SDSEPS
Strengthening Dynamic System e-Government and Public Services
SDSEPS 1(1): 1–9
ISSN XXXX-XXXX

Institute for Advanced Science, Social and Sustainable Future
MORALITY BEFORE KNOWLEDGE

Benefits of technology control systems in countering intelligence threats

Syuhada Satria[1]*, Asep Adang Supriyadi[2], Syachrul Arief[3]
[1] *Intelligence Technology, National Intelligence College, Bogor, 16810, Indonesia*
[2] *Sensing Technology, Faculty of Science and Technology, Republic of Indonesia Defense University, Bogor, 16810, Indonesia*
[3] *Geospatial Information Agency, BIG, Bogor, 16911, Indonesia*
*Correspondence: sylvangiovani1918@gmail.com

Received Date: December 8, 2024 Revised Date: January 6, 2024 Accepted Date: February 18, 2024

ABSTRACT
Background: Control system technology has become an important component in many aspects of life, including defense and intelligence. These technologies not only help manage new energy, but also improve military quality and protect the country from intelligence threats. However, there is a need to deeply understand the collaboration between technological control systems and elements such as energy security, military power, and biological defense. **Methods:** This research uses the literature study method by collecting and analyzing academic sources from relevant journals, books, and research reports. The literature search was conducted through various academic databases with keywords related to control systems, new energy, intelligence, and military defense. The literature selection process involved rigorous screening to ensure the quality and relevance of the sources used. **Findings:** The literature analysis shows that control system technology can be integrated with various sectors, such as wave energy conversion through Wave Energy Converter (WEC), improvement of military defense equipment with the concept of Dynamic Flight Envelope Assessment and Prediction, and development of drug production systems to counteract biological hazard threats. In addition, alarm systems integrated with control systems can increase security from intelligence threats. **Conclusion:** The use of technological control systems plays an important role in strengthening national security, whether in the aspects of energy, military, or biological defense. These technologies enable more effective and responsive management of complex and dynamic threats. The development of these technologies, when combined with intelligence, can be an important tool in dealing with resource crises and global military conflicts. **Novelty/Originality of This Study**: This study provides a comprehensive overview of the integration of technological control systems with state security, which has not previously been discussed in much detail in the context of intelligence and defense. This interdisciplinary approach offers a fresh look at how modern technology can strengthen national defense in an era of evolving threats.

KEYWORDS: defense equipment; energy security; intelligence; national defense; technology control system.

1. Introduction

A control system is designed to regulate and influence the behavior of other systems, ensuring they function within certain parameters to achieve specific objectives. According to Robert N. (1994), control systems encompass various components such as sensors, actuators, controllers, and algorithms that work collectively. Katsuhiko O. (2010) illustrates this through examples like temperature control systems, where sensors monitor room temperature, and actuators adjust airflow to maintain a stable environment. In aviation,

Cite This Article:
Satria, S., Supriyadi, A, A., & Arief, S. (2024). Benefits of technology control systems in countering intelligence threats. *Strengthening Dynamic System e-Government and Public Services*, 1(1), 1-9. https://doi.org/.....

autopilot systems use sensors to gauge an airplane's position, speed, and altitude, while actuators control critical elements like the wings and engine. Through these applications, control systems demonstrate their crucial role in achieving precision, stability, and efficiency in complex operations.

In sectors involving sensitive information or high-stakes environments, control systems also serve as a defensive measure against intelligence threats. Intelligence threats refer to any efforts by external parties to access classified information that could compromise a country, organization, or individual. Such breaches, if left unaddressed, can have severe consequences for security and operational integrity. Without adequate countermeasures, the target organization or entity risks exposure to vulnerabilities that can impact their stability and safety. Control systems, when applied effectively, create an additional layer of protection, enhancing the capacity to detect and mitigate potential threats.

To maximize security and effectiveness, implementing control systems across various technological applications is essential. Existing technological systems alone may not offer the responsiveness needed to counter intelligence threats unless integrated with advanced control mechanisms. Control systems act as a cohesive force, optimizing functionality by coordinating various elements within the system to respond to potential risks. This integration strengthens technological resilience and adaptability, ensuring that systems can meet dynamic security demands. Consequently, the deployment of control systems is critical for sustaining operational security and integrity in the face of evolving threats.

