12-2023

Automation Complacency on Humans and Cyber-Physical Systems in the Energy Sector

Shannon Olaveson

Boise State University

Automation Complacency on Humans and Cyber-Physical Systems in the Energy Sector

by

Shannon Olaveson

A project completed in fulfillment

of the CORe 591 requirements for the degree of

Master of Science in Cyber Operations and Resilience

Boise State University

December 2023

Automation Complacency on Humans and Cyber-Physical Systems in the Energy Sector

Shannon Olaveson
Boise State University, Boise, United States

Abstract: Cyber-physical systems (CPS) and the Industrial Internet of Things (IoT) enable industrial systems and technology to work together to achieve increased connectivity and operational efficiency through the use of automation. Because automation requires less human interaction to run industrial tasks, a reliance may form on this integration to take over an otherwise manual process. This reliance can cause human behavior to affect operational safety and security, leading to unintentional outcomes or vulnerable areas of adversarial opportunity. The energy sector is one of the most critical infrastructure areas becoming a part of the rise to automation, resourcing gas, oil, and electricity to all sectors. There is an urgent need to contribute to research involving the energy sector and occurrences that may have directly resulted from automation complacency to further understand causal factors and how overreliance affects real-life outcomes. Observations of post-incident events, both adversarial and unintentional in nature were used to understand how the human element may contribute to failure or misuse when systems and processes are automated. What was found was a similarity in event outcomes regardless of whether the event was adversarial or unintentional, in relation to safety, security, and human behavior. Further analysis indicated a correlation of factors contributing to this behavior, and how each plays a role in event outcomes. These were attributed to poor system management/design and lack of training for those who monitor, manage, and provide communications in relation to the CPS. Based on similarity in outcomes and contributing factors, it was concluded that behavioral decisions seem to rest on overall trust in the system and the ability for the human element to manage it, regardless of whether it's a manual or automated process. The results of this study can assist in arming those who are responsible for critical energy operations within their environment with an extension of awareness on how human behavior can change the outcome of an event based on the overreliance of automated processes.

Keywords: Cyber-physical systems, energy sector, complacency, automation, human behavior, trust

1. Introduction

Energy is a need basic to every human being (Tara Energy). Energy is required for everything we do in our daily lives. The energy sector resides at the top of the sixteen critical infrastructure sectors within the United States because it provides an essential function across all other critical infrastructures (DHS, 2015). It is responsible for supplying oil, gas, and electricity to areas like transportation, power plants, emergency services, internet and operational technology, healthcare systems, and households. As the energy sector evolves, so does the need to increase process efficiency, manage operations more effectively, and reduce costs. To keep up with increasing demand, the ability to centralize and digitize the operational capability of physical systems and processes they are responsible for becomes more imperative. CPSs have been designed to accomplish this. They represent cyber and physical components connected together to provide operational safety and efficiency. Familiar examples of this include the use of Supervisory Control and Data Acquisition (SCADA) systems for managing industrial systems and processes, smarts grids for electric transmission stations, implanted medical devices, and robotics. If automation of CPSs will take over future productivity and innovation, what do we know about the effects and potential outcomes this has on human safety and security of CPSs?

Reliance on the automation of CPS can increase complacency in individuals who operate and manage physical systems and processes and may lead to unwanted outcomes. Research has been conducted to identify the effects of automation complacency as it relates to the energy sector to provide a more focused view of what factors influence human behavior when systems are automated and how they affect physical systems and processes. What was discovered in this study will be used to determine how the effects of human behavior and potential outcomes change how we manage automation from both a safety and security perspective. A focused view will be presented on how the energy sector is transforming through industrial automation, the overreliance on operational tasks this may cause, and how it relates to human behavior and cybersecurity. Specific case studies and real-life outcomes of automation complacency and its effects will also be discussed, with the intent of presenting a culmination of consistency and similarity within the energy sector.

