CIGRE-521

2022 CIGRE Canada Conference & Expo
Calgary, Alberta, Oct.31 – Nov. 3, 2022

Unanticipated Costs of Increasingly Networked Digital HVDC & FACTS Infrastructure

C. MADSEN, M. KORETIMI, M. PARADIS
ATCO Electric
Canada

SUMMARY

Transformational changes to the electric transmission industry have taken place over the past 20 years as new substation measurement, protection, and control electronics have largely shifted from disconnected digital systems with well-defined interfaces to integrated networked systems. Vendors have been improving capabilities to match the needs of the grid while adding features for the end users. Modern digital electronics provide significant benefits over older devices, but the increase in integration has resulted in unintended costs for transmission facility Owners. This paper focuses on the following points, largely considering experiences from HVDC & FACTS facility Owners:

- Increasing costs of O&M and upgrading the control systems for HVDC facilities. The capital cost for an HVDC controls replacement has increased by several times over the last 20 years due to the increased features and capabilities of modern digital systems requiring more complex integration and validation.
- The shortened lifecycle of networked electronics versus their standalone counterparts. Analog and early digital HVDC control systems easily lasted for 15+ years. Modern HVDC control systems, while much more capable, are locked to the computer chip and OS manufacturer product lifecycles. This leads to HVDC control systems with 7-15-year lifecycle.
- Complex software composition and the effect on patch management and obsolescence. Modern applications are composed of collections of third-party products. Owners have needed to accept riskier or more expensive asset management strategies to maintain dissimilar products spanning multiple generations, some created by third parties who no longer exist.
- The compliance burden to proving cybersecurity standards in the networked HVDC or FACTS facility. HVDC systems are almost always in scope of cybersecurity standards (such as NERC CIP in North America), and due to the high count of heavily customized systems, are challenging to integrate into the existing security management systems of the Owner.
- The challenge of maintaining expertise in modern networked HVDC & FACTS control systems, due to their multidisciplinary nature.

In this paper the authors outline their experiences quantifying and addressing these costs as an Owner of several HVDC and FACTS installations, with the goal of highlighting practical examples of areas for improvement in the industry.

KEYWORDS

DIGITAL, HVDC, FACTS, NETWORK, CONTROL SYSTEM, CYBERSECURITY, LIFECYCLE

colin.madsen@atco.com

1. INTRODUCTION

In the 1980s through the 1990s, HVDC & FACTS vendors began converting their control system product offerings from analog to digital [1]. Early digital systems were largely isolated or had simple interfaces. By the early 2000s, vendors were offering fully digital systems. In the last 20 years, the digital components have continued to rely more heavily on the Internet Protocol suite (IP) [2], with the promise that these networked systems would be cheaper to install, highly flexible and would be able to increase control resiliency and performance.

That promise was largely fulfilled and today the evolution towards fully networked control systems continues to progress, with the rising popularity of IEC 61850 and other IP-based protocols within power system installations as evidence. At the same time, the power industry is realizing that while reliance on the IP suite allows industrial equipment to rely on both the Internet and communications industries for new features, evolving performance, and robust security, it is also opening energy infrastructure to new sets of vectors for cyberattacks, additional complexity, and escalating lifecycle costs. Owners of HVDC & FACTS systems face different considerations in both the technologies used and the wider environment in which they operate.

This paper will outline the scope of the additional costs and considerations for HVDC & FACTS facilities from an Owner's perspective. Some existing research focuses on this problem, but from a more generic perspective [3]. The intention for this paper is that an HVDC or FACTS facility Owner will be better prepared to estimate the lifecycle costs of modern HVDC & FACTS control systems while considering the challenges brought by maintaining a high level of cybersecurity while employing modern systems.

In general, five costs will be explored:

1. Enhanced validation requirements for higher performance systems
2. Shortened physical and software lifecycle of digital components
3. Cybersecurity driving early replacement
4. Positioning Owners for an effective cybersecurity program
5. Cost of building and maintaining new skillsets for O&M

2. MODERN HVDC & FACTS CONTROL SYSTEMS

Modern HVDC & FACTS control systems rely on mature networked communications based on a technology called TCP/IP (also called the Internet Protocol suite, or IP) forming the basis of the Internet. The origins of IP began in the early 1970s with experimental switched packet communications, specifically devices that could send arbitrary messages bidirectionally between any devices on the same "network", using shared Ethernet cables. Additional features included network redundancy with self-healing properties. With the exponential growth of the Internet in early 1990s, both due to the creation of a free web browser and the proven flexibility and reliability of what became known as the IP suite of protocols [4], power systems vendors recognized the advantages of using IP for the communications needs of substation equipment and began adopting the protocol suite. By the early 2000s, HVDC & FACTS vendors had successfully converted large portions of their controls systems to use IP communications for control and protection functions [2] taking advantage of its speed and flexibility.

