Construction of a Multi-Dimensional Integrated Security Testing and Verification Platform for Oil and Gas Pipeline Networks

Dasheng Yang, Liang Feng, Shiyu Gao, Meijia Yan
PipeChina Southwest Pipeline Co. Ltd

Abstract: The secure operation of oil and gas pipeline networks is directly related to national energy security and socio-economic stability. With the increasing development of pipeline networks towards wide-area interconnection, the cybersecurity threats they face are becoming more complex and diverse. Traditional single-dimensional functional safety assurance strategies are struggling to cope with the new challenges posed by cyber-physical attacks. Therefore, this paper proposes the construction of a multi-dimensional integrated security testing and verification platform for the Industrial Control Systems (ICS) of oil and gas pipeline networks. It aims to deeply investigate the penetration, evolution mechanisms, and physical breach mechanisms of cyber attacks across the cyber and physical domains, support the development and verification of related security technologies and products, thereby providing a solid theoretical and practical foundation for building a comprehensive defense system for China's oil and gas pipeline infrastructure.

Keywords: Oil and Gas Pipeline Network Security; Testing and Verification Platform; Industrial Control System (ICS)

In recent years, profound changes have occurred in the global energy supply and demand landscape, highlighting the critical importance of oil and gas transportation networks. According to statistics from the National Pipeline Network Group, as of 2022, pipeline transportation accounted for 28% of the national total consumption of refined oil products and as much as 60% for natural gas. This data fully demonstrates the core role of oil and gas pipeline networks in China's energy system. Simultaneously, with the acceleration of digital transformation, Industrial Control Systems (ICS) are widely used in the monitoring and dispatch of long-distance oil and gas pipelines, significantly improving operational efficiency and

management levels.

However, this highly integrated information system also brings unprecedented security risks. Historically, numerous typical cases have demonstrated that malicious attacks on ICS can lead to major safety incidents and even social unrest. For instance, the 1982 explosion of a Siberian natural gas pipeline in the former Soviet Union, caused by a implanted logic bomb, resulted in severe economic losses. Another example is the 2021 ransomware attack on the Colonial Pipeline Company in the United States, which forced a complete shutdown and directly triggered a fuel supply crisis on the East Coast.

These incidents reflect three major risk trends facing oil and gas pipeline networks as critical infrastructure: first, the diversification of attack paths, evolving from traditional network intrusion to cross-domain penetration[1]; second, the expansion of impact scope, from single-node failures to regional energy supply disruptions; third, the severity of consequences, extending beyond economic loss to involve national security and social stability. In this context, solving the comprehensive early warning and control challenges of integrating information security and functional security in pipeline network ICS is urgent.

1 Scientific Problems in Oil and Gas Pipeline Network ICS

1.1 Spatio-Temporal Evolution and Physical Breach Mechanisms of Multi-Source Attacks under Wide-Area Cross-Domain Interconnection Mode

As typical Industrial Cyber-Physical Systems (ICPS), the cross-domain interconnected structure of oil and gas pipeline networks allows cyber attacks to penetrate from the information domain to the physical domain, spreading and amplifying damage effects across time and space[2]. Currently, the causal relationship between cyber attacks and physical system failures remains unclear, hindering attack attribution and impact assessment. Therefore, it is imperative to study the propagation paths and evolution patterns of multi-source attacks within pipeline systems, construct spatio-temporal attack evolution models, and reveal the intrinsic mechanisms by which cyber attacks lead to physical breaches, providing a theoretical basis for risk identification and active defense.

1.2 Endogenous Defense Strategies for Station ICS Integrating Functional Safety and Information Security

Current station ICS primarily rely on functional safety mechanisms to ensure operational safety, but face protection blind spots when confronted with complex cyber attacks[3]. Although some information security products have been introduced to enhance protection, issues remain regarding their applicability, compatibility, and coordination with traditional functional safety mechanisms. Therefore, research is needed on the deep integration mechanisms of functional safety and information security, addressing problems such as integrated risk perception, dynamic decision-making, and coordinated response for both safety and security, to construct active security strategies with endogenous defense capabilities. This will provide theoretical support for the integrated safety design, assessment, and prevention/control of station ICS.

Addressing the above problems, this paper focuses on key aspects including attack breach mechanisms, security strategy coordination, and simulation verification environment construction. It researches core technologies such as cross-domain risk assessment, network dynamic protection, multi-dimensional situation awareness, and intelligent security control. It constructs a wide-area multi-dimensional security risk situation awareness and intelligent security control platform, as well as a multi-dimensional integrated security testing and verification platform. These are deployed and validated in typical stations of the national oil and gas pipeline network to enhance the comprehensive defense capability of China's pipeline network ICS.

2 Methodology for Building the Multi-Dimensional Integrated Security Simulation Verification Platform

2.1 Platform Overall Architecture

Based on the characteristics of oil and gas pipeline network ICS networks and pipeline regulation operations, this paper constructs a multi-dimensional integrated security simulation, testing, and verification platform for pipeline network ICS networks, secure transportation, and control systems. This platform is an offline system, not actually connected to the main pipeline network ICS network, and is primarily

used for vulnerability mining, attack-defense exercises, and security capability verification. The main contents of the platform include:

(1) Using virtual simulation and real physical equipment to build a virtual-real simulation system of oil and gas stations and control centers that proportionally restores core processes.

(2) Integrating various industrial information security test case libraries, vulnerability libraries, threat libraries, operational scenario libraries, fault libraries, and other knowledge bases to build a full-process attack-defense simulation environment featuring scenario-based attack scripts, visual attack process display, functional safety and physical safety coordination and linkage, and "sound, light, electric" result simulation.

(3) Based on the station and control center simulation system, a multi-dimensional attack-defense capability verification platform is built from the three dimensions of ICS network, secure transportation, and control system. It develops various attack-defense cases, including those targeting wide-area network attacks and SIS system safety interlock verification, supporting secondary development of attack-defense cases. By simulating attack effects and scenarios under different attack scenarios, it provides diverse means for security capability verification.

The platform constructs 3 physical stations and 2 virtual stations. The selection of physical stations covers three typical transportation media: natural gas, refined oil, and crude oil, and includes core process functions such as filtration, pressurization, off-take metering, and pressure regulation. Specific reference stations include the Nanchong Gas Station of the Zhonggui Interconnection Line, the Ziyang Oil Station of the Lanzhou-Chengdu-Chongqing Refined Oil Pipeline, and the Ruili First Station of the China-Myanmar Crude Oil Pipeline. The virtual stations select the Longchang Oil Station of the Lanzhou-Chengdu-Chongqing Refined Oil Pipeline and the Baiyun Gas Station of the Zhonggui Interconnection Line as modeling objects.

The physical station setup is as follows:

Table 2.1-1 Physical Station Setup Table

No.	Station Name	Medium	Design Pressure (MPa)	Functions
1	Nanchong Gas Station	Zhonggui Natural Gas	1.6	Pig launching/receiving, filtering, pressurization, off-take metering and pressure regulation
2	Ziyang Oil Station	Lanzhou-Chengdu-Chongqing Refined Oil	1.6	Off-take filtering, pressure regulation, degassing and metering, mainline pressure relief and pressurization
3	Ruili First Station	China-Myanmar Crude Oil	1.6	Pig launching/receiving, filtering, metering, oil storage inflow/outflow, tank transfer, pressurization, pressure relief

The virtual station setup is as follows:

Table 2.1-2 Virtual Station Setup Table

No.	Station Name	Medium	Design Pressure (MPa)	Functions
1	Longchang Oil Station	Lanzhou-Chengdu-Chongqing Refined Oil	10	Off-take filtering, pressure regulation,

				metering
2	Baiyun Gas Station	Zhonggui Natural Gas	10	Off-take filtering, metering, pressure regulation

2.2 System Modeling and Integration

Taking the distributed wide-area production system composed of five stations as the modeling object, first, the relationship model of physical entities within the stations is established, including the location, connection methods, and topological relationships of entities such as pipe segments, pumps, compressors, valves, and metering devices, as well as the dynamics of multi-phase flow oil and gas within the pipelines. Then, the communication network model of the widely distributed and cross-domain interconnected pipeline system is constructed, considering the communication requirements within stations and between stations and the control center, establishing the network topology structure, including network devices, communication protocols, and data transmission methods. Next, the control requirements of the modeling object are analyzed, and the control logic is modeled, describing the control relationships between entities, signal transmission, and their control behaviors. Integrating factors such as physical entity relationships, control logic, and communication networks, a comprehensive model of the distributed wide-area production system process is constructed. Hardware and software are selected to build a hardware-in-the-loop simulation platform, simulating the behavior, data interaction, and control processes of the pipeline system.

In terms of functional safety mechanism modeling, a model library for safety functions, logic control, and fault handling strategies is constructed, possessing the capability to simulate different fault conditions and operational errors, as well as the response strategies of safety functions, fault handling processes, and diagnostic alarm effects. In terms of information security mechanism modeling, a model library for security measures and strategies (such as firewalls, intrusion detection

systems, access control lists) is constructed at the system layer, control layer, and network layer, possessing the capability to simulate threats and attack scenarios, as well as the detection and defense effects and response times of information security mechanisms. In terms of physical safety mechanism modeling, a model library for physical safety facilities (such as pressure relief valves, containment dikes) is constructed, possessing the capability to simulate disaster and accident scenarios (leakage, fire, explosion, etc.), as well as the detection and response times of physical safety mechanisms, fault transfer, and recovery. Based on the aforementioned models, using the principle of combining virtual and physical environments, the overall platform architecture, functional settings, resource configuration, data interaction, etc., are studied to construct a high-fidelity multi-dimensional integrated security testing and verification platform, and field application verification is completed.

2.3 Application Scenarios of the Multi-Dimensional Integrated Security Simulation Verification Platform

Focusing on the safety simulation and testing needs of oil and gas pipeline network ICS, the platform is applied to research the following four types of key technologies:

2.3.1 Evolution of Cross-Domain Multi-Dimensional Network Attacks and Physical Breach Mechanisms in Oil and Gas Pipeline Networks

Analyze multi-source network attack threats; research modeling methods for attack penetration and evolution in the spatio-temporal dimension; develop composite attack separation and identification technology based on information perception; clarify physical breach mechanisms combining pipeline 本体 and operational risk factors; research static-dynamic hybrid multi-source risk quantification methods; construct a causal relationship network between attacks and breaches, revealing the intrinsic mechanisms.

2.3.2 Massive Data Protection and Network Dynamic Protection Mechanisms

Research dynamic covert transmission technologies based on lightweight entity attestation and data fingerprint authentication under the

conditions of high time sensitivity and limited computational resources in pipeline network ICS; develop hybrid network access detection methods based on behavior baselines, and terminal security access mechanisms based on entity identification; verify the effectiveness of network dynamic protection means such as abnormal traffic identification, threat traceability and deception, and OT/IT integrated intrusion protection.

2.3.3 Key Technologies for Integrating Information Security and Functional Security in Stations

Research risk perception technologies such as concurrent security probing, heuristic vulnerability identification, and risk point monitoring; construct an integrated safety and security risk assessment model; research multi-dimensional security coordination mechanisms based on protection layer theory and dynamic assignment; research self-learning risk disposal decision-making algorithms; form inherent safety control mechanisms and SCADA system endogenous defense strategies, and develop supporting tool sets.

2.3.4 Wide-Area Multi-Dimensional Security Risk Situation Awareness and Intelligent Control Platform

Construct a global risk situation indicator system; research multi-dimensional security data correlation and situation prediction technologies based on deep learning; construct a knowledge-graph-based ontology model for global early warning and emergency response; research hierarchical warning triggering mechanisms and heterogeneous data collection and processing technologies; develop a wide-area security risk situation awareness and control platform with intelligent decision support capabilities.

3 Conclusion

Based on the structural characteristics and security requirements of oil and gas pipeline network ICS, this paper proposes an overall architecture encompassing a wide-area multi-dimensional security risk situation awareness and intelligent security control platform, and a multi-dimensional integrated security testing and verification platform. This platform provides a comprehensive verification environment for cross-domain security theories, key technologies, and products related to

oil and gas pipeline network ICS. The establishment of this platform will help systematically enhance the comprehensive security defense capability of China's oil and gas pipeline network ICS, providing important support for the safe operation of energy infrastructure.

References

[1] Sang Shengjie. Research on Network and Application Security of Industrial Control Production Network[J]. Computer Security, 2014(2): 44-47.

[2] Zeng Weilin, Li Guihua, and Chen Jinwei. "Research on Network Security Protection System Model and Key Technology Based on APT Intrusion." Modern Electronics Technique, 36.17(2013): 4.

[3] Zhou Minjun. "Status and Security Analysis of Industrial Control Network." Modern Industrial Economy and Informationization, 7.15(2017): 2.