Briefing
July 2019
International Security Department

Cybersecurity by Design in Civil Nuclear Power Plants

Roger Brunt with Beyza Unal

Summary

- The application of 'security by design' in nuclear new builds could provide operators with the opportunity to establish a robust and resilient security architecture at the beginning of a nuclear power plant's life cycle. This will enhance the protection of the plant and reduce the need for costly security improvements during its operating life.
- Security by design cannot fully protect a nuclear power plant from rapidly evolving cyberattacks, which expose previously unsuspected or unknown vulnerabilities.
- Careful design of security systems and architecture can – and should – achieve levels of protection that exceed current norms and expectations. However, the sourcing of components from a global supply chain means that the integrity of even the most skilfully designed security regime cannot be guaranteed without exhaustive checks of its components.
- Security by design may well include a requirement for a technical support organization to conduct quality assurance of cyber defences and practices, and this regime should be endorsed by a facility's executive board and continued at regular intervals after the new build facility has been commissioned.
- Given the years it takes to design, plan and build a new nuclear power plant, it is important to recognize that from the point of 'design freeze' onwards, the operator will be building in vulnerabilities, as technology continues to evolve rapidly while construction fails to keep pace with it. Security by design cannot be a panacea, but it is an important factor in the establishment of a robust nuclear security – and cybersecurity – culture.

CHATHAM HOUSE
The Royal Institute of International Affairs

Introduction

Cyberattacks are increasingly challenging critical national infrastructure (CNI). Many stakeholders, ranging from governments to private-sector companies, have started to embrace cybersecurity prevention and mitigation measures. One effective measure would be to secure the CNI at the design stage: this is referred to as the 'security by design' (or 'secure by design') approach.

This paper considers the security by design approach for civil nuclear power plants, examining whether it is possible to secure the system architecture at the early stages of development and to build in layers of defence at the design stage – or whether security by design remains an elusive ideal. It refers to two examples of nuclear new build projects – Hinkley Point C in the UK and Barakah in the UAE – that rely to a greater or lesser extent on imported equipment, design or technology. The paper analyses areas of risk and opportunities for the nuclear industry.

Currently, the secure by design approach has to accept that:

- There is no incentive for manufacturers and construction companies to invest in security by design, because it is not a cost-efficient approach. There is a need for operators to exceed regulatory requirements when a project is in its infancy.
- Applying the principle of 'Defence in Depth'[1] for cybersecurity at the design stage may require the commissioning of technical expertise and investment in design, which some executive boards may consider to be both premature and unnecessary at that point in their project's development.
- Imported equipment and software are manufactured to different standards[2] and may trigger unexpected safety vulnerabilities when incorporated in another country's CNI.
- Some software companies have failed to establish robust and effective quality assurance processes before writing code for programmes. This can result in erroneous threat assessments and a failure to identify vulnerabilities before the product is introduced in the CNI.

What is secure by design?

The practical difficulties that confront security managers at existing nuclear facilities remain a significant challenge. This is particularly the case regarding the retrofit of cybersecurity controls to organizations – and their attendant systems – that were brought into service before cybersecurity risks become so prevalent. New build programmes offer the opportunity for a fresh start in the protection of a nuclear facility's sensitive digital assets. Through the installation of modern digital components and state-of-the-art software, along with the recruitment and training of a workforce familiar with an

[1] Defence in Depth was originally a nuclear safety concept. Today, it is also used in nuclear security terminology. The Defence in Depth approach suggests the creation of independent and redundant layers of defence in nuclear power plants, in order to increase safety and security. See, Madsen, M. (2014), 'Defence-in-Depth and Its Role in Nuclear Safety', IAEA, 22 September 2014, www.iaea.org/newscenter/news/defence-depth-and-its-role-nuclear-safety (accessed 6 Mar. 2019).
[2] Foreign-manufactured equipment and software may function in exact accordance with the manufacturer's claims, but without constant scrutiny from transmission system operators with the appropriate expertise, there may be additional (malicious) functions within the equipment/software, which may not have been identified.

embedded nuclear security culture, new builds could represent a step change in how the civil nuclear industry protects its sensitive digital assets. This process could be referred to as 'cybersecurity by design', especially if vendors, designers, manufacturers and constructors of a new build nuclear power plant comprehensively take account of the implications of safeguarding the plant's vulnerable, information-based systems from the very earliest design stages.

Recognizing and applying best practice in cybersecurity would be a reassuring and effective start to a new build, however, maintaining the focus on security in a project as complex as the construction of a nuclear power plant is a major challenge. Funding, design and construction complexities, the recruitment of specialists, and the impact of public, government and media scrutiny are all likely to demand the full attention of senior project managers. At the early stages of design, it would be understandable to not prioritize issues requiring less immediate attention – such as the protection of instrumentation control systems that might not themselves be procured until several years into the project.