2. Related Work

Available knowledge within the field of automation complacency as it relates to the energy sector and human behavior was found to encompass different parts of a whole. For example, Other knowledge exuded a relation between automation complacency and bias, or industry-specific tasks. Much of this field's knowledge conveys similar analysis to the idea of reliance on automated systems as leading to undesired outcomes, with varied opinions on how human behavior comes into play. Other studies have been done on industry-specific systems and processes in other critical infrastructure sectors, although there seems to be less knowledge of automation complacency as it applies to the energy sector.

3. Industrial Automation: Transformation to CPS

CPSs can increase efficiency and provide energy to areas where infrastructure isn't supported. Investments in smart grids are needed to support electric vehicles, heat pumps, and renewable energy (NIST, 2022). CPS combines physical and cyber communication and control to create more automated, efficient, secure, and reliable processes. Primary to the energy sector, distributed energy resources (DERs) bridge the connection between energy flow management and distributed control systems (NIST, 2022). They are a part of the larger Industrial IoT. Industrial IoT connects processes by networking embedded systems, machines, sensors, etc. for operational performance, automation, and efficiency. Combining the efforts of CPS with DERs and the Industrial IoT, automation is becoming more and more efficient and scalable, as adaptability is majorly integrated into many sectors of critical infrastructure and everyday practice. This merger has advanced the world into the next revolution of Industry 4.0. Automation has been advancing for years through its predecessor, although this new era brings about automation at high levels, as well as the integration of information to include the span of varied sectors (Audaces). The CPS market is projected to reach an estimation of USD $12, 356.23 million by 2028 globally (Data Bridge, 2021).

4. Reliance on System and Process Automation

Once a CPS and its processes become automated, operator focus shifts more to the role of monitoring to ensure they are working as intended and producing the correct output. The effectiveness of monitoring is dependent on situational awareness of the operator and those responsible for overseeing or using applications associated with the automation of CPS. Performance levels must be addressed for the people, processes, and technology that make up the entirety of a CPS to ensure efficiency of process and the safety and security of humans and physical components.

4.1 Components, Cybersecurity, and the Human Element

Combining CPS with the energy sector, the term Cyber-Physical Energy Systems (CPESs) has been recognized to include highly connected and remotely controlled systems for energy production, transmission, and distribution (Hao, 2021). Components typically seen within a control room or plant floor may include controllers, actuators, processors, and sensors, or devices used for connectivity, such as switches, servers, and routers. Not only do these combine to assist in running and monitoring physical processes, but they also assist in identifying enhancements to energy resource management, efficiency, and control (Macana, Quijano, Mojica-Nava, 2021).

Cybersecurity's contribution to CPSs plays a large part in protecting physical processes. Attacks rose dramatically for organizations within critical infrastructure sectors from less than 10 in 2013 to close to 400 in 2020 (Gartner, 2022). A CPS may not initially be made to provide security, and systems already in production that weren't originally designed to become part of a CPS are being added to this convergence. CPSs are being designed as "open systems" that are able to dynamically reconfigure, reorganize, and operate in closed loops with often full communication and computation capability (Trevino, 2020). Security must address every aspect of the CPS and how it relates to critical infrastructures. Components will need penetration testing, change control, and vulnerability assessments to ensure the mission of the assets cannot be jeopardized by a cyber-attack (Haber, 2022).

Bringing in the human element, the CPES is designed to automate processes and tasks, but still needs operators and administrators to be involved. As referenced above, cybersecurity tools must be run and monitored by humans. The ability to step in with manual processes and decision-making skills when adjustments need to be made will still be present. The ability to respond faster and more accurately to a situation deemed critical within the energy sector can be enhanced by automated safety protocols (Breaking Energy, 2023), but cannot take potential dangers out of the equation. Human verification of safety must be a defensive first line initiative (Breaking Energy, 2023).

