



# Applied Artificial Intelligence

An International Journal

ISSN: (Print) (Online) Journal homepage: [www.tandfonline.com/journals/uaai20](http://www.tandfonline.com/journals/uaai20)

## Cyber Battle Management Systems (CBMS) is Considered as Systems of Systems (SoS) and Emergent Behavior is Present, where Viable System Model (VSM) only Controls System Variety

Aleksandar Seizovic, Steven Goh, David Thorpe & Lucas Skoufa

To cite this article: Aleksandar Seizovic, Steven Goh, David Thorpe & Lucas Skoufa (2024) Cyber Battle Management Systems (CBMS) is Considered as Systems of Systems (SoS) and Emergent Behavior is Present, where Viable System Model (VSM) only Controls System Variety, Applied Artificial Intelligence, 38:1, 2384333, DOI: [10.1080/08839514.2024.2384333](https://doi.org/10.1080/08839514.2024.2384333)

To link to this article: <https://doi.org/10.1080/08839514.2024.2384333>



© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.



Published online: 31 Jul 2024.



Submit your article to this journal [↗](#)




View related articles [↗](#)



View Crossmark data [↗](#)

# Cyber Battle Management Systems (CBMS) is Considered as Systems of Systems (SoS) and Emergent Behavior is Present, where Viable System Model (VSM) only Controls System Variety

Aleksandar Seizovic <sup>a</sup>, Steven Goh<sup>b</sup>, David Thorpe<sup>c</sup>, and Lucas Skoufa<sup>d</sup>

<sup>a</sup>Engineering Department, University of Southern Queensland, Darling Heights, Australia; <sup>b</sup>School of Mechanical and Electrical Engineering, University of Southern Queensland, Darling Heights, Australia; <sup>c</sup>School of Civil Engineering and Surveying, University of Southern Queensland, Darling Heights, Australia; <sup>d</sup>Engineering Department, Rio Tinto Aluminium, Gladstone, Australia

## ABSTRACT

This manuscript critically examines existing research on cyber battle management systems (CBMS) and underscores the importance of advancing complex structure thinking, cybernetics, wicked problem-solving, and emerging behavior analysis. It advocates for a systems-thinking approach to solving complex problems by identifying and understanding associated systems, predicting their behavior, and managing changes. The manuscript explores the integration of cybernetics methodology and the viable system model with metasystems reductionism to address negative emergent behavior in complex systems. The study highlights the roles of individual systems, systems of systems, and metasystems, emphasizing the deterministic nature of single systems and the stochastic characteristics of systems of systems. By integrating cybernetics, viable system models, and meta-metasystems, the manuscript explores key parameters for building intelligent systems, revealing that meta-metasystems offer superior capabilities for coordinating and integrating multiple systems. The research results demonstrate the successful development of a meta-metasystem tailored for CBMS, providing a strategic framework for the future of cyber battle management.

## ARTICLE HISTORY

Received 7 May 2023  
Revised 1 April 2024  
Accepted 12 July 2024

## Introduction

This manuscript makes a significant contribution by focusing on the distribution of information within complex systems, specifically military battle management systems (BMSs) used globally. Recognizing the threat posed by cyber-physical systems (CPS) to BMS, the study justifies its rationale through an exploration of metasystems reductionism and cybernetics. The overarching goal is to mitigate

**CONTACT** Aleksandar Seizovic  [acaseizo@gmail.com](mailto:acaseizo@gmail.com)  Engineering Department, University of Southern Queensland, USQ, Toowoomba, Queensland 4350, Australia

© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

the occurrence of negative emergent behavior in complex systems and enhance system viability.

The novelty of the study lies in its examination of meta-metastystems and the integration of cybernetics, particularly the Viable System Model (VSM), to achieve overarching missions and functions beyond individual systems. By discussing the next-generation BMS for networked military applications, the manuscript exemplifies an integrated modular design based on computational, logistical, and networking analyses. This integration serves as a pioneering effort, providing insights into meta-metastystems' application in the cyber and BMS domains.

The manuscript focuses on the distribution of information across a complex system, such as military battle management systems (BMSs), used by over 30 countries worldwide. A cyber-physical system (CPS) is a serious threat to a BMS. A cyber BMS (CBMS) can be regarded as system behavior emergent from the relationship between a BMS and a CPS (Chong, Sandberg, and Teixeira 2019; Gupta et al. 2020; Nweke, Weldehawaryat, and Wolthusen 2021; O'Connell 2012; SBRI USA 2011; Stephenson 2017; Wiener 2013). The research rationale is justified by undertaking this study of metastystems reductionism and cybernetics to reduce the occurrence of negative emergent behavior in complex systems and control system viability (Ashby 2013; Bradley, Katina, and Keating 2016; Mittal and Rainey 2015; Nweke, Weldehawaryat, and Wolthusen 2021; Wiener 2013). The interactions between two metastystems pose a risk and are complex. Bradley, Katina, and Keating (2016) stated that systems are not expected to perform in isolation as they are connected and, therefore, subject to influences from other interconnected systems.

This review was conducted to demonstrate the need for introducing complex systems thinking, cybernetics (VSM) and emergence behavior in complex systems and multi-systems relationships (Ashby 2013; Becker and Wicked 2007; Bradley, Katina, and Keating 2016). The next-generation BMS for networked military applications is an example of an integrated modular design based on detailed computational, logistical, and networking analyses of BMSs, where embedded systems monitor and control the behaviors of networked soldiers (Hao et al. 2013). This study is novel in its examination of the meta-metastystems and integration of cybernetics VSM to achieve overarching missions and functions beyond those of the constituent systems. The VSM can be used for the analysis of an architecture for a command, control, communication and intelligence architecture (Ashby 2013; Mittal and Rainey 2015). Studies conducted by Ashby and Pierce (1957, 2013), Bar-Yam (2004b, 2004a), Beer (1989), Holland (2007), Jackson (2010), Maier (2009), Mingers and Brocklesby (1997), Pe'rez R'ios (2008), Rainey and Tolk (2015), Thomann (1973), Wiener (1948), Yolles (2021) for meta-methodology, Kopetz et al. (2016), Nweke, Weldehawaryat, and Wolthusen (2021), O'Connell (2012), Schwaninger et al. (2005, 2008a,

2008b, 2009) and Syamil, Doll, and Apigian (2004), have indicated that meta-metastystems should provide superior capabilities by providing a governing structure that coordinates and integrates multiple systems (Bradley, Katina, and Keating 2016; Wiener 2013).

In simpler terms, the concept of “meta-metastystems” refers to a higher-level structure that oversees and integrates multiple systems. These systems could be anything from technological networks to organizational structures. The idea is that by having this overarching governing structure, it becomes possible to better coordinate and manage the interactions between different systems, leading to improved capabilities and performance.

These studies collectively contribute to a deeper understanding of the challenges and strategies involved in managing and securing complex systems like military battle management systems. The following work is summarized:

Chong, Sandberg, and Teixeira (2019): This study might explore the integration of cybernetics into physical systems, particularly focusing on how cyber-physical systems interact and the implications for various applications, including military systems.

Gupta et al. (2020): This research could be centered on cybersecurity issues, potentially analyzing the latest cyber threats and vulnerabilities affecting military systems and proposing strategies for Defense against cyber-attacks.

Nweke, Weldehawaryat, and Wolthusen (2021): This study likely investigates emergent behaviors within complex systems, examining how interactions between different components lead to unexpected outcomes and exploring methods to predict and control these emergent behaviors.

O’Connell (2012): This work may relate to cyber-physical systems or military technology, possibly discussing the integration of digital technologies into physical systems and the challenges and opportunities this presents.

SBRI USA (2011): This reference might point to a report from the Small Business Research Initiative in the USA, potentially discussing innovative solutions developed by small businesses to address challenges in military technology or cyber Defense.

Stephenson (2017): This study could focus on complex systems theory or cybernetics, exploring the principles governing the behavior of interconnected systems and their applications in various domains, including military operations.

Wiener (2013): This likely refers to the work of Norbert Wiener, a pioneering figure in cybernetics. The study may discuss cybernetic principles and their applications in understanding and controlling complex systems, including military systems.

Ashby (2013): This study may relate to the work of W. Ross Ashby, particularly his research on cybernetics and systems theory. It could discuss how systems adapt and self-regulate in response to environmental changes, with potential applications in military systems design.

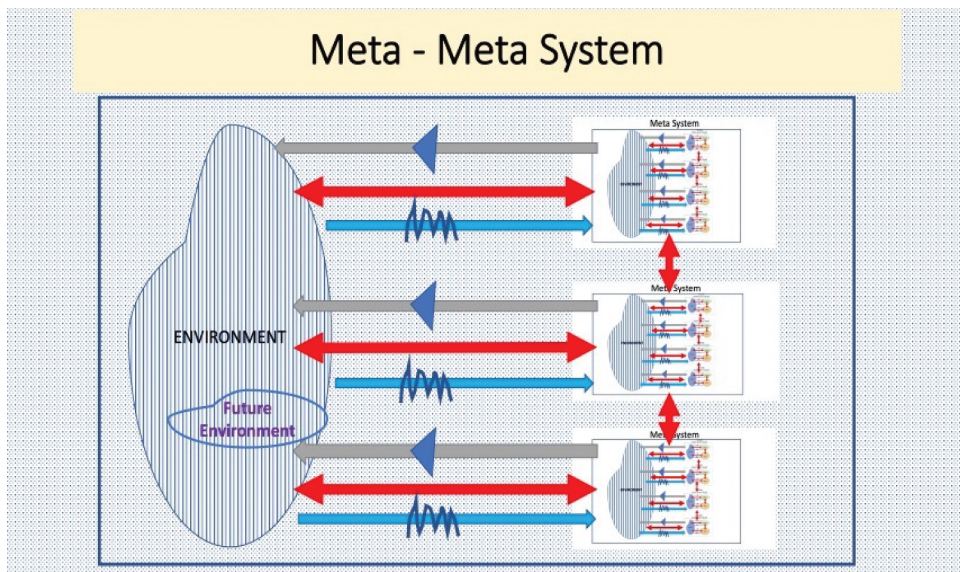


Bradley, Katina, and Keating (2016): This research might explore the dynamics of complex systems and the interactions between different components, aiming to identify patterns and principles that govern system behavior and inform strategies for system design and management.