2.1 INTRO TO THE TECHNOLOGY

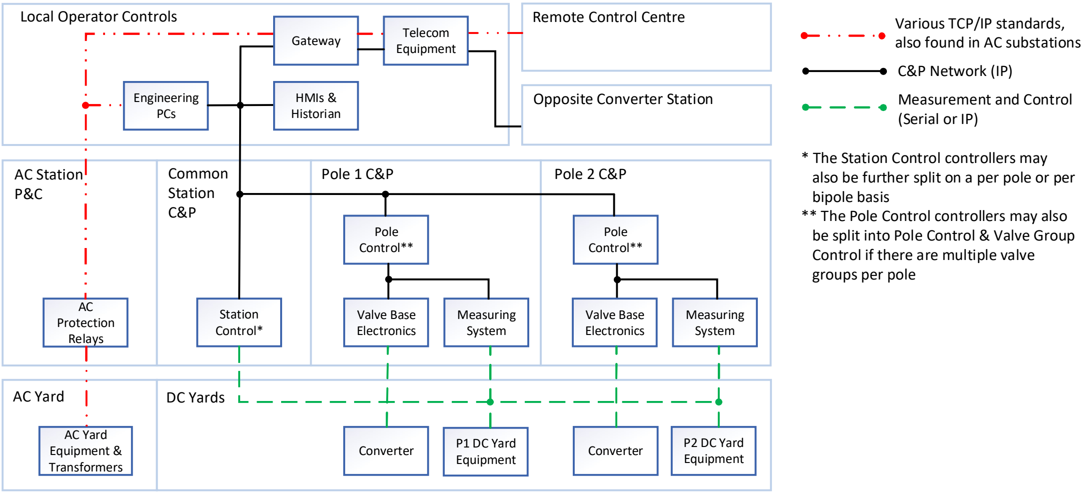
HVDC & FACTS control systems are complex, consisting of many individual controllers working together. The typical HVDC & FACTS control system is arranged in a hierarchical tree, where individual controllers communicate with the ones immediately higher and lower in the hierarchy. For a typical HVDC facility, you will have some variation of the following main controllers in that tree (see Figure 1):

- **Station Controllers:** these will receive a power order and control settings from the control centre, as well as status signals from the various pole controllers and station equipment at both ends of the link, and then instruct each local Pole Controller what its voltage and current orders should be.

- **Pole Controllers:** these monitor all the pole equipment and determine what the power electronics firing angles should be based on the voltage and current orders from Station Control or Bipole Control. This considers the control loops for voltage control mode, etc., as well as performing most of the protection calculations that are activated at the Pole level.
- **Converter Electronics:** these controllers receive control instructions from Pole Control and determine which thyristors or IGBTs, etc., should activate and when. They also consider the operating characteristics of the semiconductors, performing high-speed transient and thermal protection.

A FACTS facility will follow a similar hierarchical controller design as a HVDC facility, with variation depending on the technology being used. In all cases, however, the facility contains all the signals that an equivalently sized passive AC substation would have, plus the signals required for active power control. Due to the complexity and number of the control functions, it is not presently feasible for a single controller to replace the hierarchical control tree. It makes more sense to have separate controllers communicating with a robust and flexible protocol suite.

Figure 1 outlines a possible simplified hierarchical control architecture for a generic HVDC bipole, based on concepts observed in several in-service HVDC facilities. It is key to note that the systems connected by the solid black line are all part of the HVDC control system network and typically communicate with TCP/IP-based proprietary protocols. Instead of thousands of point-to-point wired connections, or hundreds of serial communications channels, two or three TCP/IP networks can form the core of the control system. The benefit of simplicity is evident, but the drawbacks will be discussed in the following sections.