5. Complacency of Automation

A line from *The Ironies of Automation* states, 'Automation can be seen as the solution to human failure – replace human planning, actions, and decisions with automatic devices, computer control or artificial intelligence (Human Factors 101, 2020).' Advantages as automation is adopted can show more scalability, predictability, and human error reduction (Alton, 2018). Scalability allows for a CPS to adapt to the changing environment based on the number of tasks they can complete regardless of staff size. Predictability in automated systems means, if a system is operating in a safe and secure manner, it will continue to do so as a repeatable behavior. Human error reduction ties scalability and predictability together by allowing the automation of a CPS to take over and streamline otherwise manual processes. Based on a 90 percent attribution to cybersecurity breaches by human error (Alton, 2018), much of the statistics appear to represent valid benefits for automation. Although, the energy sector is comprised of many different CPESs responsible for systems and processes that provide renewable sources, fossil fuels, nuclear energy, and electricity to the transportation, industrial, residential, power, and commercial sectors (EIA, 2023). The ability for operators and administrators to manage cybersecurity and operational tools that monitor, analyze, and alert signs of unsafe and unsecure processes is critical to the management of these sectors. Reliance on the human factor is still present and must be managed.

5.1 Relation to Human Behavior: Safety and Security

Factors influencing human behavior with automation may reflect how the job role changes. A once manual process that required specific skills and training may now be taught at a level not requiring the ability to understand the mechanics of operations, only the automated monitoring and error handling of the system. If the operator needs to intervene they are considered "out of the loop" since they are so far removed (PIARC) from those tasks. Job roles may also change based on other tasks the operator is responsible for. Stated by Parasuraman and Manzey (2010), complacency is evident when (a) there is a human operator monitoring an automated system, (b) the frequency of monitoring behavior is suboptimal or below a normative rate, and (c) suboptimal monitoring leads to performance failures. The truth in this is the inability to efficiently monitor a system if other tasks, especially some more manual in nature, are having to be completed in parallel. If overloaded, an operator may not perform well given too many cognitive responsibilities. Complacency based on the above mentioned can lead to incidents serious in nature when handling hazardous energy or materials (SafeStart, 2020) based on trust placed on the automation of certain tasks.

5.2 Relation to CPES: Safety and Security

Factors influencing CPESs with automation may be in direct relation to what an operator is responsible for. Inappropriate checking and automated function monitoring may jeopardize safety and security. A system may have been designed with security in mind or it may not. There is a possibility errors may occur due to those introduced by the designer or may be due to lack of expertise (Human Factors 101, 2020). In turn, there is also a possibility that not all of the processes associated with a particular CPES has been automated and manual processes may still exist. The complexity of the developed system, even if it has been designed with security in mind, may be influenced by automation. The system's behavior may increase unpredictability, to which reliable and safe operation are jeopardized (Johansen, I.L., and Rausand (2014), as cited in Bolbot, V., et al (2018)).

But automating industrial tasks under a CPES can also bring forth the ability to eliminate safety and security concerns by improving process and operator efficiency and error alerting from the potential for failures, as well as signs of disruption. Industrial processes can be optimized to reduce unwanted downtime, increasing productivity (UtilitiesOne, 2023). As discussed above, this is in direct relation to the operator and the ability to provide continuous monitoring of process. Physical damage to a CPES can occur if a system does not behave the way it was expected to, if the operator isn't able to identify potential disruptions, or if the system has been compromised. The physical damage can most importantly affect human safety and the productivity of the CPES.

5.3 Cyber-physical Events: Adversarial and Unintentional

A major requirement of a CPES and those who operate it, is its ability to function safely and employ secure methods to assist in mitigating the effects of an adversarial or unintentional event. What this means primarily for the energy sector is the ability to keep people safe and form a resilience against those who aim to disable some of the critical functions it is responsible for, such as communications and emergency support systems. Much of the energy sector is still trying to understand how to protect and defend automated systems. Legacy systems are unable to be upgraded or patched since they weren't made with digital transformation, and they can't just be shut down as needed (Avertium, 2022), since availability of process is critical. OT systems are being attacked at an increasing rate, 87% in 2022, with more organizations connecting their OT systems to their IT networks (Dvoskin, 2023). The following two sections were analyzed to show adversarial and unintentional misuse in respect to the energy sector.

