Dynamic Access Control Method for Cybersecurity of Metro Integrated Supervisory Control System Based on Zero Trust Architecture

Jinkui Dong[1], Yongliang Yang[1,*], Yuanchen Liu[2]，Jianmin Xu[2]
[1]Tianjin Binhai New Area Rail Transit Investment & Development Co., Ltd., Tianjin, China
[2]Shenyang Siasun Robot& Automation Co., Ltd., Shenyang, Liaoning, China
**Corresponding Author.*

Abstract: Since the metro ISCS is the critical infrastructure, it faces the complex cyber security issues, such as internal privilege abuse, external penetration, and supply chain risk, etc. which can not be well treated by the traditional static access control model. In this study, we propose the zero-trust dynamic access control method with the four-dimensional trust assessment and the adaptive policy adjustment. The simulation results demonstrate that it can improve the illegal access blocking to 96.2%, the permission overgranting to reduce 82.5%, and the response time is within 30ms, and meet the realtime requirement. At last, the practical countermeasures are given for the metro ISCS as well as the similar rail transit.

Keywords: Cybersecurity; Metro Integrated Supervisory Control System; Dynamic Access Control; Trust Assessment; Zero Trust Architecture

1. Introduction

Since metro ISCS is an important part of critical infrastructure, it is integrated power, signaling and communications and has the rising cyber threats[1]. The traditional static access control based on the trust of the perimeter is not workable against the lateral attack[2]. Zero trust is promising, but few works consider the need of ISCS in realtime. Following the logic of situationmodelverifysuggest, in this paper, we design a dynamic method with fourdimensional trust assessment and adaptive thresholds. The simulation shows that it is effective, and we give the countermeasure for metro ISCS.

2. Theoretical Basis and Practical Analysis

2.1 Connotations of Zero Trust and Dynamic Access Control

Zero trust architecture is an identitycentric paradigm that will treat all the traffic as untrusted, will require independent authentication per request and will enforce least privilege in a dynamical way. It is different from the staticRBAC/ABAC because it introduces the continuous trust evaluation, that makes the authorization from onetime to realtime and contextaware decisionmaking[3].

2.2 Current Dilemmas of ISCS Access Control

From penetration tests and logs of five metro ISCS, we have summarized four dilemmas (Table 1) in the aspect of (1) weak identity authentication, (2) coarse permission management, (3) lack of realtime behavior monitoring, (4) ignorance of environmental context. Because those problems are interwoven, the static perimeter defences cannot work against lateral movement and privilege abuse, and trustmodel should be changed.

Table 1 Key Dilemmas of ISCS Access Control

Dilemma Dimension	Manifestations	Traditional Deficiencies
Identity	Weak passwords, shared accounts, no MFA	Single identity source,no terminal verification
Permission	Coarse roles, temporary rights unrecoverable	Static roles, ignores dynamic O&M needs
Behavior	No baseline, abnormal commands undetected	Post- hoc audit, no real- time awareness
Environment	Ignores terminal state, location, time	No context, hard to distinguish risk

2.3 Mechanisms of Zero Trust Empowerment

Zero trust deals with those dilemmas by three mechanisms: 1) continuous verification (reauthenticate every request), 2) dynamic authorization (graded trustscorebased access)

and 3) least privilege with immediate revocation (sessionbound permissions). Together, they change the ISCS access control from static walls to dynamic filters, and deal with both, the insider and the intruder.

3. Construction of Zero Trust-Based Dynamic Access Control Method Framework

3.1 Design Principles and Overall Architecture

This method is the following of four principles: 1) identity as perimeter, 2) continuous measurement, 3) least dynamic privilege, 4) observability. It builds (Figure 1) a four layer (perception, trust assessment, policy decision, execution feedback) and two plane architecture. The first layer (perception) collects the user, the terminal, the network and the context data, the second (trust assessment) quantify them, the third (policy decision) enforces the actions, the fourth (execution feedback) closes the loop.

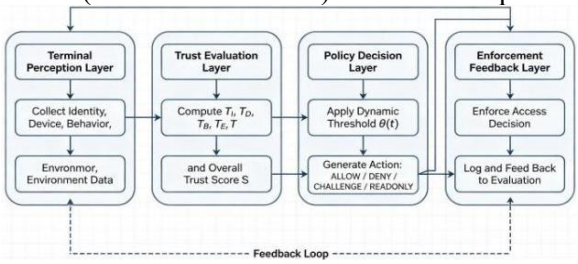

Figure 1. Overall Architecture of Zero Trust-Based Dynamic Access Control

3.2 Four-Dimensional Trust Assessment Model

In this study, trust is deconstructed into four dimensions, which are the trustworthiness of identity (T_I), the trustworthiness of device (T_D), the trustworthiness of behavior (T_B) and the trustworthiness of environment (T_E), all of which are made up of weighted sub-indicators. The total trust score S is defined as:

$$S = \alpha T_I + \beta T_D + \gamma T_B + \delta T_E \quad (\alpha + \beta + \gamma + \delta = 1) \tag{1}$$

