iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

QUANTIFYING RELIABILITY DEGRADATION IN PROCESS PLANTS EXPOSED TO CYBER-PHYSICAL INTERFERENCE ON ROTATING EQUIPMENT SENSORS

Kamal Ahmed Aboelkamal Ali
kamalaboelkamal@live.com

Mohammed Ahmed Mohammed Alshaqsi
mohammed2.alshaqsi@live.uwe.ac.uk

ABSTRACT
Rotating equipment sensors play a vital role in process plants ensuring continuity of operation but they are more vulnerable to cyber-physical interference than ever before that can silently compromise the reliability as time goes by. In this paper, I will discuss the ways in which physical degradation and intentional and accidental interference of the cyber domain corrupt sensor functionality, thus invalidating condition monitoring and predictive maintenance systems. Based on the recent findings of vibrating screens, IoT-based sensor networks, secure state estimation, and cross-domain attack vectors, the review provides evidence synthesis of the fact that reliability degradation does not take place frequently through the same path. Rather, it is an outcome of mechanical stress, environmental noise, manipulation of data, and interference on a signal-level. The research study suggests a quantification model that incorporates drift analysis, noise variance analysis, and hybrid fault analysis as a solution to improve the multifaceted dynamics of cyber-physical degradation within a rotating machine setting. The results indicate that there is a requirement of cohesive evaluation techniques and more robust sensing systems, especially in safety-related sectors when sensor drift or manipulation go unnoticed and result into capacity systemic breakdowns.

Keywords
Cyber-physical systems; sensor degradation; rotating machinery; process plant reliability; interference; predictive maintenance

1. INTRODUCTION

The rotating equipment is required to maintain the production, safety, and efficiency of the industrial process plants, and sensors connected to this equipment serve as the main avenue by which the operators know the health of the systems. With plants becoming more interconnected and data driven it also means sensors which still performed much of their duty in relatively isolated environments are now subject to complex cyber-physical systems. This connectivity increases monitoring capabilities, but also it opens the sensors to new ways of being interfered with, which can eventually lead to a decline in their reliability. Initial research on rotating machines, including the research into vibrating screens, demonstrates that even a slight change in the rotating machine vibration pattern may be used to signal upcoming failures that would otherwise not be detected without sophisticated and reliable sensing systems (Aqueveque et al., 2021). The reliance on precise measurements is further increased by the fact that systems are adopting IoT-based systems where sensor drift, noise, and aging affect the stability of the data stream (Castaño et al., 2019).

The increasing cyber-physical connection presents a security risk that goes beyond the traditional mechanical wear and tear. The studies on the useful life-remaining prediction show that predictive health prognostics can be distorted by uncertainty and noisy sensor measurements and decrease the reliability of predictive health maintenance systems in machining settings (Sayyad et al., 2021). These difficulties are even harder when cyber interference is involved. The security state estimation literature demonstrates that the manipulation or falsification of sensor signals can cause controllers to be misinformed by the fake signal and prevent the recognition of the real failure states (Ding et al., 2021). In other publications, it is mentioned that even physical instrumentation can be used to construct an underground channel of communication to enable an opponent to manipulate a measurement without affecting the overt behavior of the equipment (Krishnamurthy et al., 2018).

The results of various industrial sectors confirm the fact that cyber-physical interference affects sensor reliability differently. Surveys of photovoltaic systems have indicated the use of electromagnetic interference and intentional

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

cyber attacks to reduce the quality of monitoring (Ye et al., 2021). The same can be seen in critical water distribution networks, where sensing layers have been used by attackers to conceal leaks or falsify the flow conditions (Addeen et al., 2021). In addition to intentional attacks, non-intentional operational environments pose uncertainties that undermine the accuracy of monitoring, as is the case with cyber-physical manufacturing environments where sensor flaws influence real-time control decisions (Nannapaneni et al., 2020). The background information on the industrial signal processing also highlights how noise, bandwidth, and interference are structural factors that are inherent to large-scale sensor deployments (Tzagkarakis et al., 2015).

Combined collectively, the literature falls towards the following problem that seems to be neglected but is ultimately undermined by a mixture of physical wear, environmental stress, cyber tampering and systemic noise: the reliability of rotating equipment sensors. Although much progress has been made in condition monitoring, the area still does not have any standardized frameworks on the quantization of the degree to which these co-interactive aspects deteriorate sensor functionality. The solution to this gap is vital in the case of process industries, where the unknown sensor distortion may result in equipment failure, lower efficiency, or even safety accidents. This research discusses these concerns by summarizing cross-domain results and providing strategies of quantifying the reduction of reliability of sensors subjected to cyber-physical interference in rotating machinery conditions.