5.3.1 Adversarial Events

Attacks on a Ukrainian power grid in 2015 caused the blackout of an electric transmission station (Greenberg, 2017). It lasted only an hour but could have been more severe. Initial access was suspected to be from phishing emails, infecting victims' systems in order to target devices, while utilizing a feature of the malware to obtain associated network logs. Dragos founder Robert M. Lee, in an article from *Wired* pointed out that reconnaissance scans from malware are noisy and stick out like a sore thumb, suggesting power grid operators monitor their control system networks more closely (Greenberg, 2017).

Observation: Interpretation is based on the ability to monitor network logs from the OT and IT side of the network, taking time to investigate "noisy" anomalies visible to operators with automated management and process analysis. What allowed the attack to gain traction was the ability to use the IT side of the network to gain access to the OT side. Lack of monitoring between and within each sector assumes complacency of human interaction.

A model of Triconex safety controller made by Schneider Electric was compromised in 2017 at a petrochemical plant in Saudi Arabia. Malicious software was deployed allowing instrumented safety systems in the plant to be taken over (Giles, 2019). Before this could occur a code flaw was detected by the system. A response was triggered, shutting the plant down. Dismissed as a malfunction, a second was triggered and the plant shut down again. Effects of this event could have been detrimental if the attackers had successfully taken over all plant operations. Maliciously placed code can result in explosions from the release of toxic hydrogen sulfide gases [Giles, 2019], leading to health and safety occurrences.

Observation: From a complacency perspective, this can be seen as lack of code monitoring and dismissal of a code flaw by operators, instead of using the automated systems ability to provide the information necessary to investigate the event. Plant operations were allowed to continue, trusting the system to take over the process once again.

5.3.2 Unintentional Events

For this discussion, unintentional events will be defined as operator error or instances occurring from internal human actions, absent of adversarial attacks, to show examples of behavior specific to the energy sector.

An oil refinery explosion at BP America in Texas occurred in 2005 resulting in 15 deaths and 180 injured workers (CSB). A distillation tower separating a hydrocarbon mixture was overfilled when an isomerization unit was started; this resulted in devices that relieve pressure opening a flammable liquid geyser, and an explosion of fire ensued (BP

Texas City, 2007). The control system didn't alert on a set-point for a critical alarm in relation to fill level. It was taken as accurate with the assumption the system was set correctly. The operator failed to confirm this with others or verify physically. Levels are also visible on the tower itself but were not able to be read based on dirty conditions obscuring the view. There were also concerns of fatigue based on average overtime rates of 27 percent, exceedingly as much as 68 percent (BP Texas, 2007 as cited in Baker et al., 2007). Skills needed to effectively solve problems and initiate good judgement were cited by BP Texas.

Observation: Some unintentional human errors were attributed to training inadequacies, a control system that was poorly designed, and fatigue. Complacency resulting from these didn't exude the familiar phrase, "trust but verify".

An Orange County oil spill in 2021 is believed to have been exacerbated by the inability of operators to shut the pipeline down immediately. A low-pressure alarm was received early in the morning on the day of the incident alerting of what was later found to be a break in the line (ABC, 2021). Further discovery showed over a thirteen-hour period went by to which operators received eight alarms detecting the leak and did not respond to them, instead shutting the pipeline down each time the alarm went off and restarting it (U.S. News, 2021). This led to over 25,000 gallons spilling into the ocean (U.S. News, 2021).