2. Methods

This essay uses a systematic literature study approach to identify and analyze key concepts related to technology and intelligence control systems in the context of state security and military development. The first step in this method is to conduct a literature search from various academic sources, including books, journals, and research reports relevant to the topic. Keywords such as "control systems," "intelligence," "threat intelligence," "new energy," and "military" were used to ensure broad coverage. The sources were accessed through academic databases with good accuracy and reference quality.

The second step was a literature screening process to evaluate the relevance and validity of each source. Only literature published within the last 15 years was used, with a focus on peer-reviewed and academically recognized research. Each piece of literature was critically analyzed by considering the credibility of the author, the research methods used, as well as the suitability of the findings to the research objectives of this essay. In addition, a literature review was conducted to understand current trends in technological control systems and the role of intelligence in security and defense development.

The third step is the synthesis of data from the selected literature. Data from various sources are combined to form a thorough analysis of the interaction between technology, energy and intelligence control systems in strengthening state security. In this process, different perspectives and theoretical approaches are integrated to identify existing research gaps as well as potential applications of new technologies. The results of this analysis are set out in an essay with in-depth and evidence-based arguments, in order to make a significant contribution to the relevant literature. The brainstorming of this research can be seen in figure 1.

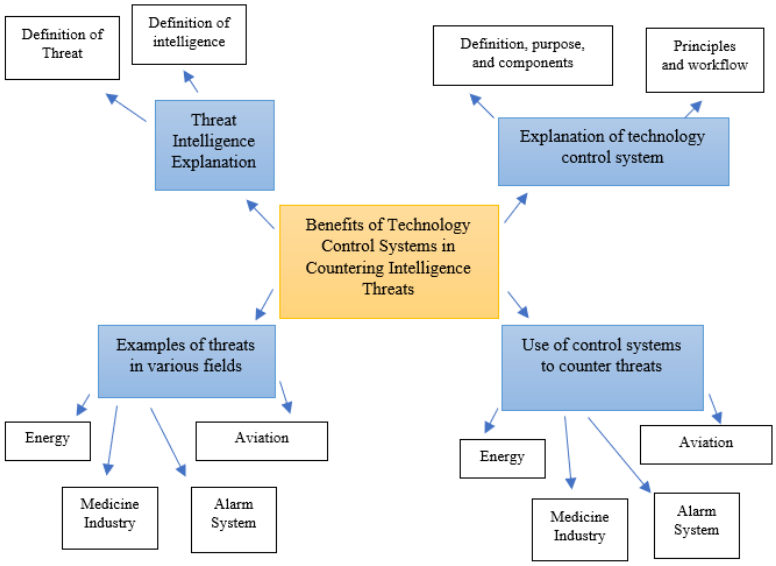

Fig 1. Brainstroming

3. Results and Discussion

3.1 Technology control system

Technological control systems are systems that are currently used in almost all areas of our lives. A system that regulates process variables to follow a reference value is called a control system (Katsuhiko O, 2010). In addition, a system that is intended to control the behavior of another system is also called a control system (Robert N, 1994). Control systems have the purpose of forcing or controlling inputs and outputs to follow a certain variable despite external disturbances (Benjamin C, 2010). Control systems are widely used in various fields, such as industry, manufacturing, robotics, and aerospace, which involve sensors, actuators, controllers, and processes as components (Katsuhiko O, 2010). There are two types of control systems, namely open-loop control systems and closed-loop control systems (Robert N, 1994). This system can be utilized for simple to very complex things. Uses that can be felt in everyday life such as room temperature control systems, motor speed control systems, and autopilot control systems on airplanes (Benjamin C, 2010).

In its use there are several working principles, the principle of classical linear control systems is one of the most frequently used. The basic principles of classical linear control, including stability, feedback regulation, and linear system dynamics, were developed in the late 1800s and became a mature theory in the 1950s (Thomas G, 2001). Power electronics systems can be classified into two types, namely DC (Direct Current) and AC (Alternating Current). This categorization is based on the fact that the circuit topologies, control techniques, and power levels of each type of system are very different.