All the dimensions are normalized to [0,100]. According to metro ISCS security grading requirements and consultation with the experts, the judgment matrices are constructed by using the Analytic Hierarchy Process (AHP), the weights are taken as α=0.35, β=0.25, γ=0.25, δ=0.15, which means the identity authentication is the core role. The sub-indicators and data source for each dimension is given in Table 2. For instance, the behavior trustworthiness is computed as $T_B=0.4\cdot R_{freq}+0.35\cdot R_{sens}+0.25\cdot R_{fail}$, where R_{freq} is the score of the compliance for operation frequency, Rsens is the score of the rationality for the sensitive command and Rfailis the score of the tolerance for the failed.

Table 2 Four-Dimensional Trust Assessment Sub-Indicators and Data Sources

Dimension	Key Sub-Indicators	Data Sources
Identity T_I	MFA strength, account type, password validity period	Authentication server logs
Device T_D	Patch version, antivirus status, certificate validity, ICS whitelist	Terminal management platform
Behavior T_B	Operation frequency baseline deviation, sensitive command call ratio	Behavior baseline engine
Environment T_E	Network latency jitter, access location, peak/off-peak periods	Network probes, clock sync

3.3 Dynamic Policy Decision and Adaptive Adjustment Mechanism

The policy decision engine performs the graded authorization as: if S80, permit all the permission of the operations (e.g., issue remote control command); if 60S80, only permit the read and query permission but not write; if 40S60, only permit the identity authentication and status query; if S40, directly deny access and raise alert. We also introduce the sliding window averaging mechanism, i.e. we use the weighted mean of the latest 5 scores (with time decaying weights) as the final decision base, in order to not interrupt the service when the score flucuates in a transient way.

Since the metro ISCS is very operation sensitive in the morning and evening peak hours, the adjustment coefficient of the adaptive design is given as follows:

$$\lambda(t) = 1 + \eta \sin\left(\frac{2\pi}{24}t\right) \cdot II_{peak} \tag{2}$$

where t means the current hour, and we set the value of the parameter,=0.1, and $II_{peak}(t)$ is the peak-hour indicator function (which takes value 1 during 7:00-9:00 and 17:00-19:00, otherwise 0). Finally, the authorization threshold is changed adaptively to $S \geq 80-\lambda(t)$, i.e. to moderately loose the conditions of admission in the peak hour in order to decrease the risk of the operation delay, but to strengthen the behavior monitoring and to tighten immediately when the

anomaly is found. This mechanism makes a trade off for the security continuity and the business availability.

3.4 Dynamic Access Control Decision Algorithm

The six steps of the core decision process is: "request capture - feature extraction - trust scoring - policy matching - action execution - log feedback", and the single decision latency is controlled in 50ms, satisfying the real time requirement of industrial control . The pseudocode of the algorithm is shown in Algorithm 2.

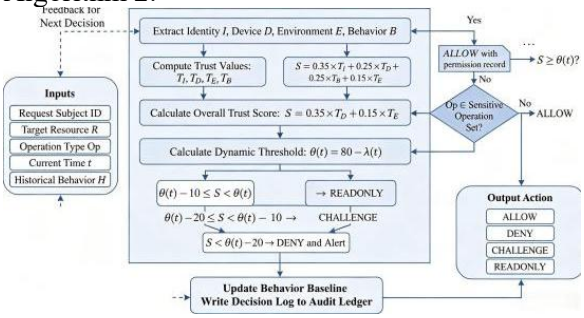

Figure 2: Overall Architecture of Dynamic Access Control Based on Zero Trust

The sensitive operation set includes train control, power supply breaker opening/closing, signal switching, etc.; the ordinary operation set includes data queries, report exports, etc. The secondary authentication can increase the trust score by 10 points temporarily for 30 minutes, to meet the emergency O&M need.

4. Simulation Experiments and Effect Analysis

4.1 Experimental Setup

We run the five simulations in an ISCS test platform (120 terminals, 16 subsystems) in five stages (from baseline to maturity). We compare the zerotrust method with the traditional RBAC+firewall, in the simulations, the traffic and the load are fixed; only the security mechanism is different.

4.2 Security Protection Effectiveness Comparison

Figure 3 shows the blocking rates and false-positive rates of the experimental group versus control group for different types of access requests. The illegal access blocking rate (the experimental group) is 96.2%, which is 22.7 percentage points more than that of the control group (73.5%). The false-positive rate (legitimate requests misjudged) is 2.1% for the experimental group versus 1.3% for the control group, which is an acceptable increase. In the case of simulated internal privilege escalation attack (low-privilege accounts invoke high-privilege commands), the blocking rate (the experimental group) is 99.1% versus only 52.6% for the control group, fully showing the defensive advantage of dynamic trust assessment against internal lateral movement.

