Towards Cyber-Secure and Hazard-Resilient Smart Civil Structures

Miguel Cid Montoya, Carlos Rubio-Medrano

Texas A&M University - Corpus Christi, Corpus Christi, Texas, USA

Ahsan Kareem

University of Notre Dame, Notre Dame, Indiana, USA

Contact: miguel.cidmontoya@tamucc.edu

Abstract

The accelerated growth of urban areas in the last decades has led to an unprecedented increase in the construction of wind-sensitive structures, e.g., long-span bridges, tall buildings, wind turbines, and solar trackers. To effectively control undesired wind- and earthquake-induced responses, a plethora of operational technology and cyber-physical systems have been introduced, including supervisory control and data acquisition systems, programmable logic controllers, and remote terminal units. All these systems are potential targets for cyberattacks and have already been attacked in other sectors, including energy, industry, education, and health. This study analyzes this threat to critical infrastructure, quantifies its potential damage, and develops possible countermeasures and cyber-defenses so the structural engineering community can effectively address this emerging challenge.

Keywords: Cybersecurity; Smart structures; Active structural control; Wind-induced responses; Operational technology; Cyber-physical systems; Cyber-secure aero-structural design.

1 Introduction

Controlling wind- and earthquake-induced responses is a challenging and fundamental step in designing structures sensitive to natural hazards, such as tall buildings, long-span bridges, wind turbines, and solar trackers. Design modifications and countermeasures, such as shape, stiffness, and mass tailoring, as well as passive control devices, such as dampers, have been shown to be effective in the past. However, more demanding design scenarios involving ambitious contemporary designs and climate adaptation require adopting further actions. As a result, smart structures equipped with active and semi-active mass dampers, flaps, dynamic facades, suction and jet systems, and active tendons and bracing systems are gaining momentum to counteract potentially disastrous earthquake or wind actions adequately [1]. As shown in Figure 1, these active devices are part of more complex systems involving Operational Technology (OT) and Cyber-Physical Systems (CPS), which include Industrial Control Systems (ICS) that are composed of Supervisory Control and Data Acquisition systems (SCADA), Programmable Logic Controllers (PCLs), and Remote Terminal Units (RTU). All these systems are under the threat of cyberattacks, as has already happened in other sectors, such as energy [2],

Figure 1. An example of a wind-sensitive critical infrastructure equipped with Operational Technology (OT) and Cyber-Physical Systems (CPS). (a) General view of the 1918 Çanakkale Bridge, Türkiye, opened in 2022; and (b) the bridge control center, key element of the Industrial Control System (ICS).

industry [3], education [4], research [5], health [6], and warfare [7], among others. The wind is the only natural hazard with enough high frequency of occurrence that makes it a leveraging force to exponentially increase the damage induced by a cyberattack. On the other hand, misleading earthquake-control devices can also cause catastrophic consequences. Changing the intended use of OT and CPS cyber-infrastructures can have a severe impact the structure's serviceability and cause severe structural damage or even its eventual collapse. This study identifies potential cyberattacks and their eventual impact on smart civil infrastructure equipped with hardware and software that detects changes by sensors, control algorithms, and actuators installed to mitigate the effects of natural hazards. Several kinds of cyberattacks, scenarios, and possible defenses are discussed. Furthermore, we study the potential impact of cyberattacks leveraging wind loads, which are identified as "wind-leveraged false data injection" (WindFDI), which were previously introduced by the authors in [8], and can target wind-sensitive structures by taking advantage of the positive feedback between wind loads and the misuse of active control systems.