The control system flow typically found in some device's working system starts from the Supervisory control layer that sends setpoints to lower-level controllers. The main design goals are usually to maintain product quality, ensure there are no production-level discrepancies, and avoid operational problems caused by recycling. Then a higher-level control layer-known as the supervisory control layer-combines the control system for each unit operation. As the stream flows through the production process, supervisory control controls the flow rate and watches for impurities to ensure that there is an increase in impurities in it. The supervisory control layer sends points to lower-level controllers, with the main design standard usually maintaining the product. The supervisory control layer sends the setpoint to the lower-level controller. The main design goals are usually to maintain product quality, ensure there are no production-level discrepancies, and avoid operational problems caused by recycling. Supervisory control systems operate on a slower timescale and can be adjusted with some analytical laboratory output, while lower-level

control loops typically use real-time measurements throughout the process. In general, however, control systems are designed to separate the timescales between supervisory level (slow) and operating level units (fast). This allows the operator to concentrate on operations at the plant level or single operating unit level.

Today, systems consist of many embedded controllers interacting at different levels of the system hierarchy, and the sheer amount of embedded code significantly affects the design of other control systems. As a result, control system verification and validation (V&V) must consider many complex elements. The considerations are that controller components are evaluated in combination and individually within a level of functional hierarchy, then the V&V process integrates the various subsystems at different levels in the functional hierarchy, and finally consider how the chosen implementation technology and design methods impact each phase of the development cycle. This systems framework then includes theory, tools, and methods for addressing optimal controller design issues across and between levels of functionality, implementation, and realization for the specific task of control system development (Thomas G, 2001).

3.2 Threat intelligence

Intelligence involves covert activities that include targeting, collection, analysis, dissemination, and action, all of which aim to enhance security or maintain a strategic advantage against competitors. These activities are crucial for providing early warnings about emerging threats and identifying opportunities to safeguard national or organizational interests (Peter Gill, 2009). Traditionally, intelligence work has focused on identifying "threats," understood as deliberate actions by adversaries, but this focus has broadened to include the concept of "risk" as a key element. The terms "threat" and "risk" are now used in tandem, where "risk" may refer to both intentional and unintentional potential losses, thus expanding the scope of intelligence beyond strictly hostile actions (Johansen). This shift reflects the growing complexity of modern security landscapes, where threats can arise from various sources, not all of which are intentional or targeted.

For intelligence professionals, threat analysis remains a core focus, encompassing an evaluation of an adversary's capabilities, objectives, and strategies. In this analysis, intelligence workers may also assess the opportunities and appeal of a threat from the adversary's perspective, as well as potential consequences for the target. This multifaceted approach allows intelligence to provide nuanced insights that go beyond basic threat detection, supporting decision-makers in crafting informed responses. By understanding both the threats and risks involved, intelligence can offer a more comprehensive view of vulnerabilities and advantages, thus reinforcing preparedness. Ultimately, the integration of both threat and risk assessments enables intelligence to address a broader range of security concerns in a rapidly changing environment.

3.3 Threats in various fields

The many threats that exist are threats that come from various fields. Both from the smallest lines in society to sectors that concern the livelihood of many people. Both deliberate from certain parties and conditions created by nature or a process that is incidental. Whatever the source or cause, any form of threat in the eyes of intelligence is something that can disrupt the sovereignty of a country. So a prototype is needed that can collaborate with existing systems and can help to prevent and overcome existing threats.

The crisis of natural resources due to the use of conventional energy is already very pronounced. Not to mention the damage to nature that is a side effect of its use. This is quite a dangerous threat to the sustainability of the environment and its people. Therefore, a new, safer energy is needed to replace conventional energy. Much attention has turned to renewable energy as a result of the recent sharp rise in oil prices, security of supply concerns, and pressure to comply with greenhouse gas emission limits such as the Kyoto Protocol. Resources to meet the growing demand for energy. Other energy sources such as

biomass, solar, and tidal power are still underutilized, but wind energy technology has developed rapidly. Wave energy has previously untapped potential, and the variability nature of wave energy has proven to benefit perennial problems with many renewables, especially wind especially when used in conjunction with wind energy (F. Fusco, 2010).