Observation: Loss of attention to detail based on the ability of automation to cause tasks to become mundane can cause failure with critical development of the system or understanding what needs to be done; like the "out of the loop" performance level.

6. Theoretical Development & Results

Theoretical development began as an interest to explore how the reliance on automation of CPSs can increase complacency in individuals who operate and manage physical systems and processes. Based on an increase in the number of cyber-attacks and other occurrences mounting within the energy sector, what do we know about the effects and potential outcomes this has on human safety and security? Once analysis was complete, it was discovered immediately how the outcome of an adversarial event versus an unintentional event within the energy sector based on automation complacency were quite similar within three specific areas.

Safety. Intentional events from the actions of an attacker signified loss of power to critical or essential services and the potential for toxic gas release that could lead to safety and health issues. This was also reflected in unintentional events previously discussed based on the potential for extended deaths and injuries and contamination of water for both humans and other species. Combined, these events signify a threat to human life, regardless of intention.

Security. Intentional events can severely affect the security of humans and CPESs if the attacker is able to compromise other areas of the network based on social engineering attempts, like the attack on the Ukrainian grid, or being able to remain undetected and compromise the system more than once. This was observed from a different perspective with unintentional events, as these were from human error, but show similarities in lack of security based on the behavior of those responsible for the CPES. Automation complacency can enable a threat actor to look for weaknesses caused by human behavior and use them to compromise the CPES.

Human Behavior. Intentional events occurred with the inability of those responsible for the operation of CPESs to provide continuous monitoring, investigate visible anomalies, and verify potential code flaws. Attribution of these actions may be based on lack of training and ownership, fatigue from long hours, or other tasks more manual in nature that deterred the attention of the operator or those responsible for monitoring. Unintentional events reflected the failure to verify set conditions, lack of physical verification, communication with co-workers, and ignoring alarms. Attribution is similar to those of intentional events and seen as a bias of automation; how those responsible for operation and monitoring may have had the tendency to favor automated system suggestions versus information that is correct, and contradictory, from other sources (SafeStart, 2020). Such as the case with the intentional Triconex safety controller compromise and unintentional oil refinery explosion. A malfunction dismissal led to repeated plant shutdowns and lack of verification, manual and automated, based on assuming correct set conditions had occurred.

6.1 Complacency Impact and Implications

Based on safety and security outcomes analyzed and human behaviors found to be causal in relation, the impact of adversarial and unintentional events as they relate to automation complacency can be much more detrimental for each affected area. The sampling of events within this discussion resembled only a small piece of history. These gave reference to each area of the energy sector, touching on electricity through the Ukrainian power grid, oil through the Texas refinery explosion and Orange County spill, and the potential hydrogen gas leak from the Triconex safety controller. The impact of some of these could have been much worse than what occurred. Implications may reflect the inability to restore power to surrounding areas supporting critical services, such as hospitals, households during extreme weather conditions, transportation, and emergency support services. Or a plant shutdown lasting a duration of longer than what has been identified as exceeding the risk tolerance of a critical resource. This could also affect other major areas of the supply chain, such as food and water for human consumption. From this, the consequences of human behavior if complacent with the use of automation can implicitly correlate to a potential cause of existing and future predicted impact.

Because automation of CPESs increases efficiency of process and frees the operator to concentrate on other tasks more manual in nature, trust in automation grows. Once a reliance forms on the CPES, the operator becomes more complacent, as implied by the previous discussion. The operator begins to deliver insufficient responses based on an over trust in the system, fails to act on or detect known signals, and delays response (Parasuraman and Manzey, 2010, as cited in Merritt, S.M., et al 2019) to system failures requiring the human element. Regardless of the type of event, whether internally or externally executed, outcomes can have similar impact based on human behavior.