2 Cyber-physical systems and vulnerability to cyberattacks

OT can be defined as the combination of hardware and software systems aimed to detect and/or cause a change in physical systems through the direct network-based monitoring and/or control of dedicated equipment, assets, processes, and events. The term OT usually describes environments containing CSP, such as Connected Automated Vehicles (CAVs), ICS, and can be composed by RTU and PLC. ICS is a sub-field of OT/CPS controlling mission-critical infrastructure such as power grids, hydraulic systems, etc. They are, of course, important assets to the economies of towns and countries. The recent trend of transferring ICS to electronic systems is due to the vast opportunities available for harnessing digital technology, such as reliability, flexibility, resilience, and efficiency [9]. Figure 2 shows a typical ICS environment, including the following components:

- **Actuator**: A hardware component that moves or operates a physical device, such as a calver, motor, and piezoelectric actuator.
- **Sensor**: A device that generates an electrical analog or digital signal representing a physical property of the process, such as temperature or acceleration sensors.
- **Controller**: A computing device that bridges the cyber and the physical worlds. It can take the form of a general-purpose computer or it may be implemented as a PLC, a small rugged, domain-purpose computer that has programmable memory, which permits controlling actuators and physical machines and receive and compile data from sensors.

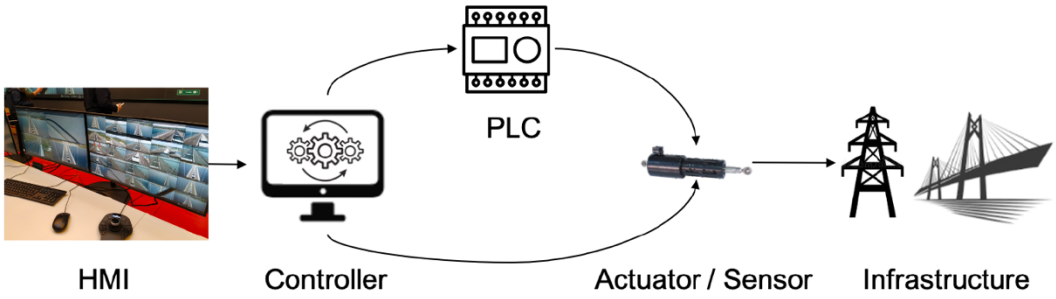

Figure 2. A conceptual overview of the components of an ICS environment.

- **Human Machine Interface (HMI)**: The hardware and/or software used to interact with the devices such as a PLC.

2.1 Attacks to CPS

The benefits of implementing these systems are unparalleled. However, cyberattacks targeting CPS have drastically increased in recent years, leading to relevant consequences, including physical damage to critical infrastructure. Recent examples are the Kyivoblenergo and Prykarpattyaoblenergo attacks (2015) [10] and the Ukrenergo transmission station attack (2016) [11]. Some specific attacks conducted on PLCs and ICS are discussed below.

Stuxnet. This was the first-ever documented malware specifically developed to target PLCs [12]. It compromised a general-purpose computer equipped with software for programming PLCs and maliciously controlled Siemens 315 and 417 PLC models to make them damage centrifuges while reporting normal operation.

Triton. Also known as TRISIS and HatMan [13], it was identified in 2017 in a petrochemical facility in Saudi Arabia. Triton compromised an engineering workstation and launched a dropper to deliver backdoor files to a Safety Instrumented System (SIS) PLC. The attack failed due to a PLC error.

Pipedream Toolkit. Also known as Incontroller [14], it consists of a modular framework that includes multiple exploits that target different PLCs. It is believed to have been developed by a nation-state and was classified by the US Cybersecurity and Infrastructure Security Agency (CISA) [14] as an Advanced Persistent Threat (APT).

Dragonfly. Also known as Havex malware [15], Dragonfly was a large-scale cyberespionage campaign that targeted ICS software in the US and European energy sectors. The targets were infected using three different attacks: (1) a span campaign using spear phishing to senior employees, (2) a Watering Hole attack that compromises legitimate websites, and (3) a final attack using a *trojanized* software to compromise various legitimate ICS software packages, ultimately inserting their own malicious code.

Crashoverride. Also known as Industroyer [16], it was designed to disrupt ICS networks used in electrical substations, and resulted in physical damage by opening circuit breakers and keeping them open even if the grid operators tried to close them back to restore the system.

3 Wind-sensitive CI equipped with OT/CPS

According to CISA [17], Critical Infrastructure (CI) is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." This impacts multiple infrastructures that may be sensitive to natural hazards. For instance, long-span bridges, tall buildings, wind turbines, and solar trackers are sensitive to wind and may be equipped with active systems that may be targeted by cyberattacks.

