessa anläggningsfunktion fungerar som tänkt.

Denna studie har undersökt olika strategier och hur problematiken hanteras inom kärnkraftbranschen men också jämfört med andra branscher.

Kärnkraftbranschen har från början inte blandat process IT (OT) med administrativ IT (IT). Det har funnits strikta regler gällande kommunikation mellan dessa system. Dessa krav och standarder har inneburit att kärnkraftverken har en robust struktur. Säkerhetssystemen är utvecklade enligt strikta regler som innebär att de oftast har dedikerade operativsystem och applikationsprogramvara.

I&C systemens arkitektur kan inverka på deras behov av uppgradering t.ex. virusdefinitioner, mjukvaruuppdateringar etc. men eftersom kärnkraftverkens arkitektur är robust uppbyggd är dessa system inte så sårbara. Kärnkraftverken har också ett fysiskt skydd med strikt tillträdeskontroll.

Inom kärnkraftbranschen är det vanligt att köra systemen så länge som möjligt med endast mindre uppgraderingar – nollalternativet. Men detta kräver ändå att kärnkraftverken har en god systemkännedom, följer upp fel och analyserar grundorsaken till inträffade fel, följer leverantörens information och rekommendationer.

Denna studie har också identifierat att I&C system uppbyggda med Windows har en kortare livslängd innan uppgraderingar är nödvändiga. Detta är något som leverantörer av operativsystem insett och de erbjuder nu operativsystem med längre livslängd.

Erfarenhet från annan industri pekar på att man följer rekommendationer från leverantörer gällande uppgraderingar och undviker specialutvecklade applikationer Detta innebär att kommande uppgraderingar blir enklare och kräver mindre testning. Trenden är att nyttja ”golden version” som innebär att tiden mellan uppgraderingar kan utökas.

Men att hitta den gyllene strategin för uppgraderingar är inte möjlig eftersom detta bygger på anläggningarnas övergripande strategier – hur många år till skall man vara i drift. Livscykelkostnaden beror på systemets status, tillgänglig kompetens och att det är möjligt att bibehålla kompetensen samt tillgången på reservdelar. Denna analys är systemspecifik och måste hållas uppdaterad under systemets livslängd.

Summary

Modern I&C systems often incorporate digital components and/or software that contains applications that requires upgrades or new software versions on a regular basis. This means that the utilities can be forced to make modernizations or system upgrades even though the actual system and its implemented plant function itself is working well.

This study has investigated different strategies about how to cope with these types of upgrades within the Nordic nuclear industry and compare to how other nuclear countries and other types of industries are managing the situation.

The Nuclear Industry has from the beginning not combined process IT (OT) and administrative IT (IT). There have been strict rules regarding communication between these systems. Requirements and standards for nuclear industry have meant that they have a robust structure. The safety systems are developed according to strict rules, which means that they usually use dedicated operating systems and application SW.

A system's architecture can affect the need for upgrading due to for example cybersecurity, software updates etc. but since the nuclear power plant has a more robust structure, they are not so vulnerable to this. The nuclear power plant also has their physical protection which provides strict access control.

One common approach within the nuclear business is to run the system as long as possible with just minor changes - ”Do nothing” strategy. But this still requires that the utility have control of the system status, follow up faults and analyze root cause, follow the vendor's message and evaluate their recommendations.

This study has also identified that an I&C system that is built up with a Windows platform has a shorter lifetime before upgrades are needed. It seems that operating system suppliers have realized this, and they are now providing operating systems with longer lifetime.

Based upon our experience from other industry the trend is to follow suppliers recommendation regarding upgrades and avoid special own developed application, which will make the upgrade easier and avoiding some of the V&V effort. The trend is also to try to use “golden version” which “stretch” the timeframe between upgrades.

But to find a general golden strategy will not be possible since Life cycle cost will depend on the powerplant overall strategy – how many years remain to operate. The life cycle cost also depends on the system status, if there is enough competence and that the competence will be possible to maintain and if there are spare parts available in case of failure. This analysis will be system specific and need to be maintained during the system lifetime.

List of content

1 Introduction

1.1 PROBLEM AND BACKGROUND

Modern I&C systems often incorporate digital components and/or software that contains applications that requires upgrades or new software versions on a regular basis. The cause for the upgrade could be that some software component in the system no longer can be supported, that a safety threat in the current software version has been discovered, that the Operating System and/or the hardware is obsolete or new requirement on the I&C system etc. This means that the utilities can be forced to make modernizations or system upgrades even though the actual system and its implemented plant function itself is working well. Facilitating these upgrades at the plant will mean spending both money and labor and will eventually drive cost for the utilities. Therefore, it will be important to find the optimal way and frequency to do these upgrades, taking into account both production cost and plant safety.

