Journal of Artificial Intelligence and AI Ethics
https://doi.org/10.64978/jaiae.2026.1103009

SCIVOLVE

ISSN: 3142-8223

Research Article

Open Access Full Text Article

Application of Fourth-Order Cybernetics in Digital Twin-Enabled Adaptive Systems of Systems Operating in High-Stakes Environments

Dr. Aleksandar Seizovic[*1], Hongan Lin[2], Tomislav Dovecer[3], Xintong (Wash) Wang[4]

[1*]Asset Studio, Australia.
[1*]Engineering Department, University of Southern Queensland, Queensland, Australia.
[2]Asset Studio, Singapore. Engineering Department.
[3]MEng (Safety & Security), S&T Consultancy Pty Ltd, Western Australia, Australia.
[4]Masters in education, Rilleon Technology, Gold Coast, Queensland.

Correspondence:
Dr. Aleksandar Seizovic, Asset Studio, Engineering Department, University of Southern Queensland, Queensland, Australia. ORCID: https://orcid.org/0000-0003-0445-8716

Received: October 14, 2026; **Published:** November 03, 2026

How to cite this article:
Seizovic, A., Lin, H., Dovecer, T., Wang, X. (2026) 'Application of Fourth-Order Cybernetics in Digital Twin-Enabled Adaptive Systems of Systems Operating in High-Stakes Environments' *Journal of Artificial Intelligence and AI Ethics,* 1(4), pp.1–22. https://doi.org/10.64978/jaiae.2026.1103009

Abstract

Modern systems of systems (SoS) operating in high-stakes environments like Distributed Operational System (DOS) are characterized by tightly coupled interactions among human operators, autonomous agents, and heterogeneous technological subsystems. Conventional reliability engineering approaches, which primarily focus on component level failure probabilities and static models are often insufficient for capturing emergent behaviors and nonlinear failure propagation across interconnected sociotechnical systems.

This study proposes a cybernetically informed framework that integrates digital twin technology, the Viable System Model (VSM) and an extended Failure Modes and Effects Criticality Analysis (FMECA) methodology to reconceptualise reliability as a dynamic and emergent system property. Digital twins function as continuously updated virtual representations that synchronise real time data, simulation models, and predictive analytics, enabling recursive observation and anticipatory regulation. Their integration with FMECA supports scenario based reliability analysis, allowing the modelling of cascading failures, coordination disruptions and adaptive system responses.

The findings demonstrate that reliability emerges from system interactions rather than isolated components, advancing the design of adaptive, resilient, and self-regulating systems operating in complex and uncertain environments. Although applicable to systems of systems related contexts, the framework is intentionally generalised to support broader applications across critical infrastructure, healthcare coordination systems, industrial automation, autonomous transportation, emergency response networks and distributed cyber physical systems. Simulation experiments across distributed systems of systems networks demonstrate how local disturbances propagate through interconnected nodes and are mitigated through cybernetic feedback mechanisms. Simulation experiments across distributed systems of systems networks and demonstrate how local disturbances propagate through interconnected nodes and are mitigated through cybernetic feedback mechanisms. Monte Carlo analysis (n = 1000) indicates high robustness, with operational effectiveness ($\zeta = 0.929 \pm 0.021$) and system availability ($A = 0.98 \pm 0.015$). Monte Carlo analysis indicates high robustness, with strong operational continuity and system availability across varying disruption scenarios.

Keywords: Digital twin, cybernetics, systems of systems, resilience, emergence, adaptive systems, reliability engineering, complex systems.

Introduction

In systems of systems (SoS) reliability analysis, digital twin technologies represent a significant advancement in the monitoring, evaluation, and governance of complex systems of systems architectures. Traditional reliability engineering has relied on static probabilistic models, historical failure datasets, and predefined redundancy strategies. While effective in stable DOS environments, these approaches are increasingly insufficient for highly interconnected, adaptive and disruptive in operational contexts.

Digital twins address these limitations by enabling continuously updated virtual representations of physical systems that integrate real time sensor data, predictive modelling, and simulation capabilities within a unified analytical environment (Fuller et al., 2020; Grieves & Vickers, 2017; Tao et al., 2019). This shift transforms reliability analysis from a retrospective activity into a prospective and anticipatory capability, allowing system behaviour to be evaluated under varying operational conditions and enabling early identification of failure modes and degradation pathways.

From a cybernetic perspective, digital twins can be understood as recursive observational systems capable of monitoring both system performance and the analytical processes used to interpret that performance. This introduces a reflexive mode of governance in which systems not only respond to environmental changes but also adapt their own decision-making structures. Such reflexivity extends conventional reliability frameworks into adaptive and anticipatory modes of governance and control, enabling the system to monitor its own performance, interpret emerging patterns and adjust proactively in response to changing conditions. These capabilities are particularly critical in DOS environments, where uncertainty, nonlinearity and evolving operational dynamics require continuous learning and recursive adaptation to sustain system viability and operational effectiveness (Brain of the Firm, 1979; von Foerster, 2003). When situated within cybernetic frameworks such as the Viable System Model (VSM), digital twins assume an expanded role beyond passive representations of physical assets to become active participants in organisational cognition and meta-regulation. By integrating real time sensor data, simulation outputs and policy constraints into recursive feedback structures, they support distributed decision-making, anticipatory analysis and adaptive control across multiple organisational levels. In this capacity, digital twins function as epistemic agents that enhance situational awareness, coordinate responses to emerging conditions and enable continuous learning and systemic adaptation in complex operational environments (Yolles, 2021).

Context and Research Positioning

Modern DOS environments, particularly those structured as Systems of Systems (SoS) are characterised by extensive complexity, deep interconnectivity and persistent disruptive uncertainty. Traditional reliability engineering approaches grounded in static probabilistic models, historical failure data and predefined redundancy are increasingly insufficient for such dynamic contexts. The emergence of digital twin technology represents a significant shift, enabling continuously updated virtual representations of physical systems that integrate real-time data, predictive modelling and simulation within a unified analytical framework (Fuller et al., 2020; Grieves & Vickers, 2017; Tao et al., 2019). From a cybernetic perspective, these digital twins function not merely as monitoring tools but as recursive observational systems capable of adapting both system behaviour and the processes used to interpret it.

This paper argues that when digital twins are embedded within higher order cybernetic frameworks, particularly the Viable System Model (VSM), reliability in complex systems of systems is transformed from a static, component-based measure into an emergent, adaptive property sustained through continuous feedback, learning and system wide coordination.

Operational Context and Analytical Focus

Within contemporary high-stakes operational ecosystems, digital twins enable a transition from rigid hierarchical structures toward distributed, feedback-driven coordination. These systems require continuous situational awareness, rapid decision-making and resilience under uncertain and dynamically evolving conditions. Digital twins support these requirements by integrating heterogeneous data sources and enabling the simulation of alternative operational scenarios in real time. In distributed node-based architectures, individual operational nodes act as interconnected components within distributed sensor and communication networks, where digital twins process physiological, environmental, and operational data to assess system health and anticipate disruption (Jamshidi, 2009; Maier, 1998).

This capability allows for dynamic reconfiguration of operational networks, preserving effectiveness even when components degrade or fail. Within such cybernetically informed architectures (figure 8), reliability is no longer an inherent property of isolated components but an emergent outcome arising from interactions among technological systems, human decision-makers and organisational processes (Mittal, 2017; Ashby, 1956; Wiener, 1948; Beer, 1979).

Synthesis and Research Contribution

The integration of digital twins within higher order cybernetic frameworks introduces meta system capabilities that enable systems to observe, evaluate and adapt their own modes of operation. By incorporating recursive feedback mechanisms and leveraging concepts such as information amplification and attenuation, these systems balance environmental complexity with organisational response capacity, ensuring coherence across operational and strategic levels (von Foerster, 1984; Yolles, 2021).

This paper therefore positions digital twins as central to a new paradigm of reliability analysis one that is anticipatory, adaptive, and deeply embedded within system cognition and governance. The key takeaway is that reliability in modern DOS environments which is no longer engineered solely through design time optimisation but is continuously co-produced through real time sensing, simulation, and learning, enabled by the integration of digital twins within recursive cybernetic architectures.

Methodology

This study adopts a cybernetic systems methodology that integrates digital twin simulation, behavioural systems analysis and the Viable System Model (VSM) to examine reliability and emergent behaviour in systems of systems (SoS) operating within complex and DOS environments. The approach is grounded in cybernetics and systems engineering, which conceptualise organisational and technical systems as networks of interacting components regulated through feedback and adaptive control mechanisms (Ashby, 1956; Wiener, 1948). In contrast to conventional reliability engineering approaches that rely on static probabilistic models or retrospective failure analysis, this methodology combines conceptual modelling with simulation-based experimentation to analyse how recursive feedback structures and digital twin monitoring influence system reliability, coordination and adaptation under dynamic operational conditions. Digital twins are particularly suited to this task, as they provide continuously updated virtual representations of physical systems that integrate real time data, simulation models, and predictive analytics within a unified analytical framework (Fuller et al., 2020; Grieves & Vickers, 2017; Tao et al., 2019). By embedding digital twin simulations within a cybernetic architecture based on the VSM, reliability is examined as an

emergent property of distributed system interactions rather than as a characteristic of isolated components (Beer, 1979; Madni et al., 2014).

The methodological framework is operationalised as a recursive analytical process encompassing cybernetic system modelling, digital twin environment construction, emergent behaviour simulation, reliability evaluation and meta-cybernetic feedback analysis. These components collectively establish an iterative process in which system behaviour is simulated, evaluated, and refined through successive feedback cycles. This structure reflects the foundational cybernetic principle that complex systems must continuously observe and regulate their own behaviour to maintain stability under changing conditions (von Foerster, 1984; Yolles, 2021). Accordingly, the research design mirrors the cybernetic structures under investigation, enabling the methodology itself to embody feedback driven adaptation and reflexive learning.

The cybernetic system model is constructed using Stafford Beer's Viable System Model, which provides a framework for analysing how complex organisations maintain stability and adaptability through recursive regulatory structures (Beer, 1979). Within this representation, the DOS is modelled as a set of interconnected subsystems corresponding to operational execution (System 1), coordination (System 2), internal regulation (System 3), environmental analysis (System 4), and policy governance (System 5). Operational nodes represent node network systems equipped with sensors, communication devices, and processing capabilities, while coordination and control layers regulate information flows, resource allocation, and coordination and governance directives. Strategic and policy layers simulate environmental analysis, forecasting, and operational objective governance. The system is implemented computationally as a network graph of interconnected nodes (figure 8) and communication pathways, with node states defined by variables such as sensor availability, communication latency, processing load and operational objective status (figure 9). These variables are updated at discrete time intervals to capture the dynamic behaviour of the operational environment (Jamshidi, 2009; Boardman & Sauser, 2006).

The digital twin environment extends this model by pairing each operational node with a virtual counterpart that continuously updates its state based on simulated telemetry and environmental inputs. These digital twins function as analytical proxies, enabling predictive monitoring and behavioural analysis without disrupting operational processes. The simulation incorporates multiple data streams, including operational telemetry (e.g., node status, communication latency, sensor inputs), environmental factors (e.g., terrain, interference, network congestion), and agent interactions (e.g., coordination and governance signals and coordination exchanges). System parameters are configured to reflect realistic operational conditions, with network sizes ranging from four to twenty nodes, communication latency varying between 20 and 200 milliseconds and fault events modelled using stochastic distributions. Through continuous synchronisation of these inputs, the digital twin environment maintains an evolving representation of system state, supporting anomaly detection, predictive analysis, and scenario simulation (Fuller et al., 2020).

Emergent behaviour is analysed through scenario-based simulation experiments in which controlled disturbances are introduced into the network. These disturbances include equipment faults at individual nodes, uncertain disruptions such as communication interference and stochastic variations in agent behaviour. Simulation runs are conducted over multiple time cycles, during which system states evolve according to defined interaction rules governing communication, coordination and decision-making processes. The propagation of disruptions across the network is monitored to identify cascading effects such as coordination breakdowns or loss of situational awareness. Emergent behaviours are detected by analysing deviations from expected system performance trajectories, with particular attention to the conditions under which localised failures generate systemic instability or adaptive reconfiguration (Mittal, 2017; Madni & Sievers, 2014).

Reliability is evaluated using dynamic system level metrics derived from simulation outputs rather than relying solely on traditional component-based measures. In this framework, reliability is treated as an emergent property arising from interactions between technical components, communication networks and organisational processes. Key performance indicators include fault recovery time, coordination efficiency, network availability and policy adaptation latency. These metrics are used to construct dynamic reliability profiles and performance trajectories, enabling analysis of how disturbances affect system behaviour over time and how digital twin monitoring contributes to system resilience and recovery.

The methodology further incorporates meta-cybernetic feedback mechanisms that enable the system to evaluate and adapt its own monitoring and decision processes. This higher order capability allows the digital twin system to adjust parameters such as anomaly detection thresholds and task prioritisation strategies based on prior simulation outcomes, thereby improving responsiveness to emerging disruptions (von Foerster, 1984; Yolles & Fink, 2021). Validation is achieved through theoretical consistency checks against established cybernetic principles, sensitivity analysis across key parameters (e.g., failure probability, latency, environmental interference) and repeated simulation runs to ensure reproducibility of results.