3.1 Long-span bridges

Passive countermeasures, such as deck tailoring [18, 19], appendages, and intertidal devices, are effective alternatives to mitigate wind-induced

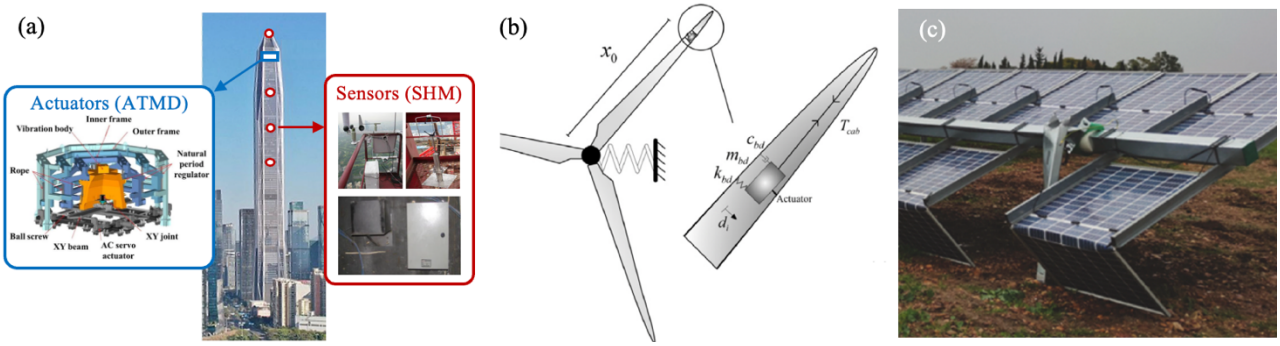

Figure 3. Examples of wind-sensitive critical infrastructure equipped with OT/CPS. (a) Ping-An Finance Center (PAFC), China [24], equipped with an ATMD, (b) wind turbine blade control using CCATMD [29] (c) damager on a single-axis solar tracker due to wind-induced torsional load [35].

responses. However, as the requirements increase, passive countermeasures are effective up to a particular limit [19], and active devices are required to increase their performance under wind loads further. Active control devices can be classified into (1) structural (inertial) control devices, (2) aerodynamic control devices, and (3) combined devices. Inertial control devices have been installed in long-span bridges in decks, in the form of Active Mass Dampers (AMD) and Semi-Active Mass Dampers (SAMD), and in the towers in the form of AMD. Aerodynamic control devices can be classified into (1) shape control devices and (2) flow control devices. Shape control devices include active winglets [20], active flaps [21], and active wind barriers. Flow control devices are still in the research realm and include suction, jets, and rotors to control the flow separation.

3.2 Tall buildings

According to [22], about 11% of tall buildings above 250 m worldwide are equipped with dynamic modification systems, and 97% of those have been equipped in the last three decades. This approach is prevalent in the US, where 25% of tall buildings are damped, and the percentage of damped tall buildings built in the last decade reached 42%. Currently, 12% of damped buildings worldwide use AMD systems [23, 24], and this trend is expected to grow as architectural requirements increase. Reviews about passive and active systems installed in tall buildings can be found in [1, 25]. Active systems can be classified into structural or aerodynamic modifiers. A more concise classification would categorize these devices into (1) stiffness control, (2) inertial control, (3) façade shape control, and (4) flow control. Stiffness control devices include Active Variable Stiffness (AVS), semi-active magneto-rheological (MR) dampers, semi-active electro-rheological (ER) dampers, semi-active fiction dampers, and active cable/tendon control devices. Inertial control devices include AMD, multiple active mass dampers (MAMD), semi-active tuned mass dampers (SATMD), semi-active variable stiffness tuned mass dampers (SAVS-TMD), semi-active tuned liquid dampers (SATLD), semi-active movable facades damping systems, hybrid mass dampers (HMD), active gyro stabilizes (AGS), and twin rotor dampers (TRD). Façade control devices [26] include active cross-sections, active plates, and active porosity and roughness. Finally, flow control devices are investigated in the form of rotors for corner flow control and suction and jets.

3.3 Wind turbines

The wind energy sector is rapidly growing thanks to the fast-growing support for green energy policies. In fact, wind energy reached 10.3% of the share of total US energy consumption in 2022. This figure is even bigger in Europe, reaching 31.5% in November 2023 [27]. Furthermore, the European Wind Energy Association (EWEA) predicts that the European wind energy share will reach 50% by 2050. Wind turbines are equipped with active systems for both operation control and wind mitigation goals. Structural control devices [28] include (1) the inertial control in tower and nacelles, such as AMD, TRD, semi-active MR dampers, semi-active TMD, SATLD, and HMD, (2)

inertial control of blades in the form of AMD in blades and cable-connected active tuned mass dampers (CCATMD) [29], and (3) stiffness control in blades using techniques such as active tendons and active strut controllers for controlling damping. Another group of control devices in turbines are blade control methods, which can be classified into collective blade control and individual blade control and permit the right operation of the turbine in the different operational modes depending on the wind velocity [30]. Wind farm control [31] is another system that may be targeted by cyberattacks, potentially causing damage at both the turbine and farm levels.

3.4 Solar Trackers

Another growing sector involving wind-sensitive critical infrastructure is solar energy. Solar panels are commonly organized in arrays and controlled by trackers in order to maximize the production of solar energy. According to [32], automatic tracking systems can increase the power generated by up to 25%. However, given the size and geometry of the panels, these structures are sensitive to wind loads and require specific aerodynamic and aeroelastic studies [33]. A comprehensive review of the multiple kinds of trackers and array configurations can be found in [34]. The effect of wind loads on panel trackers, which can lead to the collapse of the array, as studied in detail in [35].

4 Potential attacks on CI equipped with OT/CPS

We classify the potential cyberattacks on wind-sensitive CI equipped with OT/CPS based on three criteria: (1) kind of affection based on the actuation or nature of the CPS, (2) attack scenarios depending on the available data to plan the attack, and (3) kind of cyberattack depending on the formulation of the action on the CPS. The first classification is based on the discussion and literature review reported in Section 3. A major and straightforward categorization can be done between mechanical and aerodynamic affectations. The second classification is based on the information available, including (i) mechanical information of the structure, (ii) local wind data, (iii) aerodynamic and aeroelastic properties of the structure, and (iv) information about the CPS that permits the actuation on the target structure. This permits a bread classification into (a) informed cyberattacks, where the plan is based on previous knowledge of the structure, (b) uninformed cyberattacks, when there is no information of the target and the attack involves extracting the data by hacking weather stations, structural health monitoring systems, and others, and (c) semi-informed (Hybrid) cyberattacks, halfway between informed and uninformed attacks. The third classification includes (a) Denial of Service (DoS) attacks [36], (b) False Data Injection (FDI) attacks, and (c) Wind-leveraged False Data Injection (WindFDI) attacks, which are described below and conceptually explained in Figure 4.

4.1 Denial of service (DoS)

A denial of Service (DoS) attack disables the OT/CPS, leaving the target structure without the benefits of the active control system. The DoS attack can block the operation of only some specific actuators or all of them. This attack does not cause any direct damage to the target structure. The structure is only damaged if the attack is executed during a natural hazard that requires a mitigation action by the blocked actuator. Hence, it is opportunistic since its effect is conditioned to the occurrence of the natural hazard. The mathematical formulation is based on the maximization of the damage $\mathfrak{D}(\boldsymbol{\pi}_{\mathrm{DOS}}, \boldsymbol{w})$, and can be written as:

$$\begin{aligned} &\text{Find:} && \boldsymbol{\pi}_{\mathrm{DOS}} = (\pi_i), \quad i = 1, \dots, n \\ &\text{Maximize:} && \mathfrak{D}(\boldsymbol{\pi}_{\mathrm{DOS}}, \boldsymbol{w}) \\ &\text{Subject to:} && \\ & && \pi_i \in \{0, 1\}, \ \forall\, i = 1, \dots, n \end{aligned} \tag{1}$$

Where $\boldsymbol{\pi}_{\mathrm{DOS}}$ is the vector containing the DOS attack policy of the actuators controlled by the adversary: an n-dimensional binary vector that indicates what actuators the adversary will disconnect. $\boldsymbol{w}$ is the weather scenario, *k* is the number of actuators that are blocked, and *n* the total number of existing actuators.