1.2 OBJECTIVE

Investigate different strategies about how to cope with these types of upgrades within the Nordic nuclear industry and compare to how other nuclear countries and other types of industries are managing the situation.

1.3 DEFINITIONS AND ABBREVIATIONS

ASIC	Application-Specific Integrated Circuit
Attack surface	The sum of the different points (the "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment. Keeping the attack surface as small as possible is a basic security measure.
Cloud solution	On-demand availability of computer system resources via the Internet, especially data storage and computing power, without direct active management by the user.
COTS	Commercial-off-the-shelf
DCS	Distributed Control System
ENSRIC	Energiforsk Nuclear Safety Related I&C
FPGA	Field-Programmable Gate Array

Golden Version	These are bigger upgrade packages which will be released more rarely and includes operating system together with supplier's system software. Each supplier has their own naming for this type of upgrade and in this study the name "Golden Versions" has been used.
Hardening	In the context of this document: the process of securing a system by reducing its attack surface.
Hardened	In the context of this document: a system with a reduced attack surface.
HW	Hardware
I&C	Instrumentation and Control
IC	Integrated Circuit
IT	Information Technology
LCC	Life-Cycle Cost: the total cost of a system or equipment during its whole lifetime. Can be used when comparing different investments. The most common way to calculate total cost in the manufacturing industry.
NPP	Nuclear Power Plant
NPV	Net Present Value: the difference between the present value of cash inflows and the present value of cash outflows over a period of time. NPV is used in capital budgeting and investment planning to analyze the profitability of a projected investment or project
OLE	Object Linking and Embedding
OPC	"Open Platform Communications". Earlier the abbreviation was defined as "OLE for Process Control", where OLE means "Object Linking and Embedding"
OPC-UA	OPC Unified Architecture
OT	Operational Technology
PLC	Programmable Logic Controller
Private Cloud Solution	On-demand availability of computer system resources via internal network, especially data storage and computing power, without direct active management by the user. The data storage is controlled by the owner e.g. NPP.
Removable media	Computer data storage designed to be inserted and removed from a system, e.g. optical discs, USB flash drives etc.

SvKFS	Regulations from Svenska Kraftnät (Svenska Kraftnäts författningssamling)
SW	Software
TCO	Total Cost of Ownership: financial estimate to help buyers and owners determine the direct and indirect costs of a product or system. Includes procurement costs as well as operational costs. Resembles LCC but puts more emphasis on indirect costs and is mostly used within computer/IT-industry.
TCP/IP	Transmission Control Protocol/Internet Protocol
Thin client	Lightweight computer with a remote connection to a server-based computing environment, where the server does most of the work.
TVO	Total Value of Ownership: a methodology of measuring and analyzing the business value of an investment. TVO differs from TCO in that TVO considers the benefits of alternative investments.
V&V	Verification and Validation
Virtualization	Creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources. In "hardware virtualization" or "platform virtualization" a virtual machine is created, acting like a real computer with an operating system. Software executed on a virtual machine is separated from the underlying hardware resources.

2 Methodology

This study is broken down to identifying upgrade strategies, finding main drivers for upgrades, looking at trends in the industry and if different system setup influence upgrades. This work is based upon experience within the project group, based upon several years of working with I&C systems both in the nuclear industries but also from other industries. Chapter 3, 4, 5 and 6 cover these areas.

Chapter 7 discusses V&V different approaches based upon experience.

Chapter 8 discusses Life Cycle Cost perspective and here Internet research has been the basis.

Chapter 9 and 10 discuss upgrade strategies outside the Nordic Nuclear power plants and other industries. Interviews are basis for these chapters.

In chapter 11 the conclusion from this study is presented and chapter 12 discusses recommendations for further work.

3 Different Upgrade Strategies

There are different upgrade strategies that could be utilized independent of the system setup. This section describes the different strategies one by one and in section [3.5] a comparison is provided.

3.1 DO NOTHING – "ZERO ALTERNATIVE"

In this strategy there could be different types or grades of doing nothing or "Zero alternative"

- Do nothing and run to the system fails
- Maintenance alternative where failed components are replaced with identical or compatible parts, spare parts are either stocked or purchased or the different maintenance approach described in earlier ENSRIC publications are used (7R) – see reference [12]

This strategy is quite common for non-safety applications and requires that the utility has a good maintenance strategy regarding system status, spare parts handling, competence and seeking information from around the world.

3.2 "GOLDEN VERSIONS" APROACH

This strategy follows the recommendations and upgrade plans from the system supplier. These are bigger upgrade packages which will be released more rarely and include operating system together with suppliers' system software.