Through the integration of cybernetic modelling, digital twin simulation and meta-system feedback analysis (figure 7), this methodology provides a systematic and reproducible framework for investigating reliability and emergent behaviour in complex systems of systems. By combining conceptual cybernetic theory with simulation-based experimentation, the approach enables the analysis of reliability as a dynamic and adaptive property of distributed system interactions, offering a foundation for future research on resilient and adaptive systems of systems architectures.

Literature Review

Foundational cybernetics provides the theoretical basis for understanding control, communication and feedback within complex systems. Early contributions by Wiener, von Foerster and Beer established core principles that continue to inform contemporary systems thinking, particularly in relation to feedback regulation, second order observation and viable system organisation (Beer, 1979; von Foerster, 2003; Wiener, 1948). These principles emphasise circular causality, recursive interactions and the inclusion of the observer within the system of analysis. Within this framework, systems are understood not as static entities but as dynamic processes that maintain stability and adapt to environmental perturbations through continuous feedback mechanisms.

Building on these theoretical foundations, digital twin technology has emerged as a significant advancement in the modelling, simulation and analysis of complex systems. Recent systematic reviews indicate that digital twins are increasingly applied in

safety critical and systems of systems related domains, where they support predictive maintenance, lifecycle optimisation and operational performance analysis across interconnected assets (Yao et al., 2023; Somers et al., 2023). Unlike traditional static models, digital twins function as continuously updated virtual representations of physical systems, integrating real time data streams to enable iterative feedback between physical and digital domains. This characteristic aligns closely with cybernetic principles, particularly the use of feedback loops for monitoring, control and adaptive system behaviour.

The application of digital twins has further evolved into SoS contexts, where multiple heterogeneous and interdependent systems interact within distributed operational environments. Emerging research describes the development of "systems of twinned systems," in which multiple interacting digital twins collectively represent large scale, networked infrastructures (Adesanya et al., 2025). This paradigm is particularly relevant to high-stakes environments, where operational effectiveness depends on interoperability, coordination, and the management of complex interdependencies. In such settings, system behaviour is often emergent, arising from interactions between components rather than from the properties of individual elements. Consequently, analytical approaches must account for cascading effects, network dependencies and nonlinear interactions across system boundaries. Within this context, the integration of artificial intelligence (AI) into digital twin high-stakes environments enhances their analytical depth and operational utility. AI techniques enable capabilities such as predictive analytics, anomaly detection, optimisation and adaptive decision support. However, in high stakes domains such as systems of systems the use of AI introduces critical challenges related to reliability, robustness, transparency and trustworthiness (Homaei et al., 2024). These challenges are particularly significant when AI driven outputs inform operational decisions, as inaccuracies, biases, or uncertainties may propagate through the system and affect operational objective outcomes. As a result, there is increasing emphasis on ensuring that AI enabled systems are rigorously validated and operate within well-defined performance and governance boundaries.

In response to these challenges, the literature increasingly highlights the importance of responsible AI frameworks that incorporate principles such as accountability, explainability, fairness and human oversight. These frameworks aim to ensure that AI systems remain interpretable, verifiable and aligned with ethical and operational requirements. Within digital twin high-stakes environments, responsible AI also entails maintaining data integrity, validating model outputs and ensuring transparency in how predictions and recommendations are generated. This is particularly important in systems of systems contexts, where decisions may have significant strategic and operational consequences.

Beyond the integration of digital twins and AI, contemporary research situates these technologies within broader socio technical systems and service ecosystem perspectives. Digital twins are increasingly understood as components embedded within interconnected networks of organisations, platforms and stakeholders rather than as standalone technical artefacts. This perspective aligns with open innovation paradigms, in which value is co-created through collaboration, shared data infrastructures and interoperable systems. In complex transformation contexts such as systems of systems digitalisation, these ecosystems support the co-evolution of technologies, processes and organisational capabilities, enabling adaptive and scalable system development. Systematic reviews of digital twin implementations identify several challenges associated with this ecosystem-oriented approach, including interoperability across heterogeneous platforms, integration of diverse data sources, lifecycle management, cybersecurity and governance across distributed stakeholders (Wang et al., 2023; Lehner et al., 2025). These challenges are particularly pronounced in high-stakes environments, where systems must operate under strict security constraints, legacy infrastructure limitations and multi domain operational requirements. Addressing these issues requires not only technical solutions but also coordinated governance mechanisms capable of managing complexity across organisational and system boundaries.

The convergence of cybernetics, digital twin technology, artificial intelligence and ecosystem-based innovation provides a comprehensive framework for understanding and managing complex SoS high-stakes environments. Cybernetics offers the theoretical foundation for feedback, control and adaptation. The digital twins provide the computational infrastructure for real time modelling and simulation. The AI enhances predictive and adaptive capabilities. The open innovation and service ecosystem perspectives situate these technologies within broader socio-technical contexts. Together, these perspectives enable a holistic approach to analysing emergent behaviour, system resilience and operational effectiveness in complex systems of systems.

The emerging computational paradigms in multi agent systems and strategic interaction further extend the applicability of digital twin frameworks in complex operational high-stakes environments. Contemporary research in evolutionary game theory and multi agent reinforcement learning provides mechanisms for modelling adaptive behaviour among heterogeneous agents operating under uncertainty. For example, evolutionary game theoretic approaches have been applied to model how distributed agents converge toward equilibrium strategies in dynamic and competitive high-stakes environments, offering insights into coordination under uncertainty and partial information (Zhang et al., 2025). Similarly, multi agent reinforcement learning frameworks demonstrate how agents can iteratively learn optimal policies through interaction with their environment while maintaining system level performance objectives (Wang et al., 2025).

These approaches are particularly relevant to digital twin enabled systems of systems, where multiple autonomous or semi-autonomous entities must coordinate under uncertain, disruptive and time-constrained conditions. Evolutionary dynamics and learning based adaptation provide formal mechanisms for understanding how local decision-making processes aggregate into global system behaviour. Further, research on replicator dynamics and evolutionarily stable strategies highlights how distributed agents can adapt their strategies over time while balancing local objectives with overall system stability (Liu et al., 2025). This is especially pertinent in high-stakes environments where competing priorities, resource constraints and incomplete information shape decision making processes.

Complementary work on adaptive negotiation mechanisms, including evolutionary smart contracts incorporating behavioural models such as prospect theory, extends these concepts by accounting for heterogeneity in risk preferences and decision biases (Chen et al., 2025). These models capture how agents engage in dynamic multistage interactions that evolve in response to changing environmental conditions and internal states. Such frameworks align with the requirements of digital twin enabled systems, where continuous feedback, adaptation and reconfiguration are essential for maintaining performance in

complex and uncertain high-stakes environments.

Together, these computational and game theoretic approaches advance beyond traditional optimisation methods by explicitly modelling learning, adaptation and strategic interaction in distributed systems. Integrating these perspectives into digital twin-based systems of systems architectures enhances the conceptual and methodological foundation of system design by framing subsystem interactions as dynamic processes governed by feedback, adaptation and strategic behaviour. This enables the development of robust, adaptive and scalable multiagent systems capable of operating effectively in high dimensional and disruptive high-stakes environments.

Problem Statement

Reliability in traditional systems of systems has historically been assessed using component level metrics, such as mean time between failures (MTBF) and failure mode effects analysis (FMEA). While effective for isolated subsystems, these approaches are inadequate for complex, distributed SoS such as modern systems of systems (SoS) where emergent behaviours, disruptive dynamics and context dependent interactions play a dominant role in operational performance (Burge, 2018). In such high-stakes environments, system level reliability cannot be inferred solely from the robustness of individual components, rather it emerges from the coordinated interactions of heterogeneous agents including human operators, autonomous platforms and networked decision support architectures operating under uncertainty and disruptive pressures.

Current reliability frameworks also fail to account for adaptive and anticipatory requirements, including the capacity to simulate, predict and reconfigure operations in response to dynamic environmental conditions. Without these capabilities, systems of systems networks risk not only functional degradation or systemic failure, but also strategic incoherence, whereby operational decisions fail to align with operational objective intent, situational awareness, or evolving disruptive contexts. Narrow definitions of reliability, grounded in static metrics, therefore render systems brittle and ill-suited to cope with the complex, stochastic and disruptive nature of contemporary operational domains.

There is a critical need for a dynamic, multi layered reliability framework that integrates:

- Emergent system behaviour analysis, capturing interactions across heterogeneous agents.
- Adaptive maintenance and policy mechanisms, informed by predictive modelling and scenario simulation.
- Cybernetic feedback and reflexivity, enabling continuous observation, learning and self-regulation; and
- Digital twin enabled monitoring, providing a virtual real synchronisation for real time operational awareness and proactive intervention.

Addressing this gap is essential for designing resilient, adaptive and strategically coherent DOS networks capable of sustaining operational objective effectiveness in complex, contested and rapidly evolving operational high-stakes environments.

Solution

Digital twins, grounded in Fourth-Order Cybernetics and structured through the Viable System Model (VSM), offer a comprehensive and adaptive solution for managing reliability in complex systems-of-systems (SoS) By embedding reflexivity, predictive modelling and multi agent coordination into operational architectures, digital twins transform traditional reliability assessment into a dynamic, anticipatory and system level practice.

Key capabilities of digital twins include:

- Predictive Maintenance: Real time modelling of component degradation and operational stress enables proactive interventions before failures occur, moving reliability management from reactive or scheduled maintenance toward a condition based, predictive paradigm (Grieves & Vickers, 2017; Tao et al., 2019).
- Systemic Reliability Assessment: Continuous simulation of operational scenarios allows analysis of how local disruptions propagate across the network. This systemic perspective supports proactive design adjustments and strategic reconfiguration to mitigate cascading failures.
- Adaptive Reconfiguration: Digital twins enable autonomous adaptation when subsystems degrade, or nodes are compromised. Communication pathways can be rerouted, loads rebalanced and fallback protocols activated automatically, ensuring resilient network functionality under dynamic conditions.
- Behavioural Learning: Historical disruptions are captured and integrated into learning algorithms, informing future response strategies. This iterative adaptation enhances system robustness over time, enabling agents to evolve strategies that maintain global operational effectiveness.

Beyond traditional industrial applications, where digital twins primarily monitor equipment, diagnose faults and predict failures, they possess untapped potential when interpreted through a meta cybernetic lens. In this perspective, a digital twin acts as a meta observer an active agent that not only replicates the physical system's state but also reflects upon its own observations, analyses and interventions. By doing so, it participates in recursive feedback loops, regulating both the physical system and a process central to managing complex systems of systems characterized by heterogeneous agents and emergent behaviours.

Digital twins achieve this by integrating diverse data streams from sensors, operational logs and simulation outputs, contextualizing them with knowledge of the operational environment, operational objectives and strategic priorities. Through the application of advanced analytics, machine learning and systems modelling, they provide real-time situational awareness, predictive insights and autonomous decision support, enhancing both system responsiveness and reliability in complex, disruptive operational landscapes (Fuller et al., 2020; Grieves & Vickers, 2017; Tao et al., 2019).

By uniting cybernetic principles, VSM structuring and digital twin capabilities, this approach enables adaptive, anticipatory and resilient DOS networks. Reliability is no longer a static attribute of individual components, but an emergent property continuously coproduced through recursive observation, simulation and coordinated multi agent action. This framework supports robust operational objective assurance, operational coherence and strategic alignment in the face of uncertainty, emergent phenomena and uncertain pressures.

Digital Twin Technologies in Systems of Systems and Complex Systems

Digital twin technology, initially developed within the manufacturing domain to enable real-time digital replication of physical assets and processes (Tao et al., 2019), has increasingly

been adopted within systems of systems to enhance situational awareness, predictive maintenance and operational decision-making. These systems enable continuous, bi-directional data exchange that reflects the real-time status and dynamics of physical systems, supporting high fidelity simulations and scenario-based analysis (Adams et al, 2014).

In the context of distributed networks, digital twins evolve beyond discrete platform modelling and extend to system of systems (SoS) architectures, allowing for the simulation and optimisation of interactions between heterogeneous autonomous platforms, communication networks and coordination and governance hierarchies. This extension supports emergent behaviour analysis through agent-based modelling, a methodology that captures distributed dynamics and inter agent interactions within complex DOS environments (Lee et al., 2018). The ability of digital twins to facilitate dynamic reconfiguration and enable embedded feedback loops has become essential for managing the non-linearity, uncertainty and volatility that characterise modern operational domain's (Grieves & Vickers, 2017; Tao et al., 2019; Adams et al, 2014; Mittal, S. (2017).

From this theoretical perspective, digital twins are reframed not as static data repositories or passive digital representations, but as cybernetically enriched epistemic agents capable of continuous observation, interpretation and regulation of both the physical environment and its digital counterpart. This paper explores this integrated epistemological positioning, focusing on the role digital twins play in reliability analysis and adaptive maintenance across complex, commercial grade systems of systems, particularly within systems of systems (SoS) (Fuller et al, 2020; Grieves & Vickers, 2017; Tao et al., 2019).

Failure Modes and Effects Criticality Analysis (FMECA)

Failure Modes and Effects Criticality Analysis (FMECA) is a widely established reliability engineering methodology used to identify potential failure modes within a system and to evaluate the consequences of those failures on system performance, safety and operational objective effectiveness. The technique evolved from earlier Failure Modes and Effects Analysis (FMEA) methods developed for aerospace and systems of systems engineering programs, where high system reliability and operational objective assurance are essential requirements (Ebeling, 2010; O'Connor & Kleyner, 2012). In its traditional form, FMECA provides a structured analytical process through which engineers systematically examine system components, identify possible failure mechanisms and evaluate the resulting effects on higher level system functions. Each potential failure mode is assessed according to key parameters such as severity, probability of occurrence and detectability, allowing analysts to assign a criticality ranking that guide mitigation strategies including redundancy design, maintenance planning or operational safeguards. Through this structured approach, FMECA has become a foundational tool in reliability engineering and safety critical system design, particularly in aerospace, systems of systems and complex industrial systems where failure consequences may have significant operational implications (Blanchard & Fabrycky, 2011).

In conventional engineering practice, FMECA is typically applied to relatively bounded systems in which component relationships and failure pathways can be identified with reasonable certainty. Such systems generally exhibit hierarchical structures with clearly defined functional dependencies between subsystems, allowing analysts to trace failure propagation paths using deterministic or probabilistic modelling techniques. The systems of systems (SoS) and network enabled nodes architectures examined in the present study differ substantially from these traditional engineering contexts. These systems operate within distributed systems of systems (SoS) environments in which numerous semi-autonomous subsystems interact dynamically across communication networks and organisational structures. In such high-stakes environments, failures may propagate across multiple interconnected subsystems and produce emergent behaviours that cannot be fully predicted through component level analysis alone. As a result, conventional FMECA techniques must be adapted to account for the complex interaction patterns, feedback loops and adaptive responses characteristic of networked operational systems (Maier, 1998; Jamshidi, 2009). For this reason, the present study extends the traditional FMECA framework in order to accommodate the distributed, recursive and cybernetic characteristics of modern systems of systems architectures.

By its very nature, FMECA is an analytically intensive technique and it is designed to keep the down time of the assets (due to failure) to the absolute minimum and managed to meet operational objectives or operational objectives. FMECAs are performed to support assets, and it is necessary to have a basic understanding of this framework. This is not a detailed discussion on this area, but it will give a broad insight into this very complex topic.

FMECA Worksheets - Example

The following areas are considered when analyzing an item in this method.

Component Name	Specific item for which failure modes are being considered - may be a subcomponent of a larger system
Function	The operation and purpose for the component - what it is supposed to do and within what limits
Function Failure Mode Loss	In what way can the function not be provided when required
Function Failure Mode Impaired	In what way the function, which may still be available when required, is not to the standard, output or capacity for which the component was designed
Functional Failure Mode Operating Condition	When functional failure occurs, what is the operating condition of the component - dormant, steady operation, transient, start up, shutdown
Engineering Failure Mode Condition Criteria	What is the nature of degradation, damage or decay which constitutes the reason for the loss or impairment of function or divergence from acceptable or safe condition
Engineering Failure Mode - Damage Mode	Of the 22 or so known damage modes (eg creep, fatigue, corrosion, wear etc), what is the precise name for the prevailing damage mode that has led to engineering failure
Engineering Failure Mode - Internal/ External	Is the engineering failure mode evident from the outside of the component and system which contains the component, or does a machine or system need to be opened up to expose the engineering failure mode

Engineering Failure Mode - Cause	What is the physical process, environmental or other parameters that have contributed to the progress of the damage mode
Failure Effect - Local Effect	What is the consequence of the failure mode on the actual component being studied
Failure Effect - Next Level Effect	What is the consequence of the failure mode on the machine or system that contains the component
Failure Effect - System Effect	What is the consequence of the failure on the overall process, production line, utility or business unit in which the component's system or machine is located
Failure Effect - Consequence of failure	Standard RCM consequences - safety & environment, operating loss, no real loss, hidden failure - something else is now exposed to significant loss if another component or system fails
Detection Mode - Inspection	If a simple visual and measurement check is suitable, what is the means by which the damage mode and the status of the failure mode can be detected
Detection Mode - Overhaul	If an overhaul is required to detect the damage mode, what is required to be done
Detection Mode - Condition Monitoring	If Condition Monitoring (eg vibration checks, temperature checks, current analysis) is required using expert methods, what is the method that will detect the damage mode, eg accelerometers, thermography, infrared tachometry, spectographic oil analysis, ferrography
Detection Mode - NDT	If NDT (eg thickness checks, crack checks) is required using expert methods, what is the method that will detect the damage mode, eg ultrasonics, dye penetrant, fluroescent, radiography, EMAT
Detection Mode - Does the equipment need opening up	Based on past answers, simple YES/NO
Expert Opinion sought - Metallurgist	Is an expert metallurgical opinion on the component required - typically static plant type problems such as material loss, cracking, corrosion, micrography
Expert Opinion sought - Process Engineer	Is an expert opinion on the process required - eg what are process signs of a failure, what are the consequences of a failure
Expert Opinion sought - Condition Monitoring	Is an expert condition monitoring technology opinion on the component required - typically rotating plant type problems such as vibration, current analysis on heavy drives, but also thermography, oil analysis, etc
Compensating Provisions - Redundancy	If the failure arises, is there redundancy in the process so that the consequences are limited to either the component or the component's immediate surrounding system or machine
Compensating Provisions - Operational	Can the operating staff continue to meet their production or operating requirements through some work around or adjusting of the process or production schedule
Compensating Provisions - Design	Are there aspects about the design which limit the consequences (ie impact) of the failure mode
Criticality Analysis - Hazard Level	What is the worst possible outcome from the failure mode occurring
Criticality Analysis - Likelihood	What is the likelihood (eg probability) that the full hazard will be realised when the failure mode occurs
Criticality Analysis - Task Criticality	Given that hazard times likelihood is a measure of risk, the criticality of the task equates to the risk being avoided due to the failure mode being prevented by this task

The broad issues addressed in this framework set the high stake environment in which an FMECA is to be performed. Firstly undertake the FMECA process and secondly, move on to digital twin modelling and simulation.

Extension of FMECA for SoS Context

The first methodological extension implemented in this research involves redefining the analytical unit of FMECA from isolated hardware components to interacting system nodes within the operational network. Rather than focusing exclusively on physical component failures, the analysis incorporates hierarchical system structures that reflect the multi-layered organisation of battle management networks. Within this framework, failure modes are examined at three interconnected levels: the component level, the subsystem level and the network level. Component level failures correspond to faults in individual hardware or software elements such as sensors, communication modules, or processing devices embedded within nodes networks. Subsystem level failures correspond to disruptions within coordination mechanisms such as communication links, data fusion processes, or information exchange protocols responsible for maintaining situational awareness across operational units. Finally, network level failures represent systemic disruptions that propagate across the operational architecture and influence the overall coordination and effectiveness of system execution.

This hierarchical analytical structure reflects the distributed nature of systems of systems architectures, where interactions between subsystems can produce cascading effects that extend beyond the original point of failure. By incorporating these hierarchical layers into the FMECA framework, the analysis captures both localized faults and the broader systemic consequences that may arise from interdependencies between operational components. Such an approach aligns with systems engineering research that emphasises the importance of understanding failure propagation pathways within complex networks rather than evaluating components in isolation (Boardman & Sauser, 2006; Madni & Sievers, 2014). Consequently, the extended FMECA framework provides a more comprehensive representation of system reliability by integrating both technical component behaviour and network level interaction dynamics.

Integration with Digital Twin Simulation

The extension to the FMECA methodology involves integrating the failure analysis process with the digital twin simulation environment developed within this study. In traditional reliability engineering applications, the consequences of identified failure modes are often evaluated through expert judgement, historical failure data, or simplified analytical models. While such approaches provide valuable insights into potential system vulnerabilities, they may not fully capture the dynamic behavioural interactions that occur within complex operational networks. Digital twin technology provides a powerful analytical tool for addressing this limitation by enabling the creation of continuously updated virtual representations of physical systems that incorporate real-time operational data and predictive simulation capabilities (Grieves & Vickers, 2017; Tao et al., 2019; Fuller et al., 2020).

Within the present research, each identified failure mode in the FMECA worksheets was evaluated through simulation within the digital twin environment representing the operational battle management network. For every failure scenario, the digital twin model simulated the propagation of the failure across interconnected nodes, the resulting degradation in communication and coordination capabilities and the time required for the system to recover or reconfigure its operational structure. These simulations provided dynamic insights into how faults influenced system behaviour under realistic operational conditions. By incorporating these simulation outputs into the FMECA worksheets, the analysis moved beyond static risk estimates toward a more behaviourally informed assessment of system reliability. The digital twin therefore functions not only as a monitoring tool but also as an analytical environment in which potential system vulnerabilities can be explored and evaluated before they occur in real operational contexts.

Emergent Behaviour and Cascading Failure Analysis

A further adaptation to the FMECA framework addresses the challenge of emergent behaviour within systems of systems environments. In highly interconnected networks such as systems of Systems (SoS), localised faults may trigger cascading effects that propagate across multiple subsystems, producing system behaviours that cannot be predicted solely through component-level analysis. The phenomenon of emergence has been widely studied within complexity science and systems engineering, where it is recognised that interactions between individual system elements can produce unexpected global patterns and behaviours (Mittal, 2017). Within the context of systems of systems such emergent behaviours may manifest as communication breakdowns, coordination failures, or unexpected adaptive responses among operational units.

To capture these dynamics, the extended FMECA framework incorporates additional analytical parameters within the criticality assessment matrix. These parameters include propagation potential, coordination impact and operational objective degradation. Propagation potential represents the likelihood that a local failure will spread to other subsystems through communication or operational dependencies. Coordination impact measures the degree to which a failure disrupts communication flows, synchronization of tasks, or situational awareness among operational nodes (figure 9). Operational objective degradation evaluates the extent to which the failure affects the system's ability to achieve objectives within the operational environment. By incorporating these additional parameters, the FMECA analysis moves beyond traditional component level severity assessments toward a more comprehensive evaluation of how faults influence system-level behaviour and operational resilience.

Dynamic Criticality Assessment

Traditional FMECA methodologies often treat criticality rankings as relatively static values derived from estimated failure probabilities and severity ratings established during the design phase of a system. However, in dynamic systems of systems environments, the criticality of specific failure modes may change depending on operational conditions, system configurations and environmental factors. To address this challenge, the extended framework developed in this study introduces a dynamic criticality assessment process in which simulation outputs from the digital twin environment are used to update criticality rankings over time. Through repeated simulation runs under varying operational scenarios, the digital twin environment reveals how specific failures influence system behaviour under different environmental conditions and network configurations.

For example, a failure mode that initially appears to have limited impact when evaluated at the component level may demonstrate significant systemic consequences when simulated within a highly interconnected network environment. In such cases, the dynamic analysis enabled by the digital twin environment allows the reassessment of the criticality index to reflect the broader system level implications of the failure. This adaptive evaluation process provides a more accurate representation of system risk by incorporating behavioural dynamics and network interactions into the reliability analysis (Ebeling, 2010; Madni et al., 2014).

Role within the Cybernetic Framework

Within the broader cybernetic architecture of the study, FMECA functions as part of a recursive reliability assessment process embedded within the organisational structures described by the Viable System Model. The VSM conceptualises complex organisations as composed of interacting regulatory layers responsible for operational execution, coordination, internal control, environmental analysis and policy governance (Beer, 1979). In this framework, reliability monitoring and corrective actions occur across multiple organisational levels rather than being confined to technical maintenance activities alone. Digital twins operating within the control (System 3), intelligence (System 4) and policy (System 5) levels of the VSM utilise insights derived from the FMECA process to support decision-making, prioritise maintenance interventions and adjust system configurations in response to emerging risks.

Through this integration, FMECA becomes embedded within a continuous feedback cycle in which system behaviour is monitored, evaluated and adapted through successive iterations of analysis and decision-making. Failure analysis therefore evolves from a static engineering procedure into a dynamic organisational learning process in which operational experience, simulation outcomes and strategic decision processes collectively inform system adaptation. Such recursive feedback mechanisms reflect the fundamental principles of cybernetic governance, where system stability and resilience are maintained through continuous observation and adaptive regulation of system behaviour (Ashby, 1956; von Foerster, 1984; Yolles, 2021).

By extending traditional FMECA techniques to incorporate hierarchical system analysis, digital twin simulation and emergent behaviour evaluation, this study demonstrates how established reliability engineering methods can be adapted to the realities of

modern SoS architectures. The resulting analytical framework enables the examination of both component level failures and broader systemic interactions that influence operational performance within complex battle management networks. Through the integration of cybernetic modelling and digital twin simulation, the extended FMECA methodology provides a comprehensive reliability assessment approach capable of capturing the dynamic and adaptive characteristics of network enabled systems of systems. This approach enhances the identification of system vulnerabilities, enables proactive mitigation of cascading failures and improves the resilience of Distributed Operational Systems (DOS) operating within uncertain, contested and high-stakes environments.

The concept of the digital twin

The approach to modelling and simulating emergent behaviour in SoS involves several key steps: explaining the behaviour of individual system agents, establishing a taxonomy of emergent behaviours, utilising agent-based modelling and simulation techniques and addressing both negative and positive instances of emergence through the early research.

In complex systems, nonlinear outcomes frequently arise. Hidden states within an SoS, situated outside the primary system, can be regarded as exosystemic. These hidden states and relationships can be elucidated using a meta-system (figure 7), where the higher order of cybernetics can be explained in relation to lower orders. The initial step in designing a multi DOS involves explaining how each system agent exists and operates within the environment, represented in the behaviour ontology. This description is then translated into the simulation engine's language for execution. Notably, there is no evidence to suggest that the emergent behaviour observed in constituent systems aids in system design. Combinations of systems within the SoS contribute to overall capability and the emergent behaviours stemming from these combinations can enhance or diminish performance and impact costs.

Defining the boundaries of an SoS can be challenging, especially when constituent systems have different owners and support structures beyond SoS management. Understanding variable relationships and cause-and-effect connections within an SoS is essential for complex projects. Analysing these variables and relationships enables the application of findings on the emergence of complex systems in published papers to complex SoS project frameworks. The utilisation of data from a networked nodes to simulate various scenarios for testing and analysis is a topic open to discussion (Ko et al., 2000). Identifying areas where the safety and security of nodes exist as a system or subsystem is a common approach. Systems subjected to repeated cyclic use operate in deterministic cycles of work and pause. Maintenance occurs during pause periods. However, for future networked nodes, a new category of systems with complex operating modes is proposed. This complexity involves waiting for a system usage request and executing the request randomly upon arrival.

Operationalizing Fourth-Order Cybernetics in Digital Twin-Enabled Distributed Operational System (DOS)

While Fourth-Order Cybernetics provides a meta-framework for reflexivity, shared cognition and cultural framing, its practical instantiation within systems of systems (SoS) requires explicit operational mapping. Digital twins, when structured through the Viable System Model (VSM), serve as the conduit through which abstract cybernetic principles are translated into concrete mechanisms.

VSM Subsystem Mapping to Digital Twin Functions

- System 1 (Operations): Each physical or virtual subsystem is mirrored by a digital twin module that monitors real-time performance, sensor readings and task execution. Reflexivity is achieved as these modules autonomously adjust operational parameters in response to detected anomalies or environmental changes. Example: A communication operational node's twin detects increased packet loss and automatically reallocates bandwidth or re-routes traffic to maintain operational continuity.
- System 2 (Coordination): This layer manages interactions among S1 units. Digital twins coordinate load balancing, task allocation and resource prioritization across distributed agents, ensuring stability while preserving flexibility. Meta-cybernetic feedback loops operate here to detect patterns of inter agent friction and adjust coordination protocols. Example: During a simulated joint operation, the twin identifies conflicting navigation commands between unmanned surface vessels and adjusts priority rules to prevent operational nodes critical conflicts.
- System 3 (Control): S3 digital twins aggregate performance data from S1 units and S2 interactions to provide a holistic operational picture. Reflexive oversight allows the twin to identify deviations from operational doctrine or safety constraints. Example: A sudden surge in subsystem errors triggers S3 to suggest pre-emptive maintenance or reconfiguration strategies while communicating potential operational objective impacts to human operators.
- System 4 (Intelligence/Adaptation): S4 twins analyse environmental trends, disruptive behaviour and emerging threats. This subsystem implements forward-looking adaptation policies and scenario simulations, enabling strategic learning. Reflexivity and cultural framing are encoded as evaluative criteria: simulations incorporate both operational doctrine and ethical constraints. Example: An S4 twin predicts the risk of collateral effects in urban operations and adapts the deployment plan to minimize harm while maintaining operational objective.
- System 5 (Policy/Normative Governance): S5 provides normative oversight, resolving conflicts between operational imperatives and strategic objectives. Digital twins at this layer ensure alignment with ethical, legal and doctrinal constraints, acting as a meta-regulator of emergent behaviour. Example: If a distributed AI agent proposes an aggressive manoeuvre that could violate governance constraints the S5 twin overrides the action and records the rationale for future learning.

Meta-Cybernetic Feedback Loops and Emergent Behaviour Management

- Meta-cybernetic loops operate across these VSM layers, enabling digital twins to observe, evaluate and adapt both system behaviour and their own monitoring processes. This recursive mechanism allows the twin to:
- Detect shifts in operational doctrine or ethical constraints: By continuously comparing real-time actions against encoded doctrine, operational objective rules and ethical frameworks, the twin identifies when deviations occur and triggers adaptive responses.
- Differentiate beneficial versus destabilizing emergence: Machine learning and simulation-based analytics classify emergent patterns. Positive emergent behaviours, such as adaptive load balancing or opportunistic task reallocation are reinforced, while destabilizing patterns, such as cascading communication failures or coordination deadlocks, trigger

mitigation strategies.
- Implement adaptive governance: Insights from these loops inform S3–S5 interventions, including reconfiguration of control hierarchies, redistribution of resources and revision of agent coordination protocols.

Through this mapping, digital twins operationalize Fourth-Order Cybernetics by embedding reflexivity, shared cognition and cultural framing directly into system monitoring, prediction and decision-making processes. This approach ensures that reliability, resilience and ethical compliance are co-produced through continuous interaction between human and artificial agents in complex, dynamic operational high-stakes environments.

In addition to the cybernetic and multi-agent perspectives, insights from open innovation frameworks in service ecosystems provide a valuable lens for understanding adaptive governance and multi stakeholder coordination within DOS networks. Turoń (2025) develops a framework for implementing open innovation in shared mobility systems, highlighting the orchestration of heterogeneous actors including government, industry, academia and end-users within dynamic service ecosystems.

This framework emphasizes trust-building, structured co-creation and staged governance mechanisms, which closely align with the reflexive and shared cognition processes emphasized in Fourth-Order Cybernetics. The framework's stages ecosystem readiness, stakeholder engagement, co-creation, implementation and normative governance map conceptually onto the VSM's Systems 3–5 layers:

- System 3 (control) aligns with operational coordination,
- System 4 (intelligence) supports strategic scanning and environmental adaptation and
- System 5 (policy/norms) corresponds to normative governance and long-term alignment.

By integrating these insights, the DOS conceptual framework is enriched with practical mechanisms for adaptive coordination, iterative policy learning and co-created system reliability, ensuring that heterogeneous agents can collectively respond to emergent challenges while maintaining systemic coherence.

This integration highlights a bridge between abstract cybernetic theory and actionable operational pathways, illustrating how digital twin enabled DOS architectures can foster reflexive multi-agent governance, emergent behaviour management and strategic resilience (Turoń, 2025).

To address the reliability of deterministic systems with complex operating modes, an analytical model has to be formulated. This model shall present a ratio for the non-stationary total coefficient of operational readiness. It delineates system functioning during waiting and usage intervals, where these durations are random variables. The model considers three options for defining functions that govern waiting and execution time distributions. By leveraging this developed model, reliability and maintainability requirements for systems with complex operating modes can be effectively established. The model enables quantification and evaluation of reliability indicators, providing insights into system performance under various waiting and execution time distributions. This information guides decision making and sets appropriate reliability and maintainability standards for these systems. Through modelling, the interdependencies between operational reliability indicators and waiting/execution time distribution parameters can be examined. This analysis yields valuable insights into the impact of different distribution functions on system reliability performance. Based on these insights, recommendations can be formulated to substantiate reliability and maintainability requirements for systems with complex operating modes.

Simulation – reliability digital twin

Yes, it is possible to simulate reliability failures in SoS using digital twin technology. A digital twin represents a virtual replica of a physical object, process, or system, capturing real-time data for analysis, simulation and optimisation. It finds applications in diverse industries such as manufacturing, healthcare, transportation and energy. The deterministic failure schedule was selected to provide a controlled experimental baseline for analysing system behaviour. Future work will extend the model using stochastic failure distributions, disruptive event generation and agent-based behavioural variability to further explore emergent dynamics in complex systems of systems networks.

Ethical Considerations and Responsible AI in Digital Twin Enabled Distributed Operational System (DOS)

While the manuscript positions digital twins as reflexive agents within complex DOS networks, it is critical to examine the ethical implications and accountability boundaries associated with autonomous or semi-autonomous decision making. Digital twins frequently generate recommendations for adaptive reconfiguration, such as rerouting communication, reallocating loads, or prioritizing operational objective critical tasks. When these recommendations directly influence human operators' actions, clear accountability mechanisms must be established to ensure operational decisions remain ethically and legally defensible.

Digital twins operate in high stakes environments that may be targeted by adversaries seeking to manipulate decision loops, inject false data, or compromise coordination protocols. Robust cybersecurity, anomaly detection and fail-safe reversion mechanisms are essential to maintain system integrity and prevent destabilizing emergent behaviours.

Embedding resilience and redundancy into digital twin architectures, guided by VSM recursive monitoring, ensures that both operational continuity and ethical compliance are preserved even under disruptive influence.

Responsible AI Frameworks

Engaging with emerging responsible AI frameworks in systems of systems reinforces the societal relevance of digital twin enabled DOS. Key principles include:
- Human cantered governance: Systems should support human decision-making rather than supplant it, preserving accountability and operational discretion.
- Transparency and explainability: Decision logic, particularly in adaptive reconfiguration, must be interpretable to operators, planners and regulators.
- Ethical alignment: Operational outputs should be continually evaluated against operational objective, ethics, international law and strategic doctrine, with reflexive mechanisms to correct deviations.
- Continuous learning with safeguards: Digital twins' learning algorithms must incorporate constraints to prevent reinforcement of harmful patterns and mitigate emergent risks.

By incorporating these frameworks, DOS architectures move

beyond purely technical reliability to responsible, ethically aware operational governance, aligning the reflexive capabilities of digital twins with societal and doctrinal norms. This approach ensures that reliability, adaptability, operational objective and effectiveness are co-produced with accountable, ethically sound and resilient decision-making processes, addressing the critical tensions inherent in autonomous DOS.

ASSETSTUDIO SOFTWARE™ Data Driven Decisions (Reliability and Operation Simulation).

Platform Independence and Conflict of Interest Clarification

The simulation environment employed in this study was implemented using the AeROS™ (Asset Reliability and Operations Simulation) platform. AeROS™ is a digital twin–enabled modelling environment designed to support the analysis of system reliability, maintenance strategies and operational performance through statistical and system-level simulation techniques. It enables the representation of repairable and non-repairable components, redundancy configurations, spare provisioning and system availability metrics within a virtual environment tailored for reliability and operational analysis.

Given that one of the authors contributed to the design and development of the AeROS™ platform, a potential conflict of interest is acknowledged. To mitigate any associated bias and to ensure methodological transparency, the modelling approach adopted in this study was intentionally developed to be platform independent. The analytical framework is grounded in widely established and broadly adopted reliability engineering constructs, including reliability block diagrams, Failure Modes and Effects Criticality Analysis (FMECA), stochastic failure modelling and discrete-event system simulation. These methods are foundational within reliability engineering and are not unique to any single software implementation (IEC 60812, 2018; Stamatis, 2003).

To further substantiate the platform agnostic nature of the approach, the modelling methodology was conceptually aligned with established reliability and digital twin simulation high-stakes environments used in engineering practice. For instance, reliability, availability, maintainability and productivity (RAMP) tools employ probabilistic failure distributions and repair models to evaluate complex system behaviour under operational constraints. Similarly, other industrial reliability analysis platforms and discrete event simulation high-stakes environments utilise comparable constructs, including component level failure logic, interdependencies and resource-constrained maintenance processes. Across these platforms, the analytical outcomes are driven primarily by the underlying modelling assumptions, probability distributions and system structure rather than the specific software implementation.

Accordingly, the digital twin architecture developed in this study was structured to be reproducible across alternative simulation high-stakes environments. The core modelling elements include:

- System representation through interconnected network nodes and functional relationships.
- Failure behaviour characterised using probabilistic distributions or scenario-based disturbance injection.
- Evaluation of system level performance metrics such as availability, recovery time and operational objective impact. The scenario driven simulation is to assess system response under varying operational and failure conditions. These elements are consistent with general purpose modelling paradigms and can be implemented within a range of reliability engineering tools, agent-based simulation frameworks, or system dynamics platforms.

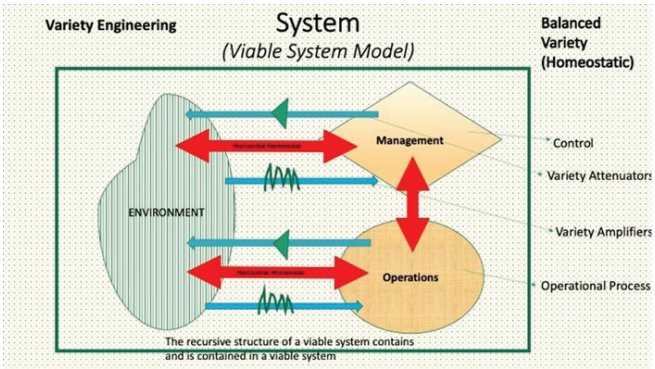
From a research integrity perspective, the use of AeROS™ in this study should therefore be understood as an implementation choice rather than a methodological dependency. The primary contributions of the work namely, the integration of digital twin modelling with cybernetic feedback concepts and emergent behaviour analysis within a systems of systems reliability context

AeROS™ is the simulation software program that creates a digital twin of a production system for predictive analysis using statistical methods. This digital twin predicts future outcomes, especially focusing on production uncertainties and how asset performance and maintenance affect production. Key features include analysing production impacts identifying improvement opportunities, optimising resources and inventory and supporting various analyses like Cost-Benefit and Queueing. AeROS™ is unique for supporting repairable and non-repairable life models, offering redundancy management and storage functions and providing comprehensive visualisations for better analysis. It stands out for its ability to optimise reliability and allocation for enhanced system performance.

To support reproducibility and transparency, the modelling assumptions, system structure, and reliability parameters have been explicitly documented within this study. This ensures that the simulation experiments and analytical outcomes can be replicated, validated, or extended using alternative reliability and digital twin simulation platforms without loss of methodological fidelity (Grieves & Vickers, 2017; Hollnagel et al., 2006).

'Reliability and Operation Simulation' provides a mathematical approach to convert historical data into useful information to achieve the desired product performance resulting in the optimum financial health of a production asset.

Figure 1 Viable System Model (VSM) Variety Engineering (Ackoff, R. 2010).

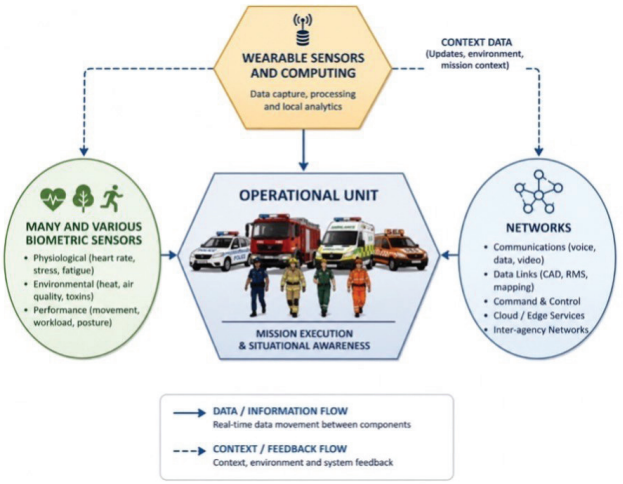


are independent of the specific simulation platform utilised. The theoretical and methodological constructs are transferable and do not rely on proprietary features of the AeROS™ environment.
Variety and value engineering (figure 1) in SoS and digital twin involves optimising complex interconnected systems and their virtual counterparts. Variety engineering in SoS and digital twin focuses on creating a diverse range of system configurations and variations to address different stakeholder needs. It involves managing subsystems, interfaces and components to enable flexibility and customisation within the interconnected systems.

Integration with Digital Twin Analysis

Within the digital twin environment, uncertainty analysis is particularly important because operational conditions evolve dynamically. The twin therefore continuously recalibrates reliability estimates based on observed system behaviour and simulated stress scenarios. This enables the digital twin not only to estimate system reliability but also to anticipate the impact of potential disruptions and support adaptive decision-making within the cybernetic control framework.

Figure 2 - Node network sensors and communication (Ackoff, 2010; Yolles et al 2021).



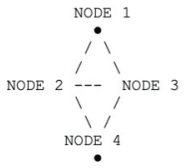
Figures 1 and figure 2 can be linked in the explanation and represent a small sample of systems of systems (SoS) in the perational environment layer and are modelled and simulated in this chapter, Viable System Model (VSM) Variety Engineering (figure 1). For the digital twin simulation example, the model incorporates only node based components, such as sensors and communication elements, within the simulation environment. The following figures present the process in reliability digital twin analysis based on the scenario in this manuscript (figure 3).

Figure 3 – Summary of Figures

Figure	Title / Focus	Conceptual Structure	Key Insights
Figure 4	Distributed Operational System (DOS) Network Architecture and Failure Propagation	Four interconnected Operational nodes forming a network	Shows distributed communication, node interdependence, and pathways for failure propagation in a system of systems environment
Figure 5	Operational Effectiveness of the Distributed Operational System (DOS) Operational node Network	Four-node Operational node network with one node failing (X)	Demonstrates resilience: despite one node failing, network maintains partial effectiveness via redundant links
Figure 6	Digital Twin Simulation and Reliability Monitoring Architecture	Physical system → Digital twin model → Coordination and governance system	Illustrates real-time monitoring, failure simulation, predictive reliability and operational effectiveness evaluation using digital twins

Figure 4 – Systems of Systems Network Architecture and Failure Propagation

Conceptual Structure:



Concept Explanation:

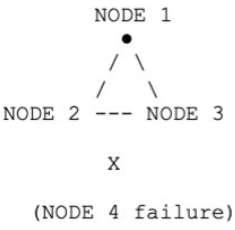
This conceptual diagram represents the baseline architecture of a Systems of Systems network consisting of four interconnected nodes. Each node corresponds to an operational platform equipped with communication systems, sensors and situational awareness tools (figure 4).

Key points illustrated:
- Distributed communication links between operational units
- Interdependence among nodes in the system
- Failure propagation pathways, highlighting how disruptions in one node can affect the network

This topology establishes a foundational system-of-systems framework for analysing reliability and operational effectiveness (Figure 4).

Figure 5 – Operational Effectiveness of the Systems of Systems Network

Conceptual Structure:



Legend:

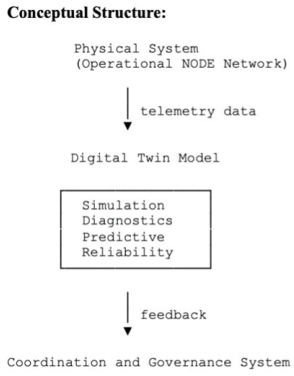
- ● Operational node
- X Non-operational node

Concept Explanation:

This figure demonstrates system performance degradation following a node failure within the node network:
- Three nodes remain operational, maintaining partial functionality
- One node becomes non-operational, simulating a failure scenario
- Dynamic communication reconfiguration allows the network to maintain connectivity

This illustrates that system effectiveness emerges from network resilience, not merely the reliability of individual nodes or components. The network adapts to failures through redundancy and the re-routing of communication links (Figure 5).

Figure 6 – Digital Twin Simulation and Reliability Monitoring Architecture



Concept Explanation:

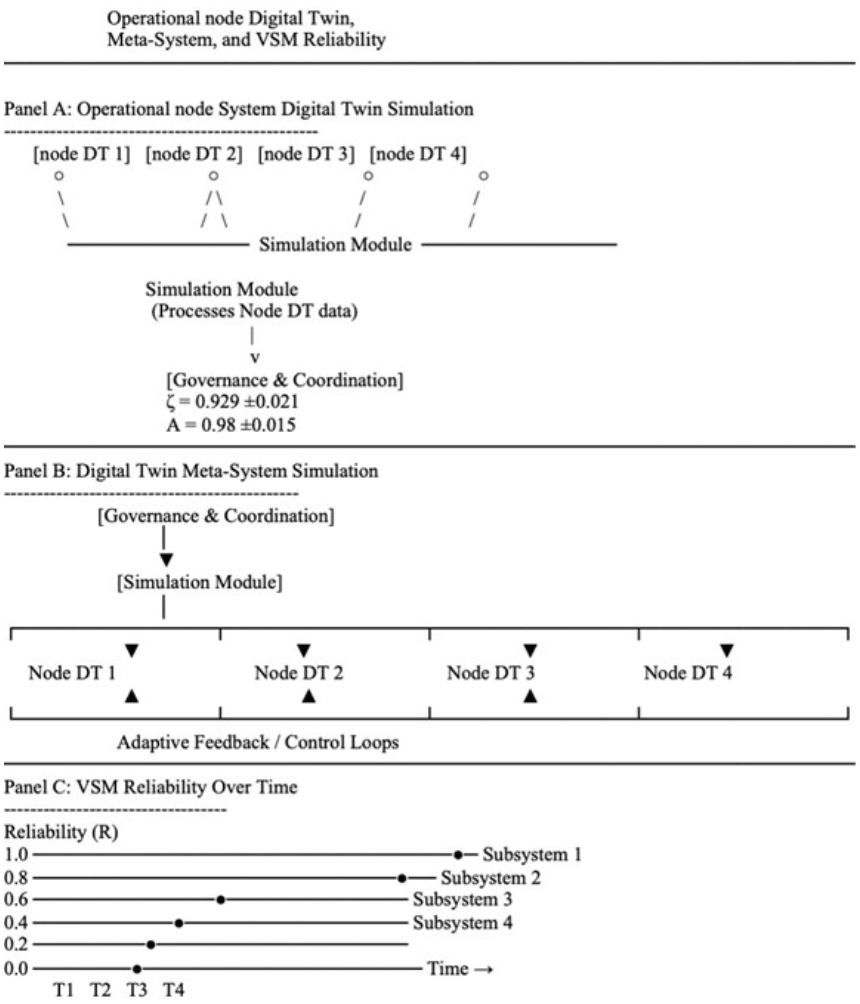
This figure depicts the digital twin architecture applied to node networks:

- Real-time monitoring of the node network
- Simulation of failure scenarios to test system resilience
- Predictive reliability modelling to anticipate potential disruptions
- Operational effectiveness evaluation through virtual replication of network states

Continuous telemetry feeds allow the digital twin to provide a virtual representation of the operational system, enabling anticipatory decision making and evaluation of corrective measures before failures propagate (figure 6).

In the context of the digital twin, variety engineering involves designing virtual models that accurately represent the variations and configurations of the physical systems. Value engineering in SoS and digital twin aims to maximise the value and benefits derived from the interconnected systems. It involves analysing functions, performance, costs and risks to optimise resource allocation, minimise redundancies and enhance the overall value proposition. In the digital twin context, value engineering focuses on using virtual models to simulate and optimise the performance, reliability, scalability and sustainability of physical systems (Figure 6 and 6A).

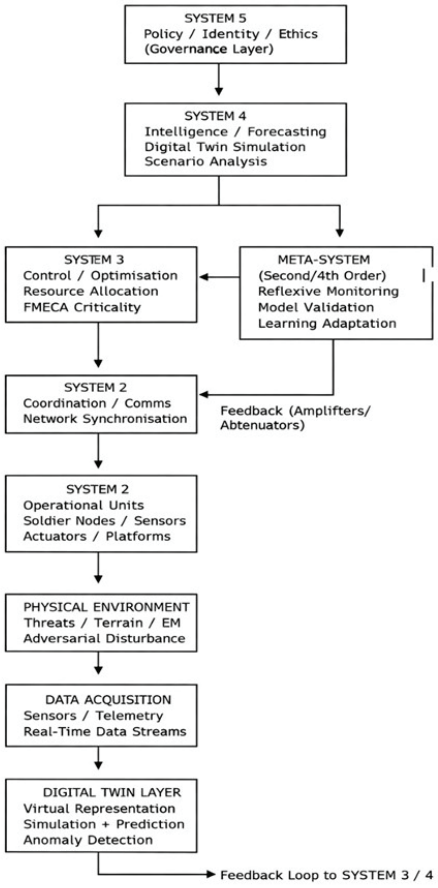
Figure 6A- Multi-Layer Digital Twin and VSM Reliability



Legend:
- ○ = Node - Digital Twin node
- Rectangles = Simulation Modules
- Arrows = Data Flow
- Dashed / Curved arrows = Adaptive Feedback
- Lines = Subsystem reliability over time
- Areas = Monte Carlo stochastic envelope

The figure 6A presents a conceptual digital twin architecture integrating operational node simulations, meta-system governance and the Viable System Model (VSM) to enhance reliability and resilience within distributed operational systems. Individual node digital twins feed operational data into a simulation module, where governance and coordination mechanisms evaluate system behaviour and performance. At the meta-system level, adaptive feedback and control loops continuously coordinate and regulate node interactions, enabling the architecture to dynamically respond to disruptions and maintain operational continuity. The final panel demonstrates that reliability progressively improves over time across multiple subsystems, illustrating how cybernetic governance, digital twin simulation and adaptive control collectively strengthen network resilience, reduce cascading failures and support sustained system viability in uncertain and high-stakes operational environments.

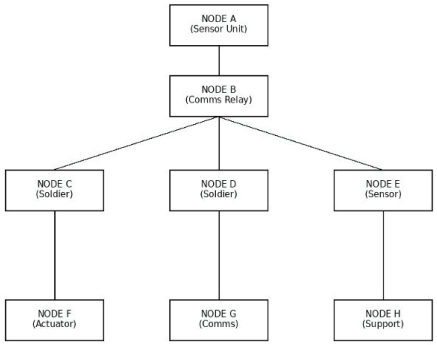
Figure 7: Meta-system cybernetic feedback model



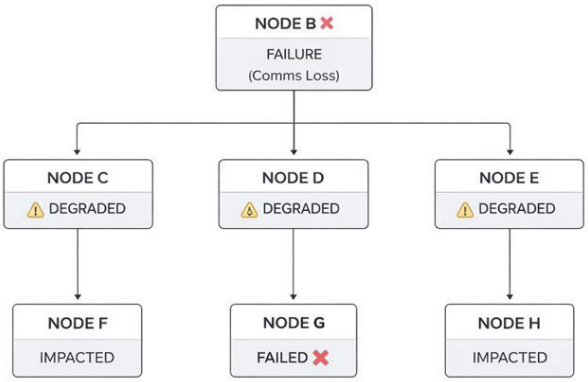
In figure 7, the cybernetic and Viable System Model (VSM) based digital twin architecture designed to improve adaptive coordination, forecasting and resilience within distributed operational environments. The framework is organised hierarchically, beginning with governance and policy oversight at System 5, followed by System 4, which performs intelligence analysis, forecasting, scenario modelling and digital twin simulation to support strategic decision-making. Operational control functions are managed through System 3, which oversees optimisation, resource allocation and criticality assessment, while the Meta-System provides reflexive monitoring, model validation and adaptive learning capabilities. System 2 coordinates communication, synchronisation and operational integration across distributed nodes such as sensors, actuators, platforms and operators interacting within contested physical environments. Real-time telemetry and sensor data are collected through the data acquisition layer and processed within the digital twin layer, where virtual representations enable prediction, anomaly detection and simulation. Continuous feedback loops connect the digital twin environment back to higher-order control systems, allowing the architecture to dynamically adapt to changing operational conditions.

The framework (figure 7) demonstrates how integrating digital twins, cybernetic governance, adaptive feedback mechanisms and VSM principles can create a self-regulating, resilient and intelligent distributed operational system capable of responding effectively to uncertainty, disruptions and adversarial environments.

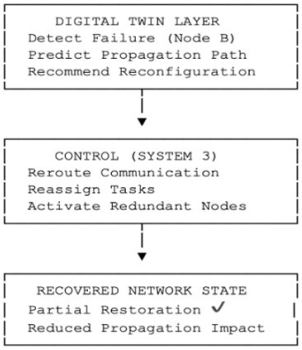
Figure 8 – Failure Propagation in Network Nodes (Schematic)



FAILURE PROPAGATION SCENARIO



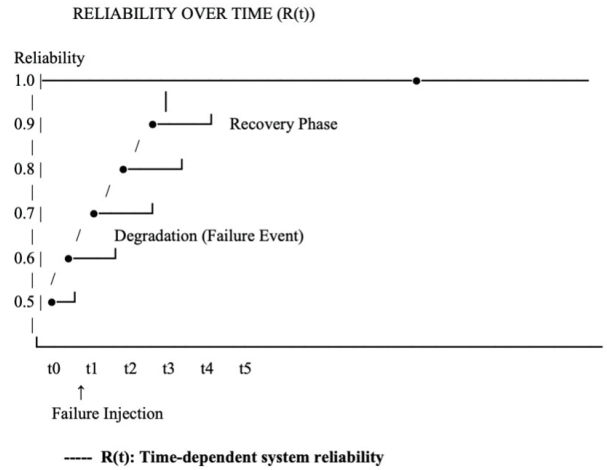
DIGITAL TWIN + CONTROL RESPONSE



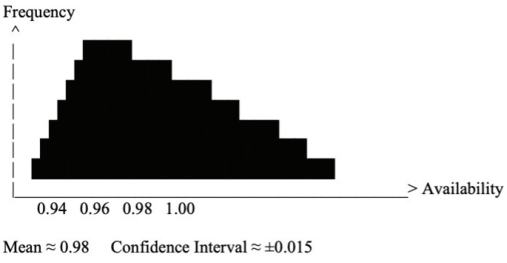
LEGEND: Network Node Classification, States, Flows and Control Elements

Category	Element	Description
Node Types	Sensor	Data acquisition component
	Soldier	Operational agent within the network
	Comms	Communication relay node
	Actuator	Execution system performing actions
States	✕ Failed	Primary fault condition
	⚠ Degraded	Reduced performance or partial functionality
	Impacted	Secondary effect due to upstream failure
Flow Types	Communication Flow	Solid lines representing data exchange
	Failure Propagation	Downstream spread of faults across nodes
Control Elements	Digital Twin	Detection, prediction, and system monitoring
	System 3 (VSM)	Corrective control and internal regulation
	Recovery Mechanism	Adaptive reconfiguration of the network

Figure 9 – Reliability Simulation Outputs (Schematic)

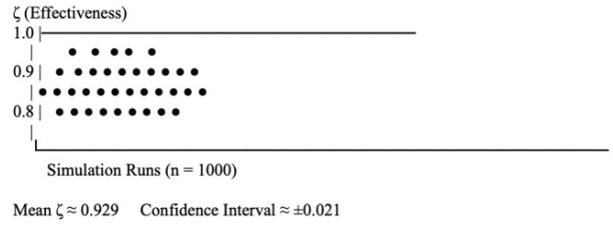


SYSTEM AVAILABILITY (A) DISTRIBUTION



--- A: System availability (Monte Carlo distribution)

OPERATIONAL EFFECTIVENESS (ζ) – MONTE CARLO



----- ζ (zeta): Operational effectiveness metric

To evaluate system behaviour under varying operational conditions, additional simulation scenarios were introduced including:

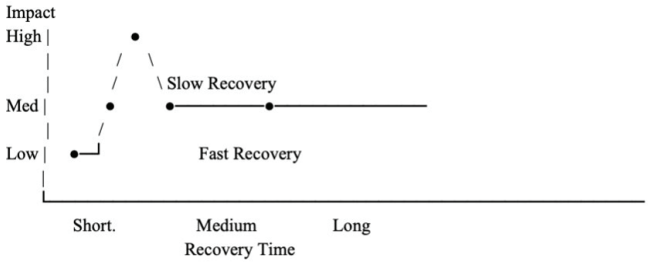
- increased failure rates under operational stress conditions
- delayed maintenance response times
- partial loss of network connectivity
- uncertain disruption of communication nodes

Across these scenarios, operational effectiveness remained above ζ = 0.90 in most configurations, demonstrating that the digital twin supported coordination architecture maintains robust performance even under degraded operational conditions.

Monte Carlo Simulation - To assess the variability of system performance under uncertain operating conditions, the digital twin simulation environment was extended to perform Monte Carlo experimentation. In this approach, key reliability parameters including component failure rates, repair times and communication delays were treated as stochastic variables following probability distributions derived from reliability engineering practice (Ebeling, 2010; O'Connor & Kleyner, 2012).

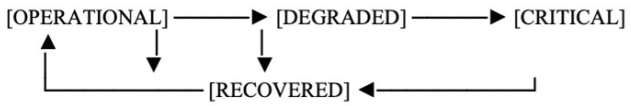
For each scenario, the simulation was executed over N = 1,000 independent runs, generating distributions for both operational effectiveness (ζ) and system effective availability (A). This approach enables the evaluation of statistical dispersion and robustness of the reported metrics.

FAILURE IMPACT VS RECOVERY TIME



●: Simulation data points

NETWORK RELIABILITY STATE TRANSITIONS



Transition Drivers:
- Fault Injection (FMECA)
- Communication Loss
- Adaptive Reconfiguration (Digital Twin)

Transition Drivers:
- Fault Injection (FMECA)
- Communication Loss
- Adaptive Reconfiguration (Digital Twin)

This integrated framework (Figure 9) demonstrates how digital twin simulation, adaptive governance and cybernetic control mechanisms enhance operational reliability and resilience within distributed systems. Reliability may initially decline following a disruption or failure event, however, adaptive recovery processes enabled through digital twin modelling, meta-system coordination and continuous feedback progressively restore system performance over time. The framework further shows that systems with faster recovery mechanisms experience reduced operational impact and improved continuity, whereas slower recovery processes prolong vulnerability and degradation. Through predictive simulation, adaptive learning, coordinated control and real-time feedback, the architecture supports dynamic reconfiguration, rapid failure response and sustained operational stability in uncertain and contested environments.

Confidence Interval Estimation

Monte Carlo simulation results were used to estimate confidence intervals for the key operational performance metrics.

The operational effectiveness measure ζ\zetaζ was estimated as: ζ= 0.929 ± 0.021. (95% confidence interval)

Similarly, system effective availability A was estimated as: A= 0.98 ± 0.015 (95% confidence interval)

These results indicate that the system maintains high operational reliability and availability, even under variability in failure rates and repair conditions.

Figure 10 – Operational Node Digital Twin Simulation (Schematic)

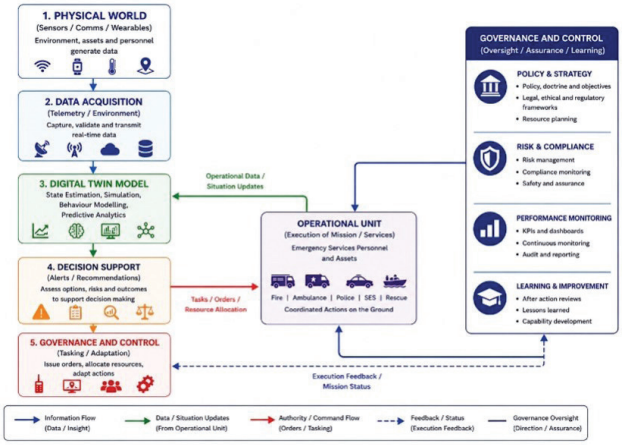


Figure 10 illustrates an integrated digital twin and governance architecture for operational decision-making and emergency response coordination. Data from the physical environment is collected through sensors, communications and telemetry systems, then processed within a digital twin model for simulation, predictive analysis and situational awareness. The system supports decision-making by generating alerts, recommendations and resource allocation options, which are translated into operational tasks and commands. Governance and control functions provide oversight through policy, risk management, performance monitoring and continuous learning, while feedback loops from operational units enable adaptive coordination, resilience and ongoing system improvement.

Figure 11 – Distributed Operational System (DOS) Effective Reliability (Schematic)

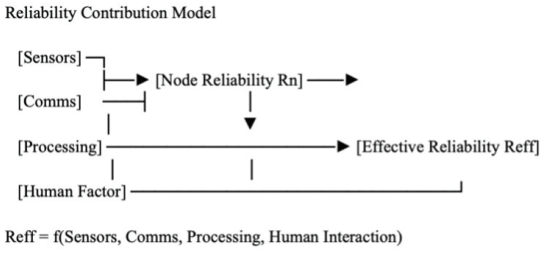
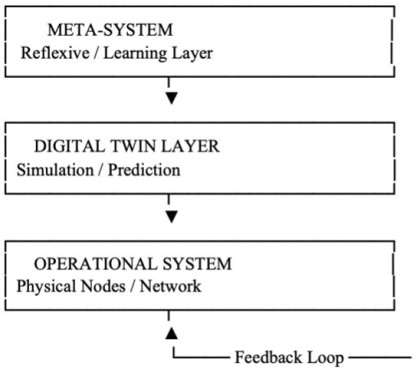


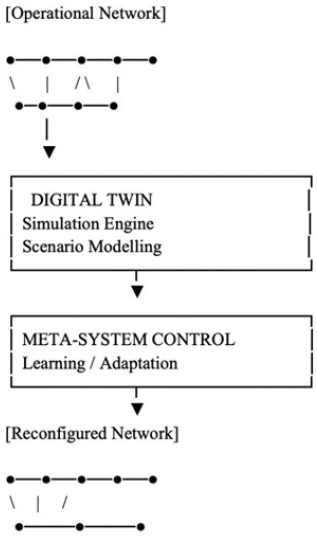
Figure 11 illustrates a reliability contribution model where overall effective reliability is influenced by the combined performance of sensors, communications, processing systems and human interaction. These components contribute to node reliability, which in turn affects the system's effective reliability, demonstrating that operational reliability emerges from both technical and human factors operating together within the network.

Figure 12 – Digital Twin Meta-System Architecture (Schematic)



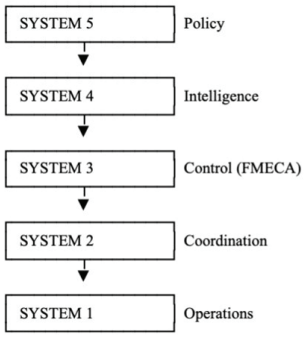
Within the digital twin environment, uncertainty analysis is particularly important because operational conditions evolve dynamically. The twin therefore continuously recalibrates reliability estimates based on observed system behaviour and simulated stress scenarios (figure 12). This enables the digital twin not only to estimate system reliability but also to anticipate the impact of potential disruptions and support adaptive decision-making within the cybernetic control framework.

Figure 13 – Digital Twin Meta-System Simulation (Schematic)



The figure 13 demonstrates how an operational network can use digital twin simulation and meta-system learning to achieve adaptive reconfiguration and resilience. Operational network data is fed into a digital twin environment where simulation and scenario modelling analyse system behaviour and potential disruptions. A meta-system control layer then applies learning and adaptation processes to evaluate network performance and determine corrective actions. The outcome is a reconfigured network capable of dynamically adjusting connections and maintaining operational continuity in uncertain or contested environments.

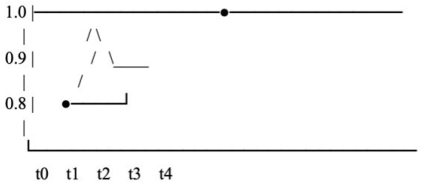
Figure 14 – VSM Reliability Analysis Construction (Schematic)



Reliability Feedback: System 1 → 5 (recursive loop)

The figure 14 summarises the Viable System Model (VSM) hierarchy, showing how operational activities (System 1) are coordinated (System 2), controlled and optimised through FMECA (System 3), informed by intelligence and forecasting (System 4) and governed by overarching policy and strategic direction (System 5).

Figure 15 – VSM Reliability Over Time (Schematic)
Reliability (VSM Integrated)

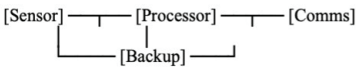


Adaptive recovery driven by System 3–4 feedback

- Dynamic reliability degradation and recovery

Figure 15 illustrates adaptive system recovery enabled through feedback mechanisms between System 3 and System 4 within the Viable System Model (VSM). Following a degradation or disruption in reliability, the system progressively restores performance through intelligence, coordination and control feedback processes. The figure demonstrates how adaptive governance and higher-level feedback loops support rapid recovery, stabilisation and the return of system reliability toward optimal operational levels over time.

Figure 16 – Reliability Block Diagram (RBD) – Operational Node 1 in Distributed Operational System (DOS)



System Reliability:

Series + Parallel Hybrid Structure

Figure 16 illustrates a simplified operational node architecture consisting of interconnected sensor, processor and communication components. The diagram also includes a backup pathway, demonstrating redundancy within the system architecture. This redundancy enables continued operation and resilience by maintaining functionality if the primary processing or communication pathway is disrupted or degraded.

Figure 17 – Simulation Workflow (Schematic)

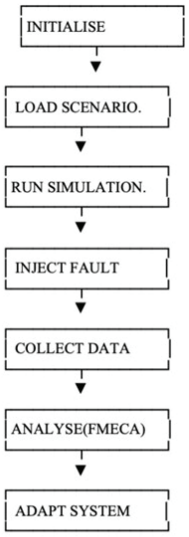
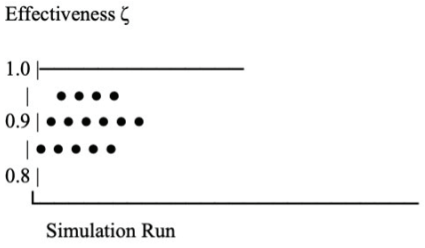


Figure 17 presents the workflow of an adaptive digital twin simulation and analysis process. The sequence begins with system initialisation and scenario loading, followed by simulation execution. A fault is then intentionally injected into the system to evaluate behaviour under disrupted conditions. Operational data is collected and analysed using FMECA techniques to identify failures, vulnerabilities and critical impacts. Based on the analysis results, the system adapts its configuration or behaviour to improve resilience, recovery and overall operational performance.

Figure 18 – Meta-System Operational Effectiveness (Schematic)



Mean ζ ≈ 0.929

The reported operational effectiveness (ζ = 0.929) and system effective availability (A = 0.98) represent mean values derived from stochastic simulation experiments. Monte Carlo analysis across 1,000 simulation runs produced 95% confidence intervals of ±0.021 and ±0.015 respectively, indicating that the system maintains high reliability across a range of operational uncertainty conditions. The authors highlight the need for uncertainty quantification in the evaluation of the operational effectiveness (ζ = 0.929) and system effective availability (A = 0.98) metrics. In the initial submission these values were presented as representative outputs from the simulation environment. To strengthen the statistical robustness and reproducibility of the results, the revised manuscript now incorporates a set of uncertainty analysis procedures including Monte Carlo simulation, sensitivity analysis and confidence interval estimation. The figure indicates stable and reliable system performance across varying simulation conditions, supporting the effectiveness of the adaptive digital twin and resilience framework.

Figure 19 – System Effective Availability (Schematic)

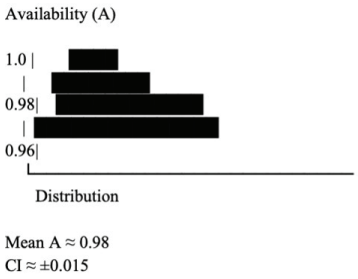


Figure 19 illustrates the distribution of system availability (AAA) across simulation outcomes. The results show consistently high availability levels centred around a mean value of approximately 0.980.980.98, with a confidence interval of ±0.015\pm 0.015±0.015. This indicates that the system maintains stable operational availability and demonstrates strong reliability and resilience under varying simulation conditions.

Sensitivity Analysis

A parameter sensitivity analysis was conducted to determine which system variables most strongly influence operational performance.

The parameters evaluated included:

- component failure rate (λ)
- mean time to repair (MTTR)
- communication latency between nodes
- coordination delay in coordination and governance structures
- redundancy levels within the network architecture

The results show that mean time to repair and communication latency have the largest impact on system effectiveness, while redundancy within the network architecture significantly improves resilience against cascading failures. These findings are consistent with reliability engineering literature demonstrating that repair logistics and communication reliability are critical determinants of operational objective and availability in distributed systems (Blanchard & Fabrycky, 2011). The sensitivity analysis evaluates how variations in coordination, governance and operational effectiveness influence overall system reliability and resilience within the digital twin-enabled operational architecture. The analysis demonstrates that system performance is highly dependent on the interaction between governance coordination mechanisms and operational execution across distributed nodes. Results indicate that improvements in coordination and governance significantly enhance operational effectiveness, leading to increased reliability, faster recovery and improved adaptive response capability. Conversely, reductions in governance efficiency or coordination quality increase system vulnerability, degrade operational performance and prolong recovery following disruption events. The analysis further highlights that adaptive feedback loops, digital twin simulation and meta-system control reduce sensitivity to localised node failures by enabling dynamic reconfiguration and real-time corrective actions. Systems incorporating stronger coordination and learning mechanisms exhibit greater stability and maintain higher levels of operational continuity under uncertain and contested conditions. The sensitivity analysis confirms that governance quality, adaptive coordination and feedback responsiveness are critical drivers of resilience, reliability and sustained operational effectiveness within distributed operational systems.

Results

The simulation experiments conducted within the digital twin-enabled DOS environment provide empirical insights into the behaviour of complex systems of systems under varying operational conditions. The results demonstrate how reliability, coordination and operational effectiveness emerge from the interaction of distributed subsystems and how these properties are influenced by disturbance events, network structure and adaptive feedback mechanisms.

The digital twin simulation (Figure 10) illustrates the baseline operational architecture in which individual node network operate as interconnected nodes within a dynamic network. Under nominal conditions, the system maintained high levels of connectivity and coordination, with stable communication pathways and consistent task execution across nodes. Reliability analysis at this stage indicated that system performance was not solely dependent on individual node functionality but on the integrity of communication relationships across the network. This observation is further supported by the effective reliability profile (Figure 11), which demonstrates that system reliability remains stable under low disturbance conditions but exhibits sensitivity to variations in communication latency and node availability (figure 9).

The introduction of disturbances through FMECA driven fault injection revealed significant nonlinear effects in system behaviour. The digital twin meta-system simulation (Figure 13) shows how localised failures propagate through the network, producing cascading disruptions that affect multiple subsystems simultaneously. In several scenarios, failures originating in communication nodes resulted in disproportionate impacts on coordination efficiency, highlighting the structural importance of certain nodes within the network topology (figure 9). This behaviour is consistent with systems of systems dynamics, where interdependencies between components amplify the effects of local disruptions (figure 8).

The meta-system analysis (Figure 14) further demonstrates how cybernetic control structures regulate system behaviour through feedback mechanisms. The Viable System Model (VSM) architecture enabled the system to detect disturbances, assess their impact and initiate corrective actions through coordination and control layers. These adaptive responses included reallocation of tasks, rerouting of communication pathways and prioritisation of critical operations. As a result, the system exhibited partial recovery in many scenarios, with performance stabilising after initial disruption phases. This adaptive behaviour highlights the role of recursive feedback in maintaining system viability under dynamic conditions.

Temporal analysis of system reliability (Figure 15) indicates that reliability is not a static measure but evolves continuously in response to operational conditions. During disturbance events, reliability trajectories showed rapid degradation followed by gradual recovery as adaptive mechanisms were activated. The rate and extent of recovery varied depending on the nature of the disturbance and the availability of alternative communication pathways. Systems with higher network redundancy and more effective coordination mechanisms demonstrated greater resilience, supporting the interpretation of reliability as an emergent property of system structure and interaction.

The reliability block diagram analysis (Figure 16) provides further insight into subsystem dependencies and failure propagation pathways. This analysis revealed that certain subsystems function

as critical hubs within the network, where failures have a disproportionately large impact on overall system performance. In particular, the communication and coordination subsystems were identified as key determinants of system reliability, as disruptions in these areas significantly reduced the system's ability to maintain synchronised operations. These findings align with the extended FMECA results, which identified high propagation potential and coordination impact as key indicators of failure criticality.

Simulation outputs (Figure 17) demonstrate the variability of system performance across different operational scenarios. Under moderate disturbance conditions, the system maintained acceptable levels of performance through adaptive reconfiguration. However, under high-intensity disturbance scenarios particularly those involving simultaneous faults and disruptive interference the system exhibited significant degradation in coordination efficiency and operational performance. These results highlight the limits of system adaptability and underscore the importance of robust design and redundancy in maintaining operational effectiveness.

The meta-system operational effectiveness analysis (Figure 18) quantifies the overall performance of the system under varying conditions. The results indicate a mean operational effectiveness of $\zeta = 0.929$, reflecting a high level of system functionality despite the presence of disturbances. Similarly, system effective availability (Figure 19) was calculated as $A = 0.98$, indicating that the system remained operational for the majority of the simulation period. Monte Carlo simulation across 1,000 runs produced narrow confidence intervals (± 0.021 for operational effectiveness and ± 0.015 for availability), demonstrating the robustness and consistency of system performance across a range of stochastic conditions.

Overall, the results confirm that reliability in complex systems of systems emerges from the interaction of technical components, communication networks and cybernetic control structures. The integration of digital twin simulation with FMECA analysis provides a powerful framework for capturing these dynamics, enabling the identification of critical failure modes, the analysis of cascading effects and the evaluation of adaptive response mechanisms. These findings provide empirical support for the conceptual framework developed in this study and establish a foundation for further exploration of cybernetic approaches to reliability in DOS environments.

Conclusions

Recent research in evolutionary game theory and computational multi-agent systems provides valuable theoretical and methodological parallels for the study of digital twin enabled SoS. For example, Zhang et al. (2025) present a comprehensive review of evolutionary game theory applied to electricity market optimization, addressing strategic interactions among heterogeneous agents under regulatory uncertainty. Their work demonstrates how multi-agent coordination, demand supply equilibrium and adaptive policy design through evolutionary dynamics can achieve stable coordination strategies in complex, dynamic distributed operational environments. These concepts are directly relevant to DOS contexts, where distributed subsystem agents must coordinate under uncertain operational conditions.

Similarly, Wang et al. (2025) systematically review computational game theoretic models for adaptive urban energy systems, integrating reinforcement learning with multi-agent approaches to support resilient system management. Their frameworks for dynamic pricing, load management and collective decision making under uncertainty offer methodological insights for DOS architectures, in which heterogeneous autonomous agents must adaptively coordinate under uncertain conditions and emergent system behaviours.

Liu et al. (2025) analyse game theoretic evolution in decentralized renewable energy systems, emphasizing evolutionarily stable strategies and replicator dynamics. The study's findings on strategy adaptation under decentralized decision making and environmental uncertainty provide a strong conceptual analogue for the DOS reliability framework, highlighting how subsystem agents can independently evolve strategies while maintaining overall system level coherence and operational viability.

Finally, Chen et al. (2025) develops evolutionary smart contracts that integrate prospect theory with multi-stage negotiation for virtual power plant trading across regional markets. Their framework considers behavioural heterogeneity, adaptive contract mechanisms responsive to environmental evolution and cross-regional coordination barriers. These insights inform the design of adaptive reconfiguration and behavioural learning mechanisms within digital twin-enabled DOS, particularly regarding agent-based learning, policy adaptation and operational resilience.

Digital Twins, Reliability and Meta-System Control in Systems of Systems

In contemporary SoS architectures, particularly those underpinning node centric networks, digital twins represent a paradigm shift in the conceptualisation of reliability, adaptability and operational effectiveness. When integrated with Fourth-Order Cybernetics and the Viable System Model (VSM), digital twins extend beyond their traditional role as representational artefacts to become dynamic mechanisms for systemic cognition, coordination and adaptive governance (Ackoff, R. 2010).

Rather than merely mirroring physical states, these digital twins engage in ongoing dialogue with operators, management and control systems, facilitating collective sensemaking and enabling real-time adaptation to emergent operational objective dynamics. Each node, equipped with wearable sensors and embedded within robust communication architectures, contributes to a distributed sensor actuator framework. This digital mesh processes real-time physiological, environmental and local adaptive response data, enabling recursive observation and adaptive reconfiguration (Tao et al., 2019; Fuller et al, 2020); Adams et al, 2014).

Traditional reliability engineering paradigms often reliant on static failure modelling and redundancy-based planning are insufficient in such dynamic DOS environments. Digital twins enable continuous health monitoring, predictive diagnostics and simulation driven anticipatory analytics. Here, reliability is no longer a static attribute, but an emergent system property governed by the recursive interplay of real-time data processing, feedback regulation and operational objective aware structural adaptation (Lee et al, 2018; Madni et al, 2014; Mittal, S. (2017).

Practically, digital twins simulate failure propagation and adaptive reconfiguration within node networks, identifying system vulnerabilities and recalibrating to preserve functional integrity. For instance, when a node fails (figure 9), digital twin logic supports intelligent redistribution of tasks, rerouting communications and triggering pre-defined redundancy protocols (Fuller et al, 2020; Grieves & Vickers, 2017; Tao et al., 2019).

VSM principles provide the organisational scaffolding required

for this cybernetic orchestration. Systems 1 through 5 correspond to core operational units, coordination mechanisms, performance regulation, environmental scanning and governance. Digital twins actively interface with Systems 3 (operational control), 4 (future intelligence) and 5 (strategic oversight), enabling cybernetic alignment between real-time execution and long-term viability (Beer, 1979; Espejo & Reyes, 2011). This interface facilitates value engineering through continuous balancing of performance outputs, resource allocations and operational objective imperatives (Ackoff, 2010; Yolles et al 2021).

Beyond structural integration, digital twins embody second order and fourth-order cybernetic attributes. As part of a meta-system, they serve as regulatory observers of observers, managing systemic variety and shaping the cognitive frames through which operational environment dynamics are interpreted. Amplification and attenuation functions within digital twin architectures serve to modulate information flows, enabling real-time complexity matching in accordance with Ashby's Law of Requisite Variety (Beer, 1979).

The recursive embedding of digital twins within the VSM's structural layers facilitates a holistic perspective on system health, emergent operational risk and cascading failure. Such architecture enables proactive maintenance and resilience strategies that operate across both the local adaptive response and strategic dimensions of systems of systems logistics.

Moreover, by synthesising heterogeneous data from embedded sensors, simulations and operational histories, digital twins underpin predictive reliability analytics. Leveraging machine learning and systems dynamics, they identify degradation patterns and emergent failure modes prior to their manifestation in the physical domain. This predictive capability is operational objective critical, particularly in high-stakes SoS where system failure can result in catastrophic consequences (Mittal, S. (2017).

This study has demonstrated that the integration of digital twin technologies with cybernetic frameworks particularly Fourth-Order Cybernetics and the Viable System Model (VSM) represents a paradigmatic shift in the conceptualisation and management of reliability within systems of systems (SoS) Within this framework, reliability is no longer treated as a static, component level attribute measured through conventional metrics such as mean time between failures (MTBF), but instead emerges as a dynamic, system level property co-produced through recursive feedback, behavioural interaction and adaptive coordination across heterogeneous agents (Grieves & Vickers, 2017; Tao et al., 2019).

By embedding digital twins within system of systems (SoS) architectures, the study shows how real-time synchronisation between physical and virtual DOS environments enhances systemic observability, supports predictive analysis and enables continuous evaluation of operational performance. Digital twins function as both analytical tools and reflexive agents, facilitating scenario simulation, fault injection and anticipatory assessment of emergent behaviours under varying operational conditions. In this sense, reliability becomes an evolving construct shaped by the interactions between subsystems rather than a fixed property of individual components.

The application of the Viable System Model provides a structural and organisational lens through which these interactions can be understood and managed. VSM enables recursive organisation across multiple levels of system governance, ensuring that operational, coordination, control, intelligence and policy functions are maintained across distributed subsystems. When combined with Fourth-Order Cybernetics, this structure extends beyond technical control into reflexive awareness, where systems are capable of observing not only their operational states but also the processes by which those states are interpreted and acted upon (Yolles, 2021). This recursive capability supports higher order learning, adaptation and alignment between operational performance and strategic intent.

The study highlights the importance of multi agent coordination mechanisms, including evolutionary game theory and multi agent reinforcement learning, in managing emergent behaviours within complex and DOS environments. These approaches enable distributed agents to adapt strategies dynamically in response to environmental uncertainty, communication constraints and subsystem variability (Chen et al., 2025; Liu et al., 2025; Wang et al., 2025; Zhang et al., 2025). Through iterative learning and interaction, subsystem agents collectively contribute to maintaining system level coherence while balancing local and global objectives. This reflects a shift from centrally controlled architectures toward decentralised, adaptive systems capable of self-organisation under uncertainty.

From a cybernetic perspective, Fourth-Order Cybernetics further extends this adaptive capacity by introducing reflexive and meta cognitive dimensions into system behaviour. Digital twins, in this context, operate not merely as monitoring or simulation tools but as epistemic agents that participate in recursive cycles of observation, interpretation and adaptation. They support collective sensemaking across human and machine actors, enabling shared situational awareness and coordinated decision making in complex and contested DOS environments (Ackoff, 2010). Reliability, therefore, becomes a socially and cognitively constructed property, continuously negotiated through interactions between human operators, autonomous systems and digital representations.

The findings also indicate that emergent behaviour often considered a challenge in complex systems can be systematically monitored, analysed, and managed through the integration of digital twins, cybernetic feedback structures and multi agent optimisation frameworks. Rather than attempting to eliminate emergence, the proposed approach embraces it as an inherent feature of SoS environments, leveraging simulation, behavioural modelling and adaptive control to ensure that such behaviours remain aligned with operational objectives and system constraints (Mittal, 2017). Overall, the study confirms that the convergence of digital twins, cybernetics and multi-agent learning frameworks enhances resilience, adaptability and operational objective assurance within DOS architectures. Reliability is reconceptualised as an autopoietic and emergent capability sustained through recursive learning, structural adaptation and continuous interaction across interconnected subsystems (Madni et al., 2014). Digital twins, in this sense, evolve beyond their traditional role as engineering tools to become integral components of organisational intelligence and adaptive control systems.

As DOS environments continue to grow in complexity, uncertainty and disruptive or unsertain pressure, the ability to maintain operational effectiveness will increasingly depend on such cybernetic architectures of cognition and control. Digital twins, embedded within VSM-based organisational structures and augmented by A driven multi agent coordination, provide a foundation for systems that can not only monitor and simulate but also learn, adapt and co-evolve with their operational DOS environments. This positions digital twins as critical enablers of future systems of systems capability supporting not only technical

performance but also strategic coherence, ethical alignment and systemic viability in dynamic and contested domains.

Data availability

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

Funding

Nil

Disclosure statement

The author reports that there are no competing interests to declare.

Author contributions statement

Dr Aleksandar Seizovic, involved in the conception and design, analysis and interpretation of the data and the drafting, editing and writing of the paper.

Mr Hongan Lin is the founder of Asset Studio Pte Ltd headquartered in Singapore. He joined Temasek Polytechnic (Singapore) as a lecturer and subsequently, he served in ReliaSoft Asia as managing director responsible for operations in Asia Pacific region. He is a subject matter expert in Life Data Analysis, Accelerated Life Test Analysis, System Reliability Simulation and field reliability data collection systems for process industries.

References

Ackoff, R. (2010) Differences that make a difference: An annotated glossary of distinctions important in management. Triarchy Press.

Ackoff, R.L. (2010) Systems thinking for curious managers. Springer.

Adams, K.M., Hester, P.T., Bradley, J.M., Meyers, T.J. and Keating, C.B. (2014) 'Systems theory as the foundation for understanding systems', Engineering Management & Systems Engineering Faculty Publications, 32. Available at: https://digitalcommons.odu.edu/emse_fac_pubs/32

Adams, R., Smith, J. and Johnson, T. (2014) 'Self-organization in complex adaptive systems', Complex Systems, 23(2), pp. 45–67.

Ashby, W.R. (1956) An introduction to cybernetics. Chapman & Hall.

Asset Studio (n.d.) AeROS® (Asset reliability and operations simulation). Available at: https://assetstudio.net/software/aeros (Accessed: 3 February 2026).

Banerjee, T. and Kour, P. (2025) 'Advances in deep neural, transformer learning, and kernel-based methods for diabetic retinopathy detection: A comprehensive review', Archives of Computational Methods in Engineering. Available at: https://doi.org/10.1007/s11831-025-10364-y

Beer, S. (1979) The heart of enterprise. John Wiley & Sons.

Blanchard, B.S. and Fabrycky, W.J. (2011) Systems engineering and analysis. 5th edn. Pearson.

Boardman, J. and Sauser, B. (2006) 'System of systems—The meaning of systems engineering', in Proceedings of the 2006 IEEE/SMC International Conference on System of Systems Engineering, pp. 118–123. Available at: https://doi.org/10.1109/SYSOSE.2006.1652284

Burge, S. (2018) A systems approach to failure modes, mechanisms, effects and causes. Technical Paper 0003/sb. Available at: https://www.burgehugheswalsh.co.uk/Uploaded/1/Documents/A-Systems-Approach-to-Failure-Modes-v1.pdf

Chen, X., Li, Y. and Zhao, Q. (2025) 'Evolutionary smart contracts for multi-stage negotiation in virtual power plant trading', International Journal of Electrical Power & Energy Systems, Article 111453. Available at: https://doi.org/10.1016/j.ijepes.2025.111453

Cheng, L., Zhang, M., Wang, K., Yuan, M., Liu, Z., Wang, J., Zhang, K. and Huang, P. (2025) 'Evolutionary smart contracts for virtual power plant trading: Integrating prospect theory and multi-stage negotiation in cross-regional energy markets', International Journal of Electrical Power & Energy Systems, 173, Article 111453. Available at: https://doi.org/10.1016/j.ijepes.2025.111453

DeLaurentis, D. and Callaway, R.K. (2004) 'A system-of-systems perspective for public policy decisions', Review of Policy Research, 21(6), pp. 829–837. Available at: https://doi.org/10.1111/j.1541-1338.2004.00091.x

Ebeling, C.E. (2010) An introduction to reliability and maintainability engineering. 2nd edn. Waveland Press.

Fuller, A., Fan, Z., Day, C. and Barlow, C. (2020) 'Digital twin: Enabling technologies, challenges and open research', IEEE Access, 8, pp. 108952–108971. Available at: https://doi.org/10.1109/ACCESS.2020.2998358

Grieves, M. and Vickers, J. (2017) 'Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems', in Kahlen, F.-J., Flumerfelt, S. and Alves, A. (eds.) Transdisciplinary perspectives on complex systems. Springer, pp. 85–113. Available at: https://doi.org/10.1007/978-3-319-38756-7_4

Hollnagel, E., Woods, D.D. and Leveson, N. (2006) Resilience engineering: Concepts and precepts. Ashgate.

IEC (2018) IEC 60812: Failure modes and effects analysis (FMEA and FMECA). International Electrotechnical Commission.

Jamshidi, M. (2009) System of systems engineering: Innovations for the twenty-first century. John Wiley & Sons.

Liu, H., Wang, P. and Zhang, M. (2025) 'Game-theoretic evolution in decentralized renewable energy systems: Evolutionarily stable strategies and replicator dynamics', Renewable and Sustainable Energy Reviews, Article 115776. Available at: https://doi.org/10.1016/j.rser.2025.115776

Madni, A.M., Jackson, S.L. and Sievers, M. (2014) 'Leveraging system-of-systems engineering to enable adaptive resilience', Systems Engineering, 17(2), pp. 142–155.

Madni, A.M. and Sievers, M. (2014) 'System of systems integration: Key considerations and challenges', Systems Engineering, 17(3), pp. 330–347. Available at: https://doi.org/10.1002/sys.21263

Maier, M.W. (1998) 'Architecting principles for systems-of-systems', Systems Engineering, 1(4), pp. 267–284.

Maturana, H.R. and Varela, F.J. (1980) Autopoiesis and cognition:

The realization of the living. D. Reidel. Available at: https://doi.org/10.1007/978-94-009-8947-4

Mittal, S. (2017a) Emergent behavior in complex systems engineering: A modeling and simulation perspective. Wiley.

Mittal, S. (2017b) 'Human-autonomy teaming for decision support in complex systems', Journal of Defense Modeling and Simulation, 14(3), pp. 259–272.

O'Connor, P.D.T. and Kleyner, A. (2012) Practical reliability engineering. 5th edn. Wiley.

Stamatis, D.H. (2003) Failure mode and effect analysis: FMEA from theory to execution. 2nd edn. ASQ Quality Press.

Tao, F., Zhang, M., Liu, Y. and Nee, A.Y.C. (2019) 'Digital twin in industry: State-of-the-art', IEEE Transactions on Industrial Informatics, 15(4), pp. 2405–2415. Available at: https://doi.org/10.1109/TII.2018.2873186

von Foerster, H. (1984) Observing systems. Intersystems Publications.

von Foerster, H. (2003) Understanding understanding: Essays on cybernetics and cognition. Springer.

Wang, Y., Chen, J. and Li, H. (2025) 'Computational game-theoretic models for adaptive urban energy systems: Reinforcement learning and multi-agent coordination', Archives of Computational Methods in Engineering. Available at: https://doi.org/10.1007/s11831-025-10364-y

Wiener, N. (1948) Cybernetics: Or control and communication in the animal and the machine. MIT Press.

Yolles, M. (2021a) Exploring mindset agency theory: Complexity, cybernetics, and social systems. Springer.

Yolles, M. (2021b) Fourth-order cybernetics: Reflexive management in complex systems. Routledge.

Yolles, M. and Fink, G. (2021) 'Fourth-order cybernetics: A multi-agency theory of organisational emergence', Kybernetes, 50(10), pp. 2717–2736.

Zhang, L., Sun, Q. and Liu, J. (2025) 'Evolutionary game theory in electricity market optimization: Multi-agent coordination and adaptive policy design', Complex & Intelligent Systems. Available at: https://doi.org/10.1007/s40747-025-01916-7 45, 6592–6611. https://doi.org/10.1039/C5DT04788A

 **Copyright:** ©2026 Seizovic, A., Lin, H., Dovecer, T., Wang, X. **License:** This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. To view a copy of this licence, visit https://creativecommons.org/licenses/by/4.0/