4.2 False Data Injection (FDI)

Besides blocking the actuators to deny their capacity to mitigate wind loads, CPS can be

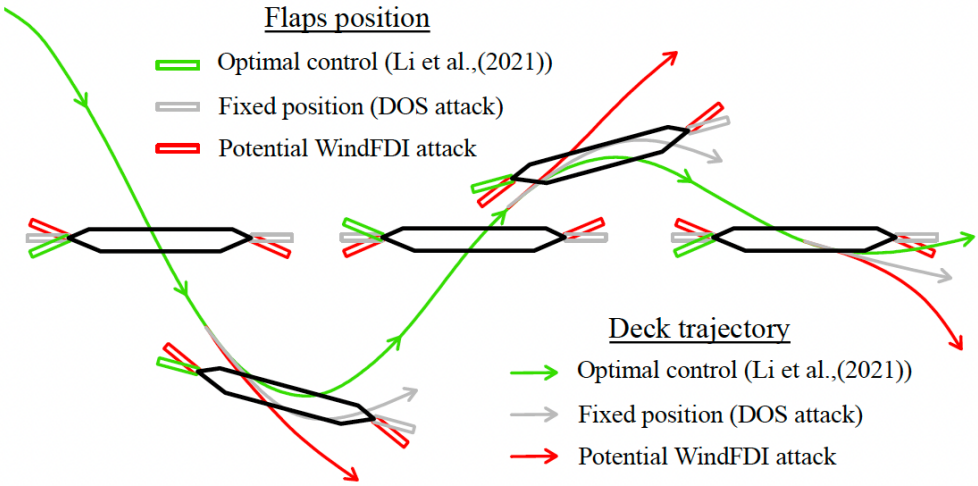

Figure 4. Graphical explanation of the potential effect of cyberattacks (DoS and WindFDI) on a bridge deck equipped with flaps compared to the optimal control pattern reported by [21].

maliciously used to damage the target structure using only their own actions. A malicious policy $\boldsymbol{\pi}_{\mathrm{FDI}}$ can be defined as seeking the maximization of the damage $\mathfrak{D}(\boldsymbol{\pi}_{\mathrm{FDI}})$ considering not only how many actuators must be controlled but also the specific action in terms of movements they will perform during the execution of the attack. This kind of attack does not depend on the weather; hence, it can be executed at any time, regardless of wind conditions. The FDI attack is formulated as:

$$\text{Find:} \quad \boldsymbol{\pi}_{\mathrm{FDI}} = (\pi_i), \quad i = 1, \dots, n$$
$$\text{Maximize:} \quad \mathfrak{D}(\boldsymbol{\pi}_{\mathrm{FDI}}) \qquad (2)$$

Where $\boldsymbol{\pi}_{\mathrm{FDI}}$ is the vector containing the FDI attack policy of the actuators controlled by the adversary, and *n* is the total number of existing actuators.

4.3 Wind-leveraged False Data Injection (WindFDI)

The Wind-leveraged False Data Injection (WindFDI) attack seeks to exploit all the potential damage that a CPS can create on the target structure by using the wind as an "external help" to increase the attack's impact. This cyberattack is planned to pursue the opposite goal of control theory: maximize the wind-induced responses (damage) $\mathfrak{D}(\boldsymbol{\pi}_{\mathrm{WindFDI}}, \boldsymbol{w})$ instead of mitigating the wind-induced responses. This can be achieved by taking advantage of the positive feedback of the wind loads and the CPS action. The effectiveness of the attack rely on the wind conditions $\boldsymbol{w}$, and can be carried out under frequent winds or even daily winds as long as they permit the amplification of the structural response. Hence, it can be classified as an opportunistic attack since its performance depends on the weather scenario. The mathematical formulation of the WindFDI attack is an optimization problem seeking to identify the optimum policy that maximizes the damage:

$$\text{Find:} \quad \boldsymbol{\pi}_{\mathrm{WindFDI}} = (\pi_i), \quad i = 1, \dots, n$$
$$\text{Maximize:} \quad \mathfrak{D}(\boldsymbol{\pi}_{\mathrm{WindFDI}}, \boldsymbol{w}) \qquad (3)$$