Each supplier has their own naming for this type of upgrades and in this study the name "Golden Versions" has been used.

3.3 "ACTIVE" UPGRADE APPROACH

This strategy follows every release from the system supplier. These are smaller upgrade packages which will be released more frequently and include operating system and security patches and updates from suppliers. The system will get benefits of new system functions.

3.4 "PASSIVE" UPGRADE APPROACH

With this approach the system has not been updated for a longer period and supplier has released extensive software versions. When an upgrade is performed this could mean a quite big step and often go from one version and skip some or several versions in between. The new version could include new features and a different user interface.

3.5 STRATEGY COMPARISON

This section discusses the different strategies and lists pros and cons for each strategy.

Strategy	Pros	Cons
"Zero alternative"	• Low cost • Stable system – the system has been running and probably will run for long time • Minimize system downtime	• A fault could require a long system downtime • Forced to replace/upgrade within short time • Limited lifetime • Limited expandability • Dependent on spare parts • Require good System health check • Competence fade out
"Golden versions" approach	• System continually up-to-date including the most important security patches • Avoiding costly and time-consuming major system retrofits or upgrades	• Could have impact on end-users (maintenance, operators) • Cost
"Active" upgrade approach	• Always up to date with all patches including security patches • Support for new functions and new hardware	• First users of patches which could have problems that has not been detected and could cause system problem and affect system availability • Requires resources – time and money
"Passive" upgrade approach	• Minimized system downtime over time	• Might require that the upgrades must be done in several steps – via the different software versions. • Might require different technology • Competence might be hard to find for unique "in between versions" for example display upgrades. • High upgrade cost – but few occurrences • Higher risk for system downtime close to investment

4 Main Drivers for upgrade

The identified main drivers are listed below, together with measures to minimize the impact of a certain driver. The drivers are divided into two groups:

A. To safeguard the operation of the plant

B. Financial or technical importance, but no direct threat to the operation of the plant

4.1 GROUP A: TO SAFEGUARD THE OPERATION OF THE PLANT

4.1.1 System reliability

Unclear availability, difficulty of forecasting system status.

This driver could be minimized by the following measures:

- Predictive/proactive maintenance
- Objective system health check/analysis
- Upgrade although system is still running OK

4.1.2 Impossible to find spare parts (HW)

Computer Hardware could be a driving factor for upgrades. When spare parts are not available and the only solution is to install newer hardware, this could force users to upgrade.

According to Ref[2], one of the main drivers for upgrades or replacements is the policy of system and component manufacturers to develop new products and end the sales and support of existing products. Upgrades or replacements are thus not performed because of system degeneration, but instead because spare parts can't be purchased, neither physical components (e.g. IC) nor software.

This driver could be minimized by the following measures:

- Using virtualization, see section 5.1 and/or emulation, see section 5.4]
- Predictive/proactive maintenance, spare parts strategy

4.1.3 IT/Cyber security

The general design of the system may make it vulnerable for cyber security threats. Critical or highly necessary IT/Cyber security patches should be applied to the system software in order to reduce vulnerability.

This driver could be minimized by the following measures:

- Ensure that the relevant standards and recommendations have been applied to the system design from the beginning, see Appendix A:.

4.1.4 Competence (HW+SW)

According to Ref[2], lack of competence in existing systems is an important challenge for a plant organization. Elderly competent staff retire, and younger employees may not be interested in becoming experts on old systems. A system may become a "black box" where no one understands neither the internal function nor the connections to other systems.

This driver could be minimized by the following measures:

- Long term plan for knowledge transfer and staff training

4.2 GROUP B: FINANCIAL OR TECHNICAL IMPORTANCE, BUT NO DIRECT THREAT TO THE OPERATION OF THE PLANT

4.2.1 Maintenance costs

Maintenance cost of an existing system becomes unacceptable.

This driver could be minimized by the following measures:

- Predictive/proactive maintenance
- Upgrade although system is still running OK

4.2.2 Recommendations and upgrade plans from the I&C system supplier

The system supplier/manufacturer provides general recommendations and update plans which are expected to be followed by the plant owner in order to ensure a stable and reliable function of the system.

These recommendations and update plans should indicate whether there is a risk of a 'cumulative/accelerating obsolescence', i.e. the 'non-linear' added complexity of a future upgrade, when a critical number of intermediate 'small' upgrades have been neglected. For example, could the 'large' future upgrade be much more complex than the sum of the intermediate upgrades

4.2.3 New system functions/features desired (e.g. in Application SW)

New features, for example support for new communication protocols (Hart, Profibus, Profinet, IEC 61850, new libraries etc.), which are related to application software could also be a driver for upgrades.