In the midst of conflicts that occur everywhere, strengthening the military fleet, especially the air is important. The conflict will become an external threat that disrupts the sovereignty of a country if its military sector is weak. Therefore, it is necessary to develop the quality of the country's military by increasing the capabilities of the fleet or defense equipment owned. Military aviation safety is critical to military operations as aviation accidents can cause personnel loss of life, asset damage and mission failure. Therefore, it is important to implement effective safety measures to reduce the risk of accidents and ensure flight operations run smoothly (Fajar Adriyanto, 2020). One of the new technologies involving control systems is Dynamic Flight Envelope Assessment and Prediction. NASA will have a Dynamic Flight Envelope Assessment and Prediction system that will improve flight safety by allowing them to measure changes in structure dynamics modes caused by damage and find online fault anomalies for damaged air vehicles. In addition, the system provides adaptive control to ensure that the damaged aircraft stays outside the permissible limits of the structure. This is done to avoid adverse relationships between dynamic structural modes and flight control systems. The main focus of this paper is Control Centered Modeling; this combines load models and rigid body models with flexible dynamic structures to provide the basis for adaptive control of the load properties of aircraft structures over the internet.

Biological Hazard is a new field that was originally a threat due to natural processes, but recently it has become a tool used by certain parties to attack others. The impact of this biological threat is very broad. Therefore, there is a need for a control system that supports the industrialization of biological drug manufacturing to cope with future threats. Under the Defense Advanced Research Projects Agency's (DARPA) Biologically Derived Medicines on Demand (Bio-MOD) program, the Integrated and Scalable Cyto-Technology (InSCyT) platform is a prototype biomanufacturing platform that aims to develop a platform that enables rapid biological purification and protein production (Amos E, 2015). Modeling unit operations is a major focus in the bioprocessing industry. Models for bioreactors and chromatography have been completed and will be briefly discussed in the following sections. However, unit operations do not run in isolation, and downstream processing will be affected by changes in unit operating conditions. This is the reason why an integrated plant model is suggested.

Any infrastructure in a country is vulnerable to being targeted by foreign and domestic intelligence threats. To increase our vigilance and response in the face of incoming threats, an alarm system is needed. Alarms can be highly functional when collaborated with the right control system. The International Society of Automation (ISA) states that “Alarm management is the set of processes that ensure alarm systems are effective.” ANSI/ISA-18.2 (2009) states that alarm systems notify operators of abnormal processes, conditions or malfunctions of plant equipment. Across industries, various techniques and technologies have been used to improve the overall alarm system. These include alarm rationalization, alarm configuration procedures and practices, and design and maintenance techniques (Errington, Reising, Burns, & Consortium, 2009; Kvalem, Haugset, & Øwre, 2000).

3.4 Use of control systems to counter threat intelligence

To deal with these threats, technological control systems need to be maximized. Of the several threats that have and could potentially arise, the utilization of the control system used must be appropriate, so that the process is more effective and efficient. In the field of energy processing, the control system can be collaborated with WEC or Wave Energy Converter. This device can convert energy from ocean waves into electrical energy (John V, 2014). However, the results are not optimal with the current device, so a system that can amplify the energy output is needed. A proper control technology system can multiply the

energy extracted from the WEC, although there is still much work to be done to optimize the basic geometry of the WEC and develop an efficient PTO system, the control community plays an important role in making wave energy extraction economical. Device size and configuration, maximizing energy extraction from waves, and optimizing energy conversion in the power take-off (PTO) system are some aspects of WEC design and operation that can be influenced by dynamic analysis and control system technology. In addition, predictive control of dwell periods, a control strategy, is claimed to increase average annual power production by preventing the control system from unnecessarily disabling devices when sea conditions become too bad. "Discrete Control-Latching and Declutching" for other control methods based on discrete control.

Secondly, the world of aviation also needs a touch of control system in some parts. With the concept of Dynamic Flight Envelop Assassment and Prediction will improve flight safety through the process of online fault identification for damaged air vehicles and measurement of changes in structural dynamics modes caused by damage (James M, 2008). The Generation I IFCS flight control concept uses an indirect adaptive approach to compensate for abnormal or damaged flight conditions. Basic pre-trained neural networks are programmed to generate appropriate control and stability derivatives to describe the aircraft dynamics under specific flight conditions. The linear quadratic regulator control system incorporates these parameters. The online solution of the Riccati algebraic equations determines the optimal tracking gain. The derivative estimation algorithm works with a basic neural network to estimate stability and control parameters. NASA developed this algorithm, which continues to work.