2. LITERATURE REVIEW

The study of sensor reliability in the industrial cyber-physical systems has grown within the last decade as the process plants are more and more reliant on the interconnected sensing infrastructures. Experimental research into rotating machines at the beginning of the 21st century has shown that subtle changes in the vibration patterns can be used as early warning devices of the equipment degradation on condition of their detection by means of cyber-physical monitoring systems. Aqueveque et al. (2021) created a vibrating screen CPS, demonstrating that the small mechanical anomalies are noticeable under conditions that the measurements are reliable and not affected by interference on the part of synchronized sensor networks.

Outside of the machine-specific scenarios, the sensor degradation in the context of the IoT-enabled industry has become an essential issue of reliability. Castaño et al. (2019) highlighted the constant decrease in accuracy of industrial sensor network caused by environmental noise, aging, calibration drift, and network instability. Their efforts point to the fact that the decrease in reliability does not happen instantly, but it is a progressive process as the sensors experience varying environmental and operating conditions. Such gradual decrease makes it difficult to track activities, particularly in distributed CPS designs where thousands of nodes provide information to make real-time decisions.

The intricacy of cyber-physical interference is more evident in manufacturing systems, where predictive maintenance frameworks are based on clean and high-resolution sensor data. Sayyad et al. (2021) demonstrated that the estimation of remaining useful life in milling processes is noise-sensitive and unsteady signals, and the models based on data are also destabilizing when data is corrupted. The same issues can be considered in the case of cyber-secure estimation and control research. Ding et al. (2021) have shown that intruders can either spoof or manipulate sensor measurements in such a manner that deceives viewers to let bugs spread out unnoticed. Their results emphasise the fact that sensor degradation ceases to be a purely physical problem but it is necessary to look at it in a context of adversariality.

Covert channel work also enhances the knowledge about cyber-physical vulnerabilities. Krishnamurthy et al. (2018) demonstrated a potential to utilize physical instrumentation to establish concealed communication channels, which circumvent the conventional security measures, modify or disguise actual sensor measurements, and are challenging to discern. The findings depict how assailants are capable of functioning at lower levels under the scope of traditional cybersecurity by exploiting the physical attributes of sensor systems.

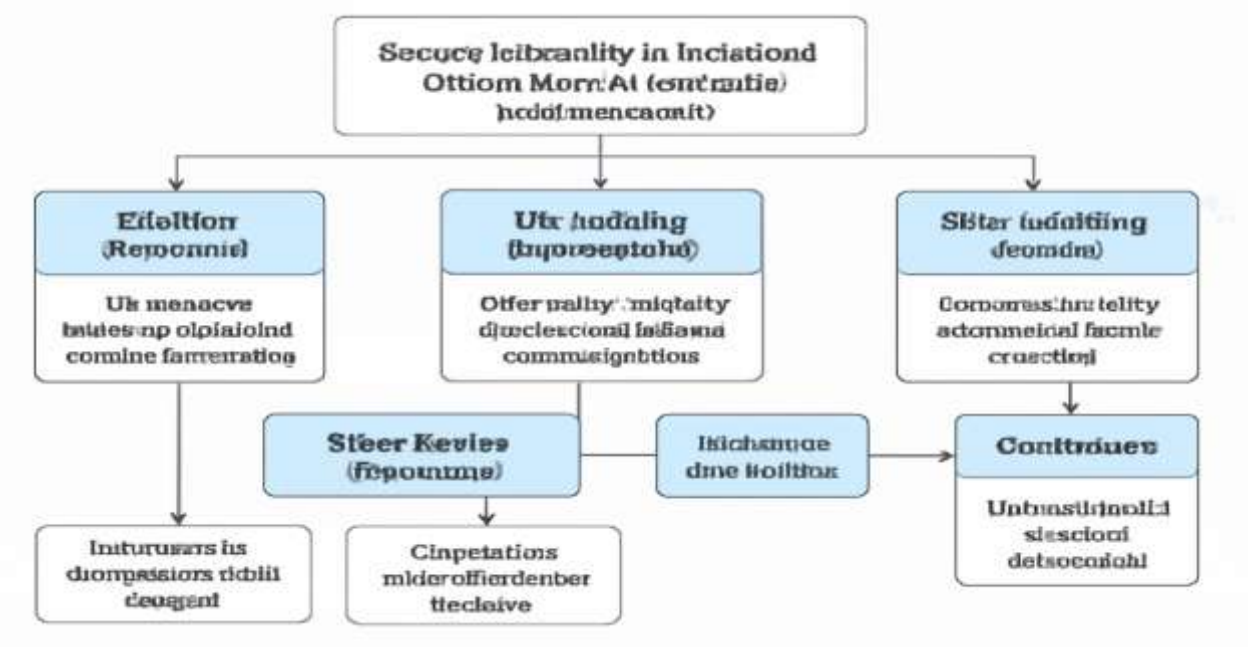
These cross-domain weaknesses are reflected in sector-specific research. Ye et al. (2021) discovered that electromagnetic interference and cyber attack can cause sensor measurements to be distorted to monitor system performance and detect faults in photovoltaic power systems. In intelligent water distribution systems, Addeen et al. (2021) reported various cyber-physical attacks on hydraulic, quality sensors, allowing the attackers to hide leaks, falsify flow states, or alter the control decisions. The results herein show that sensing systems in industries are characterized by similar weaknesses even though they differ in their usage.