4.2.4 Not possible to expand the system

Some characteristic of the system (e.g. number of I/O channels) needs to be expanded but is fixed and impossible to change.

This driver could be minimized by the following measures:

- At system design stage and during procurement, focus on system suppliers promoting open and expandable system solutions, try to avoid closed, 'monolithic' proprietary systems.

- In financial analysis, include the possibility of added costs of a proprietary solution in a TCO-analysis, and the possible savings of an open solution in a TVO-analysis (see section 8).

4.2.5 Operating system / system SW

The operating system is often one of the main drivers for upgrades, for example original supplier has stopped their support and customer are forced to upgrade.

This problem has been recognized and the solution could be to use a Golden Version.

See also section 5.3 that discusses trends regarding operating systems.

5 Current Trends in the industry

5.1 VIRTUALIZATION

Virtualization has been ongoing for several years in the industry and also in the nuclear business for non-safety applications. The current trend shows that virtualization will increase.

Today's hardware performance has the capability to host several servers or operating workstations in one single computer. The number of physical computers could be reduced which has positive impact on power consumption but also lowers the maintenance cost since there are fewer units to maintain.

When an I&C System is virtualized the dependence on specific hardware is eliminated which has been a driving factor for upgrades earlier.

Virtualization technology also supports redundant solutions which has a positive effect on the running time and system ability.

As the use of virtualization has expanded dramatically in the business and financial sector amongst others, many vendors are now providing the ability to take advantage of virtualization in the process industries. Virtualization can be used in many different systems to combine multiple server nodes onto a single computer. The total number of physical computers required in an installation is reduced significantly. This also reduces the required space for the computers, hardware acquisition cost for computers and cabinets, and the operating costs (such as energy costs).

The following are the benefits with use of virtual workplaces:

- Reduced room space requirements
- Reduced room power and cooling requirements
- Reduced room noise
- Fast replacement of thin client
- Ability to move virtual client to new hardware without reinstallation
- Standard installation of virtual machines
- Added security by setting up virtual client without USB
- Clients now in server room with cost effective remote solutions

Disadvantages with virtualization is that it can increase the complexity of the I&C Systems due to redundancy requirements and introducing an additional layer to support virtualization.

5.2 CLOUD SOLUTION

There is a possibility to run server applications via cloud solutions. But this solution needs to consider internet vulnerabilities and information security.

Private cloud solution could be one possibility to secure both internet and information security.

Cloud solutions are common and increasing within IT solutions but within industry solutions (OT) this is today very uncommon.

5.3 GOLDEN VERSION

Since the operating system is one driving factor for upgrades Golden Version could be the way for extending the time between upgrades. The system supplier selects one version of the operating system and keep support of the system suppliers' software during this time.

Long-Term Servicing Branch (LTSB) is a licensing option for Windows 10 Enterprise and is available only for customers with a Volume License agreement. Each LTSB release receives standard monthly security and reliability updates for an extended 10-year support period. No new features are added over its servicing lifetime.

Figure 1 below describe the lifetime of each LTSB/LTSC versions.

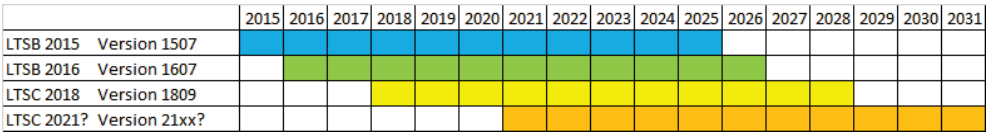


Figure 1

Microsoft officially discourages the use of LTSB outside of "special-purpose devices" that perform a fixed function such as I&C system, since these system do not require new user experience features. According to a Microsoft announcement, this servicing option was renamed from Long-Term Servicing Branch (LTSB) in 2016 to Long-Term Servicing Channel (LTSC) in 2018.

According to interviews and own experience's this is the trend for Windows based I&C systems.

5.4 EMULATORS + CURRENT SOFTWARE

Emulation as described in Wikipedia, "In computing, an emulator is hardware or software that enables one computer system (called the host) to behave like another computer system (called the guest). An emulator typically enables the host system to run software or use peripheral devices designed for the guest system. Emulation refers to the ability of a computer program in an electronic device to emulate (or imitate) another program or device."

In the context of this document, by 'Emulation' we mainly mean using a specific software to emulate/imitate a certain hardware/computer platform.

Old HW can be emulated in SW. It is especially server/computer HW which is emulated in this way. The goal for the end user is to avoid or to postpone an upgrade of the physical HW, and to continue to use an old, tried, tested and stable

version of the operating system (e.g. Microsoft Windows, Unix). It does not seem to be common to emulate a PLC/Controller, see Ref[2], Ref[3], Ref[7].

