Survey on international standards and best practices for patch management of complex industrial control systems: the critical infrastructure of particle accelerators case study

Ugo Gentile* and Luigi Serio

Engineering Department,
CERN,
Geneva, Switzerland
Email: ugo.gentile@cern.ch
Email: luigi.serio@cern.ch
*Corresponding author

Abstract: Industrial control systems (ICSs) are control and data acquisition systems employed to control distributed assets with a centralised data acquisition and supervisory control. ICSs strictly rely on computer-based systems and on installed remote controllers, which are subject to a constant patch deployment to upgrade functionalities, to resolve security issues and to reduce potential flaws. The patch management is not a trivial process since it can introduce new vulnerabilities within the systems. A key factor to perform successful patch management is to comply with the recommendations provided by the international standards and by the best practices currently adopted in the industry. This paper surveys the few existing international standards on patch management and the best practices, currently adopted in industry, and evaluates the relevance of standards and the best practices to the context of critical infrastructures for particle accelerators.

Keywords: industrial control systems; ICSs; patch management; critical infrastructure; particles accelerators; critical computer-based systems; international standards.

Reference to this paper should be made as follows: Gentile, U. and Serio, L. (2019) 'Survey on international standards and best practices for patch management of complex industrial control systems: the critical infrastructure of particle accelerators case study', *Int. J. Critical Computer-Based Systems*, Vol. 9, Nos. 1/2, pp.115–132.

Biographical notes: Ugo Gentile is a Post Doctoral Researcher in the Engineering Department at CERN (Geneva, Switzerland). He received his PhD in Computer and Automation Engineering at the University of Naples Federico II focusing on the verification and validation of safety-critical systems. His main research topics include the application of machine learning to complex industrial systems, the formal modelling of critical and complex systems, the application of model-driven principles to support the system development lifecycle and the application of ICT technologies to critical infrastructures. He has been actively involved in different international FP7 projects as MASSIF, CRYSTAL and SVEVIA.

Luigi Serio is Senior Staff and Group Leader in the Engineering Department at CERN (Geneva, Switzerland), Chairman of CERN's Technical Infrastructure Operation Committee and Senior Project Leader. He worked at CERN, ITER and JET Joint Undertaking in the accelerator technology and nuclear fusion fields. He Graduated from Politecnico di Milano (Italy) with an MSc in Nuclear Engineering and was awarded a PhD in Mechanical Engineering from Cranfield University (UK). He is a chartered nuclear engineer, radiation protection adviser and PMP. He has more than 100 papers in the field of nuclear and cryogenic engineering and technology, an international patent and two theses.

1 Introduction

Industrial control systems (ICSs) are a set of control and data acquisition systems employed in several domains to control distributed assets with a centralised data acquisition and supervisory control (Krutz, 2013). Several national critical infrastructures, as power, gas and water distribution, strictly rely on the correct functioning of the ICSs, which shall guarantee high levels of reliability and security. During the years, the growing complexity of the infrastructures monitored and the less connectivity of the ICSs, has also introduced new issues to be addressed, related to the cyber-security and the physical protection. A lot of academic and industrial efforts have been spent to identify the best technologies or the physical defence mechanisms to be adopted, to be less prone to failures which can compromise the control services provided. However, to the best of our knowledge, only a few of these works, explicitly address the topic of the patch management, which indeed is an essential activity for the functioning of the ICSs. Patch management is the process responsible for the identification, the installation, the scheduling and the verification of the patches to be applied to a system, to add new functionalities or to resolve vulnerabilities and issues. Despite the wide set of procedures for general purpose software systems (e.g., daily or weekly updates of operating systems), the patch management process has not been rigorously applied for a long time to the control systems, since, by design, they have been conceived to work in isolated networks, managed by expert personnel. A well-known event that began to raise awareness on the topic was the Stuxnet worm attack (Karnouskos, 2011) that, in 2010, affected several computer-based systems, including some supervisory control and data acquisition (SCADA) systems (Chen and Abu-Nimeh, 2011), showing the need to introduce proper countermeasures to preserve such systems. Recently, the Meltdown and Spectre vulnerability forced ICSs vendors to start a patching campaign quickly. However, due to the short implementation time, the patch release is now affecting in a significant way the performances of several ICSs (https://wonderwarepacwest.com/support/tech-news/important-tech-alert-287/). These are only a few examples but clearly show that, even when ICSs are based on proprietary solutions and network configuration, they are exposed to the limitations and vulnerabilities introduced by the architectures and the technologies available on the market. According to this, the patch management process is essential to guarantee the operation of ICSs and, it shall not be underestimated, but rather, it shall be continuously and proactively reviewed and enhanced in agreement with the existing international standards and with the successful experiences gathered in several industrial domains.

This work focuses on the definition of a workflow able to support the patch management process in the context of complex and critical infrastructures. The workflow definition has been done surveying international standards and industry best practices and gathering the relevant key points, coming from the review of such works. The workflow, therefore, has been tailored to the specific case of the technical infrastructure supporting particle accelerators. The particle accelerators technical infrastructure (TI) is a wide system of systems providing backbone services, as the electrical power, the cooling, and ventilation services, the access facilities and the communication network to allow the operation of highly technological and large distributed systems such as cryogenics and superconducting magnets, requiring a high level of reliability and availability. A problem occurring to the ICSs supporting one or more of the TI systems can jeopardise for several hours the running of experiments and can even cause, with the loss of the supervision system, additional problems and delays linked as an increasing reaction time for intervention inside underground tunnels and caverns, hosting the particles accelerators. To effectively manage the different ICSs in such a wide infrastructure, is essential to have a well-defined patch management process which clearly defines stakeholders roles and responsibilities, documents to be produced and exchanged and deployment and recovering procedures to be performed, before the application of a patch.

