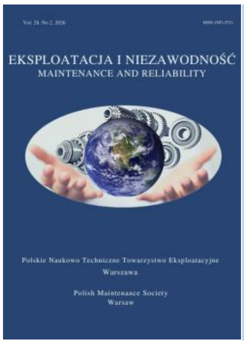

Eksploatacja i Niezawodnosc – Maintenance and Reliability
Volume 28 (2026), Issue 2
journal homepage: http://www.ein.org.pl

Article citation info:
Guo H, Cao H, Liu W, Cai Y, He Y, Inherent safety-oriented mission reliability modeling of manufacturing systems considering energy activities, Eksploatacja i Niezawodnosc – Maintenance and Reliability 2026: 28(2) http:/10.17531/ein/210685

Inherent safety-oriented mission reliability modeling of manufacturing systems considering energy activities

Indexed by: Web of Science Group

Hanjun Guo[a], Haibin Cao[a], Wei Liu[a], Yuqi Cai[b], Yihai He[b,*]

[a] China Energy Investment Corporation Limited, China
[b] School of Reliability and Systems Engineering, Beihang University, China

Highlights

- Connotation of mission reliability considering energy activities is presented.
- Assessment model for mission reliability considering energy activities is analyzed.
- Integrated mission reliability model with inherent-safety orientation is proposed.
- A manufacturing system example of electrochemical is implemented.

Abstract

According to the theory of unintended energy release in accidents, the root cause of a large number of production failures and accidents is usually related to abnormal energy transfer activities during the operation of the manufacturing system. Therefore, from the perspective of inherent safety assurance, a novel mission reliability modeling method that integrates energy activities is proposed. First, the dynamic interaction relationships of production factors are analyzed from the perspective of energy activities, and the connotation of the mission reliability of manufacturing systems oriented to inherent safety are expounded. Moreover, an assessment model for mission reliability of manufacturing systems considering energy activities is analyzed and constructed in terms of self-stabilization capability, anti-disruption capability, and risk-isolation capability. Finally, an industrial case study based on electrochemical ammonia synthesis production system is provided to verify the effectiveness of the proposed method.

Keywords
mission reliability, manufacturing system, Inherent safety, energy activities, risk isolation capability.

1. Introduction

In the context of economic globalization, focusing on system reliability has become a common concern internationally[1]. In this context, improving equipment system reliability can not only enhance the competitiveness in the market, but also has a positive impact and important role in ensuring the safety and efficiency of related operations[2]. At present, inherent safety has been widely used and studied in the industrial field, especially in the chemical industry[3][4].The inherent safety design technology of chemical processes is an important part of chemical process safety. Its core lies in reducing dangers from the source rather than relying on end-of-line protection measures. The root cause of a large number of production failures and accidents is usually related to abnormal energy transfer activities during the operation of the manufacturing system[5].Conventional manufacturing systems rely more on passive safety measures, while modern intelligent manufacturing systems emphasize safety control from the design stage and take safety characteristics as one of the design goals. Therefore, for manufacturing systems, on the basis of conventional reliability assessment, it is necessary to establish

(*) Corresponding author.
E-mail addresses: H. Guo, 10000271@ceic.com, H. Cao, 10000308@ceic.com, W. Liu, liuweicm@163.com, Y. Cai (ORCID: 0009-0002-4600-400X) yuchitsai@buaa.edu.cn, Y. He (ORCID:0000-0002-9110-2672) hyh@buaa.edu.cn

a mission reliability assessment model for inherent safety assurance to adapt to the system reliability assessment of modern manufacturing systems.

There have been a large number of studies on equipment system reliability modelling, and the trend has been from simple to complex, from equipment system unit-level reliability studies to system-level reliability studies. With the increase in complexity of manufacturing systems, scholars around the world have also introduced reliability research efforts into system-level equipment systems. In the early 1970s, there were studies on equipment system reliability modelling and analysis methods. Common reliability analysis methods such as Fault Tree Analysis(FTA), Event Tree Analysis(ETA), Failure Mode and Effects Analysis (FMEA) have been applied in the safety field, in addition to Reliability Block Diagram (RBD) which has also been widely used in practical engineering[6][7].Subsequent scholars introduced simulation methods into manufacturing system reliability modelling and achieved some remarkable research results[8][9][10][11].Dynamics is a typical characteristic of complex manufacturing systems nowadays, and as the drawbacks of static reliability modelling are gradually exposed, methods for dynamic reliability modelling of complex equipment systems have gradually received the attention of a large number of scholars[12]. Currently, the methods used for dynamic reliability modelling of manufacturing systems mainly include dynamic fault tree (DFT)[13], Markov model[14], Petri net[15], GO method[16], etc. As a powerful tool for studying discrete-event dynamical systems, Petri net and Petri net-based extension methods have been widely applied in the field of equipment system reliability modelling and analysis and have made great achievements. The field has been widely applied and significant research results have been achieved[17][18][19].

Energy activity is the key driving force for system operation, and its rational use and control are crucial to system reliability and efficiency[5]. On the one hand, insufficient or interrupted energy supply may lead to equipment downtime, production interruption, or even equipment damage, thereby increasing the risk of failure of the manufacturing system[20]. On the other hand, inefficient energy use will not only increase production costs, but also cause environmental problems due to energy waste and excessive consumption, which runs counter to the concept of green manufacturing[21][22]. Relevant studies have shown that by optimizing energy management and control strategies, the energy efficiency of the manufacturing system can be significantly improved, thereby improving its overall performance and reliability[23][24]. Therefore, when conducting mission reliability analysis, the impact of energy activities must be fully considered to achieve efficient, reliable, and sustainable operation of the manufacturing system.

The system reliability analysis methods described above usually model and analyze risk from a subsystem perspective, reducing a manufacturing system to several subsystems and other components, and then treating each part independently. In practice, the production operation process rarely fails directly because of a single event, but more often because of a combination of mutually contained and interrelated risk events that may lead to one or more failures, and assessing the system reliability of a production process requires further consideration of the interaction of resources such as energy and materials within the system, which has been investigated only by a relatively small number of researchers. Massrur [25] proposed a fast decoupling model of energy flow for large-scale integrated electric, gas, and thermal energy systems and demonstrated that the reliability and simulation time of the solution algorithm are better than the Newton-Raphson method. Zhao et al.[26] proposed an entropy-based Markov model to analyze the reliability of hybrid multicarrier energy systems by obtaining the reliability of the whole multicarrier energy system based on the reliability of individual energy carriers. Zhang et al.[27] investigated different stochastic characteristics in wind energy integration, including resource availability, generation facility outage and transmission availability, and proposed a probabilistic framework for modelling the reliability of renewable energy integration such as wind energy conversion systems. Liu et al.[28] consider the construction of virtual energy storage and demand response and propose rigid and flexible reliability evaluation metrics at the energy and time levels. Meng et al.[29] developed a reliability modelling of an integrated electricity-gas-heat energy system considering multiple energy forms of electricity, gas and heat, complex coupling relationships and multiple energy storage from the user's perspective. Mission reliability is the core indicator for measuring the inherent safety capability of a manufacturing system. It directly reflects the system's ability to complete the scheduled production tasks under specific conditions. A manufacturing system with high mission reliability can maintain stable operation and effectively complete production tasks in the face of various internal and external interferences and risk factors, thereby ensuring the safety and efficiency of the production process. Therefore, building a mission reliability assessment model for inherent safety is of great significance for improving the overall performance and safety of modern manufacturing systems.

In summary, a few existing studies have systematically analyzed the operating mechanisms of manufacturing systems and have failed to comprehensively consider the sources of factors affecting system reliability from the underlying mechanisms and energy perspectives. In addition, studies from the perspective of energy activities usually considers the potential damage to the equipment system, ignoring the impact of energy as an important element driving the operation of the manufacturing system and leading to safety and production accidents, which leads to the control of system reliability means to treat the symptoms rather than the root cause.

For production activities, we often pay more attention to the mission reliability of the manufacturing system, i.e., the ability of the manufacturing system to complete the specified production tasks under the specified conditions and within the specified time. Therefore, an assessment model for mission reliability oriented to inherent safety of manufacturing systems is constructed considering energy activities. The main contributions to this article are as follows.

(1) The new connotation of inherent safety-oriented mission reliability considering energy activities is presented.To bridge the existing research gap, this paper analyzes the interaction relationships among various production factors including energy in manufacturing systems and proposes the connotation of mission reliability oriented to inherent safety in manufacturing systems.

(2) An assessment model for mission reliability of manufacturing systems considering energy activities is analyzed.Meanwhile, an assessment model for the mission reliability oriented to inherent safety of manufacturing systems is constructed from three aspects: self-stabilization capability, anti-disruption capability, and risk isolation capability.

(3) Integrated mission reliability model with inherent-safety orientation is proposed. Specifically, the proposed comprehensive evaluation method could integrate the above three aspects, which provides guidance for manufacturers to make optimal reliability evaluation.

The remainder of the paper is organized as follows. Section 2 presents the foundations of mission reliability oriented to inherent safety assessment for manufacturing systems considering energy activities. Section 3 develops a model for mission reliability oriented to inherent safety assessment of manufacturing systems considering energy activities. Section 4 demonstrates the feasibility of the proposed methodology through a case study of electrochemical ammonia synthesis production system. Section 5 presents conclusions and future work.