The continuous development of more powerful microprocessors and servers/computers facilitate the emulation/virtualization of more complex hardware. However, the emulation software itself is often tailor made and must be maintained to some degree, which may require either in-house software engineering skills or dependence on external resources.

Finally, old HW can be reconstructed or emulated in HW: obsolete microprocessors/IC can be reconstructed in ASIC:s or emulated in FPGA:s (Ref[8])

Emulation has been used within nuclear business but is probably not so common in other industries.

6 System setup

6.1 VARIOUS SYSTEM SETUPS

The following system setups have been identified:

- Standalone
- Standalone with Windows
- DCS system with Windows
- DCS system without Windows

6.1.1 Standalone

A standalone setup can be operated for a longer time without upgrade, compared to other setups.

Type of equipment: traditionally COTS HW and SW.

Operating system: not Windows.

Cyber Security: this setup also has a small attack surface and therefore a low need to upgrade.

6.1.2 Standalone with Windows

A standalone with Windows setup has an intermediate operation time without upgrade.

Type of equipment: traditionally COTS HW and SW.

Operating system: Windows

Cyber Security: this setup has an intermediate attack surface and thus some upgrading will be necessary. The system could be hardened by further reduction of the attack surface, e.g. by strict control of physical access to the system, restricted or completely prohibited use of removable media, etc.

6.1.3 DCS system with Windows

In a DCS system setup using Windows there is the highest need for upgrades compared to other system setups.

Type of equipment: mix of proprietary and COTS HW/SW. Non-proprietary equipment e.g. data communication networks based on Ethernet and TCP/IP, switches, routers, servers, workstations, displays etc.

Operating system: Windows

Cyber Security: this setup has a large attack surface and therefore rather frequent upgrading will be necessary. The system could be hardened by further reduction of the attack surface, e.g. by:

- restricted physical access to the system
- restricted or completely prohibited use of removable media
- restricted or completely prohibited connection to external systems, e.g. allowing only one-way data transfer from the system 'outwards'
- firewalls
- anti-virus software
- no connection to Internet

6.1.4 DCS system without Windows

A DCS system based on operating system other than Windows.

Type of equipment: mix of proprietary and COTS HW/SW. Non-proprietary equipment e.g. data communication networks based on Ethernet and TCP/IP, switches, routers, servers, workstations, displays etc.

Operating system: e.g. UNIX, Linux.

Cyber Security: this setup has a smaller attack surface than a DCS system with Windows, and thus less frequent upgrading will be necessary. Some hardening may still be necessary.

Ref[9] lists several reasons to use Linux in industrial applications, and Ref[10] may exemplify a trend of Linux-distributions specifically tailored to factory automation, e.g. Open Industrial LINUX, OpenIL.

6.1.5 Discussion

System setup

Regarding the system setup and type of equipment, it is obvious that a system using Microsoft Windows as operating system forces the user into repeated system upgrades, see Ref[2] Ref[5]. "The further from Microsoft one gets, the longer the equipment may stay", according to Ref[2].

Cyber Security depends on system setup/architecture and size and forces the user to upgrade in order to reduce the attack surface and keep it small.

6.1.6 Conclusion

The need for upgrade depends on which type of operating system that is used and the complexity of the system architecture. The most vulnerable system setup is a DCS system with windows as operating system.

7 V&V

This section discusses, based on the chosen strategy, the impact this has on V&V.

7.1 DO NOTHING – "ZERO ALTERNATIVE"

In the Zero alternative it's important to do a good life cycle analysis where it appears which annual controls of the system that needs to be done. This analysis should also contain continuous controls towards that the supplier in order to check for known issues in the current platform. It's important to do an evaluation of how much spare parts you need in stock and also to have continues follow-ups with the supplier about future production of spare parts.

7.2 GOLDEN VERSIONS, ACTIVE UPGRADE AND PASSIVE UPGRADE

The strategies Golden version, Active upgrade and Passive upgrade should be treated equally. Before the upgrade it's important to be aware what the upgrade contains. An analysis of the upgrade should first be made and it's a great advantage if the analysis includes the supplier's own analysis that handles their own type of circuits and known issues. The analysis should then result in a regression analysis that specify the parts of the software that will be affected by the upgrade, and how the upgrade affects these parts.

7.3 V&V IN SAFETY SYSTEM

Changes in safety system are controlled by IEC 60880 and IEC 62566. IEC 62566, issued 2012, emphasizes automatic test procedures. Automatic tests mean that future validation of software changes will be easier and safer as less human impact is involved in testing. This is an opinion that one should consider when doing the life cycle analysis and design test procedures for the I&C system.

