Commentary

iMedPub Journals
www.imedpub.com

International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering

2022
Vol.5 No.9:41

# Strategic Choice of Technology Can Result In Functional Safety

**Brijraj Renu***

Department of Chemical Engineering, The University of Utah, United States of America

***Corresponding author:** Brijraj Renu, Department of Chemical Engineering, The University of Utah, United States of America, E-mail: brijiajr@123gmail.com

**Received date:** August 03, 2022, Manuscript No. IJAREEIE-22-15296; **Editor assigned date:** August 05, 2022, PreQC No. IJAREEIE-22-15296 (PQ); **Reviewed date:** August 18, 2022, QC No. IJAREEIE-22-15296; **Revised date:** August 29, 2022, Manuscript No. IJAREEIE-22-15296 (R); **Published date:** September 02, 2022, DOI: 10.36648/Ijareeie.5.9.41

**Citation:** Renu B (2022) Strategic Choice of Technology Can Result In Functional Safety. Int J Adv Res Vol.5 No.9:41

## Description

Intruders can introduce intended attacks that compromise the performance of industrial networked control systems. Denial-of-service, packet dropout, delays, and other attacks can be introduced in a variety of ways, according to the literature. The system knowledge gathered through eavesdropping can be used to design attacks. By avoiding performance-degrading uncertain exogenous dynamics, this article addresses the problem of constrained optimal switching control design with Industrial Networked Control System (INCS). On the plant side, a random distribution process that represents the attack sequence is used to characterize and detect the abnormal behavior of iNCS. Through the Bernoulli distribution process, delays and packet loss are introduced to convey the network's uncertainty and an attack by intruders on either side of a tightly coupled component. The iNCS performance is evaluated with uncertain exogenous dynamics, such as delays, malicious attack, and packet loss of 0%, 10%, 20%, and 30%, respectively. Linear-time-invariant iNCS's transient and steady-state performance are guaranteed by the proposed design. The proposed design approach was tested by simulating a numerical problem and switching the optimal predictive control performance of a networked system. Cyber-attacks against Modern Control Frameworks (ICS) can have unsafe actual effects. Due to the possibility of physical damage to the evidence, it can be difficult to investigate such attacks. With stealthy attacks, this is especially true; *i.e.* attacks that are difficult to spot. By actively collecting potential evidence of stealthy attacks, our goal in this paper is to engineer Forensic Readiness (FR) in safety-critical, geographically distributed ICS.

## Industrial Control Systems

Due to the large volume of such data, it is impossible to collect all ICS-generated data at once. As a result, our strategy only initiates data collection when a potential stealth attack poses a threat. Predictive, model-based safety checks help us determine the conditions for such an event. Additionally, we identify relevant data by utilizing the ICS's geographical layout and safety predictions to identify data at risk of loss due to damage. Finally, we select a subset of relevant data to collect by making a trade-off between the anticipated impact of the attack and the estimated cost of collection in order to reduce the control performance overhead that results from real-time data collection. Using simulations of the widely used Tennessee–Eastman Process (TEP) benchmark, we demonstrate these concepts. When compared to the scenario in which all of the data generated by the ICS is collected, we demonstrate that the proposed method does not miss relevant data and has a lower control performance overhead. Tracing the sources of cyber-attacks in Power Industrial Control Systems (PICS) can assist defense systems in blocking attacks and support the decision-making process for grid control policies. In addition, we demonstrate how our method can be applied to improve the effectiveness of existing ICS forensic log analysis tools. However, there has been no work done on PICS's cyber-attack source trace back, and the Internet's methods are incompatible with PICS in terms of their fineness, real-time performance, and support for communication protocols. As a result, a way to track cyber-attacks in PICS is suggested. PICS's communication network architecture and cyber security threats are examined first. Then, a packet marking and packet logging-based Extended Hybrid Tracing method is proposed. To achieve more precise attack tracing, this strategy involves all devices working at the data link layer and higher layers. A coarse-grained tracing mode is also presented to speed up tracing, taking into account the costs of attack tracing. In addition, a storage-saving log database optimization scheme is provided. A cyber-attack source tracing system and its deployment architecture are made for PICS to make it easier to put this method to use. In addition, the ExtHT's applicability and limitations are examined, theoretical arguments are presented to support our ExtHT, and its performance is contrasted with that of existing mainstream methods. Finally, the viability of ExtHT is tested on two different cyber-attack scenarios against PICS. For the purpose of identifying cyber-attacks against Industrial Control Systems (ICSs), Neural Networks (NNs) have recently been proposed.