Furthermore, in the medical field, especially in advanced manufacturing of biological drugs. It is very clear that industrializing a product requires a systematically organized and complex production system, including the manufacture of biological drugs (Amos E, 2015). The control system can organize in such a way that the production process of a drug that emphasizes effectiveness and efficiency, so that the results obtained are quality, precision, a lot and in a short time. One example of controlling this system is like when proteins and salts enter a chromatography column, they are regulated from the end of the bioreactor to the separation unit. In a chromatography setup, sensors can only be placed at the entrance and exit of the column, not inside it. This limits the use of conventional feedback control. For example, premature breakthrough during the loading phase would be the only way to know if the loaded solution has a very high protein concentration. Once breakthrough is found, loading will be stopped. During the wash phase, additional proteins would be lost, which inhibits recovery. Not only that, ideal open-loop control can also be used as a control strategy to reduce this effect. In this situation, the measures of the load solution concentration, obtained through UV280 uptake or Raman spectroscopy, can be used as parameters for the chromatographic model presented earlier. Thereafter, optimization can be used to select operating conditions that will allow for optimal process performance.

Further applications are more broadly useful because they can be system monitoring as well as other functions in various sectors. An alarm system affiliated with the control system will increase the use value of the device. During the early stages of control system development in the chemical and petroleum industries, wall-mounted process indicators, lights, switches and recorders were used to observe, control and record process parameters. Operators saw alarms with flashing lights (visual signals) and horns (audio signals) in a hinged rectangular array called a "lightbox" (Hollifield & Habibi, 2010). Alarms serve as the primary means of communicating between the operator and the automatic control system (Bristol, 2001). The larger number of configured alarms in a system is due to limited rules, simplified procedures for configuring alarms, and engineering and organizational procedures followed during the alarm system design and maintenance process. This increases the likelihood of alarm flooding (Bergquist, Ahnlund, & Larsson, 2003; Stanton & Baber, 1995). The value of a process variable (PV) at a given time is compared to a configured set point (low or high), known as an alarm setting, in a process control system. Alarms are driven by electronic circuits (M. Mannan & West, 2005). Alarms

are displayed in the alarm display window and dynamically stored in the DCS database with pre-set priority levels (Matthew Bransby, 2001; Skjerve & Bye, 2011).

4. Conclusions

Although the term "threat" stemming from a deliberate act has traditionally been used by intelligence, the concept of "risk" is now part of its language, as with other policy areas. The many threats that exist are threats that come from various fields. The crisis of natural resources due to the use of conventional energy is already very pronounced. Therefore, a new, safer energy is needed to replace conventional energy. In the field of energy processing, the control system can be collaborated with WEC or Wave Energy Converter. In the midst of conflicts that occur everywhere, strengthening the military fleet, especially the air is important.

Therefore, it is necessary to develop the quality of the country's military by increasing the capabilities of the fleet or defense equipment owned. With the concept of Dynamic Flight Envelop Assessment and Prediction will improve flight safety through the process of online fault identification for damaged air vehicles and measurement of changes in structural dynamics modes caused by damage (James M, 2008). Medicine is one of the weapons to deal with intelligence threats from biological hazard attacks. It is very clear that the industrialization of a drug product requires a systematically organized production system. One of the security measures to avoid intelligence threats to a country is an alarm system. An alarm system affiliated with a control system will increase the use value of the device.

Author Contribution
The author contributed fully to the research.

Funding
This research did not receive funding from anywhere.

Ethical Review Board Statement
Not applicable.

Informed Consent Statement
Not applicable.

Data Availability Statement
Not applicable.

Conflicts of Interest
The authors declare no conflict of interest.