8 Strategy from a Life Cycle Cost perspective

8.1 SMALLER UPGRADES FREQUENTLY, LARGE UPGRADES SELDOM?

In Ref[1] a TCO model is developed in order to find the optimal refresh/upgrade cycle for office computers. Although the focus is on office computers, not I&C/automation, the findings could still be applicable on servers in a DCS system.

Ref [2] (original, full report in Swedish) and Ref[3] (summary in English), analyze the concept of ageing and upgrades, and based on survey results, conclude that there are similar challenges in many different areas such as Water and sewer, Transport, Energy (district heating and gas distribution), Process industry. In a topologic model, the ”Information Level” (high) drives change request towards ”Automation Level” (middle), whereas the ”Field Level” (low) resists change request towards ”Automation Level” (middle). The critical goal for the plant owner is to retain the compatibility between the Automation and Field levels.

Ref [4] describes a case study at a hydro-electrical plant, where the obsolete equipment is similar to that found in some NPP:s, and the optimal upgrade strategy is determined using a cost benefit analysis (TCO) similar to the one described in Ref[1].

Ref [5] points out the life cycle of third-party COTS SW (e.g. operating systems from Microsoft) as a challenge. The following scenario may arise: the current OS version (e.g. Windows XP) becomes obsolete and is not maintained anymore due to Microsoft ”Planned Obsolescence” strategy and monopoly position in the market. The DCS is not compatible with new OS version (e.g. Windows 7), which forces the user to upgrade DCS to a version compatible with new OS. Finally, the current HW (server) is not compatible with new OS, user is forced to upgrade HW.

Ref [6] states that TCO is the preferred metric as it takes into account all relevant financial factors affecting the justification for a DCS upgrade or replacement. Another accurate financial metric is Net Present Value (NPV).

Ref [7] states that Windows-based servers and workstations have introduced new maintenance procedures that must be managed carefully, and that the migration to COTS brings the age of Microsoft and Internet to the plant floor. The reason to use COTS technology in plant automation systems is to reduce TCO and improve the level of system integration. However, the usable life of a COTS-based system will be rather short, 3-5 years on average. Sustainable technology becomes iterative and must be refreshed more frequently, i.e. an endless cycle of patches and SW updates to maintain system integrity.

In Ref[11] a Cost Breakdown Structure (CBS) together with a model and an operational template combining both TCO and TVO are developed to support analysis and financial investment decisions for industrial robots, which can be classified as a specific case of an automation system. It is specifically stated that an investment decision should be based on the TCO of the automation system, but also on which value the system creates, i.e. the TVO. TCO is a subset of LCC, i.e. TCO considers the life cycle cost of a system after purchase.

Ref[11] states that because of comparatively high labour costs in Sweden, automation systems are used in order to achieve fast and flexible production. The traditional factor affecting an automation investment is the initial cost of the automation system. Low price products are preferred because of a low initial cost, but successive costs are forgotten. A reason may be that the concept of ownership cost is not properly understood. The initial cost can be misleading from a life cycle perspective. If, on the contrary, the investment decision is based on the life cycle cost, it will include costs accumulated during the lifetime of the automation system, e.g. operation, maintenance, software, license costs, test, support, training, supply, warranty and retirement/disposal. These costs could add up to much more than the initial investment.

Ref[11] states that the total life cycle cost is not "visible", it could be pictured as an iceberg floating in the sea. Only the top (initial investment, purchase price) is visible above the surface, whereas the above-mentioned accumulated costs are hidden beneath the surface. Life cycle Costing can be used as a tool to 'look beneath the surface', i.e. to identify all costs and select the financially best alternative for the whole life cycle of the system. Life cycle Costing methods are successfully applied e.g. in the Swedish building sector and in the automotive sector.

8.1.1 Conclusion

"There is no single answer and probably no simple answer" Ref [8]. It is not possible to identify a general, simple, 'magic' strategy, which would be directly applicable for all plants.

Each and every plant is unique and must thus be analyzed thoroughly Ref[5]. This analysis must contain the technical perspective in close cooperation with the supplier of the currently installed DCS equipment, understanding the product life cycle and the obsolescence strategy of the supplier. But it is equally important to include the economical/business dimension of the plant by performing an analysis using tools like e.g. TCO- and TVO-analysis, Net Present Value (NPV) or similar, in order to minimize life cycle cost (LCC) Ref[4], Ref[6], Ref[8], Ref[11].

In the nuclear area, system *availability* is a value-adding factor to include in the TVO, whereas system *downtime*, maybe causing plant standstill, rapidly results in very large costs which should be assessed in the TCO.

Risks should also be included in the analysis, and the resulting obsolescence strategy can be either proactive or reactive Ref[5].