Extremely rapid advances in both digital hardware and software often mean that, in a relatively short time, technical capabilities and vulnerabilities can change

Decisions on the protection of sensitive digital assets in a new build project will also be influenced by the significant time it currently takes to design, plan and build a nuclear power plant. Extremely rapid advances in both digital hardware and software often mean that, in a relatively short time, technical capabilities and vulnerabilities can change. In addition, there is a valid consideration that design assumptions made at the outset of a project might be overtaken by technological developments that could be difficult to ignore. In the design of sensitive digital assets for new build projects, there must come a point of 'design freeze', when technology, software and components have to be chosen for the new build plant and when, under the imperative of completing the project on time and on budget, a halt must be called on incorporating future innovations and improvements in the design. Perversely, this has the potential to create similar conditions to those confronted today by the operators of existing nuclear facilities. In other words, the hardware and software may achieve their original objective, but this would not necessarily incorporate the latest advances in protection or system performance when the plant begins operation.

More broadly, the application of security by design in nuclear new builds could provide operators with an opportunity to consider the protection of sensitive digital assets, at least at the beginning of a nuclear power plant's life cycle. In the long run, security by design cannot be taken for granted, because cyber risks change and evolve rapidly and new ways to infiltrate the system architecture will emerge. Establishing layers of security – for instance, by designing a secure software development life cycle, and by creating a framework for nuclear security culture and by establishing cybersecurity best practices – is key to minimizing the risks, but it is essential that these initiatives are complemented by robust quality assurance programmes, which check for vulnerabilities in a product both before it is integrated into the critical system and then subsequently during its operating life.

Careful design can – and should – achieve levels of protection that exceed current norms and expectations, but the sourcing of components from a global supply chain means that the integrity of even the most skilfully designed security regime cannot be guaranteed without exhaustive checks of its components. Once a system designed to protect sensitive digital assets is operational, it will no doubt have an appeal to a cyberattacker as a challenge to be beaten.

A 2015 Chatham House research paper highlighted a point of view – held by many in the civil nuclear industry at the time – that nuclear facilities were de facto protected from cyberattacks by a perceived 'air gap' between instrumentation and control systems and the internet.[3] However, recently there have been enough successful attacks on sensitive digital assets in the nuclear sector and other industries to discredit that assumption. It is more likely that hackers will regard elaborate cybersecurity architecture as simply another target to defeat or discredit, and it cannot be assumed that cybersecurity by design will ever deliver infallible protection against the range of threats that the sector faces. Cybersecurity by design, however, may provide a resilient security architecture that could protect a plant's system, software and networks from malicious access, at least until new threat vectors arise. Therefore, cyber defences must evolve along with the threat.

Many operators will rely on in-house experts who will use their experience and their detailed knowledge of a nuclear facility's systems to meet regulatory and operational requirements

Regulators will expect nuclear operators to continue to employ plans and policy in order to fend off cyberthreats. Many operators will rely on in-house experts who will use their experience and their detailed knowledge of a nuclear facility's systems to meet regulatory and operational requirements. However, even in-house expertise may not be enough, and some form of outside assistance could be required, if only to provide a source of impartial assurance to the facility's executive board that the facility is adequately protected. Cybersecurity by design may well include a requirement for a technical support organization to conduct quality assurance and penetration testing, but after the new build facility has been commissioned, the executive board should give direction – ensuring that such practices and testing occur regularly, and that board members themselves understand the implications of the vulnerabilities unearthed by the penetration test procedure.

Over the life cycle of a new nuclear plant, implementing recommendations made in the 2015 Chatham House research paper in the context of a robust design promoting cybersecurity may contribute to the protection of sensitive digital assets. Sharing experiences through effective information exchange, as well as training and motivating the executive boards of nuclear operators and their employees to improve their personal approaches to nuclear security culture – including cybersecurity, setting rules and standards in dealing with cybersecurity challenges and addressing supply chain vulnerabilities – may each have an effect out of all proportion to the resources required to implement such recommendations.

Cybersecurity regulations and guidance for civil nuclear facilities

There is no internationally recognized 'gold standard' on how nuclear cybersecurity should be organized, but several international organizations and regional bodies have published guidance. This paper notes the position of the International Atomic Energy Agency (IAEA) that security is a national responsibility. For the civil nuclear sector, the IAEA publishes nuclear security recommendations that reflect internationally accepted best practice, but there are no recognized international regulations as such. Other non-governmental organizations and lobbying groups, such as the World Institute for Nuclear Security (WINS),[4] have issued high-level guidance documents on how

[3] Baylon, C., Brunt, R. and Livingstone, D. (2015), *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, Chatham House Report, www.chathamhouse.org/sites/default/files/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf (accessed 6 Mar. 2019).
[4] World Institute for Nuclear Security (2014), *4.3 Security of IT and IC systems at Nuclear Facilities*, WINS International Best Practice Guide, https://wins.org/document/4-3-security-of-it-and-ic-systems-at-nuclear-facilities (accessed 6 Mar. 2019).

national infrastructure for cybersecurity might be prepared, while instructions from organizations that set industry guidance in CNI have also provided useful technical advice.[5] Some national authorities have created comparable technical frameworks and processes. For instance, the National Institute of Standards and Technology (NIST), a non-regulatory agency of the US Department of Commerce, has developed guidance specifically to assist nuclear facilities in complying with multi-faceted regulations to verify that the computers, digital communications and systems in CNI are protected from cyberattacks.[6]

Guidance for greater cybersecurity at nuclear facilities has also been issued through regional advisory bodies, such as the European Union's Energy Expert Cyber Security Platform (EECSP). A cross–sectoral EECSP report from February 2017 identified vulnerable cybersecurity gaps in EU member states' energy sectors, and recommended various initiatives for the European Commission to develop a European strategic framework and auxiliary legislative acts to promote greater cybersecurity in the nuclear sector.[7] At the international level, successive UN Groups of Governmental Experts (GGE) delivered reports in 2010,[8] 2013[9] and 2015[10] on cyber developments in the context of international security. An important recommendation from the 2015 GGE report was that states should not conduct or knowingly support activity that intentionally damages or otherwise impairs the use and operations of critical infrastructure. It also recommended that states should take appropriate cybersecurity measures to protect these facilities.[11] Despite a consensus regarding the desired inviolability of CNI from cyberattacks, conflicting national interpretations of how international law applies to state responses in the event of a cyberattack have thwarted further discussion,[12] emphasizing the shortcomings in multilateral decision-making in the context of cybersecurity.