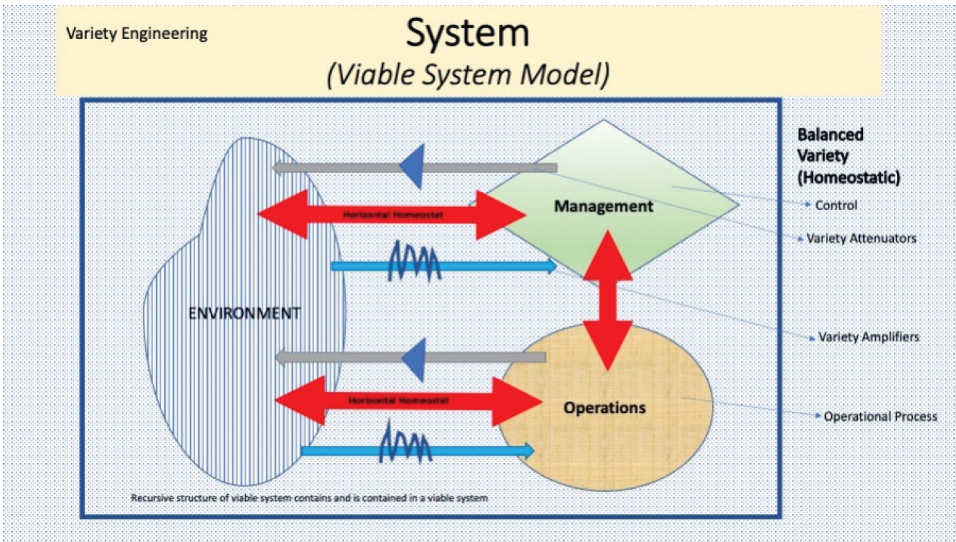
Mittal and Rainey (2015): This study could focus on emergent behaviors in complex systems, investigating how interactions between components lead to collective behaviors that are not apparent from the individual parts, with potential implications for military systems.

The studies cover various aspects related to complex systems, particularly focusing on military battle management systems and cybersecurity. For instance, Chong et al., Gupta et al., and O'Connell likely explore cyber threats and the integration of cybernetics into physical systems, such as military technologies. Stephenson, Wiener, and Ashby's works contribute to understanding complex systems and cybernetics, providing frameworks to analyze system behavior. Bradley et al. and Mittal and Rainey may offer insights into emergent behaviors within complex systems and strategies for control. Additionally, studies like Hao et al. and Bar-Yam likely delve into the design and analysis of networked military applications.

In this manuscript, the meta-meta system discussion consists of the environment, operation, and associated management unit, and we address VSM as a system (see Figure 1). The meta-metasytem introduces systems thinking, cybernetics, and emergent stochastic systems with emergence behavior into CBMS. The systems-thinking approach (Ackoff and Wilson 2010) aims to organize and structure the problem-



**Figure 1.** Meta-metasytem and cybernetics (only the variety is associated with VSM) coupling and feedback loops.



**Figure 2.** Deterministic system and VSM.

solving process from a set of explicit perspectives by selectively handling details that can obscure the underlying features of a situation. Meta-modeling is the analysis, construction, and development of frameworks, rules, constraints, models, and theories applicable and valuable to pre-defined classes of problems (Chen et al. 2015; Zalewski, McKinna, and Morris 2020). A meta-methodology is a critical component of a systematic review (Thomann 1973; Zalewski, McKinna, and Morris 2020). The novelty of this review is that it provides insights into the application of cybernetics VSM, and systems thinking in meta-metasytems, such as in cyber and BMS domains and environments. The meta-metasytem for CBMS is developed for the design, execution, and evolution of systems of systems (SoSs) (Bradley, Katina, and Keating 2016; Stocchero et al. 2022). CBMS necessitates resilient defense techniques to evaluate systems for current threats and potential design weaknesses (La and Kim 2010). A CBM SoS is termed “mission-aware” if it shares information across a computer network to improve situational awareness and organizational effectiveness (Buchler et al. 2016; Ward and Chapman 2011). Therefore, a complex problem-solving meta-methodology is required to minimize the occurrence of disasters, accidents, and malicious acts in cyberspace (Sternberg and Frensch 1991). Several researchers have applied systems-thinking theory and cybernetics principles to complex problem solving via meta-methodologies (Von Foerster, Mead, and Teuber 1950). Rittel and Webber (1973) stated that cyber-security is a subset of complex problem solving and identified such problems.

## Contributions and hypothesis

This review highlights the need for incorporating complex systems thinking, cybernetics (VSM), and emergence behavior into CBMS, paving the way for the integration of these principles in the design of next-generation BMS for military applications. The novelty of the study lies in its exploration of meta-metastystems and the integration of cybernetics VSM, providing insights into overarching missions and functions beyond individual systems. The developed meta-metastystem for CBMS focuses on the design, execution, and evolution of systems of systems (SoSs), requiring resilient defense techniques to evaluate current threats and potential weaknesses (Silva and Batista 2017; Stocchero et al. 2022). The hypothesis centers around the application of cybernetics VSM and systems thinking in meta-metastystems, particularly in the cyber and BMS domains. The study introduces the meta-meta system, encompassing the environment, operation, and associated management unit, along with VSM as a system. The systems-thinking approach, meta-modeling, and meta-methodology are emphasized as tools for organizing problem-solving processes and conducting systematic reviews.

Natural systems ranging from animal flocks to socio-ecological systems, as well as sophisticated artificial systems such as the Internet and social networks, consist of several components and involve intricate interactions. These systems exhibit nonlinear spatiotemporal interactions among numerous components and subsystems and are commonly known as complex adaptive systems (CAS) (Bowers 2014). These interactions may produce emergent properties or emergencies, which cannot be derived from the characteristics of individual components. Although some researchers have attempted to define the meaning of emergence, a widely accepted definition remains elusive. Ants and bees are autonomous agents that follow the rules of natural systems. Similarly, a network of bases and electronic warfighting platforms has military assets as agents within a network guided by defense doctrines (such as rules, policies, procedures, and precedence). The rationale is that, despite each subsystem being reliable, when multiple subsystems interact, the potential permutations and combinations of interactions can cause unpredictable negative or positive feedback loops, resulting in unpredictable and unwanted outcomes.

To further expand on the comparison between the behaviors of ants and bees and the functioning of military battle management systems (CBMS), as well as how the concept of meta-metastystems applies in this context. Ants and bees operate within highly organized colonies where individual members exhibit simple behaviors, yet collectively they achieve remarkable feats. For example, in ant colonies, individual ants carry out tasks such as foraging, nest maintenance, and caring for the young. Each ant follows local rules based on simple interactions with its immediate environment and other ants, such as following pheromone trails laid by foragers. This decentralized decision-

making allows ants to efficiently respond to changes in their environment and find optimal solutions to complex tasks like food collection and nest Defense.

Similarly, in bee colonies, individual bees perform specialized roles such as scouting for food, tending to the queen, or regulating hive temperature. Through intricate communication methods like the waggle dance, bees convey information about the location and quality of food sources to their nestmates. This collective decision-making process ensures the effective allocation of resources and the overall health and survival of the colony.

In the context of military battle management systems, these natural systems serve as powerful analogies. Military systems consist of various components, including bases, personnel, equipment, and communication networks, each performing specialized functions. Just as ants and bees work together to achieve common goals, military systems rely on the coordination and integration of these diverse components to accomplish missions effectively and adapt to changing circumstances on the battlefield.

Just like natural systems, military systems can face challenges due to the interactions between different subsystems. The interactions between bases, electronic warfighting platforms, and other military assets can lead to emergent behaviors, both positive and negative. For example, miscommunication between different units or delays in decision-making processes can result in inefficiencies or even mission failure.

To address these challenges, researchers propose the concept of meta-metasytems for CBMS. Meta-metasytems provide a governing structure that coordinates and integrates multiple subsystems within the military system, similar to how the organization within ant and bee colonies ensures collective success. By applying principles from systems thinking, cybernetics, and emergence behavior, researchers aim to develop meta-metasytems that can anticipate and mitigate the effects of complex interactions between various components within military systems. The ants and bees demonstrate how simple rules can lead to complex behaviors and efficient problem-solving in natural systems, the study of meta-metasytems aims to apply similar principles to military battle management systems, enhancing their effectiveness and resilience in complex and dynamic environments like the modern battlefield.

Cybernetics is a domain of deterministic systems where behavior is predictable and organized using communication, feedback, and control, leading to regulation and stability. The VSM is about managing variety as addressed by Ross Ashby and further elaborated upon by Beer (see [Figure 2](#)). In a deterministic system (predictable), variety is managed through the application and specification of constraints that determine the permissible output values or behaviors. When information is lacking, the variety or constraints will progress to emergence behavior that requires the generation of new information to handle both variety and constraints. When the information



set is available and complete in the deterministic domain, the resulting complex behavior is classified as simple or weak.

A stochastic system is unpredictable and emergent behavior or plain emergence is present. When the stochastic nature of the complex system (Systems of Systems) results in variety and constraints that are available in the domain space but not yet used in regulation and control, we witness assertive emergent behavior (Stocchero et al. 2022).

In the transition or cross over area between deterministic to stochastic systems the subject matter experts can provide greatest value in providing valued information's and recommendations to solving complex problems and control variety. The information available through subject matter experts (SMEs) is the only hallmark of assertive emergence behavior that provides us with an opportunity to handle the apparent variety and application of constraints. Assertive emergence behavior, although undesirable in the real world, is a significant advantage in the computational world, as it provides an opportunity to engineer control mechanisms to bring a system back into the deterministic domain from the stochastic domain. From the knowledge-based perspective of solid emergence, which becomes causal only if knowledge exists to exploit the behavior (see Figure 3).

The categorization of solid emergence in the stochastic region in this article allows the manifestation of novel behavior, although understandable by SMEs. Two concepts have been drawn from Cybernetics by William R. Ashby. First is the Law of Requisite Variety: To control a system, the controller must have equal or more states (Ashby 1956) (i.e. variety as termed by Ashby) than the system being controlled. The second is the Conant – Ashby Theorem: Every

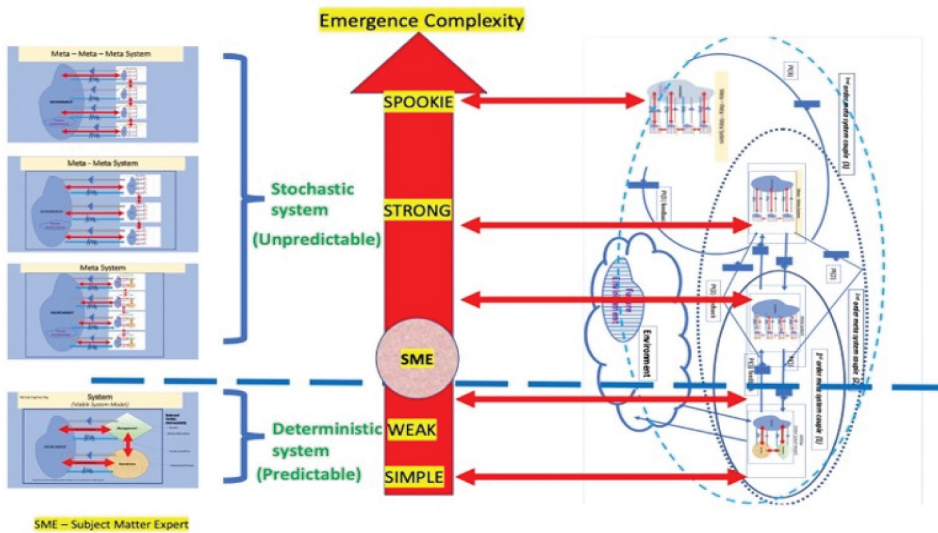


Figure 3. Categorisation of emergence in meta-metastystems design.

good regulator of a system must be a model of the system itself (Ashby 1956; Ashby 2013; Ross 1958).

The research on aggregate systems, titled “Cybernetics and Battle Management System (CBMS),” places an even greater emphasis on the interface design of SoS and reliance on interface standards (Ross 1958). The SoS and taxonomic grouping focuses on distinctive classes within the system. The BMS network soldier assists stakeholders in breaking through communication barriers and exploring/showing how current and alternative development paths may affect the future. The ability to illuminate issues and break impasses makes finding sustainable solutions to the challenges extremely effective in opening new horizons, strengthening leadership, and enabling strategic decisions (Lewin and Regine, 2003). How data from a networked soldier can be used to simulate different scenarios for testing and analysis is open to discussion (Ko and Chung 2000). Areas where the safety and security of an army soldier exist as a system or subsystem need to be identified (Lewin and Regine, 2003; Ko and Chung 2000).

The study makes a substantial contribution by delving into the distribution of information within complex systems, focusing specifically on military battle management systems (BMSs) used globally. Acknowledging the threat posed by cyber-physical systems (CPS) to BMS, the paper grounds its rationale in metasystems reductionism and cybernetics, aiming to mitigate negative emergent behavior and enhance system viability.

The research landscape concerning complex systems, cybernetics, and emergent behavior has seen significant contributions. Notably, the work by Chong, Sandberg, and Teixeira (2019), Gupta et al. (2020), Nweke, Weldehawaryat, and Wolthusen (2021), and O’Connell (2012) establishes the foundation for understanding the relationship between BMS and CPS. These studies highlight the complexities arising from interconnected systems, emphasizing the need for comprehensive frameworks to address emergent behaviors.

Bradley, Katina, and Keating (2016) emphasize the interconnected nature of systems, challenging the expectation of isolated system performance. The manuscript builds upon this idea, advocating for a shift toward meta-metasystems and cybernetics integration. The incorporation of Viable System Model (VSM), particularly in the context of CPS and BMS, introduces a novel framework. This aligns with the findings of studies by Bar-Yam (2004b, 2004a), Yolles (2021), Pe ´rez R ´ios (2008), and others, supporting the notion that meta-metasystems offer superior capabilities by coordinating and integrating multiple systems. The discussion extends to the next-generation BMS for networked military applications, emphasizing integrated modular design based on computational, logistical, and networking analyses. Studies by Hao et al. (2013) inform this approach, illustrating the significance of embedded systems in monitoring and controlling the behaviors of

networked soldiers. The manuscript's novel exploration of meta-metasytems contributes to the ongoing discourse on cybernetics, VSM, and systems thinking within the cyber and BMS domains.

The study aligns with the principles of systems-thinking theory (Ackoff and Wilson 2010), emphasizing the organization of problem-solving processes from various perspectives. Meta-modeling and meta-methodology, as discussed by Thomann (1973) and others, serve as critical tools for conducting systematic reviews and addressing emergent behavior in complex systems. The research highlights the application of cybernetics VSM and systems thinking in meta-metasytems, bringing valuable insights into cyber and BMS environments.

### Comp cyber-physical systems (CPSs), cybernetics, cyber-security and complex problems

The complex problem framework can help clarify the nature of complex problems surrounding us (Becker and Wicked 2007; Miller and Lessard 2008; O'Connell 2012; Sheffield, Sankaran, and Haslett 2012; Snowden and Boone 2007). Cyber-security is a prime example of a complex problem requiring continuous and rigorous analysis and experimentation. Over many years, oversimplification of such problems has been a significant reason for their persistence in defying the best efforts of governments and societies. This is reflected in cyberspace by the subjective application of national or international laws and the varying motivations of governments and societies in



**Figure 4.** Cyber-security incorporating critical systems thinking, cybernetics methodology, and complex problem-solving.



addressing cyber-security problems (Miller and Lessard 2008; Murray, Webb, and Wheatley 2019; O’Connell 2012; Ruhl 2009; Sheffield, Sankaran, and Haslett 2012; Snowden and Boone 2007; Song, Fink, and Chapter 2017) (see Figure 4).

Determining the contributions of cyber-physical systems (CPSs) and their designs requires the detailed modeling of dynamic environments and a clear understanding of the interactions among embedded cyber-systems (CSS) (Chong, Sandberg, and Teixeira 2019; Gupta et al. 2020; Nweke, Weldehawaryat, and Wolthusen 2021; SBRI USA 2011). Complex systems or Systems of Systems (SoS) are characterized by unusual emergent behaviors, which appear to be fundamentally tractable through structured analyses (Miller and Lessard 2008; Stocchero et al. 2022). However, this is rarely possible in chaotic systems because cause-and-effect relationships tend to shift constantly, and no manageable patterns occur (Sheffield, Sankaran, and Haslett 2012; Snowden and Boone 2007) (see Figure 5).

In the world of social dynamics, chaos often manifests when a group of friends attempts to decide on a dinner destination. Each individual brings their own preferences, dietary needs, and restaurant suggestions to the table, sparking a lively yet chaotic discussion. One friend might passionately advocate for Italian cuisine, citing their love for pasta and pizza, while another insists on Asian fare, craving the tangy flavors of sushi or spicy noodles. Meanwhile, a third friend, committed to a vegan lifestyle, suggests a plant-based restaurant, emphasizing the importance of ethical dining choices. As the conversation progresses, more ideas are thrown into the mix, each with its own set of proponents and detractors, leading to a cacophony of opinions and conflicting desires.

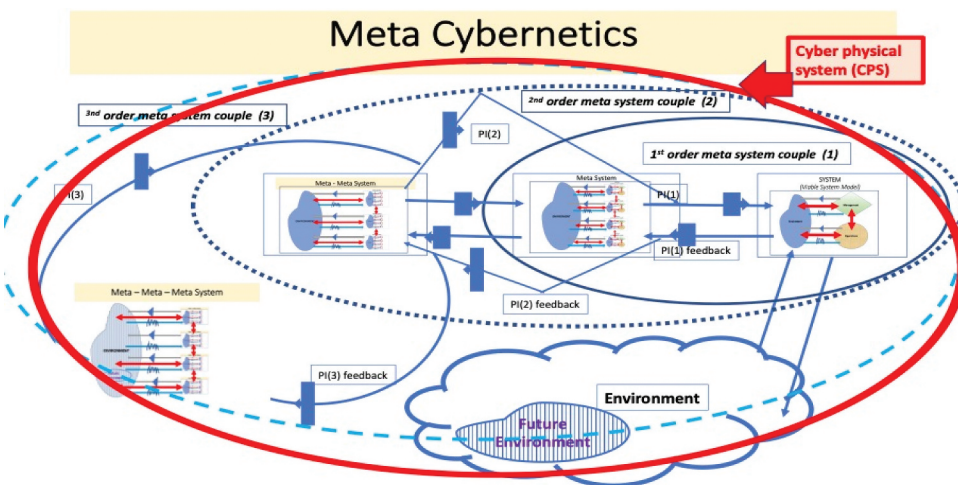


Figure 5. Cyber-physical system (CPS), meta cybernetics, and meta-methodology.

In a similar scenario, chaos lurks in distributed systems, such as cyber-physical systems (CPSs), where interconnected components interact dynamically to perform various functions. Consider a smart city's infrastructure – traffic lights, surveillance systems, transportation networks, and environmental sensors – all seamlessly integrated to enhance urban living. However, this intricate web of interconnectedness also introduces vulnerabilities, as unforeseen events can disrupt the system's equilibrium. For instance, a sudden traffic accident or road closure can trigger a cascade of effects, causing traffic congestion, rerouting public transportation, and impacting overall city operations. Just as in the dinner discussion, where divergent preferences clash and compromise becomes elusive, the interactions among CPS components can lead to unpredictable outcomes, challenging traditional control mechanisms and predictive models.

In both scenarios, chaos emerges from the intricate interactions among diverse elements, challenging traditional methods of analysis and problem-solving. Structured approaches may offer some insights into emergent behaviors, but the dynamic nature of chaos necessitates a more adaptive and holistic perspective. Critical systems thinking, cybernetics methodology, and complex problem-solving become essential tools for navigating the complexities of social dynamics and distributed technological environments like CPSs. By embracing these approaches, stakeholders can better understand the underlying dynamics, anticipate potential disruptions, and devise resilient strategies to mitigate the impact of chaos on both human interactions and technological systems.

The meta-methodology of systems design (Thomann 1973) employs popular cybernetic methods such as Bowers' multi-paradigm system theory (Bowers 2014), Jackson's critical systems practice (Jackson 2010), and Mingers and Brocklesby's multi-methodology theory (Mingers and Brocklesby 1997). These provide a clear understanding of the SoS theory required to evaluate the emergent behavior phenomena in CPS metasystems (Rittel and Webber 1973). Understanding the various approaches for managing emergent behaviors in complex CPS metasystems necessitates investigating the nature of emergence processes, principles, operations, and outcomes from the perspective of modern warfare and SoS engineering (Chong, Sandberg, and Teixeira 2019; Gupta et al. 2020; La and Kim 2010; Nweke, Weldehawaryat, and Wolthusen 2021; SBRI USA 2011). Defense domains are highly flexible environments, vulnerable to computer and network attacks. The use of quantum computing to attack and destroy existing cryptosystems has motivated the development of a new discipline named "cyber-physical system protection" to handle post-quantum cryptography. Rainey and Loerch (2007) described the architectural modeling of complex systems within the CPS SoS construct, where emergent behaviors can be critically observed

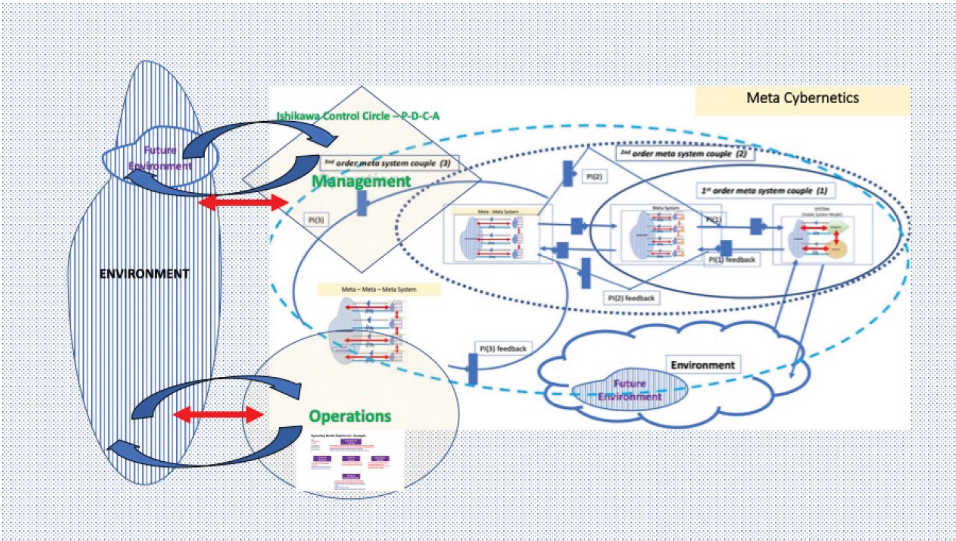


Figure 6. Cybernetics with Coupled SoSs and VSM feedback loop

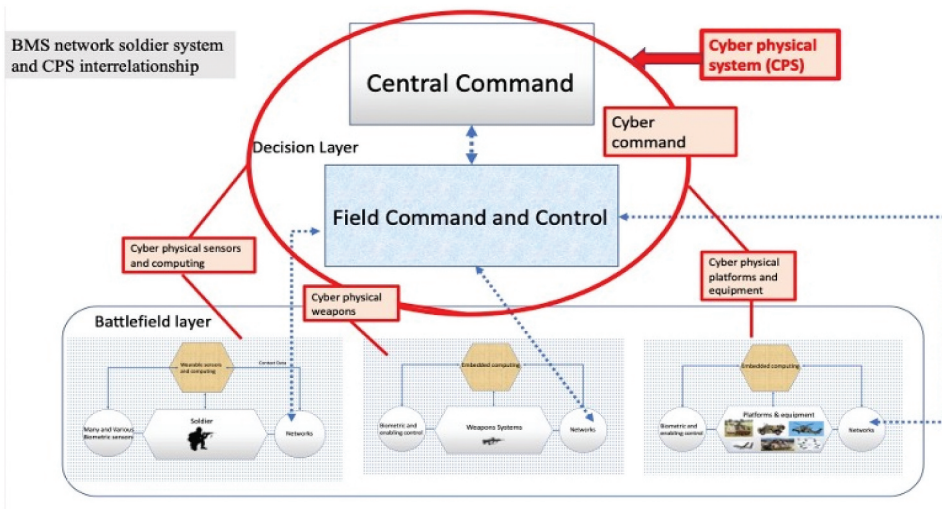
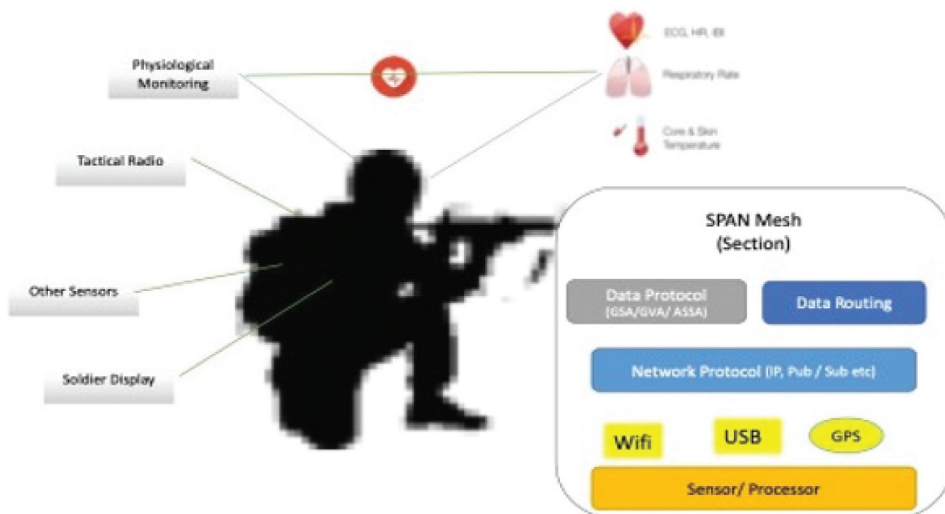


Figure 7. BMS network soldier system and CPS interrelationship.

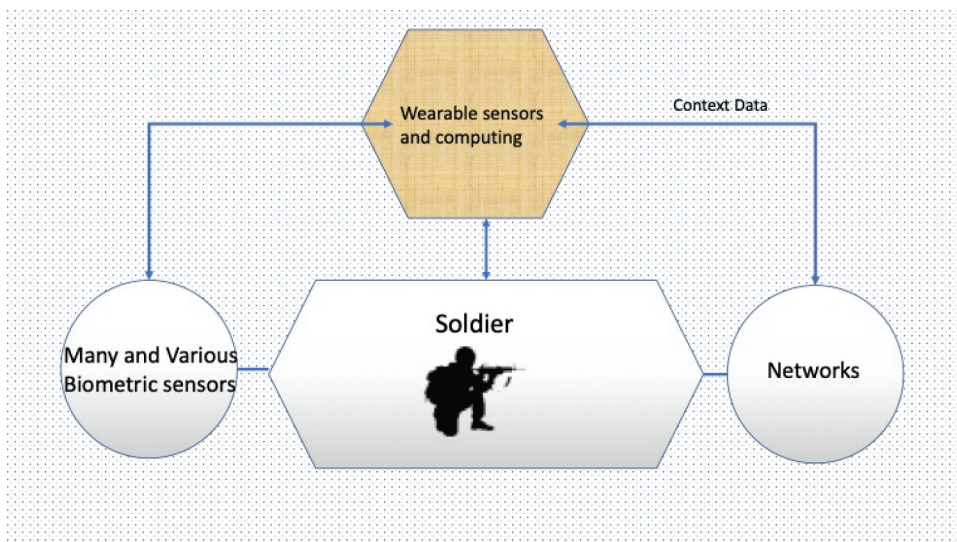
owing to the interactions among battlefield participants engaged in warfare gamification.

Rittel and Webber's (1973) research on complex problem solving in the cyber-security domain has been instrumental in helping researchers and practitioners understand cyber-security breaches and their occurrences in various industries. It provides a clear understanding of the SoS theory required to evaluate the emergent behavior phenomenon in CPS metasystems (Rittel and Webber 1973) (see Figure 6).





**Figure 8.** Illustration of network soldier basic technology.



**Figure 9.** Network soldier wearable sensors.

Defense CPS security in physical and computing environments consists of optimal structures that allow sensors to observe and actuators to influence their environments. An SoS constitutes a collection of independent autonomous and technical constituent systems, such as CSS, providing valuable services (Kopetz et al. 2016). However, each proposed solution to a cybersecurity problem has several layers and features that add complexity owing to terminological inconsistencies, immature or non-existent legal structures, and disparate business and social interests. The search for solutions inevitably

results in the identification of numerous stakeholders eager to define the problem differently and propose contradictory solutions (Stacey 2007).

A potential limitation arises from the reliance on subject matter experts (SMEs) to manage assertive emergence behavior. While acknowledging their importance, this dependency introduces the risk of bias and subjective interpretations, potentially compromising the objectivity of emergent behavior management. The manuscript identifies the challenge of managing complexity during the transition from deterministic to stochastic systems. The practical implementation of control mechanisms within this transitional zone may face technical obstacles or demand substantial computational resources, posing a potential limitation to the feasibility of the proposed approach. Despite the manuscript's focus on understanding emergent behavior in cyber-physical systems (CPSs) and Systems of Systems (SoS), a limitation is evident in the lack of in-depth exploration into predictive modeling or forecasting of emergent phenomena (Stocchero et al. 2022). Incorporating predictive analytics could significantly enhance the proactive management of emergent behaviors, addressing a notable gap in the research.

The manuscript stands out for its comprehensive integration of cybernetics principles with emergent behavior analysis, particularly within the intricate realms of CPSs and SoS. This interdisciplinary approach not only enriches the theoretical foundations but also contributes to a deeper understanding of the dynamic complexities inherent in complex systems. The distinctive feature of the manuscript is the exploration of meta-metastystems, encapsulating systems thinking, cybernetics, and emergent stochastic systems. This innovative framework goes beyond traditional systems engineering paradigms, providing a holistic perspective on system design and management. The incorporation of meta-metastystems introduces a new dimension to the understanding of complex system dynamics.

### **Cyber-physical systems (CPSs), SoS and emergent behaviour**

CPSs are at the core of digital innovations, transforming the world and redefining the interactions with intelligent machines in many industrial sectors and social contexts (see Figure 7). As mentioned, properly engineered CPSs rely on the seamless integration of digital and physical components and the possibility of human interaction (Becker and Wicked 2007; Miller and Lessard 2008; O'Connell 2012; Sheffield, Sankaran, and Haslett 2012; Snowden and Boone 2007). Therefore, CPS technologies are transforming how people interact with engineered systems in the physical world in the same way that the Internet has transformed how people interact with information (Ko and Cho 2000; Ruhl 2009). However, owing to the complexity of CPSs, developers are challenged by the lack of simulation tools

and models for design and analysis (“European Defence Agency EDA advances work towards open architecture for soldier systems” 2017; Ackoff and Wilson 2010; Modul 2017; Murray, Webb, and Wheatley 2019; Ruhl 2009; Song, Fink, and Chapter 2017; Zalewski, McKinna, and Morris 2020). The extant literature provides several emergence detection techniques, ranging from statistical analyses to formal approaches (Chen, Nagl, and Clack 2007; Holland 2007; Maier 2009; Nweke, Weldehawaryat, and Wolthusen 2021; O’Toole, Nallur, and Clarke 2014; Stephenson 2017; Wiener 2013; Wincek 2011).

Although crisis literature (Loosemore, Raftery, and Reilly 2005) has demonstrated that emergencies occur for specific reasons, these reasons are frequently dismissed, hidden, or unrecognized. Such events have a low probability of occurrence, and their potentially significant consequences are seldom considered in contingency plans. Such conditions may be best addressed via an emerging strategy (Arndt 2011; Mintzberg, Ahlstrand, and Lampel 2020; Mittal and Rainey 2015). Miller and Lessard (2008) argued that successful projects were shaped rather than selected. US federal intelligence and defense agencies have examined several generic project failure examples and discovered that several early warning signs frequently occur (Maier 2014; Mittal and Rainey 2015). Therefore, emergence can be regarded as a system characteristic that cannot be predetermined. The taxonomy of different emergent behaviors is based on the interrelationship between the macro- and micro-levels (O’Toole, Nallur, and Clarke 2014). First, taxonomy must establish a theoretical framework for modeling and simulation (M&S).

The literature suggests that meta-metastystems provide superior capabilities by providing a governing structure that coordinates and integrates multiple systems. This thesis by publications reviews existing battle management systems (BMS) as systems of systems (SoS) research and highlights the need to develop complex structure thinking, cybernetics, deprived problem-solving and emerging behavior analysis considering the relationship between complex and multi-structural systems (Stocchero et al. 2022). The system-thinking approach aims to organize and structure the problem-solving process by selectively handling details that can obscure the underlying features of a situation from a set of explicit perspectives. The significance of the literature review lies in its contribution to the understanding of the foundational principles, hidden relationships, emergent behavior, and effective management strategies within metastystems and SoS (Stocchero et al. 2022). This understanding can spur future research, guide decision-making in system design and operation, and enhance the overall performance and safety of complex programs. The review also explores the foundations of operational capability and project control, which are critical for safe and efficient project management. By comprehending the underlying principles and factors that contribute to operational capability and project control, researchers and practitioners can develop strategies to enhance the performance and safety of complex systems (Silva and Batista 2017).

## Networked soldier applications for the next-generation BMS software

The networked soldier is an excellent illustration of an integrated modular design based on thorough computational, logistical, and networking assessments of BMSs, with embedded systems monitoring and managing the behaviors of networked soldiers (Hao et al. 2013) (see Figure 8). In addition, stakeholders will benefit from more potent next-generation BMS networked troops to overcome communication obstacles and comprehend how potential future development routes may impact operations (Ko and Cho 2000).

Developing more powerful next-generation BMS networked soldiers will assist stakeholders in overcoming communication barriers and understanding how current and alternative development paths may affect future operations (“European Defence Agency EDA advances work towards open architecture for soldier systems 2017; Ko and Cho 2000; Modul 2017; Murray, Webb, and Wheatley 2019; Sinclair 2022). In the case of the networked soldier, wearable medical sensors (to measure vital signs such as temperature and heart rate) may be utilized to identify those showing symptoms of medical distress (Syamil, Doll, and Apigian 2004; Walker and Nogeste 2008). Historically, submitting such data to a central repository required voluntary, self-managed, and laborious transfer. These and other issues arise when a CPS connects to a BMS through a tactical network.

In the networked soldier example, wearable medical sensors may detect signs of medical hazards. Historically, such data had to be voluntarily and manually transferred to a central authority (see Figure 9). When a CPS is connected to a BMS via a tactical network, these and other conditions can be measured and assessed, even before the soldier is aware of a problem (Syamil, Doll, and Apigian 2004; Walker and Nogeste 2008). Theoretically, if several soldiers signal similar alerts simultaneously, the BMS could predict an attack (Ko and Cho 2000; Syamil, Doll, and Apigian 2004).

For a dismounted soldier unit to be safe, effective, and efficient, it must be possible to monitor the physical status of the soldiers remotely (Ko and Cho 2000, 24). A physiological monitoring system gathers, transmits, and saves data from soldiers to a central system (“European Defence Agency EDA advances work towards open architecture for soldier systems,” 2017; Ko and Cho 2000; Modul 2017; Sinclair 2022). It consists of wearables and minimally intrusive sensors that gather information and track a range of biophysical characteristics (such as electrocardiographic data, heart rate, and core and skin temperatures). Then, using algorithms, the data are effectively gathered, correlated, and dispersed (“European Defence Agency EDA advances work towards open architecture for soldier systems,” 2017; Ko and Cho 2000; Modul 2017; Sinclair 2022).

In the world of networked soldiers, the advent of wearable medical sensors represents a significant advancement in ensuring troop health and operational



readiness. These sensors possess the capability to detect early signs of medical hazards, such as fluctuations in vital signs or environmental conditions. Previously, the transmission of such critical data to central authorities required manual and voluntary efforts. However, with the integration of Cyber-Physical Systems (CPS) linked to Battle Management Systems (BMS) via tactical networks, these sensors now facilitate continuous monitoring and assessment of soldier health in real-time. This real-time monitoring provides invaluable insights into potential risks, even before soldiers themselves are aware of them. For instance, in the event that multiple soldiers within a unit simultaneously trigger similar alerts indicating physiological abnormalities, the BMS could swiftly identify patterns suggestive of an imminent attack. Such preemptive detection enables commanders to take proactive measures, potentially averting or mitigating threats before they escalate. This capability underscores the significance of leveraging technology to enhance operational safety and effectiveness.