To deal with the change in the monitored signals over time, these detectors are frequently retrained using system operation data. However, by taking advantage of this mechanism, an adversary can poison the learning process of the detector and fake the signals provided by corroded sensors during training, allowing cyber-attacks to remain undetected during testing. The possibility of producing adversarial samples that deceive anomaly detection models in ICSs without compromising their training process was the subject of previous research. We are the first to demonstrate poisoning attacks of this kind on neural

network-based ICS cyber-attack online detectors with this study. We demonstrate the efficacy of two distinct attack algorithms: back-gradient-based poisoning and interpolation-based poisoning. Diverse data sources are used in the evaluation: ICS tested data from the real world, synthetic data, and a Tennessee Eastman process simulation. The difficulties of poisoning dynamically controlled systems are highlighted in this first practical evaluation of poisoning attacks performed with a simulation tool. The proposed approaches' applicability to a variety of NN parameters and architectures is investigated. Last but not least, we suggest and evaluate some potential approaches to reducing the risk.

## Modern Control Frameworks

Diverse manufacturing and technological services and devices are a part of the Industrial Internet of Things (IIoT) networks. Cyber-attacks can target IIoT systems and their associated networks due to their communication and data exchange characteristics. Therefore, it is essential to provide IIoT systems with robust security and prompt attack detection. The Internet Industrial Control Systems (IICS) and their networks are frequently targeted by cyber-attacks, which are often detected by Intrusion Detection Systems (IDS). In recent times, numerous countries' nuclear and critical infrastructures have sustained significant damage as a result of various attacks against IICS setups, including seismic, flame, and duqu attacks. The current intrusion detection techniques typically have high false alarm rates, misclassification errors, and insufficient generalization. In order to accomplish this, this paper presents deep-auto encoder-based IDS that can instantly differentiate between IIoT-driven IICS networks and malicious actions. The LSTM auto-encoder design serves as the foundation for the proposed model, which uses IICS networks to identify invasive events. By achieving an accuracy rate of 97.62 percent for the UNSW-NB15 dataset and 97.95 percent for the gas pipeline data, respectively, the experimental results of the proposed IDS on two benchmark datasets show that it is superior to other compelling models. Because their sub-components communicated within private networks in the previous generation of Industrial Control Systems (ICSs), it was assumed that ICSs are immune to cyber-attacks. However, in order to control and monitor their dispersed structure, the brand-new advanced ICS sub-components require Internet connectivity. Security issues arise when you connect to corporate networks and the public Internet.

ICS networks now face a serious threat from the growing number of attacks. Multiple steps are used in these sophisticated attacks, which target various devices. The fact that current attack detection methods only detect attacks without assisting security analysts in determining their root causes is a major flaw. As a result, in order to identify and isolate the attack's cause, manual analysis is required. An aid in tracking an attack's spread is causal analysis. There is insufficient research on the causal analysis of attacks in ICS networks, despite the network's lack of security. We present a method for filling this ICS network research void by analyzing causal dependencies in ICS logs to identify attacks' causal effects. There are two phases to our ICS Causal Anomaly Detection (ICS-CAD) method. It first identifies the ICS device that is producing the malicious traffic and detects attacks. Second, it looks at the causal relationships between the ICS logs to figure out what the attacker will do in the future. In order to find causal relationships in ICS logs, we employ a technique known as causal decomposition. Two datasets from actual ICS networks are used to evaluate the ICS-CAD's performance. The ICS-CAD can pinpoint attacks and their underlying causes with an accuracy of 98%. With the commitment of a synergistic effect on the Proficiency Carefulness Compromise, Showcasing is progressively advancing kinds of Modern Control Frameworks (ICS) that by certain method consolidate the two generally isolated center ICS capabilities into one. Using shared resources of some kind, a Safety-Instrumented System (SIS) and a Basic Process Control System (BPCS) are combined in a physically integrated form factor. According to the findings of this study, making such a deliberate choice of technology could lead to Functional Safety (FS) risks or security flaws, raising questions about resilience. It proposes strict separation of such functions and resources rather than taking a skeptical stance on such an approach.