Challenges to establishing greater cybersecurity

Although there has been some progress in developing enhanced cybersecurity measures across the nuclear industry, the fact remains that national responses and private-industry-led protection from cyberthreats at nuclear facilities remain fragmentary. The 2016 Nuclear Security Index,[13] published by the Nuclear Threat

[5] International Society of Automation (2007), 'ISA-62443-1-1-2007 Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models', www.isa.org/store/ansi/isa%E2%80%9362443-1-1-990101%E2%80%932007-security-for-industrial-automation-and-control-systems-part-1-terminology,-concepts,-and-models/116720 (accessed 6 Mar. 2019).
[6] National Institute of Standards and Technology (2018), *Framework for Improving Critical Infrastructure Cybersecurity*, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed 6 Mar. 2019).
[7] Energy Expert Cyber Security Platform (2017), *Cyber Security in the Energy Sector*, https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf (accessed 6 Mar. 2019).
[8] United Nations General Assembly (2010), *Developments in the field of information and telecommunications in the context of international security*, https://undocs.org/A/65/154 (accessed 6 Mar. 2019).
[9] United Nations General Assembly (2013), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf (accessed 6 Mar. 2019).
[10] United Nations General Assembly (2015), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (accessed 6 Mar. 2019).
[11] Ibid.
[12] Markoff, M. (2017), 'Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security', www.state.gov/s/cyberissues/releasesandremarks/272175.htm (accessed 6 Mar. 2019).
[13] Nuclear Threat Initiative (2016), *Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities*, www.nti.org/media/documents/NTI_CyberThreats__FINAL.pdf (accessed 6 Mar. 2019).

Initiative (NTI), demonstrated this inconsistent global approach to cybersecurity programmes at nuclear facilities by measuring highly divergent national cybersecurity frameworks.[14] A 2015 joint academic–industrial study[15] assessing national cybersecurity initiatives in the nuclear industry also noted this inconsistency. A categorization methodology grouped cybersecurity methods at state level into three modes of operation: a well-defined and institutionalized management, such as those in place in Germany[16] and the US;[17] a more fragmented and less formalized approach, but one still implementing multiple initiatives overseen by competent authorities, as found in Russia;[18] and ultimately a sporadic and ad-hoc approach to cybersecurity with little impact within nuclear plants, as found in South Africa.[19]

Divergent approaches to system updates within nuclear facilities has diminished the potential gains that may be made from those updates

Analyses conducted by industry and the academic sphere on best practices in cybersecurity share the principle that proactively addressing computer vulnerabilities is crucial to the better protection of systems.[20] From an IT engineer's perspective, patching is a reliable method of improving a system's security against cyberthreats. Software patching, which originated when digital technology was in its infancy, is a sequence of defensive reactions, protecting vulnerabilities discovered in software. However, divergent approaches to system updates within nuclear facilities, caused by conflicting priorities and cultural divides between operational technology engineers and their IT counterparts, has diminished the potential gains that may be made from those updates.[21] Even when compromises between nuclear facility personnel are achieved, patching at nuclear plants presents unique challenges.[22]

Furthermore, although software updates are designed to close security loopholes, they may also alert attackers to system vulnerabilities. A National Academy of Sciences workshop on cyber resilience observed that by comparing old software with updated versions, hackers might be able to identify the vulnerability being patched and attack systems that have not yet updated their software.[23] In conjunction with the constant evolution of viruses and worms, the protracted upgrade cycle of cybersecurity at nuclear facilities is incompatible with the critical need for expeditious software upgrades to close security gaps. Aggravating this concern is the reality that legacy products are vulnerable to discontinued manufacturer support due to obsolescence and might also be incompatible with newer software updates.[24]

[14] Ibid.
[15] Fachhochschule Brandenburg University of Applied Sciences Institute for Security and Safety (2015), *Cyber Security at Nuclear Facilities: National Approaches*, www.nti.org/media/pdfs/Cyber_Security_in_Nuclear_FINAL_UZNMggd.pdf (accessed 6 Mar. 2019).
[16] Bundesministerium des Inneren (2009), *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html (accessed 27 Mar. 2019).
[17] United States Nuclear Regulatory Commission (2017), '§ 73.54 Protection of digital computer and communication systems and networks', www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html (accessed 6 Mar. 2019).
[18] Federal Service for Technical and Export Control of Russia (n.d.), 'Information on powers of FSTEC of Russia; list of regulatory legal acts determining these powers', https://fstec.ru/en/359-powers (accessed 6 Mar. 2019).
[19] Sidhu, W. P. S. (2016), *What the Nuclear Security Summits mean for South Africa*, Brookings, www.brookings.edu/opinions/what-the-nuclear-security-summits-mean-for-south-africa/ (accessed 6 Mar. 2019).
[20] Chamales, G. (2015), *A New Approach to Nuclear Computer Security*, https://www.nti.org/analysis/reports/new-approach-nuclear-computer-security/ (accessed 6 Mar. 2019).
[21] Baylon, Brunt and Livingstone (2015), *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*.
[22] Ibid.
[23] National Academies of Sciences, Engineering, and Medicine (2017), *Software Update as a Mechanism for Resilience and Security: Proceedings of a Workshop*, Washington, DC: The National Academies Press, doi: 10.17226/24833 (accessed 6 Mar. 2019).
[24] Ibid.