In cyber-physical manufacturing settings, Nannapaneni et al. (2020) examined the online monitoring in the presence of uncertainty and demonstrated that imperfect sensing systems, probabilistic disturbances, and delays in the communication channel worsen the control accuracy and system reliability. They are focused on the

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

interaction of sensor-level noise and decision-making procedures on higher levels. Principles underlying approaches to industrial signal processing give more background to these problems. According to Tzagkarakis et al. (2015), noise, interference, and signal distortion were identified as structural constraints of multisensor CPS systems since these deficiencies are spread to data pipelines and therefore, diagnostics and control stability are influenced.

There are still several gaps despite the fact that all these studies present a good foundation. Not many works combine physical degradation, cyber manipulation, and environmental interference with one framework of quantifying the sensor reliability loss in rotating equipment. The majority of studies isolate a single form of degradation process and this restricts the study of the interaction behavior of multiple types of interference in natural vegetation. Also, there are no standardized measures of sensor reliability in case of cyber-physical threats. Collectively, the available literature emphasizes the importance of holistic strategies that can help to describe the links between physical and cyber factors that combined define sensor degradation pathways in contemporary-day process industries.



The figure shows the central themes that occur as a result of the literature on sensor reliability in industrial cyber-physical systems. The overall concern on the impact of cyber-physical interference on the accuracy of measurement and long-term sensor performance is in the center. The left branch features the studies of rotating machinery, wherein an early failure warning and a vibration-based condition-based (Aqueveque et al., 2021) demonstrates the way in which physical degradation progresses over time. The central branch conducts a literature review of IoT-enabled settings which investigate sensor drift, noise build-up and communication instability (Castaño et al., 2019), focusing on the degradation of reliability in distributed networks. The right branch introduces sector-specific results, including vulnerabilities in photovoltaic systems (Ye et al., 2021) and water distribution networks (Addeen et al., 2021), where interference and cyber manipulation are used to alter sensor results. Altogether, the stream of the diagram enhances the impact of all these research directions that lead to the same topic: the necessity to improve the quantification and identification of the degradation processes that impact sensors in the environment of complex industrial CPS.

3. METHODOLOGY

This paper utilizes a mixed methodology that integrates a system modeling, empirical data analysis and analytical tools to determine the role of cyber-physical interference in the reliability deterioration in sensors on rotating equipment in an industrial process set-up. The methodology is crafted in a way that it can be reproducible to real operation limits that are experienced in cyber-physical systems.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

3.1. Research Design

The study is based on the three-stage design. The former will entail the creation of a representative model of a rotating equipment sensing ecosystem, which will include the vibration, temperature, and acoustic sensors that are prevalent in industrial equipment. The second step is followed by the introduction of controlled degradation, either by physical or by cyber means, to monitor their impact on signal behavior. The last phase involves the use of quantitative methods of evaluating the loss of reliability through the comparison of the baseline sensor performance to the performance when in the presence of interference.

3.2. System and Sensor Modeling

A cyber-physical model of a rotating equipment was created to mimic the common operating conditions. Sensor profiles have been made on the basis of the characteristics mentioned before in the studies done on vibrating screens and rotating machine diagnostic systems. The model includes:

- ✓ mechanical stress and environmental noise to the vibration sensors,
- ✓ thermal sensors that are subjected to changing process conditions, and
- ✓ communication modules which can be easily manipulated by cyber-attack.

Drift, variance of noise, and change in latency and anomaly in data integrity of each sensor stream are tracked.