2. Basics of mission reliability assessment for manufacturing systems considering energy activities

2.1.The operational mechanism of manufacturing systems considering energy activities

Modern industrial production relies on efficient manufacturing systems to take materials as production objects and realize the functions of manufacturing systems through precise production processes and energy drive. In the process of manufacturing system interaction, production activities involve multiple links such as material processing and transportation. Through the transfer and conversion of energy, raw materials are processed into final products, and waste is generated at the same time. Based on the above analysis of the interaction between manufacturing system and environment, a dynamic interaction model of manufacturing system considering energy activities is established as shown in Fig. 1.

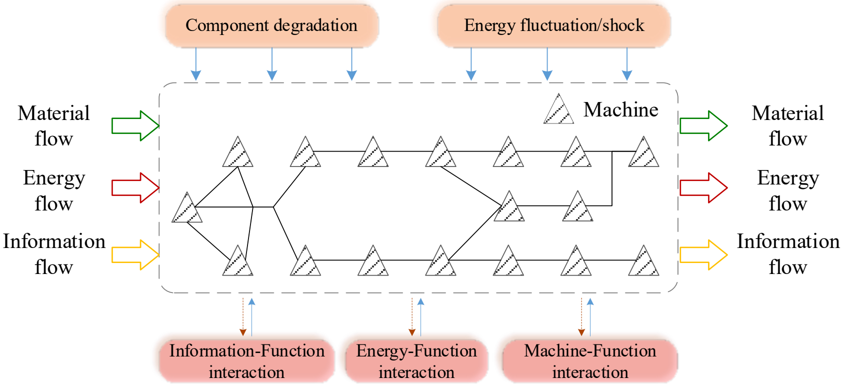

Fig. 1. Dynamic interaction model of manufacturing systems considering energy activity.

Fig. 1 shows the interactions between the elements of a manufacturing system considering energy activities. The core of the manufacturing activity lies in the processing and transfer of material objects, resulting in a material flow consisting of raw materials, semi-finished products, products, and so on. The manufacturing system relies on energy drive to realize its functions. Various energy bodies form the energy flow along with the transmission, transformation, and output of energy in the equipment system. Information flow can improve productivity and reduce costs through effective management and optimization in manufacturing systems. In addition, component degradation, energy fluctuations, and energy impacts impact the manufacturing process, reducing the safety and reliability of the entire manufacturing system. Through the interaction of information, energy, machine, and function, the above impacts can be monitored and controlled to guarantee the safety and reliability of the manufacturing system and achieve a dynamic regulation process.

2.2. Connotation of mission reliability oriented to inherent safety

According to the theory of accidental release of energy, unexpected release of energy is one of the causes of accidents, and the analysis only from the functional structure of manufacturing system cannot fully consider all the harmful factors in manufacturing system. Therefore, based on understanding and analyzing the functional structure of the manufacturing system, the interaction between energy activities and the manufacturing system is considered to obtain the mission reliability connotation of the manufacturing system. The energy that exists and can be released in the process of production activities ensures the operation of the manufacturing system, and the manufacturing system achieves the production goal through energy transmission and transfer, conversion, etc. On the basis of considering the above normal energy activities and potential abnormal energy release, the inherent safety-oriented mission reliability of the manufacturing system refers to its ability to maintain safe and stable operation during operation to accomplish the production mission.

The inherent safety-oriented mission reliability of manufacturing systems are mainly manifested in three aspects: self-stabilization capability, anti-disruption capability and risk isolation capability.

(1) Self-stabilization capability refers to the ability of the manufacturing system to self-regulate and run stably to prevent equipment damage and production interruption caused by internal reasons. It is closely related to the reliability of the system, and can maintain normal operation, significantly reducing the risk of equipment failure and production interruption. For instance, self-stabilization capability can be compared to a motor drive system that automatically adjusts current and voltage to maintain stable output under fluctuating load conditions.

(2) Anti-disruption capability means that the manufacturing system can effectively resist external risks and influences, prevent personnel errors, external environment and other factors to cause abnormal production interruptions and equipment damage, indicating the robustness of the system, in the face of uncontrollable factors can still maintain normal operation. For instance, anti-disruption capability is reflected in a CNC machine tool equipped with redundant sensors and fault-tolerant controllers that allow production to continue even when one sensor fails.

(3) Risk isolation capability refers to the ability of the

manufacturing system to protect itself from external output risks, prevent system energy release from causing personnel injury, property damage and environmental damage, and reflect the safety performance of the system. "External output risk" refers to the potential hazards arising from the output of energy, substances, or control signals by the manufacturing system during operation, which may adversely affect the external environment or surrounding entities. If such outputs are not properly isolated or controlled, they may evolve into significant safety threats. For example, in a high-temperature and high-pressure reaction unit, a control failure may result in the unintended release of high-temperature gas, posing a danger to nearby personnel or equipment. Therefore, the term "risk isolation capability" in this paper essentially refers to the system's ability to limit hazardous energy, isolate risk pathways, and ensure safe output through appropriate design or control strategies. This capability serves as an important indicator of the system’s inherent safety performance. For instance, risk isolation capability is illustrated by safety valves in chemical pipelines that immediately isolate high-pressure flow once abnormal conditions are detected, thereby preventing hazardous incidents.

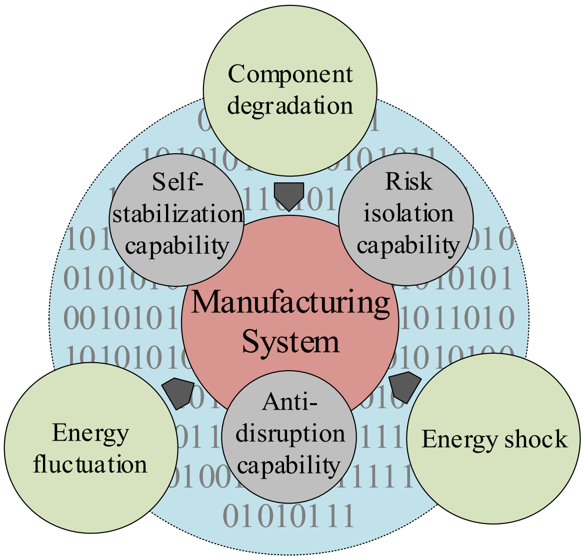

Fig. 2. Connotation of mission reliability oriented to inherent safety considering energy activities

To sum up, the inherent safety-oriented mission reliability connotation of the manufacturing system considering energy activities is shown in Fig. 2. The self-stabilization capability, anti-disruption capability and risk isolation capability of the manufacturing system are mainly reflected in the control of internal energy, the resistance to external damage energy, and the ability of the system performance and ability to adapt to internal and external energy changes and require that this ability will not be lost or weakened. Therefore, in the next chapter, the modeling will be conducted from three aspects: self-stabilization capability, anti-disruption capability and risk isolation capability to evaluate the inherent safety-oriented mission reliability of the manufacturing system.

Conventional reliability mainly focuses on the failure probability of each component in the system structure and its combinatorial relationship, emphasizing the ability to operate fault-free within a specific period, which is usually evaluated by static life distribution models (e.g., exponential distribution or Weibull distribution). This type of approach relies more on component-level failure data and the structural logic of series-parallel systems and less on the dynamic response of the system and the influence of external perturbations during mission execution. Therefore, based on the connotation of mission reliability for inherent safety, the next chapter of this paper starts from the dynamic process of system operation, focusing on the stable performance of the system in the face of internal and external energy perturbations in the process of mission execution, and constructs a mission reliability model. The mission reliability model proposed in this paper introduces the indexes of self-stabilization capability, anti-disruption capability, and risk isolation capability, which are used to comprehensively portray the system's ability to guarantee task completion under the complex and uncertain energy environment. The model not only captures the system's performance but also the system's performance in a complex and uncertain energy environment. Compared with existing methods, the model captures the basic features of structural reliability and systematically integrates the dynamic anti-jamming and cooperative defense mechanisms of manufacturing systems under the inherent safety orientation, which has stronger engineering adaptability and safety guidance value.

2.3. Nomenclature

Notations applied to this paper are outlined as follows.

- A_i: Availability of the i-th subsystem
- α, β: Tradeoff parameters for energy-flow control objectives
- C_c: Energy control capability of the system

- C_M: Energy monitoring capability of the system
- $C_{M\&C}$: Combined monitoring and control capability of energy flow
- $E(t)$: Fluctuating energy flow at time t
- E_c: Expected center value of energy flow
- $E_i(t)$: Energy withstood by the i-th equipment at time t
- $E_{i,th}$: Maximum energy the i-th equipment can withstand
- $E_{\epsilon,i}$: Leaked energy from the i-th equipment
- $E_{\tau,i}$: Maximum tolerance of external environment to leaked energy ($E_{\epsilon,i}$)
- F_i: Fault detectability of the i-th subsystem
- H_i: Risk isolation capability of the i-th subsystem
- I_i: Anti-disruption capability of the i-th subsystem
- $M_i(t)$: Mission-oriented performance margin of the i-th subsystem
- $MTTF_i$: Mean Time to Failure of the i-th equipment
- $MTTR_i$: Mean Time to Recovery of the i-th equipment
- $p_i(t)$: Stochastic degradation process of the i-th subsystem's performance
- $p_{i;b}$: Minimum required performance value for mission accomplishment of subsystem i
- $R_i(t)$: Fundamental mission reliability of the i-th subsystem
- $R_{sf}(t)$: Integrated mission reliability with inherent-safety orientation
- S_i: Self-stabilization capability of the i-th subsystem
- T_c: Time consumption to stabilize energy fluctuation
- T_r: Delay time of sensor monitoring
- $\overline{\tau_i}$: Mean Time to Recovery after energy disruption for subsystem i
- $\vartheta_{i,l}$: Undetectability of the l-th failure mode in subsystem i
- $\lambda_{i,j}$: State Transition Intensity (STI) from state i to j

