New HVDC control systems utilize various CPUs with dedicated operating systems in their control systems. In recent years the lifetime of these components has become shorter due to rapid development of the technology. The operating systems and software in particular have a very short life span (an HVDC converter is normally designed with 35-40 years operating life, but control systems may be obsolete after as little as 10 years).

Security updates become obsolete and cannot be updated after only a few years due to outdated platforms.

How should the existing HVDC installations manage the security issues and updates?

This issue can be segregated into two largely independent areas. A first part that considers the interface from the outside world to the HVDC sub-station/control system and a second part that considers the interfaces within the control system.

The first interface is typically protected by firewalls and devices that provide a DMZ. In this case it is suggested that all firewalls should be provided by a well-known company that provides highly respected products that are widely used. In this case a service agreement between the device manufacturer and the end user of the HVDC link may be the most effective method of keeping the security patches up to date. This service may also be able to be provided by the HVDC equipment supplier as part of a service agreement acting as an agent.

The overall system architecture and physical implementation should be designed to anticipate the obsolesce of this/these interface devices and their periodic replacement by a next generation device if the installed unit can no longer be supported by its manufacturer.

The second area tends to be related to the HVDC control system manufacturer who should routinely ensure, for example as part of their normal periodic platform development and release procedures, that the key elements of their HVDC control and protection system have been subjected to cyber security testing and review. In this case the latest platform update could, subject to a service agreement, be considered for installation during a routine maintenance outage.

Even with the timely application of security updates, there is of course still a strong requirement for end user to ensure strict cyber security policies are rigorously adhered to by all of their employees and contractors that have local or remote access to the HVDC sub-station.

How can the lifetime of control systems be extended?

The first and simple step to ensuring a long control system life is to buy the recommended quantity of spares with the initial contract, to correctly maintain the system and to take advantage of any offered “Last Time Buys”.

Market forces continuously drive established technologies to become more compact, use less components and power (driven by reliability), to offer a higher performance and to cost less to manufacture, all of which accelerate obsolescence of the parts used within any control system delivered today.

However, it is possible to design control systems that will more readily withstand the test of time by the careful selection of the system architecture and the components used within that architecture.

Control systems should therefore be designed so that the functional modularity of the system is clearly related to the physical hierarchical modularity of the system and to have well defined logically and physically simple interfaces between each element of the system. Where practical, the interfaces between elements should be governed by well adopted international standards, such as IEC 61850, and the components and modules within the system should be used in volume within worldwide industries that have similar operational life and reliably requirement to HVDC systems.

This approach allows the actual content of each element of the system, not only to remain available for longer, but to be significantly internally adapted to adopt new technologies while remaining backwards compatible with the interfaces that interconnect it to the other elements of the overall control system.

The systematic adoption of this approach allows an element or a group of elements of the system to be replaced or upgraded over time without significant impact on performance or operation of the overall HVDC system.

The other key aspect to lifetime extension in a high evolution rate technology environment is to realise that the most important aspect of a HVDC control system is the control and protection applications rather than the H/W platform on which they execute today.

The control system hardware should therefore completely insulate the application from any physical aspects of the physical HVDC system by virtualising the signal interfaces to the HVDC plant and between applications so that the physical delivery path becomes irrelevant.

The computing power now available, coupled with the almost universal use of the IEEE 802 set of communication standards to provide very cost effective, redundant, high speed and robust communication links, and the availability of IEC 61850 compliant devices to interface to the physical world, all facilitate the delivery of architectures that support a long control system life.

The use of high-level model-based design tools, rather than bespoke in-house tools makes it not only make it easier to deliver high quality robust HVDC applications, but also makes it much easier to adapt to any larger changes in interfaces that may occur if the complete control system is re-furbished in the future.