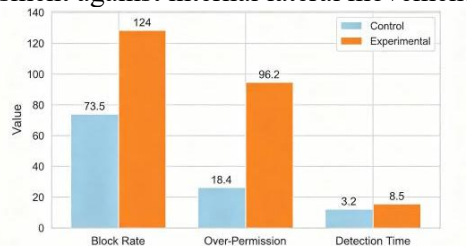

Figure 3 Comparison of Security Protection Effectiveness Between Experimental and Control Groups

4.3 Dynamic Trust Score Evolution and Response Process

Figure 4 is the trust score evolution trajectory of a typical O&M account in the experimental group in 72 hours. In the first 24 hours of normal operation, the score were stable between 82-88, in the full-authorization range. At the 25th hour, when there are 3 continuous password failure, the behavior dimension score drops sharply and the comprehensive score drops to 63, and the read-only downgrade is triggered; the secondary authentication is restored to 78, but in the read-only range, and it gradually rises to 85 after 2 hours of continuous normal operation. At 48th hour, the simulation of unpatched terminal, the trustworthiness of the device is dropped from 95 to 55, the comprehensive score drop to 71 and the challenge mechanism is triggered. This curve proves the dynamic assessment sensitive response to the risk event and autonomous recover ability of the score, it can not long-term over-authorization or one-size-fits-all denial.

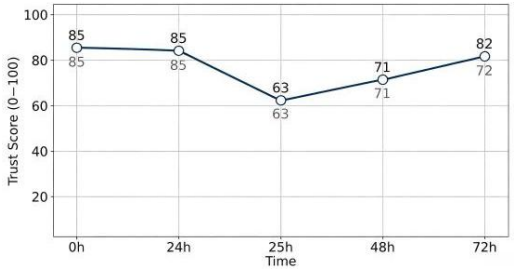

Figure 4 Trust Score Evolution Curve of a Typical Account Over Time

4.4Comprehensive Comparison of Key Performance Indicators

The comparison of six key indicators between the two groups is summarized in Table 3. We can see that the experimental group is better than the control group in all the security indicators. Especially, the average decision latency increased only by 12ms (18ms to 30ms), which fully satisfies the requirement that control command response should be less than 100ms of ISCS industry . The permission over-granting rate is reduced by 82.5%, which means the least-privilege principle is effectively enforced. All the difference is significant at p0.01 by independent-sample t-test.

Table 3. Comparison of Key Performance Indicators Between Experimental and Control Groups

Evaluation Indicator	Control Group	Experimental Group
Illegal access blocking rate (%)	73.5	96.2
Legitimate request pass rate (%)	98.7	97.9
Permission over-granting rate (%)	18.4	3.2
Average decision latency (ms)	18	30
Average attack detection time (s)	124	8.5
O&M task completion rate (%)	92.4	95.6

4.5 Operator Feedback

Postexperiment interviews with operators showed that in general, the dynamic controls were accepted and in particular, the operators appreciated that permission was automatically expired, but in case of an emergency, reauthentication should be simpler.

5. Countermeasures and Suggestions

Four measures are proposed to go on the way of zero-trust dynamic access control in metro ISCS. 1) Setup a unified identity management platform with digital certificates and mandatory multifactor authentication. 2) Deploy the protocolaware behavior analysis engines (Modbus, IEC 104) to build the operation baselines and detect the deviation. 3) Setup the hierarchical domainspecific policies with differentiated trust threshold and reevaluate cycle (for example, 5s for control core and 30s for the data) to trade the security and performance. 4) Take the policy simulation and oneclick fallback to work. It is recommended to have a path of pilotfirst, gradual expansion[4].

6. Conclusions and Prospects

The erotrust dynamic access control for metro ISCS in this paper is studied. Three conclusions are made in this paper: 1. traditional static model is not able to resist internal dynamic threats; 2. by using the proposed fourdimensional trust assessment and adaptive threshold method, the illegal access can be blocked to 96.2%, the overgranting can be reduced by 82.5%, and the latency is within 30ms, which proves that the zerotrust is applicable in the highrealtime industrial environment. In the future work, the generative AI for the anomaly semantic reasoning, federated learning for the crossline threat intelligence sharing, the longterm pilot deployments to verify the stability under the extreme environment should be done.

References

[1] Liu Xianhai, Guo Wei. Research on Differential Privacy Big Data Protection under Cybersecurity Background. Wireless Internet Technology, 2025, 22(24): 23-26.

[2] Xiong Qingchen. Design of Metro Integrated Supervisory Control System Based on Cloud Platform. Integrated Circuit Applications, 2025, 42(11): 121-123.

[3] Wang Ruokun, Zhang Ju, Li Lu, et al. Research on Data Configuration Platform for Urban Rail Transit Signaling Systems. Railway Communication and Signaling Engineering Technology, 2025, 22(9): 65-71+121.

[4] He Jiayang. Design and Implementation of Metro Integrated Supervisory Control System Based on Three-Layer Networking. Network Security Technology and Applications, 2023, (12): 111-113