3. Mission reliability evaluation approach for manufacturing systems considering energy activities

3.1. Assessment of system fundamental mission reliability

System fundamental mission reliability refers to the ability of the equipment to complete the predetermined functions without failure under specified conditions and within a specified time. It is an important indicator to measure the stability and sustainability of the equipment in actual use. In this section, we utilize the failure rate model to evaluate the frequency of failure occurrence during operation. In manufacturing systems, inherent reliability is associated with system performance and accomplishment of production missions, wherein performance is productivity for manufacturing subsystems or other key indicators for supplementary subsystems, e.g., transfer efficiency for heat exchanging subsystems. Denote the stochastic degradation process of the i^{th} subsystem's performance as $p_i(t)$, its minimum required value for mission accomplishment is $p_{i;b}$, then the mission-oriented performance margin is

$$M_i(t) = \frac{p_i(t) - p_{i;b}}{p_{i;b}} \tag{1}$$

and the mission reliability functions for the i-th subsystem and the entire system are listed below respectively.

$$\begin{cases} R_i(t) = \Pr\{M_i(t) > 0\} = \Pr\left\{\frac{p_i(t) - p_{i;b}}{p_{i;b}} > 0\right\} \\ R(t) = \prod_i R_i(t) = \prod_i \Pr\left\{\frac{p_i(t) - p_{i;b}}{p_{i;b}} > 0\right\} \end{cases} \tag{2}$$

3.2. Assessment of system self-stabilization capability

As defined previously, system self-stabilization capability refers to a system's ability to recover from internal failures without external intervention. Given the intricate nature of production equipment, characterized by diverse structures, functions, loads, and configurations, failures can manifest in various forms. Consider hot rolling equipment used in steel strip production as an example. This equipment comprises multiple subsystems, including transmission systems and finishing mills, each containing functional components such as bearings, gears, transmission shafts, and rollers. The failure of any component can lead to equipment downtime. Moreover, the types of failures that can occur within each component and the severity of their consequences vary widely.

Equipment failures that compromise system self-stabilization can generally be categorized into two types: sudden and gradual failures. In the context of energy release theory, these failure modes correspond to uncontrolled and controlled energy, respectively. Sudden failures typically result from the abrupt release of uncontrolled energy, leading to catastrophic component damage. Conversely, gradual failures occur due to the cumulative effect of controlled energy over time, gradually degrading components through mechanisms such as wear and deformation. In steel hot rolling equipment, sudden failures in bearings, gears, and drive shafts can manifest as fractures in inner and outer rings, shafts, and gear teeth. Gradual failures, on the other hand, include wear and deformation (e.g., creep) of bearing components, ball wear, gear wear, and other complex failure modes.

Hence, following from the concept of system self-stability, the system self-stabilization capability of a manufacturing system can be defined as $S = f(\boldsymbol{C}, \boldsymbol{A}, \boldsymbol{F})$, wherein:

(1) $\boldsymbol{C}$ represents the system's capability of Monitoring and Controlling (M&C) energy flow, which can be evaluated as

$$\begin{cases} C_{M\&C} = C_M + C_C \\ C_M = \frac{T_{r,REF}}{T_r} \\ C_C = \left(\frac{E_c}{max|E(t)-E_c|}\right)^{\alpha} \cdot \left(\frac{T_{c,REF}}{T_c}\right)^{\beta} \end{cases} \quad (3)$$

where in C_M and C_C denote the system's monitoring and controlling capability, respectively. Specifically, T_r and $T_{r,REF}$ respectively denote the delay time of sensor monitoring and its reference value, T_c and $T_{c,REF}$ respectively denote the necessary time consumption for a system to stabilize energy fluctuation, and its reference value, $E(t)$ and E_c denotes the fluctuating energy flow and its expected center value, α and β are model parameters representing the tradeoff between the two objectives of energy-flow controlling, i.e., "minimizing fluctuation intensity $max|E(t) - E_c|$" and "minimizing stabilization time T_c". Given the system's energy-flow M&C capability $C_{M\&C}$, and its overall reference value $C_{M\&C,REF}$, the relative margin of this capability can be evaluated as

$$M\left(C_{M\&C}, C_{M\&C,REF}\right) = \frac{C_{M\&C}-C_{M\&C,REF}}{C_{M\&C,REF}} \quad (4)$$

Therefore, whether a system can reliably monitor and control its energy flow can be described via the probabilistic metric of

$$\boldsymbol{C} = \Pr\left\{C_{M\&C} > C_{M\&C,REF}\right\} = \Pr\left\{\frac{C_{M\&C}-C_{M\&C,REF}}{C_{M\&C,REF}} > 0\right\} \quad (5)$$

which can be denoted as C_i for the i-th subsystem within the system.

(2) $\boldsymbol{A}$ represents availability, which refers to the capability of the system or equipment to operate normally and provide predetermined services when needed. It is used to measure the normal working proportion of the equipment or system over a period of time. For the manufacturing equipment with reliability function $R_i(t)$, its Mean Time to Failure (MTTF) can be estimated via the estimation

$$E(MTTF_i) = \int_t tR_i(t)dt \quad (6)$$

Given the expectation of Mean Time to Recovery $E(MTTR_i)$ according to maintenance logs, and the availability can be estimated via

$$A_i = \frac{E(MTTF_i)}{E(MTTF_i)+E(MTTR_i)} \quad (7)$$

(3) $\boldsymbol{F}$ represents fault detectability, which refers to the proportion of faults that can be effectively identified and detected during the operation of the system or equipment. It measures the response speed and accuracy of the detection system to potential faults. The evaluation of the detectability of different equipment failure modes depends on the experience of the on-site maintenance personnel in the production workshop. Therefore, for the l-th failure mode of the i-th subsystem, its undetectability is $\vartheta_{i,l}$, and the equipment failure mode undetectability index can be evaluated according to the Delphi method. Specifically, assuming that $\vartheta_{i,l}$ has n possible levels $\{x_1, x_2, \cdots, x_n\}$ (sorted from low to high), and there are m experts involved in the undetectability evaluation, then the Delphi method follows these steps: (1) Obtain the expert confidence score matrix of the severity of the failure consequences

$$\boldsymbol{\alpha} = \begin{pmatrix} \alpha_{1,1} & \cdots & \alpha_{1,n} \\ \vdots & \ddots & \vdots \\ \alpha_{m,1} & \cdots & \alpha_{m,n} \end{pmatrix} \quad (8)$$

wherein the confidence score $\alpha_{i,j}$ represents the evaluated subjective probability of the i-th expert for $\xi_l \le x_j$, (2) For the expert confidence matrix above, calculate the mean and standard deviation of each expert score by column, i.e.,

$$\alpha_{\cdot,j} = \frac{1}{m}\sum_{i=1}^{m} \alpha_{i,j} \quad (9)$$

and

$$d_{\cdot,j} = \sqrt{\frac{1}{m}\sum_{i=1}^{m}\left(\alpha_{i,j} - \alpha_{\cdot,j}\right)^2} \quad (10)$$

then perform the consistency test: given a maximum error tolerance ε, accept the expert score result if and only if $d_{\cdot,j} \le \varepsilon$, otherwise repeat steps 1, 2, and 4 until the result passes the consistency test. Afterwards, the subjective probability distribution of the severity of equipment failure consequences is constructed following

$$\Phi_{\vartheta_{i,l}}(x)=\begin{cases}0 & x\le x_1\\ \alpha_{\cdot,j}+\frac{(\alpha_{\cdot,j+1}-\alpha_{\cdot,j})}{x_{j+1}-x_j}(x-x_j) & x_j<x\le x_{j+1}\\ 1 & x>x_n\end{cases} \quad (11)$$

wherein $1 \le j \le n-1$, and the expectation can be derived from this distribution as

$$E(\vartheta_{i,l})=\int_{x=-\infty}^{+\infty}xd\Phi_{\vartheta_{i,l}}(x)=\sum_{j=1}^{n-1}\int_{x=x_j}^{x_{j+1}}xd\Phi_{\vartheta_{i,l}}(x) \quad (12)$$

and the fault detectability of the i-th subsystem can be correspondingly defined as

$$\boldsymbol{F}_i=1-\sum_l\frac{E(\vartheta_{i,l})}{\vartheta_F} \quad (13)$$

wherein ϑ_F denotes full score, and $\boldsymbol{F}_i$ correspondingly represents the confidence proportion on fault undetectability provided by the expert system.

For the i-th component within the system, S_i is subject to the constraint that $S_i \ge T_{si}$, wherein T_{si} represents the stability requirement. Given the four factors outlined above, the self-stabilization capability can be formulated as a probabilistic metric of

$$S_i=f(\boldsymbol{C}_i,\boldsymbol{A}_i,\boldsymbol{F}_i)=\boldsymbol{C}_i\cup\boldsymbol{A}_i\cup\boldsymbol{F}_i=\boldsymbol{C}_i\boldsymbol{A}_i\boldsymbol{F}_i=\Pr\left\{\frac{C_{M\&C}-C_{M\&C,REF}}{C_{M\&C,REF}}>0\right\}\cdot\frac{E(MTTF_i)}{E(MTTF_i)+E(MTTR_i)}\cdot\left(1-\sum_l\frac{E(\vartheta_{i,l})}{\vartheta_F}\right) \quad (14)$$

for the i-th subsystem, and

$$S=f(\boldsymbol{C},\boldsymbol{A},\boldsymbol{F})=\cup_{i=1}^{n}S_i=\prod_{i=1}^{n}\boldsymbol{C}_i\boldsymbol{A}_i\boldsymbol{F}_i \quad (15)$$

for the entire system.