Where $\boldsymbol{\pi}_{\mathrm{WindFDI}}$ is the vector containing the WindFDI attack policy of the actuators controlled by the adversary leveraging the external load of the wind. It is a function of the weather scenario. $\boldsymbol{w}$ is the weather scenario, and *n* the total number of existing actuators

5 Development of Cyber-defenses

It is theoretically and practically impossible to completely eliminate the risk of cyberattack in any kind of system equipped with OT/CPS. However, engineers can improve their designs and develop cyber-defenses to try to minimize the risk and damage of cyberattacks on structures.

5.1 Cybersecurity-only defenses

Redundancy is a proven strategy in the aerospace engineering field [37] to deal with the potential

failure of aircraft systems. A redundant system is a secondary system implemented in parallel to the primary system that serves as a backup in case the primary system fails.

Another approach is Moving Target Defense (MTD) [38], which consists of implementing a series of continuous, pre-scheduled changes in the configuration setting of the system in order to complicate the initial reconnaissance phase that is typically varied out before an attack is executed.

Intrusion Detection Systems (IDS) are another alternative to deal with cyberattacks. It consists of installing a secondary system to track the structural performance and identify eventual malicious actions. It can be focused on physical detection or software-based detection [39].

5.2 Cyber-secure aero-structural design

From the designer's perspective, the existence of a new design scenario (the structure under the effect of the cyberattack) changes the way active systems for wind-induced response mitigation must be designed. Active CPSs are currently designed to maximize their effectiveness in mitigating the aeroelastic response. However, it can be generally assumed that the higher their influence on the flow features around the structure, the higher their capability to damage the structure under a cyberattack. Hence, to reduce this effect, active systems must be designed to improve the aeroelastic response up to a given threshold in order to contain its capacity to damage the structure under the attack. Hence, the design problem turns into a bi-objective optimization problem where the goal is to minimize the aeroelastic response when the CPS is in regular service and also to minimize the potential cyberattack-induced loads on the structure during an eventual cyberattack. This is graphically represented in Figure 4, where a Pareto front confronting these two opposite goals is represented.

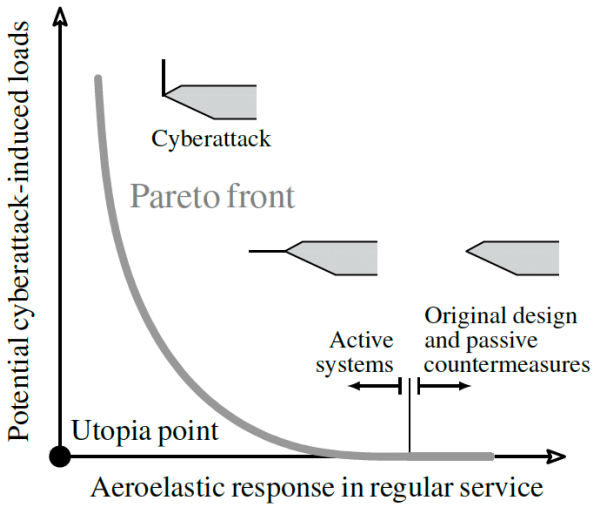

Figure 4. Conceptual description of the cyber-secure aero-structural design problem.

6 Concluding remarks

The increasing presence of cyberattacks in modern societies that are progressively more dependent on new technology affects many aspects of citizen's lives. Wind-sensitive smart structures equipped with OT/CPS are not an exception. Hence, it is fundamental for the structural engineering community to actively identify potential cyberattacks, quantify their impact, and develop effective countermeasures to guarantee the cybersecurity of wind-sensitive CI equipped with OT/CPS. These considerations must be addressed since the preliminary design stages, where the wind-sensitive structure and the CPS are first drafted. The development of new active systems must consider the potential negative effect on the main structural system under an eventual cyberattack to fully address all possible scenarios along the structure's life cycle.

7 Acknowledgments

Miguel Cid Montoya is partially supported by the United States National Science Foundation (NSF) under grant CMMI #2301824 and a start-up funds grant provided by Texas A&M University-Corpus Christi. Carlos E. Rubio-Medrano is also partially supported by NSF under grant CNS #2131263. Ahsan Kareem is supported in part by funding from the Robert M Moran Professorship.