The actual upgrade can be either a 'rip and replace' which offers the possibility to choose a separate brand and supplier for the new DCS but with a higher risk of plant downtime, or a 'phased upgrade' which means a lower risk of plant downtime, but a more complex and time consuming upgrade project.

9 Upgrade strategies for Nuclear Business outside Nordic

9.1 HUNGARY

Interviews with ÅF internally.

Their situation is very similar to the Nordic nuclear powerplants.

Safety systems are digitalized and using a supplier propriety software developed according to nuclear standards.

They have similar strategy as in Nordic countries regarding I&C upgrades which is to make upgrades with as large timespan as possible and use “Golden Versions”.

10 Upgrade strategies for other safety critical industries

10.1 FOOD & PHARMA

Interviews with ÅF representative from food & pharma.

The situation is that they have systems that are Windows based and were originally installed for 20 – 25 years. During this period, they have continuously updated the system and followed recommendations from the supplier. Driving factors for upgrading has been application, operating system updates, hardware and cyber security.

Within a short period, their plan is to replace the systems with a new system.

10.2 OIL & GAS

Interviews with oil & gas representative.

The situation is that the plants have different process areas which are controlled by separate I&C systems. There is a plant overall DCS system for supervising and controlling of the entire plant. The different I&C systems are quite old and upgrades are needed. One of the driving factors for the upgrade is that there are no expansion opportunities and new features e.g. new communication possibilities.

The plant I&C strategy is to upgrade all systems to a common platform and follow a “Golden version” from the supplier.

Upgrades has been costly and time consuming and plants would like to go to more stable and reliable versions.

10.3 PULP & PAPER

Interviews with ÅF representative from pulp & paper.

The situation is that the plants have many different process areas which are controlled by different generation of controllers but they are integrated in the same I&C system. There is a plant overall DCS system for supervising and controlling of the entire plant. The oldest controllers are around 30 years and an upgrade is needed. The work to migrate the code to a new controller is ongoing and the plan is that every controller has to be replaced before 2030 when the support from the supplier is no longer possible. One of the driving factors for the upgrade are that there are no expansion opportunities and new features e.g. new communication possibilities.

The plant I&C strategy is to upgrade all systems to a common platform and follow a “Golden version” from the supplier.

Upgrades has been costly and time consuming and plants would like to go to more stable and reliable versions.

10.4 HYDRO

Interviews with hydro representative.

Hydro and nuclear have many similarities such that the process remains the same, produce electricity, which means that process enhancement is not a driving factor for this business.

The situation for hydro powerplants in Sweden is that they have several platforms installed and many of them are quite old. They have a strategy to update and modernize and also minimize the different platforms. Hydro power plants are located all over the country but are controlled from centralized location. The utilities are required to follow Svenska Kraftnät regulations for example SvKFS 2013:1. The centralized control means that they are more "public" and vulnerable for cyber-attacks compared to nuclear industry which are easier to protect with physical protection. Upgrades due to safety issues become more important to have installed shortly after supplier has issued them.

Their I&C strategy is to upgrade all systems to a common platform and follow a "Golden version" from the supplier. Upgrades should be made with as large timespan as possible without risking having to make a complete upgrade.

11 Conclusions

The Nuclear Industry has from the beginning not combined process IT (OT) and administrative IT (IT). There have been strict rules regarding communication between these systems. Requirements and standards for nuclear power have meant that they have a robust structure. The safety systems are developed according to strict rules, which means that they usually use dedicated operating systems and application SW.

A system's architecture can affect the need for upgrading due to for example cybersecurity, software updates etc. but since the nuclear power plants have a more robust structure, they are not so vulnerable to this. The nuclear power plant also has their physical protection which provides strict access control.

One common approach within the nuclear business is to run the system as long as possible with just minor changes - ”Do nothing” strategy. But this still requires that the utility have control of the system status, follow up faults and analyze root cause, follow the vendor's message and evaluate their recommendations. The older the systems are the more important this will be and also more difficult since the suppliers might have stopped their support and there are only few systems outside that are in operation. Competence will be important to maintain, and new people must be trained so they can continue to maintain the system. If it is possible to ally with other power plants, this is a good idea instead of being alone.

This study has also identified that an I&C system that is built up with a Windows platform has a shorter lifetime before upgrades are needed. It seems that operating system suppliers have realized this, and they are now providing operating system with longer lifetime (Golden version). This development will mean that upgrades could be less frequent and have impact on systems life cycle cost. But also for these systems it’s necessary to make individual system status analyzes and monitor system status.