References

Albertini, E. (2018). The contribution of management control systems to environmental capabilities. *Journal of Business Ethics 159*, 1163–1180. . https://doi.org/10.1007/s10551-018-3810-9

Ang, K. H., Chong, G., & Li, Y. (2005). PID control system analysis, design, and technology. *IEEE transactions on control systems technology*, *13*(4), 559-576. https://doi.org/10.1109/TCST.2005.847331

Coletti, A. L., Sedatole, K. L., & Towry, K. L. (2005). The effect of control systems on trust and cooperation in collaborative environments. *The Accounting Review*, *80*(2), 477-500. https://doi.org/10.2308/accr.2005.80.2.477

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, *87*, 101589. https://doi.org/10.1016/j.cose.2019.101589

Gill, P. (2012). Intelligence, threat, risk and the challenge of oversight. *Intelligence and National Security*, 27(2), 206-222. https://doi.org/10.1080/02684527.2012.661643

Goel, P., Datta, A., & Mannan, M. S. (2017). Industrial alarm systems: Challenges and opportunities. *Journal of Loss Prevention in the Process Industries*, *50*, 23-36. https://doi.org/10.1016/j.jlp.2017.09.001

Kouro, S., Perez, M. A., Rodriguez, J., Llor, A. M., & Young, H. A. (2015). Model predictive control: MPC's role in the evolution of power electronics. *IEEE industrial electronics magazine*, 9(4), 8-21. https://doi.org/10.1109/MIE.2015.2478920

Leszczyna, R., & Wróbel, M. R. (2019). Threat intelligence platform for the energy sector. Software: Practice and Experience, *49*(8), 1225-1254. https://doi.org/10.1002/spe.2705

Lu, A. E., Paulson, J. A., Mozdzierz, N. J., Stockdale, A., Versypt, A. N. F., Love, K. R., ... & Braatz, R. D. (2015, September). Control systems technology in the advanced manufacturing of biologic drugs. In 2015 *IEEE conference on control applications* (CCA) (pp. 1505-1515). https://doi.org/10.1109/CCA.2015.7320824

Mosterman, P. J., Sztipanovits, J., & Engell, S. (2004). Computer-automated multiparadigm modeling in control systems technology. *IEEE transactions on control systems technology*, *12*(2), 223-234. https://doi.org/10.1109/TCST.2004.824280

Myerson, A. S., Krumme, M., Nasr, M., Thomas, H., & Braatz, R. D. (2015). Control systems engineering in continuous pharmaceutical manufacturing May 20–21, 2014 continuous manufacturing symposium. *Journal of pharmaceutical sciences*, *104*(3), 832-839. https://doi.org/10.1002/jps.24311

Petro, J. B., & Carus, W. S. (2005). Biological threat characterization research: a critical component of national biodefense. *Biosecurity and bioterrorism: biodefense strategy, practice, and science*, *3*(4), 295-308. https://doi.org/10.1089/bsp.2005.3.295

Ringwood, J. V., Bacelli, G., & Fusco, F. (2014). Energy-maximizing control of wave-energy converters: The development of control system technology to optimize their operation. *IEEE control systems magazine*, *34*(5), 30-55. https://doi.org/10.1109/MCS.2014.2333253

Schlette, D., Böhm, F., Caselli, M., & Pernul, G. (2021). Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, *20*, 21-38. https://doi.org/10.1007/s10207-020-00490-y

Urnes, J., Reichenbach, E., & Smith, T. (2008). Dynamic flight envelope assessment and prediction. In AIAA Guidance, Navigation and Control Conference and Exhibit (p. 6983). https://doi.org/10.2514/6.2008-6983

Biographies of Author(s)

Syuhada Satria, Intelligence Technology, National Intelligence College.

- Email: sylvangiovani1918@gmail.com
- ORCID:
- Web of Science ResearcherID:
- Scopus Author ID:
- Homepage:

Asep Adang Supriyadi, Sensing Technology, Faculty of Science and Technology, Republic of Indonesia Defense University.

- Email: aadangsupriyadi@gmail.com
- ORCID: https://orcid.org/0000-0003-1103-6669
- Web of Science ResearcherID:
- Scopus Author ID: 57201546735
- Homepage:

Syachrul Arief, Geospatial Information Agency, BIG.

- Email: syachrul.arief@big.go.id
- ORCID: https://orcid.org/0000-0002-1839-6301
- Web of Science ResearcherID:
- Scopus Author ID: 57522236500
- Homepage: