

MULTI-OBJECTIVE PRODUCTION PLANNING WITH CYBERSECURITY CONSTRAINTS IN INDUSTRIAL IOT

Feng, Y. T.^{*}; Liu, L. Q.^{**,#}; Tang, D. D.^{***}; Shu, W. B.^{*}; Yan, B.^{****} & Zhou, J.^{*}

^{*} School of Computer and Artificial Intelligence, Hefei Normal University, Hefei 230601, China

^{**} Information Management Office, Hefei Normal University, Hefei, 230601, China

^{***} Anhui Traceable Information Technology Co., Ltd., Hefei 230601, China

^{****} Hangzhou Yunzhimeng Technology Co., Ltd., Hangzhou 310000, China

E-Mail: liulequn@hfnu.edu.cn (# Corresponding author)

Abstract

The integration of the Industrial Internet of Things (IIoT) has increased the interdependence between production systems and cyberspace, making cybersecurity threats a critical factor in manufacturing performance. Traditional production planning methods rarely account for dynamic cyber risks, limiting their ability to ensure resilient and efficient operations. This study proposes a simulation-driven security–production collaborative optimization framework. Cyber threats are modelled through a dynamic coupling mechanism and embedded as operational constraints in a multi-objective production planning model. Based on digital twins and two-stage stochastic programming, the model simultaneously minimizes makespan, energy consumption, and cybersecurity risk. An improved multi-objective evolutionary algorithm with simulation-based evaluation is developed to assess schedule robustness under attack scenarios. The proposed framework enables systematic modelling and evaluation of resilient production planning in IIoT-enabled manufacturing environments.

(Received in November 2025, accepted in February 2026. This paper was with the authors 1 week for 1 revision.)

Key Words: IIoT, Cybersecurity, Production Planning Optimization, Multi-Objective Optimization, Digital Twin Simulation

1. INTRODUCTION

The Industrial Internet of Things (IIoT), as a core enabling technology of intelligent manufacturing, is driving production systems toward comprehensive interconnection and intelligent collaboration [1-3]. However, while this deep integration improves production efficiency and flexibility, it also exposes physical production processes to increasingly severe cybersecurity threats [4, 5]. Cyberattacks can directly penetrate from cyberspace into the physical layer, leading to abnormal equipment shutdowns, tampering of production data, product quality defects, or even complete production line stoppages, thereby causing significant economic losses and safety risks [6, 7]. Therefore, proactively integrating cybersecurity considerations at the production planning level and constructing resilient production systems capable of resisting uncertain threats have become key issues urgently to be addressed by both industry and academia.

At present, although substantial research achievements have been made in the fields of production planning optimization and IIoT security, these two domains have largely been studied independently, resulting in a significant research gap. On the one hand, traditional multi-objective production planning optimization models mainly focus on classical performance indicators such as makespan, cost, and energy consumption [8, 9], generally neglecting the uncertainty of cyberattacks in the operational environment. As a result, the formulated production plans may be highly vulnerable under real cyber threats. On the other hand, existing IIoT security research mostly concentrates on static risk assessment, intrusion detection, or protocol protection [10-12], lacking quantitative analysis of how security events

dynamically affect specific production scheduling logic. A few studies attempting to integrate the two typically use simple static weights or penalty factors to represent cybersecurity risk [13, 14], failing to characterize the randomness and propagation of cyberattacks as well as the chain production disturbances they trigger [15-18]. Such static and isolated modelling approaches are unable to cope with dynamic and complex attack scenarios such as advanced persistent threats, and are also insufficient for evaluating and optimizing the actual resilience performance of production plans under attack. Based on this, this study aims to address a core scientific question: how to formulate production plans that simultaneously optimize production efficiency and energy consumption while possessing high resilience under dynamic and uncertain cybersecurity threats.

To address the above issues, this study proposes a simulation-driven security-production collaborative optimization and evaluation integrated framework. The core objective of this research is to provide new theoretical methods and tool support for production planning decision-making under dynamic cyber threat environments through the deep integration of mechanism modelling, optimization algorithms, and simulation validation. The main contributions of this paper are reflected in the following three aspects. At the theoretical level, the first multi-objective production planning optimization framework integrating dynamic cybersecurity constraints is proposed. At the methodological level, a real-time quantitative model of cyber threats-production disturbances is established, a simulation-embedded multi-objective evolutionary algorithm is designed, and a digital twin simulation testbed supporting hardware-in-the-loop is constructed. At the practical level, a decision-support tool capable of quantitatively evaluating the production benefits of cybersecurity investment is provided.

The remainder of this paper is organized as follows. Section 2 systematically elaborates the overall architecture of the proposed simulation-driven optimization framework, and details the security-production dynamic coupling modelling method, the two-stage stochastic programming model, and the design of the simulation-embedded optimization algorithm. Section 3 introduces the construction of the digital twin-based simulation experimental platform, case parameter settings, and multi-scenario experimental design, presents and analyses the experimental results in depth, and verifies the superiority of the proposed method through visual comparison. Finally, the paper concludes and discusses future research directions.

2. METHODOLOGY

2.1 Overview of the overall framework

This section proposes a simulation-driven five-layer integrated framework aimed at achieving closed-loop collaborative optimization between dynamic cybersecurity constraints and multi-objective production planning. As shown in Fig. 1, the framework consists of the physical layer, model layer, algorithm layer, simulation layer, and application layer from bottom to top. Its core innovation lies in breaking the limitations of traditional static optimization through the dynamic coupling mechanism established in the model layer and the simulation evaluation loop embedded in the algorithm layer. The real-time status of actual production equipment and network facilities in the physical layer is mapped in real time. In the model layer, an extended attack graph model is innovatively constructed, in which the node asset attributes integrate production context such as equipment criticality, controlled processes, and downtime cost, enabling network vulnerabilities to be quantified as a time-evolving production risk function $R(t)$. The algorithm layer operates the proposed simulation-embedded multi-objective evolutionary algorithm. The key innovation of this algorithm is that the fitness evaluation of each candidate production plan is not obtained

through analytical calculation, but is generated by driving the high-fidelity digital twin in the simulation layer to run under simulated dynamic cyberattack scenarios. The simulation layer utilizes millisecond-level synchronization between high-fidelity discrete event simulation and a cyberattack simulation engine to accurately simulate the chain event flow of attack penetration, production disturbances, and response action triggering. Finally, the application layer relies on the deep simulation data obtained from this closed loop to provide a Pareto-optimal production plan set that balances efficiency, energy consumption, and security resilience, as well as a dynamic decision dashboard. The entire framework achieves continuous evaluation and improvement of the dynamic resilience of the production system under uncertain cybersecurity threats through the data closed loop of “perception-modelling-optimization-simulation-decision”.

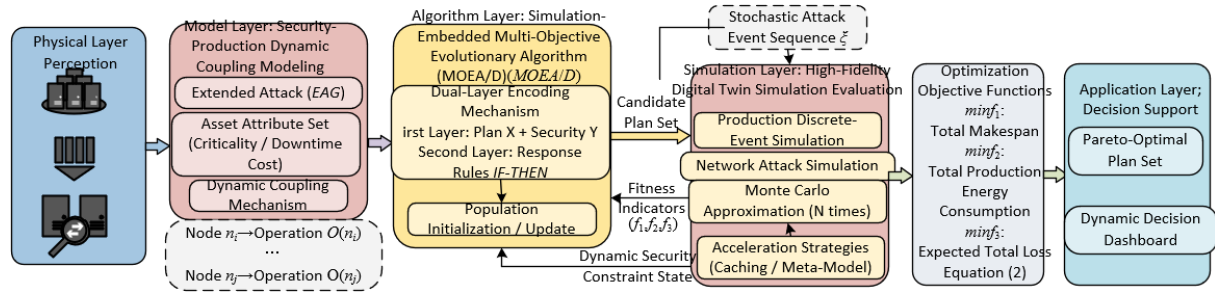


Figure 1: Simulation-driven optimization framework.

2.2 Security-production dynamic coupling modelling in the industrial internet of things environment

To construct a dynamic coupling model between cybersecurity threats and physical production processes, this study first formalizes the IIoT production system as a quadruple: $SP = \langle P, N, J, A \rangle$, where $P = \{p_1, p_2, \dots, p_m\}$ denotes the set of physical resources; $N = \{n_1, n_2, \dots, n_l\}$ denotes the set of network devices; $J = \{j_1, j_2, \dots, j_k\}$ denotes the set of production tasks; $A = \{a_1, a_2, \dots, a_h\}$ denotes the set of potential cyberattack vectors. One of the core innovations of this study is the proposed extended attack graph model $EAG = (N, E, Attr)$. Unlike traditional attack graphs that only include the node set N and directed edge set E , the EAG assigns each node n_i a multi-attribute vector $Attr(n_i) = [D(n_i), O(n_i), Cd(n_i), \omega_i]$, where $D(n_i) \subseteq P$ represents the set of physical devices it controls; $O(n_i) \subseteq J$ represents the set of production processes directly affected when its functionality is compromised; $Cd(n_i)$ denotes the unit-time downtime cost caused by its failure; and ω_i is its criticality weight in the production context. When an attack $a_q \in A$ successfully exploits edge $e_{ij} \in E$ to penetrate from node n_i to n_j , a primary production disturbance $\Delta P_{primary}(n_j, a_q)$ is triggered, which may cause equipment in $D(n_j)$ to shut down or degrade the processing quality of operations in $O(n_j)$. Its severity is quantified by the function $Severity(a_q, n_j)$.

Based on the primary disturbance, this study constructs a dynamic model for the propagation of production cascade effects. The production system is described as a dynamic directed graph $G_s(t) = (V_s, E_s, S(t))$, where vertices V_s represent processes or resources, edges E_s represent material or control flows, and $S(t)$ denotes the system state at time t . The primary disturbance, as an initial event, propagates in $G_s(t)$ through the state transition function $f_{propagate}: S(t) \times \Delta P_{primary} \rightarrow S(t + \Delta t)$, thereby triggering secondary disturbances such as subsequent process delays and resource idleness. This propagation process is dynamically computed by the discrete event simulation engine rather than statically estimated. Finally, the dynamic security risk is transformed into scheduling constraints. For a critical task j_k , the cumulative real-time risk value of the subgraph composed of all its related resource nodes $G(j_k) \subseteq N$ must satisfy:

$$R_t(G(j_k)) = \sum_{n_i \in G(j_k)} [\omega_i \cdot Vul(n_i) \cdot Impact(n_i, S(t)) \cdot (1 - Eff(n_i))] < \tau_k \quad (1)$$

where, $Vul(n_i)$ is the inherent vulnerability score of node n_i , $Eff(n_i) \in [0, 1]$ is the effectiveness of deployed defence measures, and $Impact(n_i, S(t)) = C_d(n_i) \cdot T_d(n_i, S(t))$ is the dynamic impact function, which depends on the estimated interruption duration $T_d(n_i, S(t))$ caused by node failure under the current state $S(t)$ fed back by the simulation. The threshold τ_k is determined by production criticality. This constraint ensures the adaptability of the production plan to dynamic cybersecurity risk.

2.3 Two-stage stochastic programming model considering cybersecurity incident response

Based on the aforementioned dynamic coupling model, this study constructs a two-stage stochastic programming model to integrate proactive defence and incident response. The innovation of this model lies in explicitly combining the decision sequence with the randomness of cyberattacks. In the first stage, at the beginning of the planning horizon, the production planning variable X and the basic security resource allocation variable Y are determined based on known information. X defines operation sequencing, machine assignment, and start times; Y is a binary decision vector indicating whether preventive measures such as intrusion detection or enhanced authentication are deployed at specific network nodes. When the simulated execution enters the second stage and a random attack event ξ , which follows a discrete probability distribution $P(\xi)$, occurs, the model triggers real-time response decisions, including activating mitigation measures Z_ξ and implementing production rescheduling plans W_ξ . This two-stage structure fully characterizes the full-cycle security-production collaborative decision-making process from prevention to response through the decision variables (X, Y, Z_ξ, W_ξ) .

This model aims to minimize three mutually conflicting objectives: the total makespan $f_1(X, Y) = \max(C_j)$, where C_j is the completion time of task j ; the total production energy consumption $f_2(X, Y)$, which is the sum of processing energy consumption and idle energy consumption of all machines; and the key innovative objective – the expected total loss under cybersecurity incidents f_3 , which is defined as the sum of preventive cost and the expected response loss under random attacks, and its mathematical expression is:

$$f_3(X, Y) = C_{pro}(Y) + E_\xi[Q(X, Y, \xi)] \quad (2)$$

where, $C_{pro}(Y) = \sum_i (c_i \cdot y_i)$ is the fixed cost of deploying preventive measures Y ; $Q(X, Y, \xi)$ is the second-stage cost under a given attack ξ , including dynamic response cost $C_{res}(Z_\xi)$ and production loss $C_{loss}(W_\xi, \xi)$. The expectation is:

$$E_\xi[] = \sum_{\xi \in \Xi} P(\xi) \cdot Q(X, Y, \xi) \quad (3)$$

It is approximated through a large number of concurrent simulation samplings, which is the core of the proposed solution strategy. All decisions must simultaneously satisfy traditional capacity constraints, material balance constraints, and the dynamic cybersecurity constraint defined by $R_t(G(j_k)) < \tau_k$. This constraint is continuously evaluated in the simulation according to the attack event ξ and the response action Z_ξ , thereby ensuring the resilience of the optimized solution under all scenarios.

2.4 Simulation-embedded multi-objective evolutionary algorithm

To solve the above two-stage stochastic programming model, this study designs a simulation-embedded multi-objective evolutionary algorithm. The core innovation of this algorithm lies in embedding the high-fidelity co-simulation engine as the fitness function directly into the optimization loop of MOEA/D, thereby achieving precise evaluation of the dynamic resilience of solutions. The algorithm adopts a two-layer encoding mechanism to

represent the complete solution. The first layer is hybrid encoding, in which operation sequencing adopts job-based real-number encoding, machine assignment adopts integer encoding, and the basic security configuration Y adopts binary encoding. The second layer is response strategy encoding. In this study, a fixed-length rule sequence encoding is adopted, in the form of a rule set IF [attack pattern] THEN [response action]. This encoding determines the dynamic response decisions Z_ξ and W_ξ triggered when specific cyberattack events ξ are encountered during simulation execution. Unlike traditional optimization algorithms that evaluate solutions only through analytical models, in this algorithm the fitness value of each individual must be obtained by driving simulation experiments.

The fitness evaluation process is the key technical detail of the algorithm innovation. At the beginning of evaluation, the algorithm independently instantiates a digital twin simulation environment for each individual in the population. During the advancement of the simulation clock, the platform randomly injects attack event sequences according to the predefined attack probability distribution. The simulation engine triggers response actions in real time according to the second-layer rules in the individual encoding, and fully records production logs and security events. The key objective function values, such as makespan f_1 , energy consumption f_2 , and the most challenging expected total loss f_3 , are all collected from this simulation. Among them, the evaluation of f_3 involves the expectation calculation over random attacks ξ . We perform Monte Carlo approximation by executing N independent simulations for each individual, that is,

$$E_\xi[Q(X, Y, \xi)] \approx \frac{1}{N} \sum_{r=1}^N Q_r \quad (4)$$

To address the substantial computational cost of simulation-based evaluation, the algorithm integrates two efficiency optimization strategies. First, a simulation cache is established to reuse intermediate results of production plan segments and security configurations with identical hash values. Second, in the early stage of evolution, a surrogate model based on Gaussian process regression is introduced for fast approximate evaluation, and full simulation evaluation is conducted only for elite solutions generated in the later stage of iterations. In this way, a balance between accuracy and efficiency is achieved to ensure the feasibility of the algorithm.

2.5 Implementation of the industrial internet of things production-network co-simulation platform

To verify the aforementioned models and algorithms, this study designs and develops a high-fidelity IIoT production-network co-simulation platform. The platform adopts a digital twin architecture, and its core innovation lies in realizing the deep integration and bidirectional interaction of the cyber-physical system in virtual space. The platform establishes real-time data connections with physical-layer equipment through the OPCUA protocol, ensuring that the equipment status in the virtual model is synchronized with the physical world. The platform consists of three core modules: a production system discrete event simulation module built on AnyLogic, responsible for refined modelling of equipment behaviour, material flow, and production control logic; a network attack simulation module built on OMNeT++, capable of simulating the complete attack chain from scanning and penetration, vulnerability exploitation to lateral movement, and accurately generating attack traffic of multiple industrial protocols including MQTT and Profinet; and a self-developed real-time interaction middleware, which serves as the central nervous system and is responsible for coordinating the concurrent execution and event-driven interaction of the above two modules under a unified simulation clock.

The key to platform operation lies in the security event-production disturbance dynamic mapping table and the event queue mechanism maintained by the middleware. The mapping

table defines deterministic or stochastic rules from cyberattack events to specific production impact actions. For example, when the network attack simulation module detects that PLC_1 has been successfully compromised, it publishes a structured event tuple to the event queue:

$$Event_c = (Type: "Node_Compromised", ID: "PLC_1", Sim_Time: t, Payload: \{\dots\}) \quad (5)$$

The middleware processes the queue in chronological order of simulation time, queries the mapping table, and then sends corresponding disturbance instructions to the production simulation module, such as triggering a shutdown of Machine_1. As illustrated in Fig. 2, the shutdown duration can be set as a fixed value according to attack severity or randomly sampled from a specific distribution. This event-driven mechanism enables the consequences of cyberattacks, such as equipment failure and data tampering, to be accurately reflected in the production simulation process with extremely low latency, thereby high-fidelity reproducing the chain dynamic process in which cybersecurity incidents lead to production delays, quality degradation, or even complete line shutdown, and providing a reliable experimental environment for evaluating the dynamic resilience of production plans.

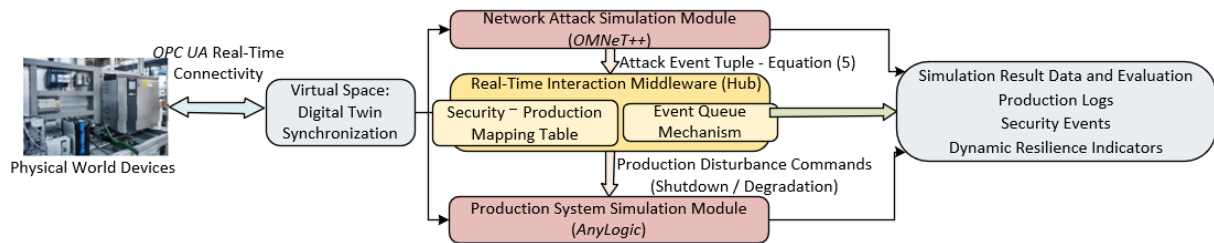


Figure 2: Operation process of the production-network co-simulation platform.

3. EXPERIMENTAL DESIGN AND CASE ANALYSIS

3.1 Case background and experimental parameters

To verify the effectiveness of the proposed framework, this study constructs a digital twin of an intelligent assembly unit that maps a real automotive component production line. The physical system of the unit includes four Computer Numerical Control (CNC) machine tools, two six-axis collaborative robots, one vision inspection station, and one Automated Guided Vehicle (AGV) conveyor line, responsible for the production of three types of steering knuckles. Each product undergoes 8 to 12 precision machining and assembly operations. Its IIoT network strictly follows the Purdue model architecture: Level 3 deploys the manufacturing execution system and database servers; Level 2 deploys Supervisory Control and Data Acquisition (SCADA) monitoring stations and Open Platform Communications Unified Architecture (OPCUA) servers; Level 1/0 consists of Siemens S7-1500 series Programmable Logic Controller (PLC), robot controllers, and various sensors, communicating through industrial Ethernet Profinet. To simulate real threats, multiple known vulnerabilities are embedded in key nodes. For example, an SQL injection vulnerability similar to CVE-2021-27878 is preset in the Manufacturing Execution System (MES) database server, and a hard-coded credential vulnerability is simulated in specific PLCs, thereby constructing an attack surface with practical basis.

The experimental parameters are strictly set to ensure reproducibility. The optimization model involves 293 decision variables, including 285 production scheduling variables and 8 binary security configuration variables. The multi-objective weights are set as $\alpha = 0.4$ (makespan), $\beta = 0.3$ (total energy consumption), and $\gamma = 0.3$ (security risk). The cybersecurity risk threshold τ of the critical path is set to 0.15. The simulation platform integrates AnyLogic 8.8, OMNeT++ 6.0, and ROS2 Galactic, and achieves cross-platform millisecond-level event

synchronization through customized middleware. As shown in Table I, the attack scenario library designs four typical scenarios, as shown in the following table, to generate a dynamic testing environment.

Table I: Four typical scenarios.

Scenario ID	Attack type	Entry point	Attack chain overview	Expected production impact
S1	Ransomware	IT network (engineering workstation)	Phishing email → privilege escalation → lateral movement to MES database → data encryption	Loss of production orders and process data, full-line schedule interruption
S2	Process tampering	OT network (OPCUA interface)	Unauthorized OPCUA access → malicious code injection into robot controller → parameter tampering	Decreased assembly precision, increased product defect rate
S3	Advanced persistent threat	IT network	Long-term latent presence → triggered at a specific time → abnormal command sent to target PLC	Unplanned shutdown of target equipment, disruption of production rhythm
S4	Combined attack	Multiple entry points	Concurrent execution of S1 and S2 with coordination	Hybrid impact, significantly increased system recovery difficulty

3.2 Multi-scenario experimental design

To systematically verify the performance of the proposed framework across different dimensions, four progressive experimental scenarios are designed. Scenario A is conducted in a static environment without cyberattacks, aiming to verify that the simulation-embedded multi-objective evolutionary algorithm proposed in this paper achieves benchmark performance comparable to advanced algorithms in traditional production optimization problems. Scenario B introduces a single deterministic attack scenario to test and compare the dynamic resilience of different production plans when facing a specific cyber threat. The core objective is to verify the effectiveness of the security-production dynamic coupling model and the simulation evaluation loop. Scenario C simulates a more realistic uncertain mixed attack environment. Stress testing is conducted using the Monte Carlo method to evaluate the superiority of the two-stage stochastic programming model and adaptive response strategies under complex threats. Scenario D verifies the fidelity of the simulation platform itself and the computational efficiency of the algorithm, ensuring the credibility of the experimental tool and the practicality of the method.

Table II: Scenario A – Performance comparison of algorithms in static environment.

Algorithm	Hypervolume (<i>HV</i>)	Inverted generational distance (<i>IGD</i>)	Average completion time (minutes)	Average total energy consumption (kWh)	Comprehensive score (weighted)
NSGA-II (Baseline)	0.725	0.058	1245	856	0.682
MOEA/D (Static risk)	0.718	0.061	1268	841	0.675
Proposed Algorithm (Sim-Embedded MOEA/D)	0.732	0.052	1227	832	0.698

The evaluation indicators and experimental designs adopted in each scenario are described below, and the corresponding quantitative results and analysis are presented in Chapter 5.

The results in Table II show that, in the absence of cyberattack interference, the proposed algorithm is slightly superior to or comparable with other advanced algorithms in terms of solution set convergence (*HV*), distribution (*IGD*), and key production indicators. This demonstrates that its underlying optimization mechanism is robust and effective, laying a reliable performance foundation for subsequent resilience testing.

Table III: Scenario B – System resilience indicators under single attack scenario.

Attack script	Method	Dynamic risk suppression rate (%)	Mean time to recovery <i>MTTR</i> (minutes)	Plane deviation degree (%)	Attack impact containment range (%)
S1 (Ransomware)	Traditional plane (NSGA-II)	12.5	143	35.2	78.6
	Static risk plan	25.7	118	28.5	65.3
	Proposed resilience plan	68.4	65	12.1	31.5
S3 (APT)	Traditional plane (NSGA-II)	8.3	95	22.8	51.7
	Static risk plan	31.2	76	18.9	42.4
	Proposed resilience plan	89.7	28	7.3	15.2

The data in Table III clearly indicate that when facing S1 and S3 attacks, the production plans generated by the proposed framework significantly outperform traditional and static risk methods across all resilience indicators. The substantial improvement in dynamic risk suppression rate and the reduction in average recovery time directly verify that the dynamic coupling model and real-time response strategies can effectively predict and mitigate attack impacts. The control of schedule deviation and impact scope reflects that the optimization algorithm successfully integrates security resilience objectives into production scheduling.

Table IV: Scenario C – Monte Carlo stress test results under mixed uncertain attacks.

Method	Average production performance degradation rate (%)	Performance degradation standard deviation	Plan success rate (degradation < 15 %)	Average number of simulation response decisions
Two-stage heuristic method	24.7	8.9	38.5 %	1.2 (Fixed rules)
Static risk plan	18.3	7.2	57.1 %	1.0 (No dynamic response)
Proposed resilience plan	9.8	4.5	86.4 %	3.6 (Adaptive)

The statistical results in Table IV are derived from 1000 Monte Carlo simulations. The proposed method controls the average degradation rate of production performance below 10% and increases the success rate to 86.4%, which is significantly higher than the comparison methods. The smaller standard deviation indicates more stable performance. The higher average number of response decisions with better effects demonstrates that the second-stage response strategy encoding can generate complex and adaptive countermeasures

rather than simple fixed rules, thereby verifying the core value of the two-stage stochastic programming model in handling uncertainty.

Table V: Scenario D – Simulation fidelity and algorithm computational efficiency.

Verification item	Indicator	Result
Simulation fidelity	Average error of key event timeline (vs. physical target scenario)	< 3 %
	Accuracy of attack success path simulation	100 % (covers all preset attack scripts)
Computational efficiency	Total number of simulation invocations (times)	12,480
	Speedup ratio after cache and meta-model adoption	5.7 ×
	Total algorithm convergence time (hours)	9.5

Table V verifies the reliability of the experimental infrastructure. The high simulation fidelity provides credibility support for the experimental results of all aforementioned scenarios. The computational efficiency data indicate that although simulation-based evaluation is computationally intensive, a 5.7-fold acceleration is achieved through the innovative caching and surrogate model strategies, and the total convergence time is controlled within an acceptable range, demonstrating the engineering feasibility of the proposed algorithm framework.

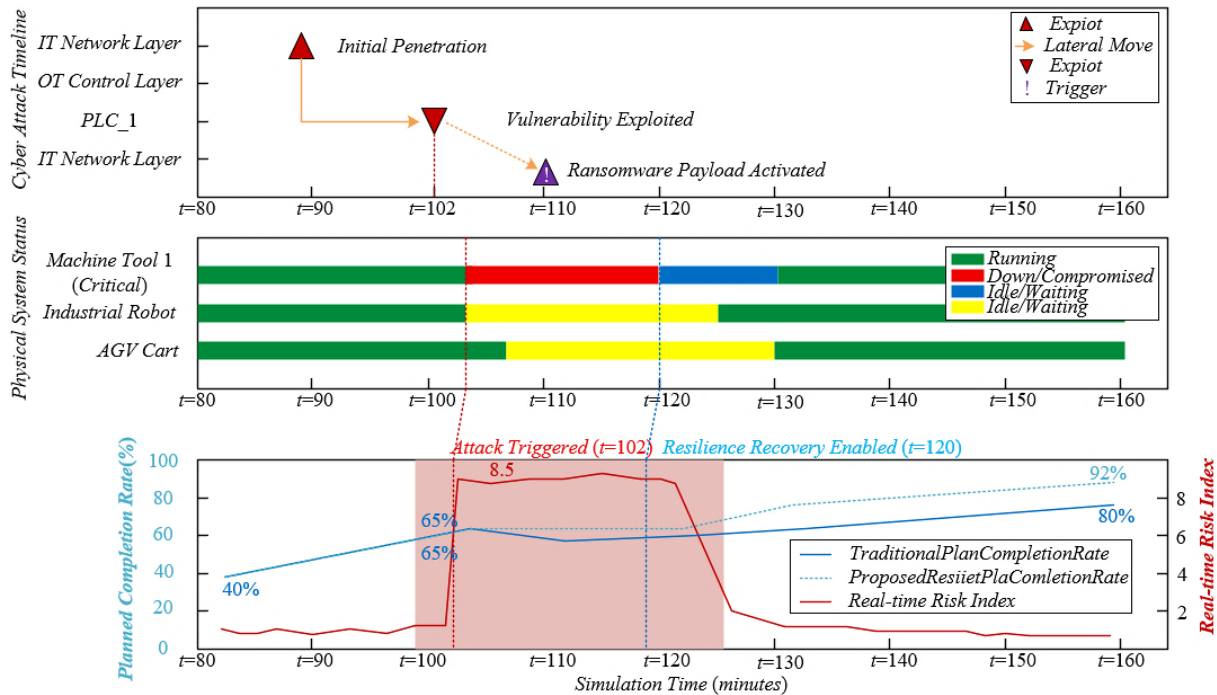


Figure 3: Time-sequence linkage diagram of dynamic process deep visualization.

To verify the effectiveness of the proposed dynamic coupling model and two-stage stochastic programming method in IIoT production scenarios and their capability to enhance resilience, this study conducts high-fidelity co-simulation experiments. As shown in Fig. 3, by reproducing a typical ransomware attack chain, the dynamic performance of multi-objective production planning under cybersecurity constraints is quantitatively evaluated. From the time-sequence linkage experimental results, it can be observed that after the attack is triggered at $t = 102$ minutes, the completion rate of the traditional production plan stagnates and remains at 65 % at $t = 120$ minutes. In contrast, although the completion rate of the resilient plan

integrating cybersecurity constraints slows down briefly, it consistently maintains a baseline level above 65 % and finally reaches 92 % at $t=160$ minutes, which is significantly higher than the 80 % of the traditional plan. At the same time, the real-time risk index rapidly rises to 8.5 after the attack, while the resilient plan activates response strategies at $t=120$ minutes, causing the risk index to quickly fall below the safety threshold and avoiding long-term paralysis of the production system. The physical equipment state matrix further shows that the critical machine tool experiences only 18 minutes of shutdown and recovery after the attack, whereas under the traditional plan the shutdown duration extends to 30 minutes, directly leading to cascading delays of subsequent operations. These results indicate that the proposed extended attack graph model and two-stage stochastic programming method can effectively transform cybersecurity risk dynamically into production scheduling constraints. While ensuring production efficiency and energy consumption objectives, they significantly enhance the dynamic resilience of IIoT systems against cyberattacks, providing quantifiable theoretical and practical support for security-production collaborative decision-making.

4. CONCLUSION

This study addressed the challenge of the deep coupling between cybersecurity threats and production scheduling in the IIoT environment, and proposed a simulation-driven security-production collaborative optimization framework. By establishing a dynamic coupling model between network attack graphs and production disturbances, time-varying security risks were quantified as real-time scheduling constraints, and a two-stage stochastic programming model integrating proactive defence and incident response was constructed. To solve this model, a simulation-embedded multi-objective evolutionary algorithm was innovatively designed, which takes high-fidelity collaborative simulation as the core of fitness evaluation, thereby achieving precise measurement of the dynamic resilience of planning schemes. Experimental results show that the framework can generate a set of Pareto-optimal plans, which significantly enhance the resilience of the production system when facing ransomware, advanced persistent threats, and other cyber attacks, while ensuring production efficiency and energy consumption performance, and controlling the degradation of production performance under uncertain attacks at a relatively low level, thus verifying the effectiveness and superiority of the proposed methodology.

However, this study still has certain limitations, which indicate directions for future work. First, the network attack scenarios in this study are based on known vulnerabilities and preset probabilities. In the future, AI-driven attack simulators can be integrated to generate more adaptive and stealthy threat scenarios, so as to test the limit resilience of the optimization framework in adversarial environments. Second, although the current digital twin simulation platform achieves high-fidelity simulation, it can be further connected with real industrial control security testbeds in the future to conduct hardware-in-the-loop validation, thereby enhancing the practical persuasiveness of the research conclusions. Finally, this study focuses on a single manufacturing unit. In the future, the framework can be extended to a supply chain network environment including multi-tier suppliers and manufacturers, to study cross-enterprise collaborative security strategies and production plan optimization problems, so as to address more systemic cybersecurity challenges.

REFERENCES

- [1] Kang, B. G.; Kim, B. S. (2024). Attachable IoT-based digital twin framework specialized for SME production lines, *International Journal of Simulation Modelling*, Vol. 23, No. 3, 471-482, doi:[10.2507/IJSIMM23-3-694](https://doi.org/10.2507/IJSIMM23-3-694)

- [2] Dakhnovich, A. D.; Moskvina, D. A.; Zegzhda, D. P. (2021). Requirements on providing a sustainability of Industrial Internet of Things, *Automatic Control and Computer Sciences*, Vol. 55, No. 8, 956-961, doi:[10.3103/S0146411621080071](https://doi.org/10.3103/S0146411621080071)
- [3] Szántó, N.; Monek, G. D.; Fischer, S. (2024). Development of an immersive, digital twin-supported smart reconfigurable educational platform for manufacturing training: a proof of concept, *Journal of Engineering Management and Systems Engineering*, Vol. 3, No. 4, 199-209, doi:[10.56578/jemse030402](https://doi.org/10.56578/jemse030402)
- [4] Vasil'ev, Y. S.; Zegzhda, D. P.; Poltavtseva, M. A. (2018). Problems of security in digital production and its resistance to cyber threats, *Automatic Control and Computer Sciences*, Vol. 52, No. 8, 1090-1100, doi:[10.3103/S0146411618080254](https://doi.org/10.3103/S0146411618080254)
- [5] Koniagina, M.; Belotserkovich, D.; Vorona-Slivinskaya, L.; Pronkin, N. (2023). Measures to ensure cybersecurity and regulation of the Internet of Things in the Russian federation: effectiveness assessment, *Journal of Economic Issues*, Vol. 57, No. 1, 257-274, doi:[10.1080/00213624.2023.2170136](https://doi.org/10.1080/00213624.2023.2170136)
- [6] Raimundo, R. J.; Rosario, A. T. (2022). Cybersecurity in the Internet of Things in industrial management, *Applied Sciences*, Vol. 12, No. 3, Paper 1598, 19 pages, doi:[10.3390/app12031598](https://doi.org/10.3390/app12031598)
- [7] Axon, L.; Fletcher, K.; Scott, A. S.; Stolz, M.; Hannigan, R.; El Kaafarani, A.; Goldsmith, M.; Creese, S. (2022). Emerging cybersecurity capability gaps in the Industrial Internet of Things: overview and research agenda, *Digital Threats: Research and Practice*, Vol. 3, No. 4, Paper 34, 27 pages, doi:[10.1145/3503920](https://doi.org/10.1145/3503920)
- [8] Mou, J. B. (2024). Multi-objective optimization for resource allocation in intelligent manufacturing, *International Journal of Simulation Modelling*, Vol. 23, No. 2, 359-370, doi:[10.2507/IJSIMM23-2-CO9](https://doi.org/10.2507/IJSIMM23-2-CO9)
- [9] Gao, J.; Yao, M.-T.; Wu, Z.; Deng, X.-Y.; Yu, X.-M.; Yu, L.-N. (2025). Strategic distribution of emergency resources: a multi-objective approach with NSGA-II and prioritization of affected areas, *Journal of Engineering Management and Systems Engineering*, Vol. 4, No. 1, 67-82, doi:[10.56578/jemse040105](https://doi.org/10.56578/jemse040105)
- [10] Bicaku, A.; Tauber, M.; Delsing, J. (2020). Security standard compliance and continuous verification for Industrial Internet of Things, *International Journal of Distributed Sensor Networks*, Vol. 16, No. 6, Paper 1550147720922731, 19 pages, doi:[10.1177/1550147720922731](https://doi.org/10.1177/1550147720922731)
- [11] Chen, H.-S.; Han, X.-T.; Zhang, Y.-Y. (2024). Endogenous security formal definition, innovation mechanisms, and experiment research in industrial internet, *Tsinghua Science and Technology*, Vol. 29, No. 2, 492-505, doi:[10.26599/TST.2023.9010034](https://doi.org/10.26599/TST.2023.9010034)
- [12] Aleksandrova, E. B.; Rekhviashvili, I. S.; Yarmak, A. V. (2020). Lattice-based ring signature with linking-based revocation for Industrial Internet of Things, *Automatic Control and Computer Sciences*, Vol. 54, No. 8, 888-895, doi:[10.3103/S0146411620080039](https://doi.org/10.3103/S0146411620080039)
- [13] Han, Y.-R.; Guo, H.; Liu, J.-W.; Ehui, B. B.; Wu, Y.-P.; Li, S.-J. (2024). An enhanced multifactor authentication and key agreement protocol in Industrial Internet of Things, *IEEE Internet of Things Journal*, Vol. 11, No. 9, 16243-16254, doi:[10.1109/JIOT.2024.3355228](https://doi.org/10.1109/JIOT.2024.3355228)
- [14] Dakhnovich, A. D.; Moskvina, D. A.; Zegzhda, D. P. (2021). Using security-through-obscurity principle in an Industrial Internet of Things, *Automatic Control and Computer Sciences*, Vol. 55, No. 8, 1061-1067, doi:[10.3103/S0146411621080083](https://doi.org/10.3103/S0146411621080083)
- [15] Yang, X.; Xiang, K.; Huang, J. (2025). An adaptive defense model for cloud computing data security, *Technical Gazette*, Vol. 32, No. 1, 267-274, doi:[10.17559/TV-20240121001277](https://doi.org/10.17559/TV-20240121001277)
- [16] Żywiołek, J. (2025). Cybersecurity analytics: harnessing business intelligence for online organizations in the digital era, *International Journal for Quality Research*, Vol. 19, No. 4, 1367-1380, doi:[10.24874/IJQR19.04-22](https://doi.org/10.24874/IJQR19.04-22)
- [17] Bhutani, M.; Ahlawat, S.; Gaur, V.; Choudhary, A. (2025). Analysing the defensive capabilities and potential threats through artificial intelligence in cybersecurity, *Proceedings on Engineering Sciences*, Vol. 7, No. 4, 2575-2584, doi:[10.24874/PES07.04A.019](https://doi.org/10.24874/PES07.04A.019)
- [18] Guo, Y.-M.; Guo, Y.-J.; Xiong, P.; Yang, F.; Zhang, C.-D. (2024). A provably secure and practical end-to-end authentication scheme for tactile Industrial Internet of Things, *Pervasive and Mobile Computing*, Vol. 98, Paper 101877, 13 pages, doi:[10.1016/j.pmcj.2024.101877](https://doi.org/10.1016/j.pmcj.2024.101877)