The paper is organised as follows: the next section provides a related work on the topic of workflow management. Section 3 surveys international standards and industrial works, explicitly addressing the topic of patch management for control systems. Section 4 defines a possible workflow, implementing the principles raised from the literature reviewed. Then, Section 5 discusses how to apply this workflow to existing ICS, in particular via a gap analysis addressing the relevant points to be reviewed in a supervision and control system, according to the principles emerging from the survey. Section 6 closes the paper with some final comments on the work.

2 Related work

To define a workflow for patch management in ICSs is an activity that usually belongs to the branch of the workflow management. Workflow management deals with the coordination of tasks and people to increase the effectiveness of given business processes such as patch management. Several works can be found within industrial and academic literature which focus on the topic, even if most of them address the problem by integrating a workflow management systems, exploiting the different solutions available on the market. Different domains can benefit from the introduction of workflow management: Yu and Buyya (2005) survey workflow management systems for GRID computing. In particular, the survey tries to identify the requirements that a workflow management system has to provide, in order to orchestrate the business process of a GRID computing system. Therefore, the authors identified weaknesses in workflow management to be addressed by further researches. Similar work is the one in Islam et al. (2012), in which a workflow management system is defined and developed to support the business processes of Hadoop, one of the widest infrastructures for the management of big data. Liu et al. (2015), indeed, provide a survey on workflow management systems for the management of business processes of data-intensive scientific workflows. Despite the rich literature, to the best of our knowledge, the topic of patch management has been widely addressed single software upgrades and mostly considering only the technical point of view. The work we propose, indeed, wants to investigate the problem of patch management in the context of ICSs of critical infrastructures, in which the technical point of view is just one perspective of the problem. Critical infrastructures are, in fact, wide systems of systems in which risks and stakeholders are higher than single systems and thus, there is a higher need to have defined processes based on strong information sharing (Rinaldi et al., 2001). According to this, we focus on international standards and industry best practices, providing a non-exhaustive list of them. Some other works, not analysed in this paper, focus on the adoption of standards in patch management. Laing (2012) dedicates a chapter of his book to the review of some real patch management industrial approaches. However, principles reported in that book are mainly based on the standards we have surveyed and, they are not summarised in a concrete workflow ready to be used. Zhu et al. (2011) focus on the information management of control systems and, concerning the patch management, it proposes a model to support the decision-making process that results in the choice of accepting or denying the patch deployment. The approach is useful for preliminary stages of patch management, but does not provide any indication other relevant aspects (e.g., how the stakeholders are informed, how the management is involved in the decision process, etc.). This makes not possible to adopt it as a reference guideline to evaluate current patch management workflows.

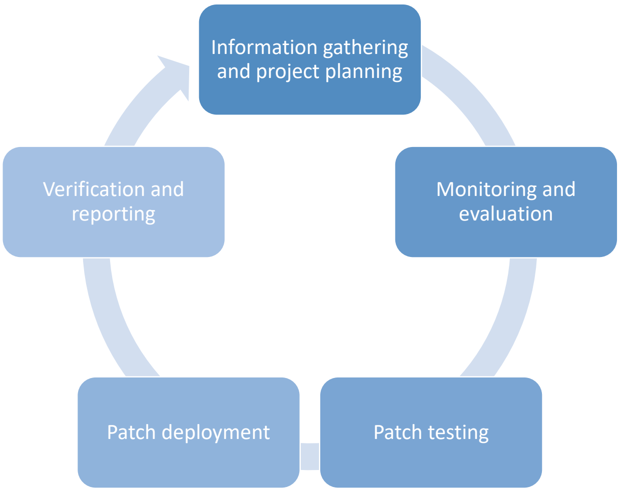
3 Standard an best practices for ICSs patch management

This section surveys the few international standards available, addressing explicitly the patch management process of the ICSs and the industry best practices found in the literature. The International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO), which are the most productive standard providers, address the topic of the patch management in the *ISO/IEC 27002* and the *IEC TR 62443*. The latter, in particular, is the reference standard adopted by the American Homeland Security best practices, described further in this section. The section will also describe the standards defined by the North American Reliability Council (NERC) and the National Institute of Standard and Technology (NIST) highly diffused in different critical contexts.

3.1 ISOIEC 62443

The IEC TR 62443 (IEC, 2015) the most diffused ICS reference standard in different application domains. It provides recommendations related to different aspects of an ICS, including the patch management processes, addressed in the part 2-3. The IEC 62443 provides the essential guidelines to put in place an effective patch management process reducing the risks of unexpected negative consequences. The workflow, suggested by the IEC 62443, is summarised in Figure 1. Below a brief description of each step is provided.

Figure 1 IEC TR 62443 patch management workflow (see online version for colours)


Information gathering and project planning
Monitoring and evaluation
Patch testing
Patch deployment
Verification and reporting

3.1.1 Information gathering

During this step, ICS assets shall be inventoried, including information related to communication interfaces, assets dependencies, software, hardware and the firmware versions of the last updates. An updated inventory can allow identifying assets that may fail during or after the patch deployment. Once the information gathering is completed, is possible to define the project planning, which serves as an interface with the enterprise management that has to authorise or deny the patch deployment. The project planning includes:

- The definition of the business case listing benefits of the patch to be applied, the costs and the possible effects in term of provided system downtimes, expected quality and time to recover in case of failures.
- The role of each stakeholder involved in the patching process.
- The description of the testing environment.
- The backup and restoration plan which is mandatory when patch management is performed for ICSs belonging to critical infrastructures. Moreover, the standard recommends a continuous and planned backup activity of assets software and firmware, to have ready-to-restore versions in case of problems.

3.1.2 Monitoring and evaluation

The monitoring and evaluation phase is responsible for the acceptance or the refusal since it focuses on the applicability evaluation. A patch is automatically applicable if the following requirements are satisfied:

1 the patch has been approved by the vendor/manufacturer

2 the patch has been designed and released for the considered asset with the current firmware/software version

3 the update is essential to resolve some vulnerabilities.

If any of the above is not matched, the patch cannot be automatically considered applicable. In any case, the following step of the evaluation is the risk analysis and assessment of the patch. The standard proposes a rich set of qualitative and quantitative approaches for the risk assessment. However, the survey of such approaches is out of the scopes even if it can be easily investigated by referring to the several academic and industrial literature works.

3.1.3 Patch testing

After a positive evaluation, the patch has to be tested. The testing process is an essential step, on which a large part of the patch management process shall be spent. The IEC 62443, in particular, recommends verifying the patch sources, considering only the ones provided by the vendors of the ICS assets. During this phase, the impact of a patch on the performances and in general on the dependability of the system should be evaluated, in qualitative or quantitative terms (for example providing possible reliability and performance indexes after the update). The installation procedure should be documented as well as the steps needed to roll back the system. The IEC 62443 however, does not provide specific recommendations on the rollback plan.

3.1.4 Patch deployment

The deployment should be performed after a successful testing process. Like the other processes, the deployment is divided into different steps: first, each of the involved stakeholders shall be notified that the update is being applied. Second, the production environment shall be prepared for the patch distribution. Different approaches can be adopted for the patch dispatching: isolate the target device in to deploy the patch without affecting the production environment, distribute the update over the network or even access to the asset and manually copying the update on it. Once the patch has been distributed, a scheduling program shall be defined, according to the business processes of the considered ICS. The last step of the patch deployment is the verification and reporting, which aims at verifying that the patch is correctly installed and the flaws are properly mitigated, or the functionalities are properly updated. The standard suggests different approaches for verification and reporting and, recommends to the asset owners to choose the best for the considered domain. A final remark of the IEC 62443 is that the patch management is not a *one-shot* plan but it needs to be constantly reviewed to refine the procedures and to reduce times and efforts for further patches, updates or firmware upgrades to be applied.

3.2 ISO 27002 series

The ISO addresses the patch management process in the ISO/IEC 27002 standard (ISO/IEC, 2013), which is a reference standard widely adopted within the context of the information security management systems. The ISO 27002 chapter addressing the patch management has been used by the European Union Agency for Network and Information Security (ENISA) to define the requirements for an international and interoperable environment for the testing and the certification of SCADA updates. The ENISA report in 2014 well describes such requirements using principles taken from the standard. Such principles are summarised below:

- The update process shall not compromise the functioning of the target devices of the patch.
- In case of known interruptions of service during the patch deployment, the system downtime shall be minimised.
- The infrastructure of interest shall provide redundancy. In particular, the update should be applied first on redundant passive assets. Redundant assets can be switched in an active state and tested in to verify the update. Only after the verification process, the update can be injected into the assets belonging to the production environment.
- The patch management process shall be followed by a working group, having the following responsibilities:

  a analyse and assess all the cyber-security issues that the patch may introduce

  b analyse and schedule the patch installation process

  c test, install and validate the patch on the target devices.

The description of steps to follow for patch management is less detailed than the IEC TR 62443. Nevertheless, the ISO/IEC 27002 has been successfully applied in different domains, as the healthcare (Tyali et al., 2010) and the oil and gas distribution (GE Oil and Gas, 2016) ones.

3.3 NERC standards

The North American Reliability Council (NERC) is the international regulatory authority, which provides the reference reliability and security recommendations for the bulk power system in North America. NERC guidelines are of interest for the survey, since they address the patch management in a more specific context, one of the electrical networks. The electrical networks represent one of the most diffused systems within critical infrastructures. The standard considered is the NERC CIP-007 (NERC, 2015), a wide-range standard focusing on the critical infrastructure protection. In particular, it addresses the topic of patch management for the remote terminal units (RTUs), usually adopted by ICSs for the electrical network monitoring and management. The NERC CIP-007 standard concerns the high-impact and the medium-impact bulk electrical systems assets, which are defined by NERC as the assets that within 15 minutes of unavailability or incorrect services can affect the other facilities of the infrastructure and in particular the ones responsible the system reliability. Although the standard considers only vulnerabilities of electrical network control systems, it provides principles that might also be applied to ICSs of another kind of systems. First, as the IEC 62443, it recommends producing documentation during each phase of the patch management process. To produce good documentation can increase the level of traceability and thus, can allow performing a backward analysis in case of problems occurred during the deployment. Another relevant aspect of the NERC CIP-007 is that it introduces the concept of *trusted sources*: patches for ICSs should be selected only from a list of trusted and certified vendors. The standard also provides other recommendations, which are not reported as they constitute a subset of recommendations already discussed for the IEC 62443 and the ISO 27002 series.

3.4 NIST standards

The National Institute of Standard and Technology (NIST) is one of the most important organisations working to enhance and secure industrial processes. NIST addressed the topic in several works: in Souppaya and Scarfone (2013), that provides a guideline for the enterprise patch management, in NIST cyber security framework, whose details can be found in NIST (2014) and in the NIST Internal Report (NISTIR) 7823, defining the requirements that a testing environment shall satisfy to verify the upgradability of the smart meters of the smart grids. Smart grids are an evolution of traditional power grids, developed to distribute the generation of the electricity, thanks to the possibility of allowing the customers to have a more active role by producing energy from renewable energy sources (such as wind, hydro and solar power). Smart meters are advanced devices, playing a crucial role in a smart grid: they are in charge to adapt the power, according to the current consumptions, and they may provoke an outage in case of failures (Gentile et al., 2016). The smart energy grid domain is plenty of reference standards for the correct functioning of the energy distribution. However, only a few of them deal with the issues related to the patch management of the smart meters (Katzir and Schwartzman, 2011). The NISTIR 7823 (Iorga et al., 2012) is one of them. The report provides principles generic enough to be applied to each context in which there are distributed and remotely accessible, monitoring and control devices. The NISTIR 7823 focuses, in particular, on the testing phase, defining the requirements that a testing environment shall satisfy to verify and validate patches of smart meters. It stresses the concept of *upgradability*, previously introduced by the National Electrical Manufacturers Association that indicates the capability to upgrade the firmware of the devices with a limited risk of incorrect operations that disrupt the service (NEMA, 2016). The description of such requirements is strictly related to the smart meters and is out of the scope of this survey. The requirements of the testing environment, indeed, are discussed below. First, three components shall interact within a testing environment:

- the upgrade management system, which is the back-end environment used to perform the update process
- the test application, which represents any environment or application to execute the test
- the unit under test, representing the target for the testing activities.

The requirements to be satisfied by the testing environment, are divided into three categories:

- mandatory requirements, which the testing environment shall provide
- conditional requirements, which are requirements that should be covered if some particular conditions occur within the system under test
- optional requirements, which are requirements which can be followed during the definition of the testing environment to increase the trustiness of the system;

The taxonomy described above is of particular interest since a major concern that one may raise in applying a patch management workflow is related to the time spent on testing activities. Depending on the considered infrastructure, patch management constraints can be relaxed considering only mandatory requirements for non-critical patches and also, conditional and optional for the critical ones. Finally, the NIST report defines three relevant objectives that should be pursued in order to reach full upgradability of the system assets:

- Define a mechanism to retrieve trusted information about the installed firmware, the status of the device and events happened during its functioning;
- Define a recovery approach from an erroneous or even from a disastrous update;
- Define mechanisms to protect against security issues (accidental or malicious), by exploiting authentication mechanisms and cryptographic algorithms, in agreement with the related international standards.

Other principles, here not reported, are very specific for the smart grids domain. Further details on the upgradability of smart meters can be found in the NISTIR 7823 (Iorga et al., 2012).

3.5 ICS-CERT best practices

To investigate the principles that a patch management workflow should consider, we also surveyed best practices coming from the application of patch management, within real industrial contexts. According to this, we review the works provided by the ICS Cyber Emergency Response Team (ICS-CERT). In 2010, a cyber-attack known as Stuxnet, affected different ICSs, showing that, the security policies until then followed, were not sufficient to guarantee the business continuity of these control systems, and therefore, of the infrastructures monitored and controlled by them. Therefore, the ICS-CERT, started to provide several recommendations to enhance the management processes of ICSs, including ones related to patches deployment. The document that well summarises these recommendations is the one in ICS-CERT (2008), adopted by the American Homeland Security, and dealing with the ICSs patch management, both in critical and non-critical domains. The main goal of ICS-CERT (2008) is to minimise the system downtime during the updating process. To achieve this objective, the ICS-CERT suggests to put in place a general patch management program, based on the following plans:

- The configuration management plan that aims at providing an archive containing the last stable versions of the asset software, all the needed libraries, a schematic of the link between the assets. It should also be able to provide a versioning management software, to trace all the changes to the code, introduced by the upgrade.
- The patch management plan, which should provide a complete vulnerability analysis related to the deployment of the updates/patches. The vulnerability analysis should be based on reference metrics to help the management to decide if the update has to be applied, delayed or even deemed.
- The backup plan, providing the information related to the frequency of the backups, the assets involved and the physical storage. Moreover, the backup plan should always consider a backup of the system before any update deployment.
- The testing plan, to be adopted before any patch application. The testing environment should be separated from the real system and should rely on dedicated hardware. Moreover, the testing environment should be as much possible similar to the real one, preferably equipped with the same hardware and software, to simulate the deployment effects of the patch. To replicate the hardware of a wide ICS can be very expensive, and thus, the rationale is to make this choice based on the considered domain.
- The disaster recovery plan that can be executed rapidly in case of any problem. The disaster recovery plan should consider both requirements related to the physical and cyber aspects of the system. Usually, a best practice is to switch on the testing environment if this last is equipped with the same software and the same hardware of the real system.

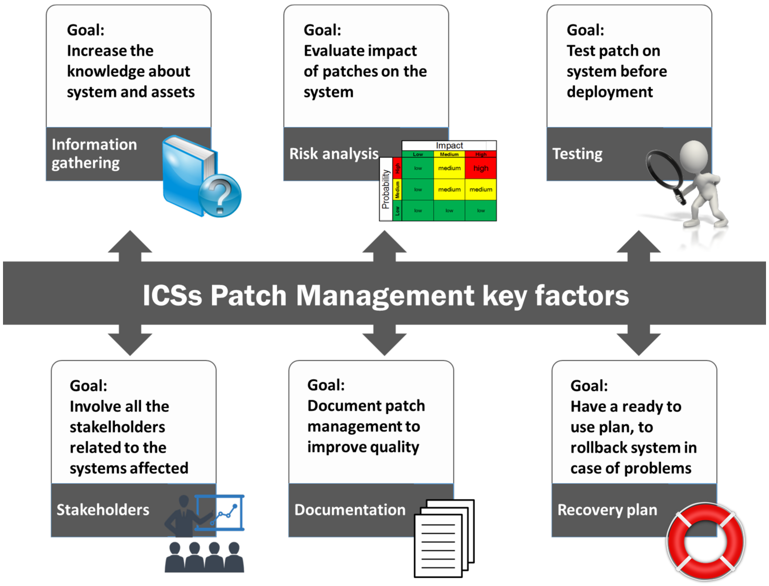
3.6 Discussion

To survey existing industry standards and recommendations is an essential step to define, refine or review a rigorous workflow for patch management of ICSs. The works reviewed share some principles but also have some particular concepts that make them difficult to merge in a single reference standard. For example, most of the surveyed standards recommend verifying the trustability of the patch sources. Such a principle, not present in the ICS-CERT best practices, can be difficult to apply. There exist, in fact, several critical infrastructures in which the design and the development have been done without using off-the-shelf hardware and software but, indeed, proprietary solutions. Therefore, especially for the software and firmware part, there are no vendors to which refer. Another common principle with limited applicability concerns to the definition of a working group, in charge to manage the whole patch management process. Some enterprises may not have enough resources to acquire skilled staff or to dedicate already existing staff resource only to patch management. Finally, according to the testing phase, a fully-redundant system is, in some cases, not feasible to put in place due to the costs and to the geographical extension of the critical infrastructure. Thus, exploiting the possibility to deal with concrete critical infrastructure, we focus on principles general enough to fit different domains, but with a feasible application in real contexts. Such principles, that we called *patch management pillars*, are summarised in Figure 2 and discussed below:

- As a preliminary step, there is the need to deeply understand the ICS in which the patch will be deployed.
- Each phase, deployment procedure included, shall be documented and documents shall be shared before the patch deployment acceptance.
- Each phase shall involve the different stakeholders and experts, related to the systems involved in the update, to consider all possible risks of the update.
- For each update, an analysis of the risks and possible impacts on the systems affected by the update should be performed and documented.
- An extensive testing program is required before the deployment. The testing shall be performed on dedicated hardware, and the testing team shall be different from the one of the developers. The testing shall provide a report that underlines possible issues emerged during the verification process.
- A recovery plan (often named disaster recovery plan in the different standards), should be always defined and approved, by all the stakeholders related to the systems affected by the update, to be ready to use in case of problems.

The concepts above, allowed us to define a possible workflow for patch management of ICS of critical infrastructure. They can be adopted all together, as in our case, to define from scratch a workflow for patch management, or can be used as references to verify, validate or enhance existing processes, via a gap analysis, to increase, where possible, the overall quality of the services provided.

Figure 2 Key factors in ICSs patch management (see online version for colours)


Goal:
Increase the knowledge about system and assets
Information gathering
Goal:
Evaluate impact of patches on the system
Risk analysis
Impact
Probability
Goal:
Test patch on system before deployment
Testing
ICSs Patch Management key factors
Goal:
Involve all the stakelholders related to the systems affected
Stakeholders
Goal:
Document patch management to improve quality
Documentation
Goal:
Have a ready to use plan, to rollback system in case of problems
Recovery plan

4 A standard-based patch management workflow

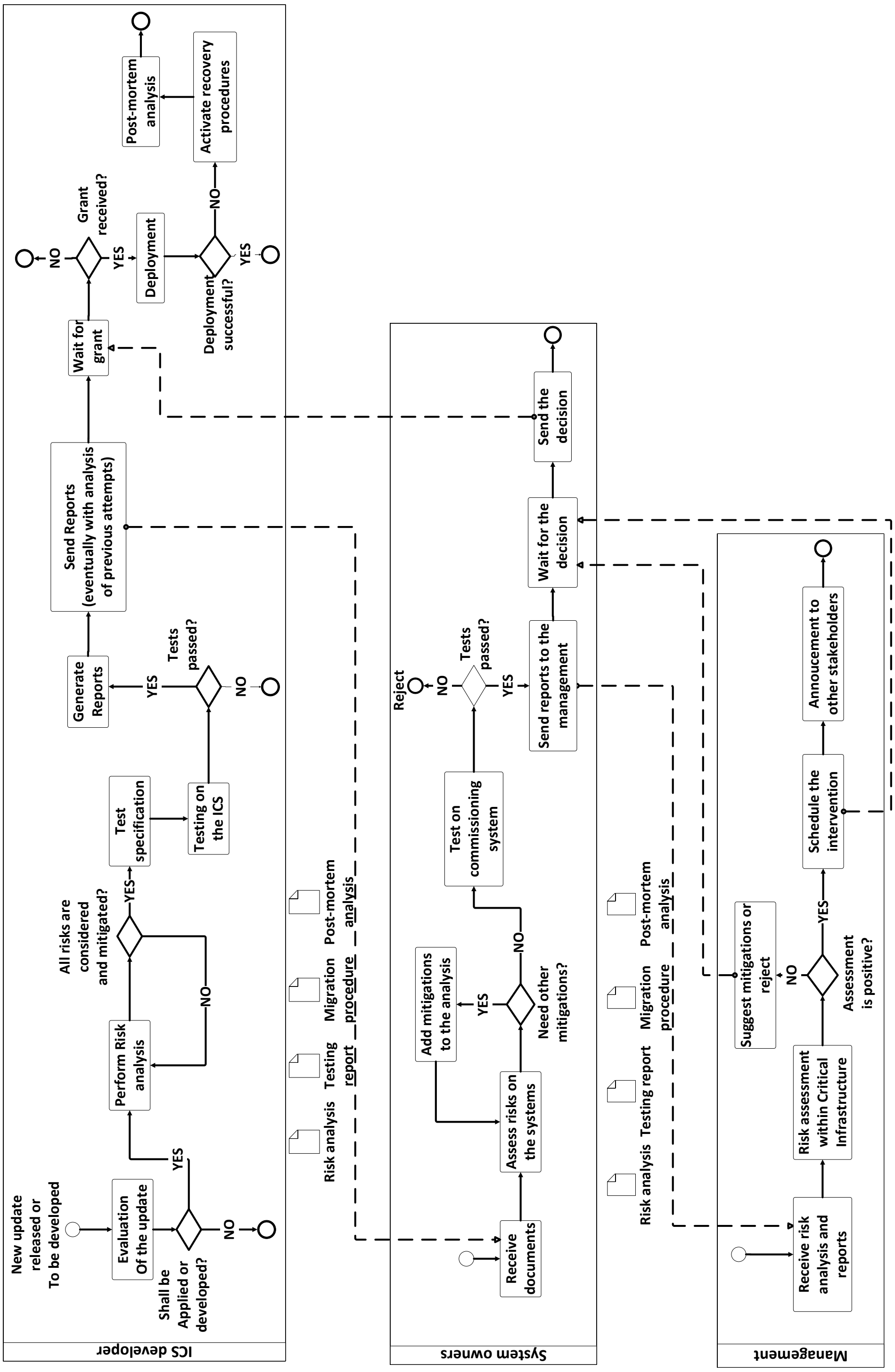
This section describes a workflow for patch management of ICSs, based on the pillars, discussed in the previous section, and tailored on the real case of technical infrastructures supporting particle accelerator systems. The workflow, summarised in Figure 3, has been modelled using basic constructs of the business process modelling and notation (BPMN), which is a modelling notation that allows each stakeholder to understand processes easily and can also enable their automation, to integrate them within other enterprise processes.

The first issue addressed by the workflow concerns with the distribution of the responsibilities during the patch management process. According to this, three different roles have been considered:

- The ICS developers, which are in charge of designing, developing and deploying the ICS and sometimes, can also be responsible for the development of the patches.
- The system owners who are responsible for one of the infrastructure systems supervised and controlled by the ICS. Since owners deeply know their systems, they can act as an interface between the ICS developers and the management, by evaluating the risks within their system and by giving to the management all the needed information to evaluate possible impacts on the rest of the infrastructure.
- The management, which uses or is responsible for the whole infrastructure. According to the standards, it gives the final agreement for the update, based on the documentation provided. Moreover, it coordinates the information exchanging, among the different stakeholders involved.

The workflow stresses in particular three principles: the risk analysis, the testing process and the need to produce documentation. The risk analysis shall always be performed and documented and should adopt both qualitative and quantitative approaches (Cherdantseva et al., 2016). Moreover, the risk analysis should consider all possible threats related to the patch management process. Usually, to evaluate the risk qualitatively, two parameters are considered: the potentiality that a patch can provoke a failure to the system and, the impact on the other systems, in case this happens. The risk analysis and the consequent assessment may also result in the decision of avoiding the patch deployment or to further investigate possible countermeasures to mitigate problems. The testing activity shall be focused on the patch itself and the deployment environment to check if the ICS assets can be considered upgradeable. The academic and industry literature is plenty of surveys and works on the verification and validation of patches of software systems (Holm et al., 2015). However, the analysis of such surveys is out of the scope of this paper. The third relevant point is the need to produce adequate documentation at each stage of the patch management process, and in particular for the risk analysis, for the report of the testing activity and the commissioning procedure. This last is one of the most important since it shall report:

Figure 3 Proposed patch management workflow



- The detailed procedure to follow to test the system specifications. Since each specification can affect one or more systems of the considered infrastructure, the commissioning procedure shall provide, for each test specification, the sequence of steps performed to verify the correct behaviour of the possible affected systems.
- Pre and post-conditions of the test. Pre-conditions usually specify the operational conditions in which tests will be performed (e.g., ten accounts have been logged, the alarm logger has been started, etc.). Post-conditions, instead, represent the expected operational conditions after the test execution.
- Eventual hypotheses or assumptions made during the test specification.

Finally, is important to document also the roll-back plan. The roll-back plan usually provides an estimation of the possible downtimes giving the possibility to the management to define, together with all the involved stakeholders, the best scheduling, for the patch deployment, and all the possible emergencies strategies, to restore quickly the system, in case of problems.

5 Workflow application within particles accelerator technical infrastructure

The workflow proposed and discussed in the previous section, results from the concepts emerged during the literature survey. It can be followed to guide the review of the patch management processes in a real system, as CERN TI, via a gap analysis and tailored to the needs and risks of the systems being investigated. The review and the gaps identification of a real patch management process can be implemented via a series of questions for the previously identified stakeholders:

Q1 Does the current process allow to collect information (software, hardware and firmware) of the control system assets of the control systems?

Q2 How the risk analysis is performed?

Q3 What are the procedures and the documents provided to the management for the review of the patch management process?

Q4 How the testing activities are performed before the patch deployment?

Q5 Does the rollback plan is defined during the patch management process?

Q6 Are all possible stakeholders involved during patch evaluation and deployment?

The questions above aim at understanding if the documentation, especially for what concerns the risk analysis and patch deployment procedures is well produced, if the testing is adequately performed and, above all, if stakeholders are properly involved in the overall process. We performed the proposed gap analysis on some existing ICSs of the CERN TI to validate and to improve the quality and robustness of the patch management processes. We focused in particular on the electrical network, which is one of the widest systems of the CERN TI. The electrical network monitors and controls over 20,000 electrical devices, from the 400kV breakers to the 48V DC systems, through over 70 industrial RTUs, with more than 140,000 digital inputs, 95,000 analogue inputs and 20,000 control data-points (CERN, 2018). Issues arising during the deployment of patches within this system can have a very wide impact on the whole operation of the technical infrastructure, decreasing the overall availability of the machines.

Below, some lessons learned from the application of the proposed workflow to the electrical network, are summarised:

- In a real ICS environment, it is necessary to consider two kinds of patches: minor and major ones. The difference is that minor patches are considered as quick hot-fixes, which cannot affect the operation of the monitored and controlled infrastructure. Thus, to reduce the time to the deployment, they can be just announced to the management but deployed without an explicit grant and without following each step of the workflow.
- The information gathering, according to the meaning of the ISO/IEC 62443, is not always feasible for large infrastructures and often, shall simply rely on the knowledge about the assets by ICSs developers and system owners, which are the ones who designed and developed the control network.
- The testing activities for wide and complex infrastructures, due to the high costs, are not always economically feasible and possible with testing and production environments completely redundant. Thus, the testing environment for the patch verification, is usually a small-scale replication, of the production ICS, or even a simulated, by software, environment.
- The patch management process responsibilities, despite even in case of refusal of deployment, can, sometimes, be bypassed for vulnerabilities patches, since, as suggested by same IEC 62443 and, by the on-field experience, the consequences of an exploited flaw are even worse than the downtimes introduced by a failing patch deployment.
- Another criticality can be represented by the technologies adopted for the management of the patch deployment process. The loose integration between the several software systems supporting the workflow activities (e.g., bug tracking systems, web-based systems, SCADA software, etc.), affects the time to deployment for the lack of notifications and of mechanisms able to consider the possible dependencies among the systems affected by the patch. To reduce times and risks, could be useful to have a reference platform, to be used as a single entry point for the release of new patches, to perform the tracking of the process at each stage, to track also the responsibilities assigned and to provide synchronisation mechanisms for the automatic send of notifications and reminders. Moreover, a platform for patch management should also be able to provide an archive of the past deployed patches, to easily backtrack the process, in case of issues arise over time. The analysis of market solutions able to cope with such requirements is currently investigating, and the outcomes will be the focus of further works on the topic.

6 Conclusions

This paper focuses on the patch management process within ICSs. The main goal is to review the available international standards and industrial works addressing the topic of patch management. To follow the standards is important since they summarise in a concise way, the experience and the knowledge gained by different sources such as industries, academicians, customers and public legislators. The adoption of standards can also increase the quality and the safety of the business processes, the interoperability between different systems, the impact of potential risks within the organisation and can allow fulfilling applicable laws and regulations. Reference standards can be strictly followed or adapted to define a set of best practices tailored on the enterprise needs, to mitigate the impact on the system availability and efficiency, at an acceptable cost weighted against the economic and social impacts of the unavailability of the overall system. The paper gathers summarises and discusses key principles and defines a general-purpose workflow, to be applied in critical infrastructure contexts, for the new system or regular verification, via gap analysis, of existing ICSs. The main pillars that each patch management process shall consider are:

- to define clear responsibilities assignment among the different stakeholders involved in the process
- to perform risks analysis and assessment
- to increase the documentation at each stage of the process
- to lie on testing environments, designed according to the related standards.

The workflow has already been adopted at CERN for some systems of the TI, for which the highest availability and reliability is required to guarantee to reach record and breaking levels of physics events productions for experiments. Further research effort will be spent in defining and developing a software platform able to support the modelled patch management workflow.

Acknowledgements

The authors would like to thank all the technical infrastructure experts and operators who contribute to the review of the patch management process at CERN.

References

CERN (2018) *CERN Electrical Network: General Presentation* [online] http://en-dep.web.cern.ch/en-dep/groups/el/netctrl/index.htm (accessed January 2018).

Chen, T.M. and Abu-Nimeh, S. (2011) 'Lessons from stuxnet', *IEEE Computer*, Vol. 44, No. 4, pp.91–93, doi: 10.1109/MC.2011.115.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K. (2016) 'A review of cyber security risk assessment methods for SCADA systems', *Computers & security*, Vol. 56, pp.1–27, doi: 10.1016/j.cose.2015.09.009.

European Union Agency for Network and Information Security (ENISA) (2014) *Window of Exposure... A Real Problem for SCADA Systems?*, EU Publications, doi: 10.2824/25757.

GE Oil and Gas (2016) *GE Oil and Gas Cyber Security Overview* [online] https://www.ge.com/digital/sites/default/files/GE-Oil-and-Gas-Cyber-Security-Overview.pdf (accessed September 2018).

Gentile, U., Marrone, S., Mazzocca, N. and Nardone, R. (2016) ‘Cost-energy modelling and profiling of smart domestic grids’, *International Journal of Grid and Utility Computing*, Vol. 7, No. 4, pp.257–271, doi: 10.1504/IJGUC.2016.081012.

Holm, H., Karresand, M. and Vidström, A., Westring, E. (2015) ‘A survey of industrial control system testbeds’, *Secure IT Systems*, Vol. 9417, pp.11–26, doi: 10.1007/978-3-319-26502-5_2.

ICS-CERT (2008) *Recommended Pratice for Patch Management of Control Systems* [online] https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_Patch_Management_S508C.pdf (accessed January 2018).

IEC (2015) *Security for Industrial Automation and Control Systems – Part 2-3: Patch Management in the IACS Environment* [online] https://webstore.iec.ch/publication/22811 (accessed September 2018).

Iorga, M., Shorter, S. et al. (2012) *Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework*, National Institute of Standards and Technology Internal reports, doi: 10.6028/NIST.IR.7823.

Islam, M., Huang, A.K., Battisha, M., Chiang, M., Srinivasan, S., Peters, C., Neumann, A. and Abdelnur, A. (2012) ‘Oozie: towards a scalable workflow management system for Hadoop’, *Proceedings of the 1st ACM SIGMOD Workshop on Scalable Workflow Execution Engines and Technologies*, ACM, doi: 10.1145/2443416.2443420.

ISO/IEC (2013) *ISO/IEC 27002 – Information Technology – Security Techniques – Code of Practice for Information Security Controls* [online] https://www.iso.org/standard/54533.html (accessed September 2018).

Karnouskos, S. (2011) ‘Stuxnet worm impact on industrial cyber-physical system security’, *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*, pp.4490–4494, doi: 10.1109/IECON.2011.6120048.

Katzir, L. and Schwartzman, I. (2011) ‘Secure firmware updates for smart grid devices’, *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)*, pp.1–5, doi: 10.1109/ISGTEurope.2011.6162728.

Krutz, R.L. (2013) *Industrial Automation and Control System Security Principles*, International Society of Automation (ISA), USA, ISBN: 9781937560638.

Laing, C. (2012) *Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection*, IGI Global, USA, ISBN: 9781466626904.

Liu, J., Pacitti, E., Valduriez, P. and Mattoso, M. (2015) ‘A survey of data-intensive scientific workflow management’, (2015) *Journal of Grid Computing*, Vol. 13, No. 4, pp.457–493, Springer, doi: 10.1007/s10723-015-9329-8.

National Electrical Manufactures Association (NEMA) (2016) *NEMA SG-AMI 2009 R2015 – Requirements for Smart Meter Upgradeability* [online] https://www.nema.org/Standards/Pages/Requirements-for-Smart-Meter-Upgradeability.aspx (accessed January 2018).

National Institute of Standard Technologies (NIST) (2014) *Cyber Security Framework* [online] https://www.nist.gov/cyberframework (accessed January 2018).

North American Electric Reliability Corporation (NERC) (2015) *CIP-007-6 – Cyber Security – System Security Management* [online] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (accessed September 2018).

Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K. (2001) ‘Identifying, understanding, and analyzing critical infrastructure interdependencies’, *IEEE Control Systems*, Vol. 21, No. 6, pp.11–25, IEEE, doi: 10.1109/37.969131.

Souppaya, M. and Scarfone, K., (2013) ‘Guide to enterprise patch management technologies’, *NIST Special Publication*, Vol. 800, p.40, 2015, doi: 10.6028/NIST.SP.800-40r3.

Tyali, S., Pottas, D. and Kelly, T.K. (2010) 'Information security management systems in the healthcare context', *Proceedings of the South African Information Security Multi-Conference*, 17–18 May, Port Elizabeth, South Africa, p.177, ISBN: 978-1841022567.

Wonderware Alert n.287 [online] https://wonderwarepacwest.com/support/tech-news/important-tech-alert-287/ (accessed September 2018).

Yu, J. and Buyya, R., (2005) 'A taxonomy of workflow management systems for grid computing', *Journal of Grid Computing*, Vols. 3, Nos.3–4, pp.171–200, Springer, doi: 10.1007/s10723-005-9010-8.

Zhu, Q., McQueen, M., Rieger, C. and Basar, T. (2011) *Management of Control System Information Security: Control System Patch Management*, Idaho National Laboratory (INL) report.