8 References

[1] Jafari, M. and Alipour, A (2021). Methodologies to mitigate wind-induced vibrations of tall buildings: A state-of-the-art review. Journal of Building Engineering, 33:101582.

[2] Anguiano, D. (2022). Attacks on Pacific north-west power stations raise fears for US electric grid. The Guardian.

[3] Pattison-Gordon, J. (2022). What's next for defending critical infrastructure? In Government Technology, April 1st, 2022. URL:https://www.govtech.com/security/whats-next-for-defending-critical-infrastructure.

[4] Bank of America (2023). Keeping higher ed students safe from cyber attacks.

[5] McFadden (2023). Huge cyberattack disables telescopes in Hawaii and Chile, Aug 26th. Interestingengineering.com.

[6] Okunyt, P. (2023). Ransomware attack spreads chaos at major hospital in Barcelona. Cybernews.

[7] Reavenlord (2022). Microsoft: Russian cyberattacks increase against ukraine, supporters. jun 27th. Tehcpowerup.com.

[8] Cid Montoya, M., Rubio-Medarano, C., Kareem A (2023). A first look at cybersecurity of structures under wind. *16th International Conference on Wind Engineering*, August 27-31, 2023. Florence, Italy.

[9] Ed Goff, Cliff Glantz, and Rebecca Massello. Cybersecurity procurement language for energy delivery systems. In Proceedings of the 9th Annual Cyber and Information Security Research Conference, CISR '14, page 77–79, New York, NY, USA, 2014. Association for Computing Machinery. ISBN 9781450328128. URL: https://doi.org/10.1145/2602087.

[10] David E. Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith. Ukraine cyber induced power outage: Analysis and practical mitigation strategies. In 2017 70th Annual Conference for Protective Relay Engineers (CPRE), pages 1–8, 2017. doi: 10.1109/CPRE.2017.8090056.

[11] Dragos, Inc (2017). Trisis malware: Analysis of safety system targeted malware.

[12] Falliere, N., Murchu, L. O., and Chien, E. (2011) W32. Stuxnet dossier. White paper, Symantec Corp., Security Response, 5(6):29.

[13] ICS-CERT (2019). Mar-17-352-01 Hatman-safety system targeted malware (update b).

[14] Cybersecurity and Infrastructure Security Agency (CISA) (2022). APT Cyber Tools Targeting ICS/SCADA Devices. https://www.cisa.gov/uscert/ncas/alerts/aa22-103a.

[15] Symantec Inc (2014). Dragonfly: Cyberespionage attacks against energy suppliers. Technicalcreport, Tech. Rep., July, 2014.

[16] Slowik, J. (2018). Anatomy of an attack: Detecting and defeating crashoverride. VB2018, October, 2018.

[17] CISA (2020). A guide to critical infrastructure security and resilience. Dec 17. Cybersecurity & Infrastructure Security Agency, US Department of Homeland Security.

[18] Larsen, A. and Wall, A. (2012). Shaping of bridge box girders to avoid vortex shedding response. J Wind Eng Ind Aerod, 104–106:159–165, 2012. doi: 10.1016/j.jweia.2012.04.018.

[19] Cid Montoya, M., Hernández, S. and Kareem, A (2022). Aero-structural optimization-based tailoring of bridge deck geometry. Eng Str, 270:114067, 2022.

[20] Sangalli, L.A. and Braun, A.L., (2020). A fluid-structure interaction model for numerical simulation of bridge flutter using sectional models with active control devices. preliminary results. J Sound Vib, 477:115338. doi: 10.1016/j.jsv.2020.115338.

[21] Li, K., Zhao, L., Hui, Y., Yang, Q., Chen, Z., and Qian, G (2022). Active flutter control of a bridge-flap system considering aerodynamic interferences in practical considerations. Smart Materials and Structures, 31:065006.

[22] Lago, A., Trabucco, D., and Wood, A. (2018). Damping Technologies for Tall Buildings: Theory, Design Guidance and Case Studies. Elsevier Science and Technology.