Cybersecurity at nuclear facilities is also exacerbated by a technical mélange of systems and equipment, including legacy analogue infrastructure. While the rudimentary hardwiring installed in nuclear plants built in the 1960s, 1970s and 1980s provided little flexibility to system operators, it perversely reduced the scope for hackers to subvert systems.[25] As legacy analogue systems at nuclear plants are progressively replaced by digital systems, 'protection by antiquity' is becoming a less viable defence measure.

Since many nuclear facilities started pursuing better integration of Supervisory Control and Data Acquisition (SCADA) systems – which are control systems that rely on human–machine interface (HMI) – with field devices and HMI computers in the 1990s, the wholescale incorporation of 'off the shelf' hardware and software, such as Windows or Linux, from a limited number of vendors[26] has become commonplace. This practice provides plant operators with greater cost savings and efficiency,[27] but at the expense of facilitating the rise of 'insecure by design' nuclear facilities, as programmable code can be altered by hackers to change the function of a device. The relatively recent inclusion of digital systems on new builds and Internet of Things (IoT) applications,[28] intermingled within an industry that still operates piecemeal analogue systems, reflects the inability of the nuclear industry to establish a consensus on technical unanimity. This approach is the antithesis to the successful maintenance of the safety culture, which is of paramount concern to the industry.

It remains a possibility that a successful cyberattack might disrupt the supply of power to the national grid, but the likelihood of this is somewhat mitigated by the reality that for such an outcome to occur, multiple safety features would have to fail simultaneously. For an industry that is so susceptible to criticism – both in terms of public image and its high potential to cause harm – it should be a priority to address the significant shortcomings in contemporary cybersecurity given the profusion of malicious actors, the variability of regulatory standards, and the existing principles governing the nuclear industry's safety and security measures.

Cybersecurity by design

Understanding the asymmetrical approach to international cybersecurity is critical in implementing universal and comprehensive initiatives to better protect nuclear facilities from cyberthreats. As well as the manifest risk to populations and environments from a release of ionizing radiation, disrupting nuclear energy production might produce severe cascading economic and social effects in the affected state. Nuclear energy is utilized in 31 countries[29] and provides around 11 per cent of the world's electricity.[30] While some nuclear power-producing nations, such as Brazil and the Netherlands, rely on minimal nuclear energy for their domestic energy consumption needs, others, such as France, Ukraine and Slovakia, generate more than 50 per cent

[25] Baylon, Brunt and Livingstone (2015), *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*.
[26] Kesler, B. (2011), 'The Vulnerability of Nuclear Facilities to Cyber Attack', *Strategic Insights*, 10(1): pp. 15–25 (accessed 6 Mar. 2019).
[27] Baylon, Brunt and Livingstone (2015), *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*.
[28] UK Department for Digital, Culture, Media & Sport (2018), *Secure by Design report*, https://www.gov.uk/government/publications/secure-by-design-report (accessed 6 Mar. 2019).
[29] IAEA PRIS (2019), 'Nuclear Share of Electricity Generation in 2017', www.iaea.org/PRIS/WorldStatistics/NuclearShareofElectricityGeneration.aspx (accessed 6 Mar. 2019).
[30] World Nuclear Association (2019), 'Nuclear Power in the World Today', www.world-nuclear.org/information-library/current-and-future-generation/nuclear-power-in-the-world-today.aspx (accessed 6 Mar. 2019).

of their electricity in the form of nuclear energy.[31] A disruption to this supply might have sweeping consequences. A 2014 publication identifying CNIs and their dependencies observed that the energy sector was so interconnected to other infrastructures that a disruption would also appreciably affect telecommunications, healthcare, transportation, manufacturing and other critical infrastructures.[32] There is a clear imperative to mitigate the possibility and the consequences of a successful cyberattack on the civil nuclear sector.

Supplementary research projects from the academic sphere (which include the seminal *Tallinn Manual 2.0*), have focused on the legal, regulatory and institutional frameworks crucial for cybersecurity implementation at nuclear fuel-cycle facilities, providing blueprints for the next steps forward.[33]

New-build case studies

Hinkley Point C

The UK is a 'developed' nuclear country with defence and civil nuclear programmes. As recently as the 1990s, the UK had been at the forefront of nuclear research and development and encouraged the growth of a significant nuclear industry across the nuclear fuel cycle, including enrichment, fuel manufacture, electricity generation and reprocessing. Levels of nuclear capability in the UK were high in terms of trained staff, research establishments and a competent, respected and well-resourced regulator, and the industry made a major contribution to the UK's economy. However, since the early 1990s, the profile of the nuclear industry in the UK has been in decline and the capability of the industry has waned to such an extent that when a decision was made to maintain the capability to generate a proportion of the UK's electricity from nuclear power plants, the domestic nuclear sector had lost the ability to design and construct a British nuclear power plant.

The Office for Nuclear Regulation (ONR) is the UK regulator for safety and security in the civil nuclear industry and is responsible for ensuring that operators comply with current UK regulatory requirements. In 2007, the ONR announced a Generic Design Assessment (GDA) process to scrutinize candidate designs for new build nuclear power plants in the UK, with the express purpose of verifying that such designs could be safely and securely constructed and operated within the UK. The process involved the development of sophisticated procedures to enable the exchange of sensitive nuclear information between national jurisdictions, particularly between the UK and France.

The GDA conducted an intense and comprehensive examination of the candidate designs submitted for approval, and the first to complete the process successfully was the predominantly French European Pressurized Reactor (EPR) for construction at Hinkley Point C in Somerset.

[31] IAEA PRIS (2019), 'Nuclear Share of Electricity Generation in 2017'.
[32] Singh, A. N., Gupta, M. P. and Ojha, A. (2014), 'Identifying Critical Infrastructure Sectors and their Dependencies: An Indian Scenario', *International Journal of Critical Infrastructure Protection*, 7 (10): pp. 71–85, doi: 10.1016/j.ijcip.2014.04.003 (accessed 6 Mar. 2019).
[33] Fachhochschule Brandenburg University of Applied Sciences Institute for Security and Safety (2015), *Cyber Security at Nuclear Facilities: National Approaches; Schmitt, M. N. (2017), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.

When construction started in 2016, the total anticipated cost of Hinkley Point C was estimated at £18 billion

The Areva-designed twin EPR that will be built at Hinkley Point C will generate 3,200 megawatts of electricity (MWe), enough to meet the electricity needs of nearly 6 million homes.[34] When construction started in 2016, the total anticipated cost of Hinkley Point C was estimated at £18 billion. However, this estimation rose by roughly 10 per cent in July 2017, to £20.3 billion, as a result of delays in complying with UK regulations.[35] It is expected that the plant will begin generating electricity for the UK market in 2025, eight years behind schedule.[36] To pay for it, the British government has entered into a complex financial agreement with the energy giant Electricité de France (EDF), of which 83.5 per cent is owned by the French government, with the remaining 16.5 per cent being distributed principally between institutional and individual shareholders. EDF energy projects cover thermal, nuclear and renewable electricity generation at sites in Africa, Asia, Europe and North America.[37] Of the 584 terawatts an hour produced by EDF, 78 per cent is supplied from nuclear facilities.[38] The company also controls a large electricity distribution network, Enedis,[39] which covers 95 per cent of the French metropolitan area.

As well as EDF's investment in the Hinkley Point C power station, China General Nuclear Power Group (CGN), a state-run Chinese energy company,[40] agreed in 2015 to acquire a 33.5 per cent stake in the construction project.[41] As part of the Hinkley Point C deal, CGN also took a 20 per cent stake in the development phase of a new project at the Sizewell nuclear power generating site, Suffolk,[42] and discussions began on proposals for the construction of a new Chinese-designed nuclear power station at an existing site at Bradwell-on-Sea in Essex.[43] CGN is the largest nuclear power operator in China and the largest nuclear power constructor worldwide.[44] CGN's domestic stature has encouraged international expansionism, and the company plans to be among the top three global producers of nuclear energy by the year 2020.[45] CGN is also vertically integrated in the nuclear industry, owning stakes in various stages of the nuclear fuel cycle, often through complex ownership arrangements. Supplementing CGN's nuclear electricity production and uranium mining, the company also has clean-energy projects

[34] UK Environment Agency (2013), 'Nuclear power: Hinkley Point', Collection, www.gov.uk/government/collections/hinkley-point (accessed 6 Mar. 2019).
[35] BBC News (2017), 'Hinkley Point: EDF adds £1.5bn to nuclear plant cost', www.bbc.co.uk/news/business-40479053 (accessed 6 Mar. 2019).
[36] Ibid.
[37] EDF (n.d.), 'EDF in the world', www.edf.fr/en/the-edf-group/who-we-are/edf-in-the-world (accessed 6 Mar. 2019).
[38] EDF (n.d.), 'From your lightbulbs to our plants', www.edf.fr/en/the-edf-group/who-we-are/activities/home (accessed 16 May 2019).
[39] EDF (n.d.), 'Transmission and distribution for a secure, reliable supply', www.edf.fr/en/the-edf-group/who-we-are/activities/transmission-and-distribution (accessed 16 May 2019).
[40] Watt, H. (2017), 'Hinkley Point: the 'dreadful deal' behind the world's most expensive power plant', *The Guardian*, 21 December 2017, www.theguardian.com/news/2017/dec/21/hinkley-point-c-dreadful-deal-behind-worlds-most-expensive-power-plant (accessed 6 Mar. 2019).
[41] World Nuclear News (2017), 'Hinkley Point C gets go-ahead for construction', www.world-nuclear-news.org/RS-Hinkley-Point-C-gets-goahead-for-construction-28031701.html (accessed 6 Mar. 2019).
[42] EDF Energy (2019), 'Sizewell C', http://sizewell.edfenergyconsultation.info/wp-content/uploads/2016/02/Sizewell-C-Community-Newsletter-December-2015.pdf (accessed 6 Mar. 2019).
[43] Bradwell B. (n.d.), 'Bradwell B Project Website: Developing Bradwell B in partnership', https://bradwellb.co.uk/ (accessed 6 Mar. 2019).
[44] China General Nuclear Power Corporation (2016), 'CGN A leader in Clean Energy', http://en.cgnpc.com.cn/encgn/c100028/Profile.shtml (accessed 6 Mar. 2019).
[45] China General Nuclear Power Corporation (2016), 'Strategy', http://en.cgnpc.com.cn/encgn/c100031/list_tt.shtml (accessed 6 Mar. 2019).

in Singapore,[46] gas- and oil-powered facilities in South Korea,[47] and the Edra project, an extensive multilateral energy operation, which provides power from 13 oil and gas facilities to five states participating in the Belt and Road Initiative (Malaysia, Egypt, Bangladesh, the UAE and Pakistan).[48]

Senior military and intelligence figures warned UK ministers that the scheme posed a threat to UK national security, as corrupted components might have hidden functions or access capabilities

CGN's investment in Hinkley Point C, and its aspiration in the long term to construct a Hualong One reactor at Bradwell, raised security concerns among the UK's defence and security community. In October 2015, senior military and intelligence figures warned UK ministers that the scheme posed a threat to UK national security, as corrupted components might have hidden functions or access (backdoor) capabilities that could be inserted into IT systems,[49] thereby allowing Chinese intelligence agencies to bypass British cybersecurity measures.[50] The EECSP noted in a 2017 recommendation report that, given the opacity of backdoors, 'a state actor might use these functions in the near or far future to control critical components of power systems'.[51] As a consequence of these concerns, in July 2016, British Prime Minister Theresa May announced a surprise review of the Hinkley Point C plan, which temporarily delayed its approval.[52] The prime minister's caution with regard to foreign investment in the UK's national infrastructure is consistent with her earlier security concerns when home secretary during the 2010–15 coalition government.[53] Theresa May's political adviser at the time, Nick Timothy, also reportedly cautioned her that Chinese investment in critical infrastructure might be troublesome, given that CGN states that part of its mission was the responsibility for 'the building of national defence'.[54]

It is important to acknowledge risks that foreign equipment and systems may pose to the UK's nuclear power plants, and to ensure that necessary resilience measures are sufficient to offset such risk. Foreign suppliers should meet all cybersecurity requirements and provide evidence that they would protect their equipment and systems throughout the latter's life cycle.

The UK is one of the leading countries in the world in implementing cybersecurity measures across the CNI sectors, and it is to be expected that the relevant UK authorities are alert to the potential threat posed by such a significant foreign interest in UK CNI. It is to be expected that the UK has the capability and financial resources to take appropriate measures against threats should the need arise. However, not all states

[46] China General Nuclear Power Corporation (2016), 'Singapore', http://en.cgnpc.com.cn/encgn/c100096/singapore.shtml (accessed 6 Mar. 2019).
[47] China General Nuclear Power Corporation (2016), 'Korea Introduction', http://en.cgnpc.com.cn/encgn/c100095/2016-08/25/content_760b64289c2d41ddb8b6e36b95fcb4af.shtml (accessed 6 Mar. 2019).
[48] China General Nuclear Power Corporation (2016), 'Malaysia Introduction', http://en.cgnpc.com.cn/encgn/c100085/2016-08/25/content_8928f6f65eb449de9e7ee5b4fdba6020.shtml (accessed 6 Mar. 2019).
[49] O'Neill, S., Haynes, D. and Pagnamenta, R. (2015), 'Nuclear deal with China is threat to UK security', *The Times*, 16 October 2015, www.thetimes.co.uk/article/nuclear-deal-with-china-is-threat-to-uk-security-jv7xnh975vj (accessed 6 Mar. 2019).
[50] BBC News (2015), 'Security fears over China nuclear power deal', www.bbc.co.uk/news/uk-politics-34549478 (accessed 6 Mar. 2019).
[51] Energy Expert Cyber Security Platform (2017), *Cyber Security in the Energy Sector*.
[52] Swinford, S. and Gosden, E. (2016), 'Theresa May delays Hinkley nuclear decision amid concerns over Chinese involvement', *The Telegraph*, 29 July 2016, www.telegraph.co.uk/business/2016/07/29/theresa-may-delays-hinkley-nuclear-decision-amid-concerns-over-c/ (accessed 6 Mar. 2019).
[53] Austin, H. (2016), 'Theresa May objected to Hinkley Point when a coalition minister says Vince Cable', International Business Times, 30 July 2016, www.ibtimes.co.uk/theresa-may-objected-hinkley-point-when-coalition-minister-says-vince-cable-1573389 (accessed 6 Mar. 2019).
[54] Hill, H. (2016), 'Hinkley Point 2) What Nick Timothy wrote on ConHome about China's role', ConservativeHome blog, www.conservativehome.com/parliament/2016/07/what-nick-timothy-wrote-on-conhome-about-china-and-hinckley-point.html (accessed 8 Mar. 2019).

with a new build nuclear programme have the same level of expertise and resources, and projects similar to Hinkley Point C should not necessarily view the UK experience as a blueprint to follow.

Barakah nuclear power plant, UAE

In marked contrast to the UK, the UAE is developing its nuclear capability with very little domestic nuclear experience but with the clear imperative to identify and deploy an affordable alternative to oil and gas to meet its domestic electricity demands, particularly for desalinization plants. Countries with similar nuclear ambitions to the UAE have in many cases chosen to develop their nuclear capability incrementally over a period of many years, 'growing' domestic expertise through education and training, gradually introducing legal and regulatory frameworks, and adequately preparing their citizens through training and experience to step up to important positions of responsibility within the national nuclear framework.

With the Bakarah nuclear power plant, the UAE's goal is to deliver nuclear energy to the country and to diversify energy sources; to increase economic growth and, through this new industry, to increase the employment opportunities in the country.[55] In embarking on their nuclear programme, the Emiratis had neither the luxury of sufficient time for an incremental approach – due to the economic requirement to reduce their dependency on oil – nor the human resources to sustain the size of programme their economic position required. Instead, they chose to rely on engaging foreign expertise across the board to enable the construction of four nuclear reactors at Barakah and to ensure that, in every respect, the UAE could comply with the nuclear safety and security expectations of the international community as articulated through guidance issued by the IAEA. In 2009, the Korea Electric Power Corporation (KEPCO) was awarded the contract to design, build and operate the UAE's first nuclear power station.[56]

This bold approach has delivered the first of four units[57] at Barakah, constructed by a South Korean consortium led by KEPCO, while the regulatory framework has been created through the recruitment of experienced expatriates, with a clear commitment to transition to Emirati citizenship over time in order to provide sustainable expertise. It remains to be seen whether those countries whose expatriates have provided these skills will be able to transfer that expertise to Emiratis in the long term. In the case of the Barakah nuclear project, employing expatriates of proven ability and broad experience has created an Emirati 'competent authority', whose standards of regulation comply with internationally recognized norms.

[55] Emirates Nuclear Energy Corporation (n.d.), 'Barakah Nuclear Energy Plant', www.enec.gov.ae/barakah-npp (accessed 28 Apr. 2019).
[56] Emirates Nuclear Energy Corporation (n.d.), 'Leaders in safety, reliability and efficiency', www.enec.gov.ae/barakah-npp/prime-contractor/ (accessed 28 Apr. 2019).
[57] See World Nuclear News (2018), 'Cold testing complete at Barakah 3', 17 December 2018, www.world-nuclear-news.org/Articles/Cold-testing-complete-at-Barakah-3 (accessed 28 Apr. 2019).

Currently, there are delays in beginning operations at the Bakarah reactors, due to the long approval process for an operating licence; the lack of availability of operating staff; and the conclusion of repairs in the second and third reactors.[58] In 2018, the Emirati Nawah Energy Company signed an agreement with EDF whereby the latter would provide operational and maintenance services.[59]

South Korea was the major source of components and assemblies for Barakah, and therefore potential concerns about the integrity of the supply chain are likely to have been limited

Despite delays, the Bakarah project has been a notable success for the Emiratis, albeit with a heavy reliance on foreign expertise and design, and with an almost total dependence on a globalized supply chain. In seeking to judge how cybersecurity by design might have been integral to this project, it is reasonable to assume that the Barakah units incorporate any improvements to the design identified at existing similar power plants in South Korea. Potential concerns about the integrity of the supply chain are likely to be limited as South Korea was the major source of components and assemblies for Barakah. The onus for maintaining the security of the facility will remain with KEPCO, which has an overwhelming financial and reputational interest in its continuing success. Furthermore, since the UAE's Federal Authority for Nuclear Regulation comprises experienced, expatriate regulators (many previously employed at the US Nuclear Regulatory Commission), it could be expected that tough, impartial questions would be asked of designers and constructors to ensure that the need for effective security was considered from the start of the project.

It is worth noting that the state-owned South Korean nuclear plant operator Korea Hydro and Nuclear Power was subject in December 2014 to a cyberattack, which was attributed to North Korea. Although the nuclear control systems were not compromised, the attack served to illustrate that the South Korean nuclear facility design was no more immune to cyberattack than its competitors. Hence, it will be important for the UAE to maintain a dialogue promoting the exchange of matters of mutual nuclear security interest with South Korea to protect its nuclear power plants against cyberattack: indeed, the UAE should benefit from the lessons learned from such attacks.

The Bakarah nuclear power plant could be a test case for establishing the desired procurement model for cybersecurity when there is total reliance on foreign companies through the supply chain. If the UAE, through its contract with KEPCO, could ensure the integrity of the supply chain for the main components and assemblies, then there would be less reason for the Emiratis to be concerned about long-term vulnerabilities within the project.

Conclusion

Since the 9/11 terrorist attacks in New York and Washington, DC, reviews of CNI in many countries have prompted numerous security improvements, often involving costly, complicated and sub-optimal retrofits in facilities nearing the end of their operating lives. Within the civil nuclear sector, the so-called 'nuclear renaissance' and the prospect of constructing a series of new build nuclear power plants has encouraged regulators

[58] Sadouki, F. (2019), 'Delays to UAE Barakah nuclear plant to support gas', Interfax Global Energy, 11 April 2019, http://interfaxenergy.com/article/34130/uaes-barakah-nuclear-delay-to-support-gas (accessed 28 Apr. 2019).
[59] EDF (2018), 'EDF and Nawah Energy Company sign operations and maintenance assistance agreement for Barakah Nuclear Energy Plant, United Arab Emirates', EDF press release, 22 November 2018, www.edf.fr/en/the-edf-group/dedicated-sections/journalists/all-press-releases/edf-and-nawah-energy-company-sign-operations-and-maintenance-assistance-agreement-for-barakah-nuclear-energy-plant-united-arab-emirates (accessed 28 Apr. 2019).

and operators to think hard about the security of nuclear facilities throughout their life cycle. In the immediate aftermath of 9/11, the object of these security reviews early in the design process was to implement physical protection measures, but the debate has been dominated increasingly over the last decade by the growing threat from cyberattacks. Moreover, rigorous regulatory reviews have been implemented and increased attention paid to security in the wake of the meltdown at the Fukushima Daiichi nuclear plant in March 2011, which followed a tsunami.

The aspiration among many is to improve resilience against cyberthreats through security by design. Whereas physical protection measures at new nuclear power plants could be designed and built to take account of how the threat of physical attack might develop in the years ahead, the rapidly changing and evolving cyberthreat presents greater challenges to designers and is likely to continue doing so. There will always be a compelling argument to design and incorporate as much security as is reasonably possible into the digital systems of a new nuclear power plant as early as possible, but it is hard to see how such design decisions can remain robust and effective in the context of exponential developments in cyber capability and cyberthreats, while being implemented within the timelines for the construction of a new nuclear power plant. This remains the biggest challenge in the concept of security by design.

There is no panacea against cyberattacks. However, strong security, built into the design of a nuclear power plant, can provide a layer of defence against current and emerging cyberthreats by limiting attack vectors and vulnerabilities in sensitive digital technology. The executive boards of nuclear operators should focus on building and sustaining an effective and demanding nuclear security culture, including cybersecurity, which all employees should adopt and practise. Boards should also recognize the contribution that can be made by technical support organizations familiar with both the cyberthreat environment and the nuclear sector to the protection of their digital assets. Above all, operators and regulators must guard against complacency and must demand sustained commitment to security, including cybersecurity, within the civil nuclear sector and across the supply chain.

Acronyms and Abbreviations

CGN	China General Nuclear Power Group
CNI	Critical national infrastructure
EDF	Electricité de France
EECSP	Energy Expert Cyber Security Platform
EPR	European Pressurized Reactor
GDA	Generic Design Assessment
GGE	UN Group(s) of Governmental Experts
HMI	Human–machine interface
IAEA	International Atomic Energy Agency
IoT	Internet of Things
MWe	Megawatts of electricity
NIST	National Institute of Standards and Technology (US)
ONR	Office for Nuclear Regulation (UK)
SCADA	Supervisory Control and Data Acquisition
WINS	World Institute for Nuclear Security

About the Authors

Roger Brunt retired from the British Army in 2004. In the same year, he was appointed director of the UK Office for Civil Nuclear Security (OCNS), a role he held until 2011. During this time, he oversaw the consolidation and improvement of security arrangements at civil nuclear sites in the UK. In 2011–16, he represented the UK as part of the IAEA's Advisory Group on Nuclear Security.

Since 2011, he has worked as a nuclear security consultant, advising on the interpretation and application of IAEA recommendations on nuclear security and promoting awareness of nuclear security issues and policy. He has taken part in an IAEA International Physical Protection Advisory Service mission; advised new-build nuclear operators on security; written and delivered high-level crisis management exercises for boards of nuclear power companies; and contributed to the development of cybersecurity within the sector.

Dr Beyza Unal is a senior research fellow with the International Security Department at Chatham House. She specializes in nuclear and cyber policies, conducting research on cybersecurity and critical national infrastructure security and cybersecurity of nuclear weapons systems. Dr Unal also conducts research on urban preparedness and city resilience against CBRN threats.

She formerly worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, taught international relations, transcribed interviews on Turkish political history, and served as an international election observer during the 2010 Iraqi parliamentary elections.

Dr Unal is interested in NATO's defence and security policy as well as security in the Middle East, and has been given various fellowships for her achievements; most notably, she is a William J. Fulbright alumna.

She has also received funding from the US Department of Energy to participate in workshops in Brookhaven National Laboratory, the James Martin Centre for Nonproliferation Studies, and Sandia National Laboratory.

Acknowledgments

The authors would like to thank the International Security Department (ISD) at Chatham House for their assistance in this study. Special thanks go to Tim Wright, a former ISD intern, who worked on previous versions of this briefing paper. Thanks to Dr Patricia Lewis and to the ISD steering committee on cybersecurity of nuclear power plants, for all their support and contributions. We are grateful to the John D. and Catherine T. MacArthur Foundation for their generous funding for this paper.

Thanks also to the peer reviewers and all those who commented on the briefing paper; to Calum Inverarity in the ISD at Chatham House; and to Vera Chapman Browne and to Michael Tsang for editing the draft briefing, together with the Chatham House editorial team.

ISBN 978 1 78413 335 1

This publication is printed on FSC-certified paper.

Typeset by Soapbox, www.soapbox.co.uk