In addition, to ensure the optimal functioning of dismounted soldier units, remote monitoring of soldiers' physical status is indispensable. A comprehensive physiological monitoring system is meticulously crafted to gather, transmit, and store data from individual soldiers to a centralized system. This system comprises an array of wearable devices and minimally intrusive sensors meticulously designed to capture a diverse range of biophysical characteristics, including electrocardiographic data, heart rate, and core and skin temperatures. The sophisticated algorithms are deployed to efficiently process and correlate this vast trove of data, furnishing commanders with actionable insights into the health and readiness of their troops in real-time. Such timely and informed interventions not only bolster situational awareness but also serve to safeguard the well-being and operational effectiveness of dismounted soldier units across diverse operational landscapes. The seamless integration of wearable medical sensors and advanced monitoring systems exemplifies the transformative potential of technology in modern warfare. By harnessing these capabilities, military forces can navigate evolving threats with heightened vigilance and precision, ensuring the safety and success of missions in dynamic and challenging environments.

### ***Future soldier system and SPAN mesh technology***

In instances of soldiers not having access to Smartphone *Ad hoc* Networking (SPAN) mesh technology, the section-level command can combine several existing wireless technologies with new and evolving methods to create low-power mesh networks using Bluetooth, Wi-Fi, and ultra-wideband architectures. Developing a data standard for mesh networks will enable sensors, devices, and computers to connect as nodes and collect and share data cohesively and securely. The desired routing

capability would enable dataflows throughout entire sections, allowing dispersed units to share critical real-time information through links provided by individual soldiers. Many sensors would be self-contained and, therefore, not require large power supplies owing to their small size, weight, and power requirements of the network components. SPAN could be integrated with broader army networks by connecting them to high-frequency networks, broadband trunks, and future waveforms. Links with the army backbone network would be established by combining existing radios with the SPAN mesh and local higher-capacity networks. A section commander, signaler, or vehicle may carry SPAN transceivers and tactical radios to facilitate such a data exchange (“European Defence Agency EDA advances work towards open architecture for soldier systems,” 2017; Ko and Cho 2000; Modul 2017; Sinclair 2022).

Furthermore, multiple sensors can be combined to provide higher-order information. Connecting sensor data to BMS processors through these mesh networks would allow more sophisticated algorithms and techniques to be applied. For example, advanced technology such as shot detectors, electronic warfare devices, and range finders may be combined for tracking red forces to share a common operational picture. Imaging and video from local support units may also be integrated with BMSs and remote vehicles to improve situational awareness (“European Defence Agency EDA advances work towards open architecture for soldier systems,” 2017; Ko and Cho 2000; Modul 2017; Sinclair 2022).

### ***SPAN mesh technology unavailability***

If SPAN mesh technology is unavailable to individual soldiers, the section-level command can combine several current wireless technologies with novel and developing techniques to build low-power mesh networks using Bluetooth, Wi-Fi, and ultra-wideband topologies. Creating a mesh network data standard would enable computers, devices, and sensors to join together as nodes and safely and cooperatively collect and share data (Syamil, Doll, and Apigian 2004; Walker and Nogeste 2008). When data can flow throughout an entire section, as is the case with the required routing capabilities, dispersed units could communicate vital real-time information via linkages provided by individual troops. Owing to the modest size, weight, and power of such network components, many sensors would be self-contained and not need significant auxiliary power. SPAN would connect to a larger army by connecting through these sub-networks (“European Defence Agency EDA advances work towards open architecture for soldier systems,” 2017; Ko and Cho 2000; Modul 2017; Sinclair 2022).

The manuscript's practical insights into applying emergent behavior analysis within military domains, particularly in the design of next-generation battle management systems, offer a tangible and real-world dimension to the research. This application-oriented approach enhances the relevance and significance of the proposed methodology, showcasing its potential impact in critical operational settings.

## Cyber risk

There will always be a risk of false-positive alerts caused by cyber or electronic warfare attacks. Therefore, any mesh network solution must be battle-tested to eliminate as many "what-if" scenarios as possible. The future effects of CPSs will considerably impact personal and professional lives, and autonomous machines with complex data environments will involve numerous unforeseen legal aspects regarding responsibility, liability, ownership, and privacy (Ward and Chapman 2011). Human interactions with information systems are vulnerable and can be easily exploited to launch cyber-attacks. A better understanding of cyber-security elements will enable information managers to overcome any misguided sense of invincibility and close such security loopholes. Cybercrime and cyber-security threats can destroy businesses and their physical assets (Wincek 2011), which could also apply in the military domain.

Example: The Cyber Battle Management Systems (CBMS) communication system interface and the configuration of the combat network in land forces include wireless networking, sensors, human biosensors, targeting, shot detection, UAVs, small arm digital sights, range finders, and data to consider important issues where an alert/deficiency/loss/failure is experienced due to cyber or electronic warfare attack that has spoofed the BMS system. In this instance, headquarters (HQ) looks at an uncommon BMS program location for something that does not exist; however, another covert operation is being carried out elsewhere. Is this possible and what is the risk?

- The ability to remotely monitor the physical condition of each soldier in a dismounted unit is an essential component for the safety, efficiency, and effectiveness of the unit.
- A cyber or electronic warfare attack to BMS and network soldier communication network causes data exchange failure. As SPAM is mobile, the section commander, signaler, or vehicle can carry the SPAN transceiver and tactical radio to allow data exchange.

## Monterey Phoenix (MP) analysis of emergent behaviours

The agent-based Monterey Phoenix (MP) M&S system demonstrates how emergent behaviors occur in SoSs. Rainey and Tolk (2015) applied agent-based modeling (ABM) and other tools to determine emergent behaviors in specific SoS engineering applications. The agent-based M&S can be used to detect emergent behavior in a SoS but cannot examine it or control it. Although MP can be used to delete negative emergence, it is the role of engineering to examine how to capitalize upon it, that is, facilitate modeling and simulation of SoS across many application domains and enable exposure and control of certain types of associated emergent behaviors.

The first task in designing a multi-agent system is to specify how each agent behaves in its environment and its role in behavior ontology (Burbeck 2015). Next, this description is transformed and expressed in the simulation engine's language and used as input for execution. The SoS is critical for meeting capability objectives and understanding inter-relationships in the body of system engineering knowledge. However, defining an SoS' boundary is difficult, as its CSS typically has different owners supporting defense organizational structures; this is beyond the scope of SoS management.

The CPS requires detailed environmental dynamics modeling and a thorough understanding of the interactions among its embedded systems. For example, in any environment, the SoS software enables participants to successfully combine and analyze network data using sophisticated algorithms in the operational environment. Understanding emergent behaviors in SoSs with MP facilitates the M&S of SoSs across several application domains and enables the exposure and control of associated emergent behaviors (Rainey and Tolk 2015). In an SoS model, emergence can be detected using MP. This allows adverse emergence to be deleted and only positive emergence to be retained in the SoS. Therefore, it precludes potential negative influences and leads to potential force multipliers. This feature is critical, as negative emergent behaviors can significantly affect SoS missions. Dr. Kristin Giammarco of the US Naval Postgraduate School developed an MP modeling tool for planners and designers to detect emergence in an SoS model (Giammarco 2017). Furthermore, ABM is gaining popularity among academics and practitioners as a robust methodology for complex adaptive system modeling. It demonstrates how simple behavioral rules and local agent interactions can produce complex patterns (Giammarco 2017).

## Cyber physical system (CPS) and emergent behaviour

The key points regarding emergent behaviors found in CPSs are summarized as follows:

- Standardized abstractions and architectures that enable modular CPS design and development are urgently needed.
- CPS applications involve components that interact with one another through a complex coupled physical environment. Reliability and security pose unique challenges in this context, necessitating the development of new frameworks, algorithms, and tools.
- Future CPSs will require highly reliable and reconfigurable hardware and software components. In many applications, certifiability and trustworthiness must be extended to the system level.

Emergent behaviors can be defined as system characteristics that are invisible at the system (macro-) level but emerge unexpectedly owing to interactions between entities at the component (micro-) level. Emergent behaviors produce unexpected and sometimes undesirable outcomes in intelligence, cybersecurity, weapons on target, and wireless networks (O'Connell (2012); Stephenson (2017)). Interactions resulting in emergent behavior manifest at system interfaces, between systems and operators, and between systems and BMS software-development elements. The emergent behavior in a CBMS cannot be predetermined with existing knowledge, as the location of the emergent behavior in the system cannot be easily identified, analyzed, or validated.

### Contributions to the field

High-risk industries are required to minimize the occurrence of disasters and accidents in the operation and delivery of engineering projects (7;47). This can be realized through systems modeling, which includes analyzing, constructing, and developing frames, rules, constraints, models, and theories applicable to predefined problem classes. These methods are critical for effective risk management (Syamil, Doll, and Apigian 2004; Ward and Chapman 2011; Zalewski, McKinna, and Morris 2020). The involvement of CPS in the emergent behavior of an SoS necessitates detailed modeling of the dynamics of the environment and a clear understanding of the interactions between the dynamics of the embedded system and its environment. Maier (2009) defined an SoS architecture in terms of communications among components.

## Conclusion

Emergent behavior produces unexpected and, occasionally, unwanted outcomes in intelligence, cyber-security, weapons, wireless networks, integrated power hubs, sensors, end-user devices, tactical routers, and network-enabled technologies (O’Connell (2012); Stephenson (2017)). Enabling technologies such as networks graphs are instantiations of Functional Performance Specification (FPS), elements (e.g. nodes and vertices), and their pairwise links (e.g. edges and connections) (Walker and Nogeste 2008)). Defense forces and other government institutions must understand the practical applications of the systems engineering process, as it maps to the development of FPSs. The objective is to understand and apply systems engineering processes and management behaviors to developing real-world FPSs. Capability roadmaps must describe the capability requirements within a defined capability area, the strategic context, specific capability goals, actions required to achieve the desired end-state, and the residual strategic or operational risks that must be mitigated or accepted (Walker and Nogeste 2008).

Emergence can manifest positively or negatively in various systems, from the simple to the highly complex. A mechanism that provides a structured approach for analyzing and controlling such behaviors is required, given that emergent behaviors and emergence are unexpected and mostly undesired. A CPS enables computer systems to monitor and interact with the physical world by merging computing and communications with physical processes. However, current computing and networking abstractions do not adequately reflect the attributes of the physical world. Networked embedded computers monitor and control physical processes, and CPSs share a *close hardware and* software relationship. They may operate on different spatial and temporal scales while exhibiting a variety of distinct behavioral modalities. Therefore, the behavior of a CPS may change in an operational or environmental context. This review significantly contributes to the extant literature, as it examines emergent behaviors in BMSs and CPSs. It also offers insights into a previously opaque domain. These valuable insights may help shape future research and policymaking in the defense industry.

A meta-methodology is a critical component of a systematic review (Thomann 1973). It is the novel research conducted in this work to improve understanding and knowledge in the application of cybernetics, VSM, and systems thinking in a meta-metasystems design like CBMS and the environments. The VSM may not be considered as a system of systems, and according to Dr. Mark Maier (Maier 1998, 2014), the true emergent behavior only occurs in his definition of a system of systems (Maier 1998). The Beer’s VSM is about managing variety not emergent behavior, as this only occurs in a system of systems as addressed by Mark Maier. Dr. Maier’s

system of system is not a viable system model. The VSM is solely constructed upon managing variety as addressed by Ross Ashby and further elaborated upon by Beer. Beer's VSM is about managing variety not emergent behavior, as this only occurs in a system of systems as addressed by Mark Maier in his manuscript *Architecting Principles for Systems-of-Systems* (Maier 1998).

The meta-metasytem for CBMS is developed for the design, execution, and evolution of SoSs. The studies conducted by researchers such as Ashby (1956), Bar-Yam (2004b, 2004a), Beer (1989), Holland (2007), Jackson (2010), Maier (2009), Mingers and Brocklesby (1997), Mittal and Rainey (2015), Pe'erez R'ios (2008), Thomann (1973), Wiener (1948), Yolles (2021) for meta-methodology, Kopetz et al. (2016), Nweke, Weldehawaryat, and Wolthusen (2021), O'Connell (2012), Schwaninger et al. (2005, 2008b, 2009), and Syamil, Doll, and Apigian (2004) suggest that meta-metasytems provide greater capability by providing a governing structure that coordinates and integrates multiple systems. This review helps elucidate the challenges and opportunities in meta-metasytems schema design for SoSs.

## Acknowledgements

Dr Larry Rainey, PhD, Systems Engineering, CEO at Integrity Systems and Solutions of Colorado United States.

Dr Maurice Yolles, PhD, Professor Emeritus at Liverpool John Moores University, United Kingdom.

Dt Ben Zweibelson, PhD Director, USSPACECOM Strategic Innovation Group (SIG), Lancaster University, Colorado Springs, Colorado, United States.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## Funding

This work was supported by the University of Southern Queensland. The author acknowledges all published materials relating to the research.

## ORCID

Aleksandar Seizovic  <http://orcid.org/0000-0003-0445-8716>



## Data availability statement

All data underlying the results are available as part of the article and no additional source data are required.

## References

- Ackoff, R., and J. M. Wilson. 2010. *The Journal of the Operational Research Society* 61 (5):713–713. doi:[10.1057/jors.2010.9](https://doi.org/10.1057/jors.2010.9).
- Arndt, F. 2011. Assessing dynamic capabilities: Mintzberg's schools of thought. *South African Journal of Business Management* 42 (1):1–8. doi:[10.4102/sajbm.v42i1.484](https://doi.org/10.4102/sajbm.v42i1.484).
- Ashby, W. R. 1956. *An introduction to cybernetics*. London: Chapman & Hall.
- Ashby, W. R. 2013. *Introduction to cybernetics*. Chapman & Hall.
- Ashby, W. R., and J. R. Pierce. 1957. An introduction to cybernetics. *Physics Today* 10 (7):34–36. doi:[10.1063/1.3060436](https://doi.org/10.1063/1.3060436).
- Bar-Yam, Y. 2004a. *Making things work: Solving complex problems in a complex world*. NECSI-Knowledge Press.
- Bar-Yam, Y. 2004b. Multiscale variety in complex systems. *Complexity* 9 (4):37–45. doi:[10.1002/cplx.20014](https://doi.org/10.1002/cplx.20014).
- Becker, K., and I. D. Wicked. 2007. Conceptual framework for considering instructional design as a wicked problem. *Canadian Journal of Learning and Technology* 33 (1). doi:[10.21432/T2CG6H](https://doi.org/10.21432/T2CG6H).
- Beer, S. 1989. The viable system model: Its provenance, development, methodology and pathology. In *The viable system model, interpretations and applications of Stafford Beer's VSM*, ed. R. Espejo and R. Harnden. Wiley.
- Bowers, T. D. 2014. Developments in critical systems theory: On paradigms and incommensurability. *Proceedings of the 58th Annual Meeting of the ISSS*, December 16.
- Bradley, J. M., P. F. Katina, and C. B. Keating. 2016. The role of “metasystem” in engineering a system of systems. *Proceedings of the 2016 Industrial and Systems Engineering Research Conference*.
- Buchler, N., S. M. Fitzhugh, L. R. Marusich, D. M. Ungvarsky, C. Lebiere, and C. Gonzalez. 2016. Mission command in the age of network-enabled operations: Social network analysis of information sharing and situation awareness. *Frontiers in Psychology* 7:937. doi:[10.3389/fpsyg.2016.00937](https://doi.org/10.3389/fpsyg.2016.00937).
- Burbeck, S. 2015. Complexity and the evolution of computing: Biological principles for managing evolving systems. *Computer System*.
- Chen, C.-C., S. B. Nagl, and C. Clack. 2007. Specifying, detecting and analysing emergent behaviours in multi-level agent-based simulations. *Proceedings of the 2007 Summer Computer Simulation Conference*, ed. G. A. Wainer, 969–76. Society for Computer Simulation International. ISBN 1565553160. doi:[10.1145/1357910.1358062](https://doi.org/10.1145/1357910.1358062).
- Chen, X., J. Cao, J. Qiu, Y. Jing, L. Yang, and B. Zheng. 2015. Optimal control of a class of warfare dynamic systems based on Lanchester (2,2) attrition model. Paper presented at: 27th Chinese Control and Decision Conference, Qingdao, China. doi:[10.1109/CCDC.2015.7162111](https://doi.org/10.1109/CCDC.2015.7162111).
- Chong, M. S., H. Sandberg, and A. M. H. Teixeira. 2019. A tutorial introduction to security and privacy for cyber-physical systems. *Proceedings of the 18th European Control Conference (ECC)*, 968–78. doi:[10.23919/ECC.2019.8795652](https://doi.org/10.23919/ECC.2019.8795652).
- European Defence Agency. 2017. *EDA Advances Work Towards Open Architecture for Soldier Systems* European Defence Agency.