3.3. Assessment of system anti-disruption capability

In manufacturing systems, anti-disruption refers to a system's ability to withstand external risks and influences, preventing abnormal production interruptions and equipment damage caused by human error, environmental factors, or other unforeseen circumstances. This capability reflects the system's robustness and resilience. Anti-disruption enables systems to maintain normal operations in the face of uncontrollable factors, mitigate excessive wear or damage to equipment during emergencies, and respond effectively to sudden external changes. By preventing shutdowns and associated costs, production delays, and potential harm to personnel and property, anti-disruption enhances overall system reliability and safety. According to the fundamentals in Section 2, the anti-disruption capability can be evaluated as

$$\begin{cases} I=f(E,\tau_{rec})\\ I_i\ge T_{Ii},\forall i=1,2,\dots,n\end{cases} \quad (16)$$

wherein $E=(E_{1,th},E_{2,th},\cdots,E_{n,th})$ represents the maximum energy that the equipment can withstand. The larger it is, the more effective the system can be in preventing the impact of external energy and reducing risks, T represents the system's recovery time from external disruption, I_i represents the system's anti-disruption capability corresponding to the disruptive factor associated with the i-th machine, and T_{Ii} represents the maximum tolerance of I_i. For the i-th machine within the system, denote the energy it withstands as $E_i(t)$ at time t, and its energy carriage margin can be defined as

$$M(E_i(t),E_{i,th})=\frac{E_{i,th}-E_i(t)}{E_{i,th}} \quad (17)$$

while the system recovery time $\tau_{rec}=(\overline{\tau_1},\overline{\tau_2},\cdots,\overline{\tau_n})$ denotes the Mean Time to Recovery after energy disruption, i.e., $E_i(t)$ exceeding $E_{i,th}$ for the i-th machine. Considering that the mean time to disruption can be estimated via

$$E(MTTD_i)=\int_t t\Pr\left\{\frac{E_{i,th}-E_i(t)}{E_{i,th}}\ge 0\right\}dt \quad (18)$$

and the anti-disruption capability can be evaluated as

$$I_i=f(E_i,\overline{\tau_i})=Pr\left\{\frac{E(MTTD_i)}{E(MTTD_i)+\overline{\tau_i}}\ge T_{Ii}\right\} \quad (19)$$

and

$$I=f(E,\tau_{rec})=\cup_{i=1}^{n}I_i=\prod_{i=1}^{n}\Pr\left\{\frac{E(MTTD_i)}{E(MTTD_i)+\overline{\tau_i}}\ge T_{Ii}\right\} \quad (20)$$

3.4. Assessment of risk isolation capability

Risk isolation refers to a system's capability to contain potential risks within its boundaries, preventing the release of harmful energy that could lead to personal injury, property damage, or environmental harm. This capability reflects the system's safety design and ensures that unstable factors within the system are controlled and isolated, minimizing their impact on the surrounding environment and personnel. According to the theoretical fundamentals, the risk isolation capability can be described via

$$\begin{cases} H=f(M,L)\\ H_i\ge T_{Hi},\forall i=1,2,\dots,n\end{cases} \quad (21)$$

wherein M denotes the energy margin, i.e., the proportional gap between the actual energy (e.g., electricity, heat, mechanical energy, etc.) that the system withstands and the maximum safe load of the system, which is $M_i = M(E_i(t), E_{i,th}) = \frac{E_{i,th}-E_i(t)}{E_{i,th}}$ for the i-th equipment. L denotes the energy leakage status. Denote the leaked energy of the i-th equipment as $E_{\epsilon,i}$, and the maximum tolerance of the external environment to $E_{\epsilon,i}$ as $E_{\tau,i}$, then the energy leakage status can be described as a margin item of

$$L_i = M(E_{\epsilon,i}, E_{\tau,i}) = \frac{E_{\tau,i}-E_{\epsilon,i}}{E_{\tau,i}} \tag{22}$$

Correspondingly, the risk isolation capability can be evaluated via

$$H_i = f(M, L) = M \cup L = M(E_i(t), E_{i,th}) \cdot M(E_{\epsilon,i}, E_{\tau,i}) \tag{23}$$

and

$$H = f(M, L) = \cup_{i=1}^{n} H_i = \prod_{i=1}^{n} \Pr\{M(E_i(t), E_{i,th}) \cdot M(E_{\epsilon,i}, E_{\tau,i}) \geq T_{Hi}\} = \Pr\left\{\frac{[E_{i,th}-E_i(t)]\cdot[E_{\tau,i}-E_{\epsilon,i}]}{E_{i,th}E_{\tau,i}} \geq T_{Hi}\right\} \tag{24}$$

3.5. Integrated mission reliability model with inherent-safety orientation

From the perspective of safety engineering, the reliability of the manufacturing system can be defined as the capability of accomplishing specified missions under specified conditions and time constraints, while maintaining the safety-oriented capabilities, i.e., self-stabilization, anti-disruption capability and risk isolation, during system operation. Hence, taking operational safety into consideration, the system reliability can be evaluated via

$$\begin{cases} R_{sf}(t) = f(R(t), S, I, H) = \prod_{i=1}^{n} R_i(t) \cdot S_i \cdot I_i \cdot H_i\,; \\ R_i(t) = \Pr\{M_i(t) > 0\} = \Pr\left\{\frac{p_i(t)-p_{i;b}}{p_{i;b}} > 0\right\}; \\ S_i = \Pr\left\{\frac{C_{M\&C}-C_{M\&C,REF}}{C_{M\&C,REF}} > 0\right\} \cdot \frac{E(MTTF_i)}{E(MTTF_i)+E(MTTR_i)} \cdot \left(1 - \sum_l \frac{E(\vartheta_{i,l})}{\vartheta_F}\right) \\ I_i = \Pr\left\{\frac{E(MTTD_i)}{E(MTTD_i)+\bar{\tau}_i} \geq T_{Ii}\right\}; \\ H_i = \Pr\left\{\frac{[E_{i,th}-E_i(t)]\cdot[E_{\tau,i}-E_{\epsilon,i}]}{E_{i,th}E_{\tau,i}} \geq T_{Hi}\right\}. \end{cases} \tag{25}$$

wherein R_M denotes system fundamental reliability that is evaluated via the performance margin model, i.e., probability that the fundamental performance margin $\frac{p_f(i)-p_{fb}(i)}{p_{fb}(i)}$ being positive, wherein $p_f(i)$ and $p_{fb}(i)$ represent the i-th equipment's fundamental performance and its lowest requirement for mission accomplishment. S, I and H are the probabilistic metrics of self-stabilization, anti-disruption and risk isolation capabilities derived from Sections 3.2-3.4.

4. Case study

4.1. Background

The ammonia synthesis production system is a common yet complex engineering system in the chemical industry, serving as an indispensable infrastructure for the fertilizer industry, fuel industry, and nitro-explosives manufacturing industry. With increasing sustainability and environmental requirements, the ammonia synthesis industry is evolving toward the technical route of electrochemistry. However, electrochemical ammonia synthesis involves complex multi-energy conversions, i.e., conversions between electricity, heat, and chemical energy. Due to the involvement of hydrogen as an intermediate product, this process carries multiple types of risks in certain scenarios, e.g., leak of liquid nitrogen or liquid oxygen, hydrogen deflagration, and water electrolysis device leakage, which results in critical safety and reliability concerns in engineering practice under certain scenarios. Consequently, this section applies the proposed method to an Electrochemical Ammonia Synthesis Production (EASP) system to provide a reference for operational state assessment. As exhibited in Fig. 3, the EASP system studied in this section consists of four functionally distinct subsystems: (a) Cryogenic Distillation Unit (CDU), which separates nitrogen from other components by gradually heating and distilling cryogenically liquefied air; (b) Water Electrolysis Unit (WEU), which is designed to produce hydrogen through the electrolysis of water; (c) NH_3 Synthesis Reactor (NSR), which facilitates the catalytic reaction $N_2 + 3H_2 \leftrightharpoons 2NH_3$; (d) Heat Exchange Unit (HEU), which maintains optimal temperature and pressure levels within the reactor through thermal exchange, ensuring reaction efficiency.

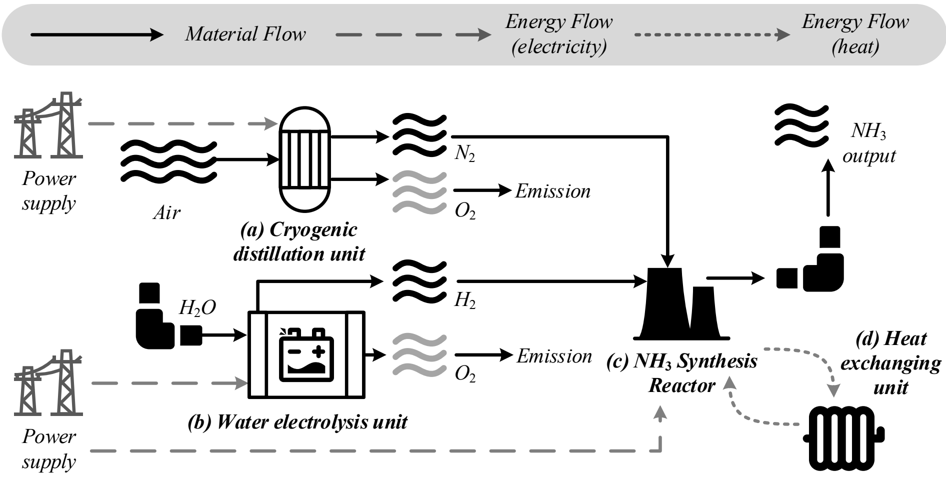

Fig. 3. Schematic of the EASP system

4.2. Numerical example

To validate the feasibility and effectiveness of the proposed method in the application of the EASP system, this section implements the following specific steps.

Step 1) Fundamental element analysis of safety and reliability. Apart from fundamental mission reliability, the elements of system operational safety and reliability consist of self-stabilization capability, anti-disruption capability, and risk isolation capability, which are respectively modeled in Sections 3.2 – 3.4. Given that fundamental mission reliability is modeled as the probability of production mission accomplishment, the practical manifestations of the latter three should be specifically analyzed as the prerequisite of the case study. These have been tabulated in Table 1.

Table 1. Fundament element analysis of safety and reliability in EASP system operation.

Subsystem	**Fundamental safety & reliability elements**		
	Self-stabilization	***Anti-disruption***	***Risk isolation***
CDU ($i = 1$)	*Maintaining its own air-tightness and temperature control capability to prevent gas leakage or contamination of output gas products with impurities.*	*Maintaining stable operation under the fluctuations in input material and energy flows (i.e., gas inlet pressure and power supply) within certain range.*	*Preventing hydrogen deflagration in the ammonia synthesis reactor by regulating oxygen concentration at the gas output below a specified threshold.*
WEU ($i = 2$)	*Sustaining optimal operating conditions for water supply pipelines, gas output pipelines, and electrical motors to ensure proper equipment functionality.*	*Maintaining stable operation within specified ranges of water pressure and voltage fluctuations.*	*Preventing water leakage and electrical faults to avoid potential harm to both operators and other integrated equipment within the system.*
NSR ($i = 3$)	*Regulating pN_2:pH_2 ratio, pressure, and temperature: (1) pN_2:$pH_2 = 1$:$(3 \pm 5\%)$; (2) $T = 425 \pm 25$℃; (3) Total pressure ≥ 150bar.*	*Activating proportional-integral control when feed velocity fluctuation $> \pm 10\%$ from setpoint or residence time variation $> \pm 5\%$ to maintain Temperature oscillations <±2°C and Conversion rate variability <±3%.*	*Preventing accidents of environment harms or personnel injury associated with unexpected NH_3 leakage.*
HEU ($i = 4$)	*Sustaining normal heat exchange functionality, i.e., keeping heat transfer coefficient $U>U_{ref}$, to maintain the reactor temperature within the aforementioned specified range.*	*Achieving proactive control of heat exchange efficiency through negative feedback regulation, enabling prompt temperature recovery to the prescribed operating range during thermal source abnormalities.*	*Capability of implementing immediate recovery/replacement after equipment failures to minimize thermal disturbances in the reactor.*

Step 2) Evaluation of system fundamental reliability. This section provides the baseline of system reliability, i.e., $R_{M,i}$ that evaluates the mission accomplishing capability of the i^{th} component using probabilistic metric. Given the memoryless property statistically observed in the performance degradation process of EASP system equipment, we adopt a Discrete-State Continuous-Time Markov Process (DSCTMP) model to characterize its state transition dynamics. Specifically, six discrete states denoted as 1,2,3,4,5,6 from optimal to fully failure can be utilized to describe the states of CDU, WEU, NSR

and WEU. Taking the unit-time productivity as the performance metric for CDU, WEU, NSR, and real-time heat transfer coefficient for WEU, then the fundamental performance margins $\frac{p_f(i)-p_{fb}(i)}{p_{fb}(i)}$ for CDU, WEU, NSR and WEU at each performance state can be tabulated as Table 2.

Table 2. Fundamental element analysis of safety and reliability in EASP system operation.

Subsystem	**Performance margin $\frac{p_f(i)-p_{fb}(i)}{p_{fb}(i)}$ at State #1 - #6**					
	State #1	State #2	State #3	State #4	State #5	State #6
CDU	0.4427	0.3139	0.1516	0.0289	*-0.0244*	*-0.1202*
WEU	0.4254	0.1688	0.1064	*-0.0065*	*-0.0421*	*-0.1853*
NSR	0.4260	0.3222	0.2363	0.1323	*-0.0029*	*-0.0334*
HEU	0.2872	0.2275	0.0461	*-0.0568*	*-0.0768*	*-0.1722*

Through statistical methods, the State Transition Intensities (STIs) of CDU, WEU, NSR and HEU are estimated as Table 3. Considering epistemic uncertainty, the estimations of STIs are presented as belief interval estimations.

Table 3. Interval estimations of fundamental performance STIs.

Subsystem	Confidence interval estimations of STIs / h^{-1}				
	λ_{12}	λ_{23}	λ_{34}	λ_{45}	λ_{56}
CDU	[0.0633, 0.0867]	[0.0750, 0.0984]	[0.0902, 0.1137]	[0.1254, 0.1488]	[0.0363, 0.0598]
WEU	[0.0879, 0.1113]	[0.0785, 0.1020]	[0.0598, 0.0832]	[0.1312, 0.1547]	[0.0891, 0.1125]
NSR	[0.0680, 0.0914]	[0.0867, 0.1102]	[0.0562, 0.0797]	[0.0715, 0.0949]	[0.0586, 0.0820]
HEU	[0.0527, 0.0762]	[0.0445, 0.0680]	[0.1078, 0.1313]	[0.0973, 0.1207]	[0.0914, 0.1148]
Note: State transition intensities not listed above are all zeroes.					

Given the STIs evaluated above, the real-time state probabilities during the performance degradation processes of CDU, WEU, NSR and WEU can be evaluated, as depicted in Fig 4, wherein the upper and lower bounds of confidence intervals are plotted in dash lines.

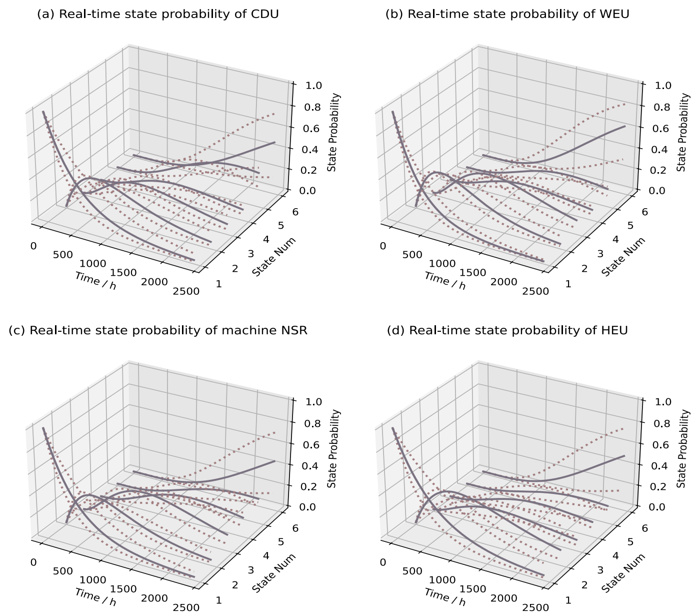

Fig. 4. Sate probabilities of CDU, WEU, NSR and WEU in degradation process.

Based on the state probabilities depicted in Fig 4, the fundamental reliabilities of each equipment, i.e., $R_{M,i} = \Pr\{M_{pf}(i)\geq 0\} = \Pr\left\{\frac{p_f(i)-p_{fb}(i)}{p_{fb}(i)}\geq 0\right\}$ can be evaluated. See the result in Fig. 5, wherein upper/lower bounds of confidence interval throughout the totally 2400 hours (100d) of system operation time have also plotted in dashed lines.

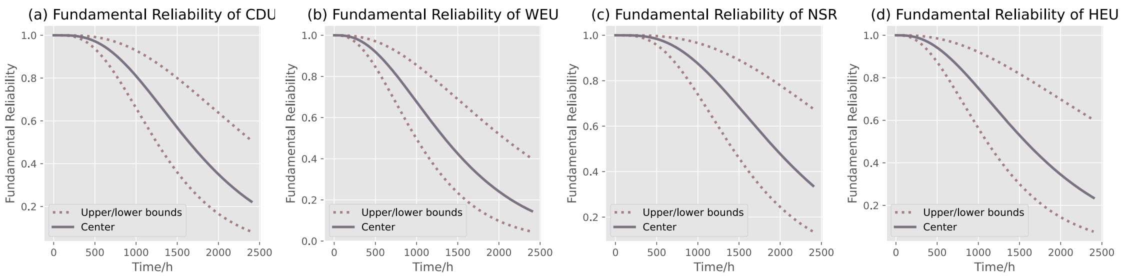

Fig. 5. Results of fundamental mission reliability evaluation for CDU, WEU, NSR and WEU.

Step 3) Evaluation of self-stabilization capability.

This step evaluates the self-stabilization capabilities for the EASP system and its four subsystems, CDU, WEU, NSR and HEU, which are

$$\begin{cases} S = f(\boldsymbol{C}, \boldsymbol{A}, \boldsymbol{F}) = \prod_{i=1}^{n} S_i = \prod_{i=1}^{n} \boldsymbol{C}_i \boldsymbol{A}_i \boldsymbol{F}_i \\ \boldsymbol{C}_i = \Pr\left\{\frac{C_{M\&C} - C_{M\&C,REF}}{C_{M\&C,REF}} > 0\right\} \\ \boldsymbol{A}_i = \frac{E(MTTF_i)}{E(MTTF_i) + E(MTTR_i)} \\ \boldsymbol{F}_i = \left(1 - \sum_l \frac{E(\vartheta_{i,l})}{\vartheta_F}\right) \end{cases}$$

The evaluation leverages real-time observation and evaluation data of energy monitoring and control capability $C_{M\&C} = C_M + C_C = \frac{T_{r,REF}}{T_r} + \left(\frac{E_c}{\max|E(t) - E_c|}\right)^{\alpha} \cdot \left(\frac{T_{c,REF}}{T_c}\right)^{\beta}$, equipment availability $\frac{E(MTTF_i)}{E(MTTF_i) + E(MTTFR_i)}$, and fault detectability $\left(1 - \sum_l \frac{E(\vartheta_{i,l})}{\vartheta_F}\right)$. Specifically, the three indices $\boldsymbol{C}_i, \boldsymbol{A}_i$, and $\boldsymbol{F}_i$ are calculated or evaluated once a day (24h). Given the expert-elicited tradeoff parameters $\alpha = 1.2$ and $\beta = 1.5$, the real-time values of $C_{M\&C}$ based on the observation data of T_r, $E(t)$, and T_c, compared to its reference value $C_{M\&C,REF}$, are plotted in Fig. 6.

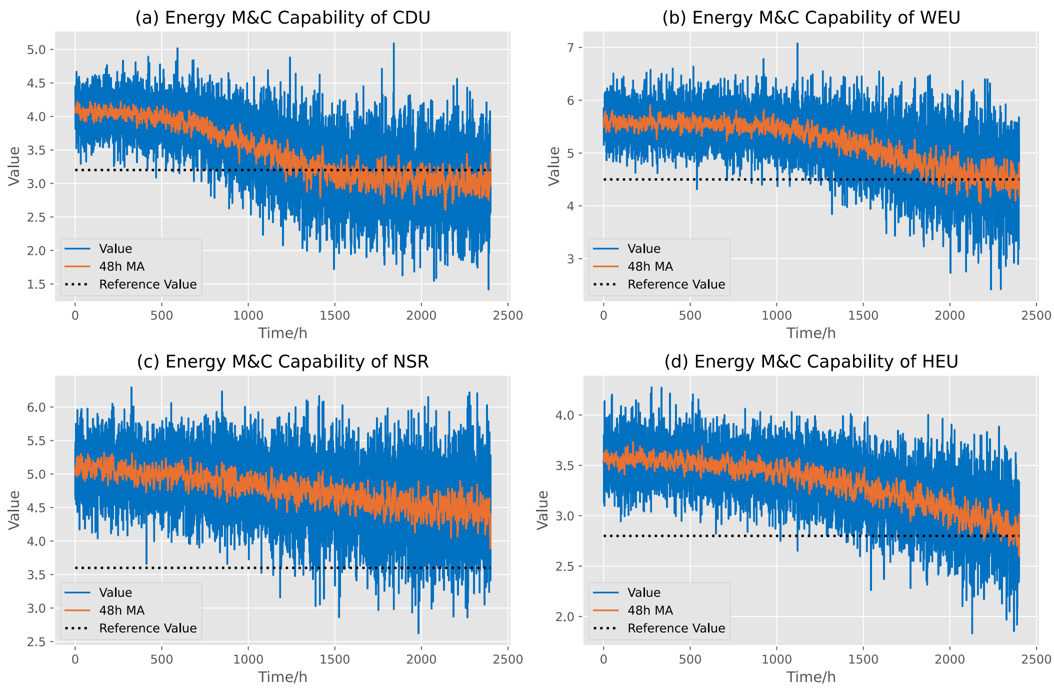

Fig. 6. Real-time energy M&C capability evaluation of CDU, WEU, NSR and WEU, wherein "48h MA" represents "48h moving average".

From the real-time evaluation data presented in Fig 5, the daily evaluations probabilistic metric $\boldsymbol{C}_i = \Pr\left\{\frac{C_{M\&C} - C_{M\&C,REF}}{C_{M\&C,REF}} > 0\right\}$ can be correspondingly estimated by the appearing frequency of samples satisfying $\Pr\left\{\frac{C_{M\&C} - C_{M\&C,REF}}{C_{M\&C,REF}} > 0\right\}$, see Fig. 7. Additionally, this step estimates $\boldsymbol{A}_i = \frac{E(MTTF_i)}{E(MTTF_i) + E(MTTFR_i)}$ and

$\boldsymbol{F}_i = \left(1 - \sum_l \frac{E(\vartheta_{i,l})}{\vartheta_F}\right)$ during the 2400h operation process. While the former is derived from timing calculation of equipment reliability, the latter is estimated via Delphi method. The results of $\boldsymbol{A}_i$ and $\boldsymbol{F}_i$ have been presented together with the $\boldsymbol{C}_i$ results derived from the previous step in Fig. 7. The final results, $S_i = \boldsymbol{C}_i\boldsymbol{A}_i\boldsymbol{F}_i$ have also been incorporated.

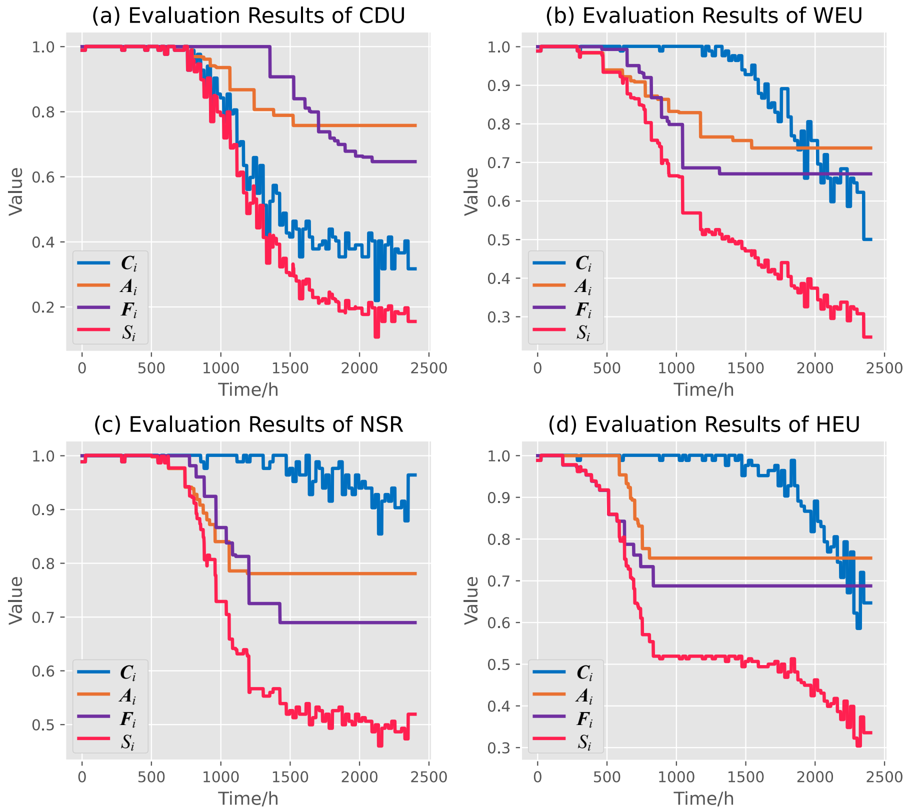

Fig. 7. Results of $\boldsymbol{C}_i$, $\boldsymbol{A}_i$, $\boldsymbol{F}_i$, and the final evaluation result S_i.

Step 4) Evaluation of anti-disruption and risk isolation capability.

This step provides the evaluations of the anti-disruption and risk-isolation capability for CDU, WEU, NSR and HEU. During the 2400h operation time, the evaluations are also implemented daily (once per 24h). The evaluation results are depicted in Fig. 7.

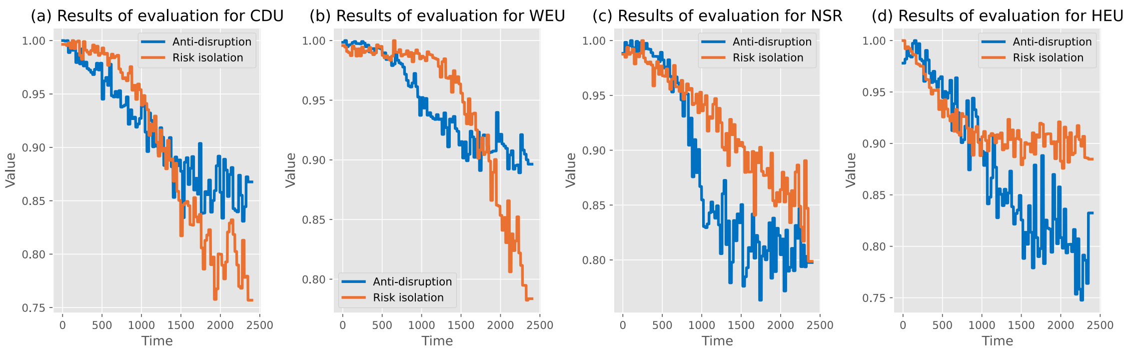

Fig. 8. One-per-24h evaluation of anti-disruption and risk isolation capabilities for CDU, WEU, NSR and WEU.

Step 5) Result derivation.

With the fundamental mission reliability, along with the capabilities of self-stabilization, anti-disruption, and risk isolation evaluated in the previous steps, the final result of integrated mission reliability evaluation, i.e.,

$$\begin{cases} R_{i;sf}(t) = R_i(t) \cdot S_i \cdot I_i \cdot H_i, \\ R_{sf}(t) = \prod_{i=1}^{n} R_{i;sf}(t) \end{cases}$$

can be obtained and plotted as Fig. 9 and Fig 10, for subsystems (CDU, WEU, NSR and WEU) and the entire system, respectively.

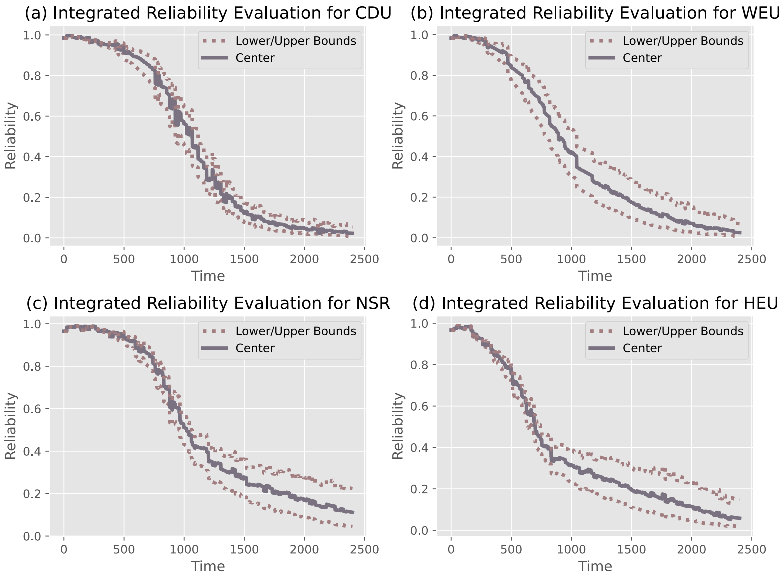

Fig. 9. Integrated mission reliability evaluation results for CDU, WEU, NSR and WEU.

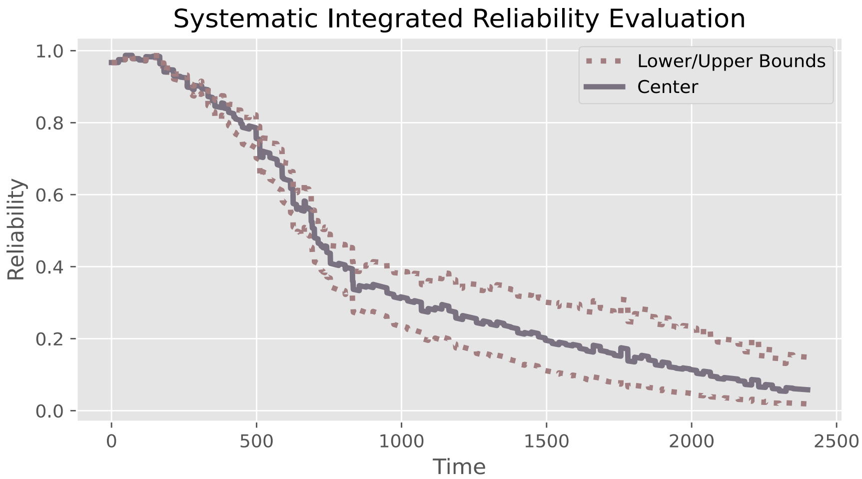

Fig. 10. Integrated mission reliability evaluation result for the EASP system.

4.3. Results and discussion

(1) Sensitivity Analysis

The integrated mission reliability assessment method proposed in this paper takes fundamental reliability, which is proposed in Section 3.1, as baseline model. In the industrial case study performed in this section, the DSCTMP model is applied for fundamental reliability analysis, and the STI parameters are estimated as belief intervals $[\lambda_{ij;L}, \lambda_{ij;U}]$ considering epistemic uncertainty. Considering that the interval estimation result of mission reliability can be highly sensitive STI interval length $\Delta\lambda_{ij} = \lambda_{ij;U} - \lambda_{ij;L}$, the sensitive analysis has been performed on the effects of $\Delta\lambda_{ij}$ variation to final results. Given that in practice, the belief evaluation generally keeps $\Delta\lambda_{ij} \leq 0.02$, we apply three levels of $\Delta\lambda_{ij}$, i.e., $\Delta\lambda_{ij} = 0.0059, 0.0017, 0.0176$, and 0.0234, to the sensitivity analysis based on invariant interval center values. The effects of $\Delta\lambda_{ij}$ to final result derivation are presented by the distribution of final reliability evaluation results, which have been plotted in Fig. 11 in boxplot form. The result of sensitivity analysis shows that when $\Delta\lambda_{ij} \leq 0.02 < 0.0234$, interval ranges of the integrated reliability evaluation results are all similar, indicating that the robustness of the proposed method is acceptable under the application scenario of EASP industrial case.

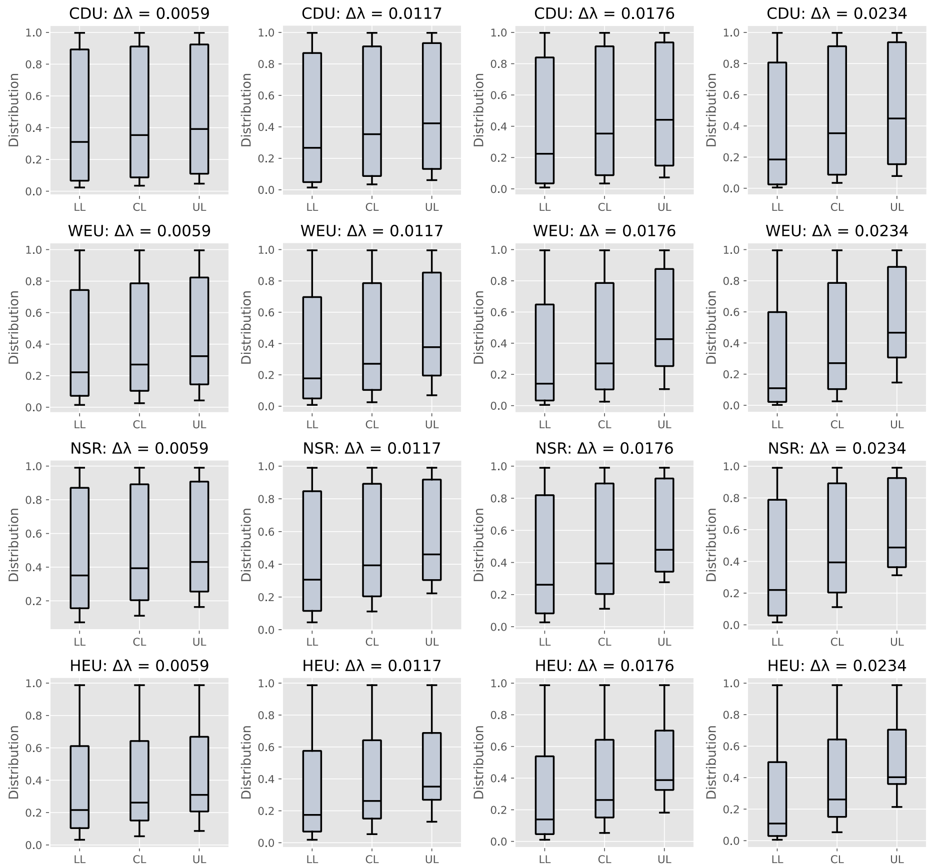

Fig. 11. Result of sensitivity analysis: effect of $\Delta\lambda_{ij}$ on final result distribution, where "LL/CL/UL" represents lower limit, central line, and upper limit.

(2) Comparative Study

When used as a safety indicator, the proposed integrated-reliability evaluation method is typically implemented within risk early-warning mechanisms, which is required to signal when reliability evaluation value descends below a minimal-acceptable limit. In this section, the signaling time of the proposed method based on different limits are compared to conventional methods that simply take fundamental reliability as evaluation results, see specific results in Table 4. Results of comparison shows that the proposed method advances the signaling time, which indicates that the method proposed in this paper is effective in identifying the deterioration of equipment self-stabilization, anti-disruption and risk isolation capability, and raise timely signals when the deteriorations are possible to be activated as safety issues by energy/material flow fluctuations.

Table 4. Result of comparative study: early-warning signal time of the proposed and conventional reliability evaluation methods

Minimal-acceptable Reliability Limit	**Signaling time (based on central-line reliability evaluation)**		
	Proposed method	Conventional method	Advancing Proportion
0.1	833.0118	1458.5765	42.8887%
0.105	830.6678	1443.6333	42.4599%
0.11	830.6678	1428.983	41.87%
0.115	830.6678	1414.9188	41.2922%
0.12	830.6678	1401.4406	40.7276%
0.125	821.2917	1388.2554	40.84%
0.13	818.9476	1375.6562	40.4686%
0.135	818.9476	1363.35	39.9312%
0.14	806.9344	1351.6298	40.2992%
0.145	774.9969	1339.9097	42.1605%
0.15	774.9969	1328.7755	41.6759%

(3) Application universality

The integrated mission-reliability framework proposed herein is not confined to the electrochemical ammonia-synthesis case. Because the three capability indices—self-stabilization, anti-disruption, and risk-isolation—are energy-centric and equipment-agnostic, the model can be readily mapped to manufacturing systems with fast, high-density energy exchange. Steel hot-rolling lines are a representative example: (i) self-stabilization corresponds to the mill's ability to maintain roll-gap force and strip-temperature uniformity under internal load fluctuations; (ii) anti-disruption capability captures the line's resilience to upstream slab-quality variance or sudden cooling-water pressure dips; and (iii) risk-isolation capability translates to rapid containment of strip breakage or hydraulic-oil ejection events to protect downstream stands and operators. Beyond steel manufacturing, analogous mappings exist for continuous casting, laser welding of battery tabs, and high-speed aluminum extrusion, all of which exhibit comparable multi-energy couplings and safety constraints. These examples demonstrate that only minor parameter tuning—primarily to the energy-flow monitoring and fault-detectability sub-models—is required to deploy the framework across diverse, energy-driven industrial scenarios.

5. Conclusion

This paper presents a novel inherent safety-oriented mission reliability evaluation method considering energy activity, which provides a valuable reference for the operational safety evaluation of manufacturing systems. According to the operation mechanism of the manufacturing system, the new connotation of inherent safety-oriented mission reliability of the manufacturing system is put forward considering the production factors of the whole process of manufacturing system including energy activities. Then, the inherent safety-oriented mission reliability is further analyzed from the three aspects of self-stabilization capability, anti-disruption capability and risk isolation capability. At the same time, the mathematical model is established. Finally, a comprehensive evaluation method is proposed to characterize the inherent safety-oriented mission reliability of manufacturing systems by integrating the above three aspects, which provides guidance for manufacturers to make better reliability evaluation. In addition, the proposed framework shows strong generalizability and can be extended to other energy-driven manufacturing scenarios such as steel hot-rolling, electrolysis, electroplating, and laser welding, with only minor parameter adjustments.

In future research, the mission reliability evaluation method of the state manufacturing system can be further improved in the following directions:

(1) The interaction between personnel and other production factors is not considered in this paper, so it can be mainly considered in the scope of modeling analysis in the subsequent research.

(2) Considering the different states of energy, subsequent mission reliability assessments need to be oriented toward different forms of energy.

(3) In future research, we will conduct in-depth discussions on the interaction between personnel and other production factors, which will bring new perspectives and innovative ideas to the field of production management. This will not only help enrich and improve the existing production theory system, but also provide practical solutions for enterprises to optimize personnel allocation, improve the efficiency of production factor utilization, improve product quality and reduce costs in the actual production process.

References

1. Chen Z, Chen Z, Zhou D, Pan E. Energy-oriented opportunistic maintenance optimization of continuous process manufacturing systems with two types of stochastic durations. Reliability Engineering & System Safety 2023;237:109385. https://doi.org/10.1016/j.ress.2023.109385.
2. Pan C, Hu B, Shao C, Xu L, Xie K, Wang Y, et al. Reliability-Constrained Economic Dispatch With Analytical Formulation of Operational Risk Evaluation. IEEE Transactions on Power Systems 2024;39:4422–36. https://doi.org/10.1109/TPWRS.2023.3317973.
3. Khan FI, Amyotte PR. Integrated inherent safety index (I2SI): A tool for inherent safety evaluation. Process Safety Progress 2004;23:136–48. https://doi.org/10.1002/prs.10015.
4. Kletz TA. Inherently Safer Design—Its Scope and Future. Process Safety and Environmental Protection 2003;81:401–5.

https://doi.org/10.1205/095758203770866566.
5. GUO H, SU G, LIN W, et al. Duality of production-related energy objects and mechanism of abnormal release of energy. China Safety Science Journal 2021;31(04):1-10.
6. Gonçalves V, Medeiros B, Alves W. Analytical Reliability Prediction for an Industrial Dynamic Furnace. 2025 Annual Reliability and Maintainability Symposium (RAMS), 2025, p. 1–5. https://doi.org/10.1109/RAMS48127.2025.10935126.
7. Amiludin MF, Firmansyah E, Wijaya FD, Hasbi W. Enhanced Satellite Power Distribution Reliability with Contingency Plan and Nonexclusive Redundancy. 2024 IEEE International Conference on Aerospace Electronics and Remote Sensing Technology (ICARES), 2024, p. 1–7. https://doi.org/10.1109/ICARES64249.2024.10767968.
8. Ding Y, Wang P, Goel L, Billinton R, Karki R. Reliability assessment of restructured power systems using reliability network equivalent and pseudo-sequential simulation techniques. Electric Power Systems Research 2007;77:1665–71. https://doi.org/10.1016/j.epsr.2006.11.010.
9. Zheng H, Cheng Y, Gou B, Frank D, Bern A, Muston WE. Impact of automatic switches on power distribution system reliability. Electric Power Systems Research 2012;83:51–7. https://doi.org/10.1016/j.epsr.2011.08.018.
10. Balijepalli N, Venkata SS, Christie RD. Modeling and analysis of distribution reliability indices. IEEE Transactions on Power Delivery 2004;19:1950–5. https://doi.org/10.1109/TPWRD.2004.829144.
11. Xujun S, Xuezhi L. Reliability simulation and analysis of phased-mission system with multiple states. Journal of Systems Engineering and Electronics 2019;30:624–32. https://doi.org/10.21629/JSEE.2019.03.19.
12. Xiuzhen Yang,Yihai He,Di Zhou,Xin Zheng.Mission reliability–centered maintenance approach based on quality stochastic flow network for multistate manufacturing systems.Eksploatacja i Niezawodność – Maintenance and Reliability.2022,24(3):455-467,https://doi.org/10.17531/ein.2022.3.7.
13. Zhang P, Chan KW. Reliability Evaluation of Phasor Measurement Unit Using Monte Carlo Dynamic Fault Tree Method. IEEE Transactions on Smart Grid 2012;3:1235–43. https://doi.org/10.1109/TSG.2011.2180937.
14. Liu Y, Singh C. Reliability Evaluation of Composite Power Systems Using Markov Cut-Set Method. IEEE Transactions on Power Systems 2010;25:777–85. https://doi.org/10.1109/TPWRS.2009.2033802.
15. Jalilvand A, Khanmohammadi S, Shabaninia F. Petri net-based modeling and simulation of a hybrid manufacturing system. Proceedings of the IEEE Symposium on Emerging Technologies, 2005., 2005, p. 382–7. https://doi.org/10.1109/ICET.2005.1558912.
16. Yi X, Shi J, Dhillon B s., Hou P, Lai Y. A new reliability analysis method for repairable systems with multifunction modes based on goal-oriented methodology. Quality and Reliability Engineering International 2017;33:2215–37. https://doi.org/10.1002/qre.2180.
17. Lu Z, Zhang Z, Zhuang L, Zhou J. Reliability Model of the Fly-By-Wire System Based on Stochastic Petri Net. International Journal of Aerospace Engineering 2019;2019. https://doi.org/10.1155/2019/2124836.
18. Yang X, Li J, Liu W, Guo P. Petri Net Model and Reliability Evaluation for Wind Turbine Hydraulic Variable Pitch Systems. Energies 2011;4:978–97. https://doi.org/10.3390/en4060978.
19. Melani AH de A, de Souza GFM, de Oliveira S Junior, Freire RLA. Improving Centralized Offshore Power Generation Design With Petri Net-Based Availability and Reliability Analysis. ASCE-ASME J Risk and Uncert in Engrg Sys Part B Mech Engrg 2024;10. https://doi.org/10.1115/1.4063394.
20. Omar Reffas,Yacine Sahraoui,Mourad Nahal,Rachida Hadiby Ghoul,Salah Saad.Reactive energy compensator effect on the reliability of a complex electrical system using Bayesian networks.Eksploatacja i Niezawodnosc – Maintenance and Reliability,2020,22(4):684-693,http://dx.doi.org/10.17531/ein.2020.4.12.
21. Chen Q, Wang J, Integrated Multi-Energy Hub Optimization: A Model for Reliable, Economically Efficient, and Sustainable Energy Systems, Eksploatacja i Niezawodnosc – Maintenance and Reliability 2025: 27(3) http://doi.org/10.17531/ein/201335.
22. Josephin Shermila P, Anu Disney D, Reeda Lenus C, Niruban R, Efficiency and Reliability: Optimization of Energy Management in Electric Vehicles Apply Monarch Butterfly Algorithm and Fuzzy Logic Control, Eksploatacja i Niezawodnosc – Maintenance and Reliability 2025: 27(3) http://doi.org/10.17531/ein/200691.
23. Jiang W, Cui L, Liang X. Optimal maintenance policies for three-unit parallel production systems considering yields. Reliability Engineering & System Safety 2024;248:110163. https://doi.org/10.1016/j.ress.2024.110163.

24. Duman E, Seckin D. Enhancing the efficiency of cabin heaters in emergency shelters after earthquakes through an optimized fuzzy controller. Build Simul 2023;16:1759–76. https://doi.org/10.1007/s12273-023-1062-9.
25. Massrur HR, Niknam T, Aghaei J, Shafie-khah M, Catalão JPS. Fast Decomposed Energy Flow in Large-Scale Integrated Electricity–Gas–Heat Energy Systems. IEEE Transactions on Sustainable Energy 2018;9:1565–77. https://doi.org/10.1109/TSTE.2018.2795755.
26. Zhao X, Liu F, Fu B, Fang N. Reliability analysis of hybrid multi-carrier energy systems based on entropy-based Markov model. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 2016;230:561–9. https://doi.org/10.1177/1748006X16663056.
27. Zhang Y, Chowdhury AA, Koval DO. Probabilistic Wind Energy Modeling in Electric Generation System Reliability Assessment. IEEE Transactions on Industry Applications 2011;47:1507–14. https://doi.org/10.1109/TIA.2011.2127435.
28. Liu H, Zhao Y, Ge S, Zhang P, Liu W, Qi X, et al. Reliability evaluation of regional energy Internet considering electricity–gas coupling and coordination between energy stations. IET Energy Systems Integration 2021;3:238–49. https://doi.org/10.1049/esi2.12014.
29. Meng Z, Wang S, Zhao Q, Zheng Z, Feng L. Reliability evaluation of electricity-gas-heat multi-energy consumption based on user experience. International Journal of Electrical Power & Energy Systems 2021;130:106926. https://doi.org/10.1016/j.ijepes.2021.106926.