7. Final Analysis: Complacency Effects on Human and CPS

The analysis of automation complacency allowed three different factors considered to be the main influence behind human behavior based on associated outcomes. First, a poorly managed system or process can lead to unintentional outcomes. If a system is not patched properly, provision verified, and typically left untouched, it is known as the perfect storm for hacking (Imprivata, 2022). Unintentional events can also occur, as in the oil refinery explosion at BP America previously discussed, from ignoring dirty conditions of physical equipment, and automated alerts or errors of impending conditions. Monitoring both the cyber and physical aspect of a CPES has its own responsibilities and requires constancy. For cyber, this occurred with the Ukrainian power grid interruption from undetected malware resonating through company mail communications to the operations network. A transmission station was compromised based on lateral movement and undetected or ignored anomalies.

Another factor is that of poor design. Many OT systems making up a CPES aren't always designed for automation with security in mind. This may include legacy hardware/software and technically incapable systems. Vulnerabilities may result from lack of protection and ability to apply defense layers to minimize the impact of intentional or nonintentional events. What was found was the possibility that disruption of a power source, faults or failures with the control system, or incorrect programming may occur (SafeStart, 2020). An implied instance of this is the previously discussed BP America refinery explosion from an overfilled tower. Assumptions that the control system was set correctly as well as failure to verify led to the unfortunate outcome.

The third factor of influence is the lack of training and communication with operators those analyzing operational processes may have had. It's said that automation is imperfect, that those who would normally have an active role in a task are now moving to a more passive role of performance (Sheridan, 1987 and Bahner et al., 2008 as cited in Merritt, S.M. et al, 2019). Were the operators in the oil refinery explosion trained in proper validation techniques, to include communication with others? BP Texas indicated this may have been caused by the inability to effectively solve problems and initiate good judgement. Did employees within business operations for the Ukrainian power grid receive frequent security awareness training in order to identify potential social engineering attempts? Were Orange County personnel trained in a level of effort and attention to detail in order to shut down the oil pipeline efficiently? It can be stated that in any situation frequency of training and expectations never hinders an organization. The answers to these questions could very likely have direct causal effect on outcomes when compliance of automation is present.

8. Future Work

The scope of analysis was limited to the energy sector using narrowly selected occurrences to present examples specific to an industry that has an effect on all other critical infrastructure sectors. Relating automation complacency through human behavior by studying real-life occurrences based on personal theories and those of others has its limitations by lack of solid evidence and testimony but can be implied based on known human behaviors and outcomes. Given the rapid advancement of automated systems and processes, much is still unknown and documented on the effects of overreliance and how it relates to each new occurrence. Future work may lean towards studies on the ground floor of facilities within the energy sector who rely heavily on CPSs to culminate the effects of purposeful analysis over a specified time frame. Relatable instances of automation complacency allow those who operate critical energy systems to gauge how others have adapted when overreliance becomes a reality for their organization.

9. Conclusion

Based on what we now know of this discussion about the effects and outcomes of automation complacency, it can be implied that the management of automation from a safety and security perspective stems from one commonality – trust in the system. A CPES represents the automated performance of a system and is trusted for its ability to produce a consistently repeatable behavior safely and securely based on its design and configuration. Humans trust the CPES to deliver this consistency based on the predicted actions of automated process and the inclination to rely on a repeatable process. What changes the safety and security of this is the human factor that must still be present for the operation of an automated system. Regardless of whether the event is adversarial or unintentional in nature, the outcome can reflect factors related to the CPES as poor design or faulty components, and human factors such as fatigue, lack of training, and communication, one crossing over to the other. Factors aside, there is one thing that never changes. The responsibility of the human element to manage the system, regardless of manual or automated process.

References

Alton, L. (2018) “Automated Systems and Security: Threats and Advantages”, [online], www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/automated-systems-and-security-threats-and-advantages.

Audaces “The differences between industry 3.0 and industry 4.0: technology and innovation”, [online], www.audaces.com/en/blog/industry-3-0-industry-4-0-2.