[23] CTBUH, 2022. CTBUH skyscraper database. Council on Tall Buildings and Urban Habitat.

[24] Zhou, K., Zhang, J.-W. and Li, Q.-S. (2022). Control performance of active tuned mass

damper for mitigating wind-induced vibrations of a 600-m-tall skyscraper. Journal of Building Engineering, 45:103646.

[25] Kareem, A., Kijewski, T., and Tamura, Y. (1999). Mitigation of motions of tall buildings with specific examples of recent applications. Wind and Structures, 2(3):201–251. doi: 10.12989/was.1999.2.3.201.

[26] Ding, F. and A. Kareem, A. (2022). Tall buildings with dynamic facade under winds. Engineering, 6: 1443–1453. doi: 10.1016/j.eng.2020.07.020.

[27] WindEurope.org. Daily wind power numbers, retrieved on November 23, 2023 from https://windeurope.org/about-wind/daily-wind-archive/2023-11-23/. Technical report, WindEurope, 2023.

[28] Staino, D., and Basu, B. (2015). Emerging trends in vibration control of wind turbines: a focus on a dual control strategy. Philosophical Transactions of the Royal Society A, 373:20140069.

[29] Fragoso, S., Garrido, J., Vázquez, F., and Morilla, F. (2017). Comparative analysis of decoupling control methodologies and H∞ multivariable robust control for variable-speed, variable pitch wind turbines: Application to a lab-scale wind turbine. Sustainability, 9:713.

[30] Fitzgerald, B., and Basu, B. (2014). Cable connected active tuned mass dampers for control of in plane vibrations of wind turbine blades. J Sound Vib, 333:5980–6004, 2014. doi: 10.1016/j.jsv.2014.05.031.

[31] Stock, A. and Leithead, W. (2022). A generic approach to wind farm control and the power adjusting controller. Wind Energy, 25(10):1735–1757.

[32] Al-Mohamad, A. (2004). Efficiency improvements of photo-voltaic panels using a sun tracking system. Appl. Energy, 79(3):345–354, 2004.

[33] Quintela, J., Jurado, J.Á., Rapela, C., Álvarez, A. J., Roca, M. Hernández, S., Cid Montoya, M., López, J.M., Ruiz, A.J., Moreno, I., and Jiménez, S. (2020). Experimental and computational studies on the performance of solar trackers under vortex shedding, torsional divergence, and flutter. Int. J. Comp. Meth. and Exp. Meas., 8(4):387–404.

[34] Hao, D., Qi, L., Tairab, A. M., Ahmed, A., Azam, A., Luo, D., Pan, Y., Zhang, Z., and Yan, J. (2022). Solar energy harvesting technologies for PV self-powered applications: A comprehensive review. Renewable Energy, 188:678–697.

[35] Valentín, D., Valero, C., Egusquiza, M., and Presas, A. (2022). Failure investigation of a solar tracker due to wind-induced torsional galloping. Engineering Failure Analysis, 135:106–137, 2022.

[36] Zambrano, A., Palacio-Betancur, A., Burlando, L., Nino, A.F., Giraldo, L.F., Soto, M.G., Giraldo, J. and Cardenas, A.A. (2021). You make me tremble: A first look at attacks against structural control systems. In CCS 21, November 15'19, 2021, Virtual Event, Korea.

[37] Collinson, R. P. G. (1999). Fly-by-wire flight control. Computing & Control Engineering Journal, 10(4):141–152.

[38] Rubio-Medrano, C. E., Lamp, J., Doup., A., Zhao, Z., and Ahn, G.-J (2017). Mutated policies: Towards proactive attribute-based defenses for access control. In Proceedings of the 2017 Workshop on Moving Target Defense, MTD '17, page 39–49, New York, NY, USA, 2017. Association for Computing Machinery. doi: 10.1145/3140549. 3140553.

[39] Mitchell, R., and Chen, I.-R., (2014). A survey of intrusion detection techniques for cyberphysical systems. ACM Comput. Surv., 46(4), mar 2014. ISSN 0360-0300. doi: 10.1145/2542049.
URL:https://doi.org/10.1145/2542049.