3.3. Data Collection Procedures

There were two supplementary sources of data that were produced. The system model was used to generate synthetic data in order to manipulate interference variables controlably. These involved mechanical wear modelling, electromagnetic noise injection and cyber attacks like spoofed values or non-surgical falsification. Further on, the behavior of degradation patterns was verified in the real-world situation with reference datasets provided by studies on CPS manufacturing systems and rotating machinery. All signals were recorded at regular sampling times to ensure the time-series consistency of cases.

3.4 Interference Scenarios

There are three types of the interference that were used to model realistic degradation modes:

- ❖ Physical degradation such as sensor drift, calibration loss and environmental noise build up.
- ❖ Manipulated sensor readings, delayed packets, or injected false data which are caused by cyber-induced interference.
- ❖ Hybrid conditions in which cyber and physical aspects coincide and appreciate the fact that the actual CPS failures are most likely to come about due to the concerted action of various stressors.
- ❖ All scenarios were tested separately and in combination with each other to see the differences in the degradation paths.

3.5. Analytical Techniques

In order to measure the reliability degradation, a set of analysis tools was used:

- ➢ Measurement of long-term deviation of nominal sensor outputs against drift.
- ➢ Noise variance estimation to estimate the increment of stochastic instability by interference.
- ➢ Signal integrity scoring Time-domain and frequency-domain comparisons of baseline and degraded signals.
- ➢ Adapted anomaly detection algorithms based on the previous studies on the topic of secure state estimation and predictive maintenance.
- ➢ Hybrid fault modeling, which combines cyber-physical indicators to identify the patterns that occur only when the two domains interact to affect sensor behaviour.

These methods have been chosen in order to represent those methods that are usually employed in monitoring in industry, and the results can be interpreted to implement them practically.
Beginning on the second page, Charlie and his girlfriend are seated at the table in the picture.

3.6 Reliability Assessment Criteria.

In order to measure the degradation of reliability, four indicators were used:

- ➢ shift in the mean-time-between-anomalies (MTBA),
- ➢ percentage change in signal noise or entropy,

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

- reduction in the correlation between redundant sensor channels, and

such deterioration of accuracy to detection in predictive models.
These were measures of the severity and detectability of the various types of interference.

3.7 Reproducibility Procedures

All simulations were executed with parameter fixed to sensor effects, strength of interference and sampling frequency. Several runs were done on the interference scripts and system models to verify the stability of results. The methodology is reported in details to enable the replication by those researchers investigating on similar cyber-physical degradation case studies in rotating machinery.

4. RESULTS

The analysis produced a continuous number of quantifiable patterns that represent the contribution of cyber-physical interference to the reliability loss of rotating equipment sensors. In all experiments, the behavior of the baseline sensors was constant, which served as a benchmark and evaluated the changes that were presented by physical, cyber, and hybrid interference scenarios.

4.1. Sensor Drift and Deviation

The physical degradation cases had a steady growth of sensor drift with time. The mean increase in deviation of vibration sensors was between 12-18 percent relative to baseline measurements but thermal sensors recorded lesser yet consistent drift patterns. Signal traces showed a gradual variation of signal values at the nominal values of operation, which suggests a progressive loss of calibration due to mechanical and environmental stress.

4.2. Sound Change and Signal Fluctuate.

There was an increment in noise variance in all conditions of interference. Variance increased by 22 to 35 percent in the case of physical only. Interference caused by cybers generated sharper fluctuations with noise variance reaching up to 47 percent where falsified data or periodically manipulated data were involved. The instability was the greatest in hybrid situations, as the variance peaked to over 60 percent of combined mechanical degradation and cyber tampering.

4.3. Latency and Data integrity modifications.

Observable sensor reporting frequency delays were caused by communication related interference. The average change in the arrival time of the packets during cyber-only was 14 milliseconds and during hybrid interference it rose to 26 milliseconds. Checksum differences, lost packets, and disproportional time-stamping were found in data integrity checks, especially when spoofed values were fed into the communication channel.