Based upon our experience from other industry the trend is to follow suppliers recommendation regarding upgrades and avoid special own developed application, which will make the upgrade easier and avoiding some of the V&V effort. The trend is also to try to use “golden version” which “stretch” the timeframe between upgrades.

But to find a general golden strategy will not be possible since Life cycle cost will depend on the powerplant overall strategy – how many years remain to operate. The life cycle cost also depends on the system status, if there is enough competence and that the competence will be possible to maintain and if there are spare parts available in case of failure. This analysis will be system specific and need to be maintained during the system lifetime.

12 Recommendations

Based on our conclusions from this study and experience the following recommendations are provided:

- Try to use "golden version" which will "stretch" the timeframe between upgrades and follow the recommendations from system suppliers
- Secure that system is hardened - reducing its surface of vulnerability
- System health check
    - This is a work that is already done in the nuclear business but anyway this is so important to have a good control of system status, spare parts inventory, competence and seeking alliances with other users and suppliers that it's worth to highlight. Without this knowledge utilities might be surprised and forced to implement system upgrades with short notice.
- Cyber security
    - Follow cyber security threat and be up to date with what's going on
- Software
    - If possible, try to use the functions in the suppliers base software instead of requiring the supplier to develop specific functions to meet your requirements as such implementations will be very costly for future upgrades
- System Architecture
    - Keep the system architecture that is used within the nuclear business

13 References

1. Intel Information Technology: Using TCO to Determine PC Upgrade Cycles. White Paper, May 2009.
2. ”NCS3 – Gammalt är inte äldst”. En studie om synen på, och hanteringen av, åldrande inom området industriella informations- och styrsystem. Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet, Totalförsvarets forskningsinstitut. Vidar Hedtjärn Swaling, Fredrik Malmberg Andersson, Jonas Clausen Mork. September 2016. FOI-R—4292—SE, MSB 2015-6559, ISSN 1650-1942.
3. “Ageing ICS - What’s the Deal?”. An interview-based study on how ageing is regarded, and dealt with, in the area of Industrial Control Systems. Vidar Hedtjärn Swaling. Swedish Defence Research Agency (FOI). FOI Memo: 5821, October 2016.
4. Best approach to upgrading a distributed control system. Case Study: Kiira Power Station. Dissertation presented to the Engineering Institute of Technology, Mildred Nanono.
5. Obsolescence and life cycle management for automation systems. Recommended practice. International Association of Oil & Gas Producers (IOGP). Report 551, July 2016.
6. Justification for Migration. How to calculate financial justification for migration from an existing distributed control system to a new automation system. Mike Vernak and Tim Shope, Rockwell Automation
7. Managing Obsolete Technologies: Strategies and Practices. AEC Advisory Group, Peter Reynolds. December 2011.
8. Obsolecense and Life Cycle Management for Avionics. DOT/FAA/TC-15/33. U.S. Department of Transportation. Federal Aviation Administration. November 2015
9. Why is Linux Trending? https://www.automationworld.com/why-linux-trending
10. https://www.openil.org/
11. Life Cycle Cost Analysis in the Swedish Automation Industry. A Case Study for developing a Total Cost of Ownership Model for Industrial Robots. Steffen Landscheidt, Bachelor Thesis, Linnéuniversitetet, Faculty of Technology, Department of Mechanical Engineering, 2015.
12. Life time extension of present analogue I&C systems, Report 2015:159, Annika Leonard
13. https://assets.new.siemens.com/siemens/assets/public.1541967609.c24e45660b0cab1e827ad5557411825446548916.simatic-pcs7-lifecycle-services-en.pdf

Appendix A: Standards used for OT Security

- ISO 27000
    - ISO 27001 describes procedures
    - ISO 27002 describes more technical controls
        - Successor ISO 17799
- IEC 62443
    - Designed for Process Automation
    - Successor ISA 99
    - NERC CIP
- North American Energy Reliability Council / Critical Infrastructure Protect
    - www.nerc.com
- NIST
    - National Institute of Standards and Technology

UPGRADE STRATEGIES FOR DIGITAL I&C SYSTEMS

Is it possible to find an optimal general upgrade strategy for digital I&C system for Nuclear Power Plants? The answer is both Yes and No. This report discusses general recommendations and conclusions regarding upgrade strategies.

Based upon experience from other industries, the trend is to follow the supplier's recommendation regarding upgrades and avoid individually developed applications.

Finding a general golden strategy is however not possible, since the life cycle cost will depend on the overall strategy of the power plant. This analysis will be system specific and need to be maintained during the system lifetime.

Energiforsk is the Swedish Energy Research Centre – an industrially owned body dedicated to meeting the common energy challenges faced by industries, authorities and society. Our vision is to be hub of Swedish energy research and our mission is to make the world of energy smarter!

Energiforsk