- Giammarco, K. 2017. Practical modeling concepts for engineering emergence in systems of systems. 12th System of Systems Engineering Conference (SoSE), 1–6. doi:10.1109/SYSE.2017.7994977.
- Gupta, R., S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim. 2020. Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges. *Institute of Electrical and Electronics Engineers Access* 8:24746–72. doi:10.1109/ACCESS.2020.2970576.
- Hao, W., Z. Xianmin, K. Yongcong, O. Gaoferi, and X. Hongwei. 2013. Solder joint inspection based on neural network combined with genetic algorithm. *Optik* 124 (20):4110–16. doi:10.1016/j.ijleo.2012.12.030.
- Holland, O. T. 2007. Taxonomy for the modeling and simulation of emergent behavior systems. *Spring simulation multiconference*, vol. 2, Norfolk, VA.
- Jackson, M. C. 2010. Reflections on the development and contribution of critical systems thinking and practice. *Systems Research & Behavioral Science* 27 (2):133–39. doi:10.1002/sres.1020.
- Ko, C.-W., and H.-W. Chung. 2000. Automatic spike detection via an artificial neural network using raw EEG data: Effects of data preparation and implications in the limitations of online recognition. *Clinical Neurophysiology* 111 (3):477–81. doi:10.1016/S1388-2457(99)00284-9.
- Ko, K. W., and H. S. Cho. 2000. Solder joints inspection using a neural network and fuzzy rule-based classification method. *IEEE Transactions on Electronics Packaging Manufacturing* 23 (2):93–103. doi:10.1109/6104.846932.
- Kopetz, H. A., A. Bondavalli, F. Brancati, B. Frömel, O. Höftberger, and S. Iacob. 2016. Emergence in cyber-physical systems-of-systems (CPSoSs). *Lecture Notes in Computer Science* 10099:73–96. doi:10.1007/978-3-319-47590-5\_3.
- La, H. J., and S. D. Kim. 2010. A service-based approach to designing cyber physical systems. 9th International Conference on Computer and Information Science, vol. 2010, 895–900. IEEE Publications/Australasian Center for Italian Studies. doi:10.1109/ICIS.2010.73.
- Lewin, R., and B. Regine. 2003. The core of adaptive organisations *Complex systems and evolutionary perspectives on organisations: The application of complexity theory to organisations*, 167–184.
- Loosemore, M., J. Raftery, and C. Reilly. 2005. *Risk management in projects*. US: Routledge.
- Maier, M. W. 1998. Architecting principles for systems-of-systems. *Systems Engineering* 1 (4):267–84. doi:10.1002/(SICI)1520-6858(1998)1:4<267:AID-SYS3>3.0.CO;2-D.
- Maier, M. W. 2009. *The art of systems architecting*. USA: CRC Press.
- Maier, M. W. 2014. The role of modelling and simulation in a system of systems development. In *Modelling and simulation support for system of systems engineering applications*, ed. L. B. Rainey and A. Tolk, 11–41. USA: John Wiley & Sons.
- Miller, R., and D. R. Lessard. 2008. Evolving strategy: Risk management and the shaping of megaprojects. In *Decision-making on mega-projects: Cost–benefit analysis, planning and innovation*, ed. H. Priemus, B. Flyvbjerg, and B. van Wee, 145–72. USA: Edward Elgar Publishing Limited.
- Mingers, J., and J. Brocklesby. 1997. Multimethodology: Towards a framework for mixing methodologies. *Omega* 25 (5):489–509. doi:10.1016/S0305-0483(97)00018-2.
- Mintzberg, H., B. Ahlstrand, and J. B. Lampel. 2020. *Strategy safari*. USA: Pearson.
- Mittal, S., and L. Rainey. 2015. Harnessing emergence: The control and design and emergent behaviour in system of systems engineering. Summer Computability Simulata Conference, Chicago, IL.
- Modul, D. S. 2017. Abstract DPOC-012: Theranostic nanoplatfrom for image–guided surgery and intraoperative phototherapy for ovarian cancer treatment. *Engineering* 23 (11\_Supplement): DPOC-012. <https://standards.globalspec.com/std/10158433/def-stan-23-012;2017:360>.

- Murray, J., T. Webb, and S. Wheatley. 2019. *Complexity theory and law: Mapping an emergent jurisprudence*. USA: Routledge.
- Nweke, L. O., G. K. Weldehawaryat, and S. D. Wolthusen. 2021. Threat modelling of cyber-physical systems using an applied  $\pi$ -calculus. *International Journal of Critical Infrastructure Protection* 35:100466. doi:10.1016/j.ijcip.2021.100466.
- O'Connell, M. E. 2012. Cyber security without cyber war. *Journal of Conflict and Security Law* 17 (2):187–209. doi:10.1093/jcsl/kr017.
- O'Toole, E., V. Nallur, and S. Clarke. 2014. Towards decentralised detection of emergence in complex adaptive systems. *Proceedings of the 8th IEEE International Conference on Self-Adaptive and Self-Organising Systems; 2015*, 60–69. London, UK: IEEE Publications. doi:10.1109/SASO.2014.18.
- Pe' rez R' ios, J. 2008. Supporting organisational cybernetics by communication and information technologies (VSMoD®). *International Journal of Applied Systemic Studies* 2 (1/2): 49. (special issue: organizational cybernetics in focus. Perez Rios, J. and Schwaninger, M. (Guest editors)). doi:10.1504/IJASS.2008.022794.
- Rainey, L. B., and A. G. Loerch, eds. 2007. *Methods for conducting military operational analysis*. In Alexandria. USA: Military Operations Research Society.
- Rainey, L. B., and A. Tolk, eds. 2015. *Modelling and simulation support for system of systems engineering applications*. USA: John Wiley & Sons.
- Rittel, H. W. J., and M. M. Webber. 1973. Dilemmas in a general theory of planning. *Policy Sciences* 4 (2):155–69. doi:10.1007/BF01405730.
- Ross, A. W. 1958. Requisite variety and its implications for the control of complex systems. *Cybernetica* 1 (2):83–99. republished *Oncology and Therapy* web by F. Heylighen—Principia cybernetica project.<http://pcp.vub.ac.be/Books/AshbyReqVar.pdf>.
- Ruhl, J. B. 2009. Thinking of environmental law as a complex adaptive system: How to clean up the environment by making a mess of environmental law. *Hous. Law Review* 34 (4):933.
- SBRI USA. 2011. Department of defense USA, Avitek and Arizona University; cyber-battle management system (CBMS), contract FA9550-11-C-0007 awarded part II, 2011. <https://www.sbir.gov/sbirsearch/detail/378027>.
- Schwaninger, M. 2005. Design for viable organizations. The diagnostic power of the viable system model. In *Viable Organizations*, WOSC world organization of systems and cybernetics. 13th international congress of cybernetics and systems and ISA international sociological association. Research committee 51 on sociocybernetics, ed. M. Matjaz and B. Eva, 45–56. Maribor: WOSC world organisation of systems and cybernetics.
- Schwaninger, M. 2009. *Intelligent organizations. Powerful models for systemic management*, second ed. USA: Springer.
- Schwaninger, M., and J. Pe' rez R' ios. 2008a. Editorial: Organizational cybernetics in focus. *International Journal of Applied Systemic Studies* R. Pe' rez, J. ios, and M. Schwaninger (Guest eds.), 2 (1/2):100–104
- Schwaninger, M., and J. Pe' rez R' ios. 2008b. System dynamics and cybernetics. *System Dynamics Review* 24 (2):145–74. doi:10.1002/sdr.400.
- Sheffield, J., S. Sankaran, and T. Haslett. 2012. Systems thinking: Taming complexity in project management. *On the Horizon* 20 (2):126–36. doi:10.1108/10748121211235787.
- Silva, E. C., and T. Batista. 2017. Refining missions to architectures in software-intensive systems-of-systems. *Proceedings of the Joint 5th IEEE/ACM Joint International Workshop on Software Engineering for Systems-of-Systems and 11th Workshop on Distributed Software Development, Software Ecosystems and Systems of-Systems*, 2–8. USA: IEEE. doi:10.1109/JSOS.2017.12.

- Sinclair, S. 2022. Development of Australian soldier systems architecture. Systematic. <https://www.systematiq.com.au/2017/07/03/development-of-australian-soldier-systems-architecture/>.
- Snowden, D. J., and M. E. Boone. 2007. A leader's framework for decision making. *Harvard Business Review* 85 (11):68.
- Song, H., G. A. Fink, and J. S. 5. Chapter. 2017. *Security and privacy in cyber-physical systems foundations, principles and applications*. USA: John Wiley & Sons, Legal Considerations of Cyber-Physical Systems and the Internet of Things.
- Stacey, R. D. 2007. *Strategic management and organisational dynamics: The challenge of complexity to ways of thinking about organisations*. Financial Times—Prentice Hall.
- Stephenson, P. R. 2017. Defining a Cyber Jurisprudence. Annual ADFSL Conference on Digital Forensics, Security and Law, 8. <https://commons.erau.edu/adfsl/2017/papers/8>.
- Sternberg, R. J., and P. A. Frensch, Eds. 1991. *Complex problem solving: Principles and mechanisms*. UK: Psychology Press.
- Stocchero, J. M., C. A. Silva, L. de Souza Silva, M. A. Lawisch, J. C. S. dos Anjos, and E. P. D. Freitas. 2022. *Secure command and control for internet of battle things using novel network paradigms*. IEEE Communications Magazine. doi:10.1109/MCOM.001.2101072.
- Syamil, A., W. J. Doll, and C. H. Apigian. 2004. Process performance in product development: Measures and impacts. *European Journal of Innovation Management* 7 (3):205–17. doi:10.1108/14601060410549892.
- Thomann, J. 1973. *Meta-methodology: An overview of what it is and how it was developed*. 58th American Educ. Res Assoc. Annual Meeting, New Orleans, LA, February 26.
- Von Foerster, H., M. Mead, and H. L. Teuber, eds. 1950. *Cybernetics: Circular causal and feedback mechanisms in biological and social systems*. USA.
- Walker, D. H. T., and K. Nogeste. 2008. Performance measures and project procurement. In *Procurement systems—A cross industry project management perspective*, ed. D. H. T. Walker and S. Rowlinson, 177–210. Taylor & Francis.
- Ward, S., and C. Chapman. 2011. *How to manage project opportunity and risk: Why uncertainty management can be a much better approach than risk management*. Hoboken, NJ: John Wiley & Sons.
- Wiener, N. 1948. *Cybernetics or the control and communication in the animal and the machine*. USA: MIT Press.
- Wiener, N. 2013. *Cybernetic or control and communication in the animal and the machine*, second ed. (reissue). USA: MIT Press.
- Wincek, J. C. 2011. Basis of safety: A concise communication method for critical process safety information. *Process Safety Progress* 30 (4):315–18. doi:10.1002/prs.10471.
- Yolles, M. 2021. Metacybernetics: Towards a general theory of higher order cybernetics. *Systems* 9 (2):34. doi:10.3390/systems9020034.
- Zalewski, J., J. McKinna, and J. G. Morris. 2020. λdB: Blame tracking at higher fidelity. *Proceedings of the First ACM SIGPLAN Workshop on Gradual Typing*, New Orleans, United States.