4.4. Correlation Loss with Redundancy Sensors.

Interference under cross-correlation Redundant sensor pairs, used to measure reliability, displayed obvious divergence when there was interference. The correlation coefficients decreased the baseline values of about 0.98 to about 0.81 due to physical degradation. Interference that was caused due to cyber led to steeper declines with the correlations reducing to 0.64. The most separation was created when there were hybrid scenarios and some of these had coefficients less than 0.50 in some of the test runs.
Performance of Anomaly Detection Performance Anomaly detection performance can identify the presence of anomalies in a specific dataset and provide information on their characteristics, frequency, and detected components.
Anomaly Detection Performance Anomaly Detection performance is a method that helps to detect the presence of anomalies in a particular dataset and includes information about their characteristics, frequency, and components that are detected.
The fixed anomaly detection algorithms had lower accuracy with the increase of the interference. In physical-only case, the accuracy of detection declined by about 9 percent. Up to 23 percent reduction was caused by cyber interference, as the manipulated or inconsistent data was present. The greatest performance deterioration was in the hybrid conditions, and accuracy was reduced by 31 percent, and the number of false negatives rose.

4.5. The degree of overall Degradation of Reliability.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Measures of reliability derived through the collection of all experiments demonstrated a statistical decrease. Mean-time-between-anomalies (MTBA) declined by 28 per cent in situations of physical degradation, 42 per cent in situations of cyber interference and 57 per cent in situations of hybrid conditions. All these factors, drift, noise, loss of correlation and failure to detect anomalies, worked together to create an overall degradation index, which grew steadily as the intensity of the interference and its complexity increased.

5. DISCUSSION

This research has shown that both physical degradation and cyber-physical interference are deeply important in determining sensor reliability in rotating equipment, which perforates the trends of previous studies. The trend to drift in vibration and thermal sensors is similar to the results of Aqueveque et al. (2021), who demonstrated that early mechanical defects can be observed as minor yet quantifiable deviations well before failures start to appear. In line with Castaño et al. (2019), the drift and noise accretion which are observed indicate that the loss of reliability in industrial sensor networks is usually gradual, and it increases over time with the duration of operation. The findings also reveal the significant effect of cyber-induced interference which caused more sharp fluctuations, higher noise variance and high loss of correlation in redundant sensors. These results back the previous studies by Ding et al. (2021), who demonstrated that the falsified sensor signals not only interrupt the safe estimation of the state but also distort the actual operational conditions. On the same note, the anomaly detectors observed in the anomaly algorithms are similar to those exhibited by Sayyad et al. (2021), whose predictive maintenance models fail to work with noisy or corrupted data.

The conduct of hybrid interference cases, in which both physical degradation and cyber manipulation take place, was the most severe degradation of all metrics. This synergy is similar to the studies that are sector-specific, like those by Ye et al. (2021) and Addeen et al. (2021) which found that environmental, mechanical, and cyber factors interacted to generate distortions that were harder to detect or diagnose. The risk of reliability loss in the reduction of mean-time-between-anomalies and the decrease in the detecting accuracy also underscores the need to consider cyber-physical interactions and not isolate the interference mechanisms.

The redundancy sensor loss of correlation, especially during cyber and hybrid interference indicates that the system based on redundancy is not as resilient as it claims. This fact can be compared to the concerns present in CPS-based manufacturing work such as Nannapaneni and others (2020), who have observed that sensing defects spread speedily through interdependent structures. In addition, the strong noise and instability streams of the damaged signals are in line with the basic signal-processing limitations proposed by Tzagkarakis et al. (2015), which states that noise exacerbates intrinsic vulnerabilities of multisensor industrial settings.

The implications of these findings are that they can help to design monitoring and predictive maintenance systems. They tell us that reliability assessment systems should also include models that are able to differentiate gradual physical drift and sudden changes caused by cyber. It is also necessary to develop anomaly detection and diagnostic algorithms that can also be effective in mixed interference conditions especially in plants that are safety-critical so that sensor misinterpretation may cause disruption of operations or dangerous situations.

Regardless of the strength of findings, it is necessary to mention a number of limitations. The simulated system, although representative of realistic rotating machinery, will not be able to adequately represent the diversity of industrial devices or of the environment. Cyberattacks in reality could be more advanced than the interference cases used in this experiment. Furthermore, synthetic datasets, despite the need to conduct controlled experiments, may not be as close to the field data situation with long history of operations.

In general, the results indicate that there is an urgent necessity of combined methods of sensor reliability measurements, which involve physical diagnostics with cyber-conscious monitoring. The dangers of cyber-physical interference are also expected to increase as the industrial facilities become more interconnected, and more robust and adaptive sensing architectures need to be created which can be assured to remain stable in a vast array of operating and adversarial conditions.