* The Station Control controllers may also be further split on a per pole or per bipole basis

** The Pole Control controllers may also be split into Pole Control & Valve Group Control if there are multiple valve groups per pole

Figure 1- Example of Typical HVDC Bipole Control Communications

2.2 VALIDATION REQUIREMENTS FOR HIGHER PERFORMANCE SYSTEMS

While the transition to highly-networked digital systems may have lowered controller hardware and installation costs, the overall costs for a control system project has not dropped – it has rather increased over the past 20 years. This can be directly contrasted with the AC substation lifecycle, where there has been a marked decrease in P&C capital costs with the implementation of IEC 61850 and similar TCP/IP-based equipment.

> **Case Study:** Modern IP-based control systems rely on mature redundancy and failover technologies. Compare this with an older redundant control system that would allow a single control system failure without impacting performance – the modern control system has enough layers of redundancy that many equipment failures can sometimes occur without impacting performance. For example, the following components could fail, and the IP

network will still heal to full functionality: a C&P router on system 1; a measurement system component on system 2; and even a pole controller on system 1. Proving the redundancy of a modern system is more difficult, however, as where there might have been a couple dozen failover validation cases with an older control system, a modern system now requires many times that.

A simplified explanation for the cost increase of a controls replacement is that the transition to more flexible and easily implemented hardware has enabled vendors to add higher performance features to their products which require additional engineering studies, design, and integration validation. The increase in control system software complexity and performance is essentially outpacing the reduction in hardware complexity.

- HVDC & FACTS Owners must expect that control system replacements do not come at a lower cost due to technological improvements (as found in the AC substation experience), but generally come at a higher cost due to overall increased system complexity driven by performance.

3. COSTS DUE TO A SHORTENED LIFECYCLE

Software systems are playing a more integral role in modern HVDC & FACTS facilities than they have in the past. Customized computing hardware is very expensive to build and difficult to change, so HVDC & FACTS vendors build as much of the control system as possible in software, which can be much more easily built and modified. This allows more general-purpose hardware to be used, decreasing the capital project costs. The downside is that modern software has reached a very high level of complexity and many components are outsourced to third parties. This third-party dependency both affects the cybersecurity approach an Owner must take to manage their infrastructure, as well as substantially limiting the useful life of modern HVDC & FACTS control systems.

3.1 SHORTENED LIFECYCLE DUE TO END OF PATCHING SUPPORT

Managing a software supply chain is a difficult problem. It is often unclear what is in a piece of software, let alone how to determine if known cybersecurity vulnerabilities are applicable, and if they can be patched. To tackle this problem there has been much discussion across industry regarding the Software Bill of Materials (or SBOM) to allow entities to manage software containing third-party code [5]. An HVDC or FACTS Vendor compliant to an SBOM standard would provide Owners with a list of all known third-party components in their software product. In theory, this mitigates a lot of cybersecurity risk. When a vulnerability is discovered in industry, the affected code can be compared against the SBOM for a particular product to determine if the vulnerability is applicable.

Industry application is not that simple, as an SBOM will list all the components a vendor put into their code but may crucially lack the subcomponents of the third-party code used, as well as the subcomponents of those subcomponents, etc. Furthermore, a detailed investigation is still needed for any identified security vulnerability, as sometimes a vulnerability is associated with a code library which was only partially used in the Vendor's product, or the vulnerability was only applicable to a particular version of the library which may or may not have been used in the Vendor's software, etc.

The North American Electric Reliability Corporation (NERC) has developed standard CIP-013 to mitigate the supply chain cyberattack risks that come with cyber systems that can affect the Bulk Electric System (BES cyber systems). CIP-013 outlines minimum requirements that Owners must impose on their Vendors, and one of those requirements can be met by the Vendor creating an SBOM [6]. CIP-013 applies to new Vendor contracts for BES sites, but much aging HVDC & FACTS infrastructure will not be documented effectively in an SBOM, especially when it comes to the third-party code components.

Owners must have an insight into the risks they are exposed to when determining if they will rely on the Vendor for patch management, or in-house expertise, and further, what risks exist when the software systems reach end-of-support from the HVDC & FACTS Vendor. Owners lack the information to effectively create an SBOM of the same quality as a Vendor and will struggle to properly define security threats or the applicability of vulnerabilities after the end of software support. When a product has reached end-of-support, the Owner will be faced with the decision to replace the system, or to accept the risk of an unpatched product in their system. In the second case, the Owner will benefit by ensuring their asset management system is compatible with the SBOM format, allowing for the following benefits [5]:

- Inform vulnerability management and asset management.
- Manage licensing and compliance.
- Quickly identify software or component dependencies and supply chain risks.