Avertium (2022) “The Top 5 Cyber Threats in the Energy Sector”, [online], www.explore.avertium.com/resource/top-5-cyber-threats-in-energy-sector.

Breaking Energy (2023) “How the Energy Sector Can Take Advantage of Automation”, [online], www.breakingenergy.com/2023/02/08/how-the-energy-sector-can-take-advantage-of-automation/.

Data Bridge (2021) “Global Cyber-Physical Systems Market – Industry Trends and Forecast to 2028”, [online], www.databridgemarketresearch.com/reports/global-cyber-physical-systems-market.

Department of Homeland Security. (2015) “Energy Sector-Specific Plan”, [online], www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.

Dvoskin, O. (2023) “Attacks Against OT & Industrial Organizations Are on the Rise”, [online], www.blog.morphisec.com/attacks-against-ot-industrial-organizations-are-on-the-rise.

Gartner (2022) “3 Planning Assumptions for Securing Cyber-Physical Systems of Critical Infrastructure”, [online], www.gartner.com/en/articles/3-planning-assumptions-for-securing-cyber-physical-systems-of-critical-infrastructure.

Giles, M. (2019) “Triton is the world’s most murderous malware, and it’s spreading”, [online], www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware.

Greenberg, A. (2017) “Crash Override: The Malware That Took Down a Power Grid”, [online], www.wired.com/story/crash-override-malware.

Haber, M. (2022) “Cyber-Physical Security: What It Is and What You Should Do”, [online], www.darkreading.com/physical-security/cyber-physical-security-what-it-is-and-what-you-should-do.

Hao, Z., Di Maio, F., and Zio, E. (2021) “Dynamic Reliability Assessment of Cyber-Physical Energy Systems (CPEs) by GTST-MLD”, [online], www.ieeexplore.ieee.org/document/9660671.

Human Factors 101, “The Ironies of Automation.” [Online]. Available: https://humanfactors101.com/2020/05/24/the-ironies-of-automation/.

Imprivata (2022) “Looking back on the Colonial Pipeline hack”, [online], www.imprivata.com/blog/looking-back-colonial-pipeline-hack.

Johansen, I.L., and Rausand (2014), as cited in Bolbot, V., et al (2018) “Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review”, [online], www.sciencedirect.com/science/article/pii/S0951832018302709.

Macana, C.A., Quijano, N., and Mojica-Nava, E. (2011) “A survey on Cyber Physical Energy Systems and their applications on smart grids”, [online], www.ieeexplore.ieee.org/document/6083194.

National Institute of Standards and Technology. (2022) “NIST SP 1800-32B: Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity”, [online], www.nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-32.pdf.

Parasuraman, R., and Manzey, D. H. (2010), as cited in Merritt, S.M., et al (2019) “Automation-Induced Complacency Potential: Development and Validation of a New Scale”, [online], www.doi.org/10.3389/fpsyg.2019.00225.

PIARC, “Automation and Human Factors”, [online], www.rno-its.piarc.org/en/systems-and-standards-human-factors-engagement-its/automation-and-human-factors.

SafeStart (2020) “How to Overcome Automation Complacency in the Workplace”, [online], www.safestart.com/news/how-to-overcome-automation-complacency-in-the-workplace.

Tara Energy. “What Is Energy? A Guide to Understanding Energy”, [online], www.taraenergy.com/blog/what-is-energy-a-guide-to-understanding-energy/.

Trevino, M. (2020) “Cyber Physical Systems: The Coming Singularity”, [online], www.ndupress.ndu.edu/Media/News/News-Article-View/Article/2053087/cyber-physical-systems-the-coming-singularity/

U.S. Energy Information Administration (2023) “U.S. energy facts explained”, [online], www.eia.gov/energyexplained/us-energy-facts/.

Utilities One (2023) “Cyber-Physical Systems in Industrial Automation and Engineering”, [online], www.utilitiesone.com/cyber-physical-systems-in-industrial-automation-and-engineering.