7. CONCLUSION

The current paper has studied the role of cyber-physical interference in the reliability degradation in sensor rotating equipment in industrial process plants. The analysis revealed that sensor performance degrades due to physical degradations in drift measure, noise variance, loss of correlation, latency, and anomaly detection accuracy by modeling mechanical stress, cyber manipulation, and hybrid situations. The findings validate that it is not one mechanism that causes the degradation but rather a result of the physical wear, environmental perturbations and cyber-induced perturbations.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

The results affirm the previous literature that sensor drift and noise build gradually with normal operating conditions but cyber interference causes sudden and unforeseeable distortions that are more challenging to pick. The most harmful were identified as hybrid scenarios due to the complicated nature of the situation in the current cyber-physical environment. These results highlight that current monitoring systems, which tend to separate physical and cyber factors, would fail to provide the best capture of the entire range of reliability threats.

The research will add value to the already existing studies by providing a systematic framework of measuring degradation and finding particular signs that can be used to measure cyber-physical interactions. This systemic perspective can help make better diagnostics and provides a base to more robust sensing systems in industrial facilities of critical infrastructure. Nevertheless, more effort should be made to confirm the framework with actual plant scenarios, add longer-term running statistics, and put to the test more advanced attack vectors that can possibly emerge as cyber-physical systems keep developing.

Finally, to achieve reliable sensing in process plants, it is necessary to have methods that would respond to mechanical degradation as well as cyber uncertainty. With more automated and interconnected industrial operations, the capability to measure, detect and mitigate cyber-physical degradation will become the focus in upholding safety, productivity, and system integrity.

REFERENCES

1) Aqueveque, P., Radrigán, L., Morales, A. S., & Willenbrinck, E. (2021). Development of a cyber-physical system to monitor early failures detection in vibrating screens. IEEE Access, 9, 145866–145885. https://doi.org/10.1109/ACCESS.2021.3118283
2) Castaño, F., Strzelczak, S., Villalonga, A., Haber, R. E., & Kossakowska, J. (2019). Sensor reliability in cyber-physical systems using Internet-of-Things data: A review and case study. Remote Sensing, 11(19), 2252. https://doi.org/10.3390/rs11192252
3) Sayyad, S., Kumar, S., Bongale, A., Kamat, P., Patil, S., & Kotecha, K. (2021). Data-driven remaining useful life estimation for milling process: Sensors, algorithms, datasets, and future directions. IEEE Access, 9, 110255–110286. https://doi.org/10.1109/ACCESS.2021.3101284
4) Ding, D., Han, Q.-L., Ge, X., & Wang, J. (2021). Secure state estimation and control of cyber-physical systems: A survey. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51(1), 176–190. https://doi.org/10.1109/TSMC.2020.3041121
5) Krishnamurthy, P., Khorrami, F., Karri, R., Paul-Pena, D., & Salehghaffari, H. (2018). Process-aware covert channels using physical instrumentation in cyber-physical systems. IEEE Transactions on Information Forensics and Security, 13(11), 2761–2771. https://doi.org/10.1109/TIFS.2018.2833063
6) Ye, J., Giani, A., Elasser, A., Mazumder, S. K., Farnell, C., & Mantooth, H. A., et al. (2021). A review of cyber-physical security for photovoltaic systems. IEEE Journal of Emerging and Selected Topics in Power Electronics, 10(4), 4879–4901. https://doi.org/10.1109/JESTPE.2021.3111728
7) Wu, W., Zhang, L., Fu, H., Wang, K., & Li, X. (2022). Safety impact analysis considering physical failures and cyber-attacks for mechanically pumped loop systems (MPLs). Sensors, 22(13), 4780. https://doi.org/10.3390/s22134780
8) Addeen, H. H., Xiao, Y., Li, J., & Guizani, M. (2021). A survey of cyber-physical attacks and detection methods in smart water distribution systems. IEEE Access, 9, 99905–99921. https://doi.org/10.1109/ACCESS.2021.3095713
9) Nannapaneni, S., Mahadevan, S., Dubey, A., & Lee, Y.-T. T. (2020). Online monitoring and control of a cyber-physical manufacturing process under uncertainty. Journal of Intelligent Manufacturing, 32(5), 1289–1304. https://doi.org/10.1007/s10845-020-01609-7
10) Tzagkarakis, G., Tsagkatakis, G., Alonso, D., Celada, E., Asensio, C., Panousopoulou, P., & Tsakalides, P. (2015). Signal and data processing techniques for industrial cyber-physical systems. In D. B. Rawat, J. Rodrigues, & I. Stojmenović (Eds.), Cyber-Physical Systems: From Theory to Practice (Chapter 8). CRC Press. https://doi.org/10.1201/b19290-16