Further research in this area is required to quantify the merits of an Owner-maintained SBOM, and to develop a proper risk analysis metric to manage software systems that have passed the end-of-support date by the original Vendors.

3.2 SHORTENED LIFECYCLE DUE TO END OF HARDWARE AVAILABILITY

Modern HVDC and FACTS control systems have a heavy reliance on third-party software, firmware, and hardware subsystems. Vendors will outsource some components of their product to specialized third parties who can provide more features at a lower cost, so that the vendor can focus on developing their core technology. The benefit to the vendor is a much quicker product development using fewer in-house resources, and often much simpler implementation of features or improvements.

The problem is that the HVDC or FACTS Vendor will now be sharing components of their platform with other industries, and that means that that the lifecycle of the components will be controlled by the dominating industry. Globally, there are far fewer HVDC links and FACTS installations than personal computers, for example. If an HVDC HMI product is built on a computer running a commercially available operating system such as Microsoft Windows, the maximum lifespan of that computer will be tied to the comparatively short lifespan defined by the software vendor rather than the life cycle of the HVDC or FACTS facility.

> **Case study: Windows XP in HVDC & FACTS HMIs**
> Microsoft released Windows XP Professional x64 (Win XP) in 2005 and continued to support it until 2014. This was an almost 10-year total lifespan, including extended security patching support [7]. Several HVDC & FACTS vendors relied on Win XP for several integral subsystems, such as control system development coding (and engineering workstations) and HMIs. It is reasonable to expect vendors to spend a couple of years to bring their new generations of product to market on a new Windows platform. This timing implies that a vendor could only rely on roughly 7-8 years of full third-party support for their new system. Furthermore, HVDC & FACTS facility owners do not only buy facilities immediately upon the creation of a new product line. If a facility owner buys an HVDC control system 7 years after the product has been introduced on the market, third-party support for certain subsystems may end while the control system is brand new.
>
> Vendors and Owners have mitigated against this dependency on the lifecycle of third-party components by purchasing spare hardware with the OS pre-installed, but that strategy is also limited. For example, when Microsoft ceased to support Win XP, they also ceased to support new generations of Intel CPU hardware. The "Ivy Bridge" generation of Intel CPUs, discontinued in 2015, was the last generation supported by Win XP. This means that after 2015 no new Intel processors were manufactured that supported Win XP, and the purchase of spare components become difficult.

This case study above is not unique. An HVDC or FACTS site will contain automation PLCs, protective relays, network switches, firewalls, SCADA gateways, industrial PCs, and of course, HVDC & FACTS controllers, where all these devices will be reliant on varying amounts of third-party hardware, as well as software, firmware, or operating systems that interface with that hardware. HVDC & FACTS vendors choose hardware and operating systems with the greatest possible longevity (typically industrial grade CPUs and operating systems with long-term support), but even with these design decisions the expectation for life expectancy of a modern HMI system is only 7 years, and for an modern overall HVDC control system is only 12-15 years [8], while analog and early digital systems would easily last 15+ years.

The timeframes given above are estimates only, with specifics dependent on the third party components in use, how mature the product was when the Owner's facility went in service, and how much risk the Owner is willing to take by life-extending the hardware after major components have reached end-of-support (see *Figure 2* for a hypothetical example). Each of these components needs to be evaluated on a case-by-case basis considering the maturity of each major third-party component, also considering the risk appetite the Owner has for unpatched systems.

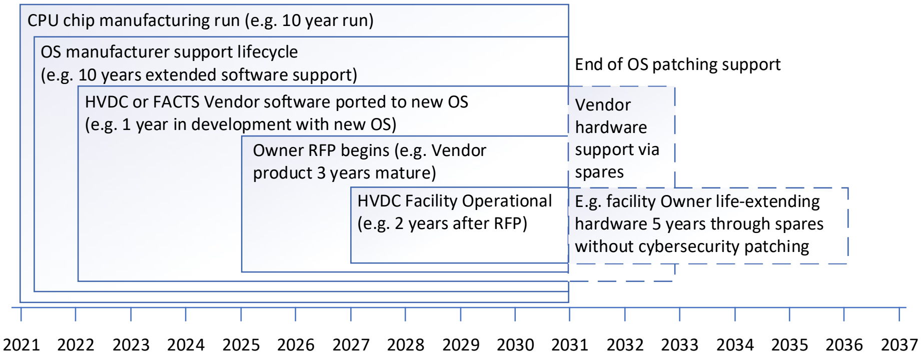

CPU chip manufacturing run (e.g. 10 year run)
OS manufacturer support lifecycle
(e.g. 10 years extended software support)
End of OS patching support
HVDC or FACTS Vendor software ported to new OS
(e.g. 1 year in development with new OS)
Vendor hardware support via spares
Owner RFP begins (e.g. Vendor product 3 years mature)
HVDC Facility Operational
(e.g. 2 years after RFP)
E.g. facility Owner life-extending hardware 5 years through spares without cybersecurity patching
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037

Figure 2 – Hypothetical Sample Timeline of HVDC or FACTS Computer Equipment Illustrating Third Party Dependencies

HVDC & FACTS facility owners will best be able to manage the short lifecycles of advanced electronics by being informed during the planning and design stage of the project:

- Require the Vendor to provide a product maturity report, and further provide an anticipated third-party end-of-support of key subsystem components during the design stage of the HVDC or FACTS project (this would include the HMIs, and the main controllers, etc.).
- Build a sparing strategy that accounts for the increased risk of spare unavailability after anticipated end-of-support, considering major third-party components where the vendor is unable to provide an estimate. Such a sparing strategy also requires robust data regarding anticipated failure rates of components over their lifetime.
- Additionally, unlike in an AC substation, the entire HVDC or FACTS control system must typically be replaced at once, meaning that some components with many years of remaining life may need be replaced at the same time as assets with a shorter lifespan.

4. POSITIONING OWNERS FOR AN EFFECTIVE CYBERSECURITY PROGRAM

This section highlights the compliance burden to proving cybersecurity minimum standards in the networked substation or converter station. In North America, entities that can affect the Bulk Electric System (BES) are required to adopt cybersecurity standards (among other standards) in alignment with the reliability standards of the NERC. The cybersecurity standards are known as Critical Infrastructure Protection (CIP) standards. These requirements are prescriptive and aim to enforce a minimum set of controls for the BES that allows for their reliable and secure operation.

This section was written from the perspective of a Utility Owner that is required to comply with the NERC CIP set of standards. As this paper only deals with the utility perspective, additional standards that may be applicable such as IEEE 1638 will not be discussed as they primarily affect the equipment manufacturers, and related international standards such as IEC 62443 will not be discussed as they are required in other jurisdictions instead of NERC CIP. However, the issues noted below will be common to most HVDC & FACTS installations. Regardless of the standard, adapting to cybersecurity best practices and maintaining a strong security program is a common struggle for all Utility Owners globally.

Five challenges faced in meeting these cybersecurity standards and further maintaining the expertise required to understand the standards are outlined below. In several cases, the challenges in meeting these standards are tied to the same principles that shorten the HVDC or FACTS system's life cycle.

4.1 SECURITY MANAGEMENT IN AN INCREASINGLY NETWORKED ENVIRONMENT

Assets making up control and protection systems in HVDC and FACTS facilities are carefully integrated and networked. These assets require ongoing security management activities not only to address cybersecurity vulnerabilities but also to comply with CIP standards. Patch sourcing, establishment and documentation of baseline configuration are critical activities to comply with CIP-007 and CIP-010 standards. The documentation requires considerable effort and diligence, and baseline configuration changes are often manually tracked on a spreadsheet or in a database. Patching assets in an integrated system may sometimes lead to unanticipated output such as the system becoming unstable. Considerable time and effort will then need to be spent troubleshooting the system.

- To address this challenge, patching test beds [9] have been proposed in industry and more time and resources need to be dedicated to their planning and implementation. Testing and validation [10] of protection and control functions may need to be conducted following patching. If an Owner does not plan to purchase a patching test bed, they must be aware of the risks of implementing untested patches on an operational system.
- These recommendations come with a high capital cost that is difficult for Owners to justify following the original project closeout. Where possible, it may be advantageous to bundle a patching test bed into the original project costs. This would be considered in addition to, or instead of, a replica control system in a test environment.

4.2 INCREASE OF IN-SCOPE ASSETS DUE TO INTERCONNECTION USING TCP/IP

A monitoring system or engineering analysis system has no mechanism to affect the BES through normal operation, but if it is compromised in a cyber attack, it would have the capability to affect any network-connected BES controller. These devices are classified as a Protected Cyber Assets, and the compliance burden to operate and maintain them is virtually the same as if they were directly BES cyber assets.

- The Owner should review the network design during the design stage to ensure that only necessary assets are connected to the HVDC or FACTS control networks, avoiding Protected Cyber Assets where possible.
- Following this, a full exercise to identify and properly classify this category of assets during the project commissioning stage will minimize unnecessary rework and ensure minimum security controls are applied before in-service date.

4.3 LACK OF AUTOMATED TOOLS FOR COMPLIANCE ACTIVITIES

Baseline configurations and a vulnerability assessment must be established by the in-service date of BES facilities to meet CIP requirements, and the vulnerability assessment repeated every 15 months. Active vulnerability assessments (using scanners) may be intrusive in a power system, meaning that station outages are often required to gather data to meet the CIP requirement. An alternative is a passive scanner, but due to the customization in an HVDC or FACTS control system, effective passive scanners may not exist. Even in cases where generic scanning software for active vulnerability assessment has been manually deployed, the authors have had difficulty in achieving reliable port scan results for non-standard ports [11].

- During the design review project stage, it will be helpful to determine the applicability of non-intrusive automated tools for gathering data, and to adapt the Owner's cybersecurity program to match. HVDC & FACTS control systems are often not compatible with commercial data collection tools and require case-by-case evaluation.

- Further research work needs to be conducted to address this difficulty, especially when considering already in-service facilities.

5. COSTS DUE TO A LACK OF EXPERTISE

5.1 LACK OF ADEQUATE SKILLS IN INFORMATION TECHNOLOGY & NETWORKING

Traditionally, electric utilities have focused their staffing needs on knowledge and skills around power system, control, and protection. And the reason for this focus is because electric utilities rightly saw these areas as the core of their operation. This problem has come into sharper focus relatively recently with the increase of networked assets growing more pronounced in HVDC and FACTS facilities.

> **Case study:** Standard CIP-005, regarding Electronic Security Perimeters, is one of the CIP standards that requires a high degree of knowledge in IT networking to adequately interpret and apply. Part of the challenges that these authors have observed over the years include inconsistencies in the CIP classification and identification of assets. If an asset is not properly classified, the minimum-security controls which the requirements stipulate may not be applied. For example, assets with External Routable Connectivity (ERC), not classified as such may only have its password changed once at commissioning, instead of every 15 months for its life, increasing risk [12] and potential for fines for not meeting the sub-requirements in the CIP-007 standard.

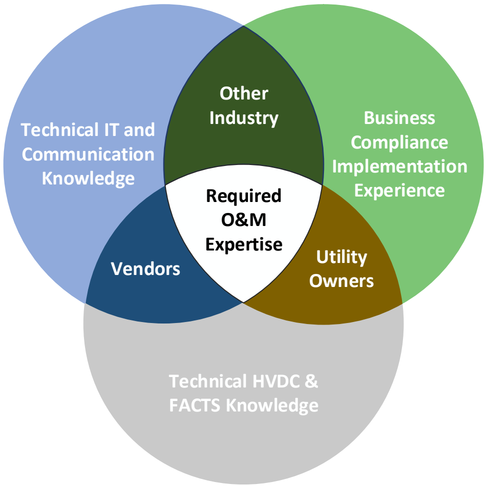

Other Industry
Technical IT and Communication Knowledge
Business Compliance Implementation Experience
Required O&M Expertise
Vendors
Utility Owners
Technical HVDC & FACTS Knowledge

Figure 3 - Required expertise involves several dissimilar disciplines

- Electric utilities should consider allocating training budget to address this gap. An investment strategy using non-monetary parameters [13] will need to be employed. This will ease compliance burden and translate to saving cost in the long run.
- Further research is recommended to quantify this cost with a view to helping electric utilities connect the potential cost of non-compliance to business value. This knowledge will incentivize electric utilities to allocate more budget to training.

5.2 THE PROBLEM OF A HETEROGENEOUS MULTI-VENDOR ENVIRONMENT

A typical substation consists of multiple assets from different vendors. The typical turn-key nature of HVDC & FACTS facilities means that the assets often differ from the Owner's existing asset standards, and there is a greater variation in asset types, and consequently greater variation in accessing, operating, and configuring devices in a networked environment. Familiarity with different configuration software and procedures is critical to both O&M as well as obtaining accurate and relevant data for cybersecurity compliance activities. While not a new problem for HVDC and FACTS facilities, it typically contrasts with AC substation experience.

- An Owner may solve this issue by having well-documented O&M procedures with a system in place to update them as configurations change during the lifecycle of the facilities.

- This problem remains a challenge in a place where there is a high level of staff turnover, and an Owner should additionally consider an extensive staff onboarding program.

6. CONCLUSION

The economics of lifecycle analysis for an HVDC or FACTS facility asset owner has been changing, and many of the risks that an Owner face regarding cybersecurity are constantly evolving. This paper looked at five areas that an Owner should consider when building a new HVDC or FACTS facility, while operating an existing facility, or when considering major upgrades.

1. Additional complexity in studies, design, and integration validation leads to higher control replacement costs.
2. The shortened physical and software lifecycle of digital components leads to a much greater frequency of control system component replacement.
3. Cybersecurity requirements may drive even earlier replacement.
4. An Owner's cybersecurity program will have many costs that should be considered, including patch testing, costs due to a lack of network segregation, and automated data collection tools.
5. There are additional costs of building and maintaining the skillsets for O&M of these facilities that historically were not required.

7. BIBLIOGRAPHY

[1] A. Praca, H. Arakaki, S. Alves, K. Eriksson, J. Graham and G. Biledt, "Itaipu HVDC Transmission System 10 Years Operational Experience," in *V Sepope*, Recife, 1996.

[2] B. Nicol, G. Wild and H. Luo, "Win-TDC: The State-of-the-Art Control and Protection System for HVDC Applications," in *IEEE/PES Transmission & Distribution Conference & Exhibition: Asia & Pacific*, Dalian, 2005.

[3] J. Malmstrom, D. Hallmans and J. Morgan, "10832: Identified challenges and opportunities with Cyber Security standard compliance in combination with a long-expected lifetime," in *CIGRE*, Paris, 2022.

[4] IBM Redbooks, "Architecture, History, Standards, and Trends," in *TCP/IP Tutorial and Overview*, Poughkeepsie, IBM Corporation, 2006, pp. 3-28.

[5] National Telecommunications and Information Administration, "Software Bill of Materials," United States Department of Commerce, 2021. [Online]. Available: https://www.ntia.gov/SBOM. [Accessed 22 August 2022].

[6] NERC, "Security Guideline for the Electricity Sector - Supply Chain: Vendor Risk Management Lifecycle," 17 September 2019. [Online]. Available: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Vendor_Risk_Management_Lifecycle.pdf. [Accessed 22 August 2022].

[7] Microsoft, "Windows XP," Microsoft, [Online]. Available: https://docs.microsoft.com/en-us/lifecycle/products/windows-xp. [Accessed 19 08 2022].

[8] CIGRE Working Group B4.54, "Guidelines For Life Extension of Existing HVDC Systems," CIGRE, 2016.

[9] S. Casavant, "Cybersecurity Tool Integration Challenges with IED in Digital Power Systems," *2020 CIGRE Canada Conference,* no. CIGRE-358, p. 4 of 12, October 19-22, 2020.

[10] Power Systems Relaying Committee of IEEE PES, "IEEE Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control," *IEEE Std. C37.231,* 2006(R2012).

[11] E. Bou-Harb, M. Debbabi and C. Assi, "Cyber Scanning: A Comprehensive Survey," in *IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 3, THIRD QUARTER*, 2014.

[12] M. Bishop, Introduction to Computer Security, Boston: Adison-Wesley, 2005.

[13] R. G. Manalo, "An Investment Analysis Framework to Prioritize Capital Projects of an Electric Distribution Utility Using Analytic Hierarchy Process," in *IEEE International Conference on Management of Innovation and Technology*, Pasig City, 2006.