Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

THREAT MODELS AND RISK ASSESSMENT FOR AUTONOMOUS TELECOM SYSTEMS OF THE FUTURE

Fedor Shagzheev
Telecommunication Expert, USA

Abstract
This article analyzes existing and prospective threat models for autonomous telecom systems, classifies assets and critical risk areas, and discusses applicable risk assessment methodologies (NIST RMF, ISO/EBIOS). An integrated risk management approach is proposed, including multi-layered threat modeling, resilience assessment of AI components, and continuous security monitoring. Recommendations for telecom operators and regulators aimed at improving the security of future 5G/6G networks are formulated.

Keywords: Autonomous telecom systems, 5G, 6G, risk assessment, threat models, network slicing, orchestration, artificial intelligence, supply chain security, SDN/NFV.

Introduction

Scientific novelty of the article. An integrated approach to risk assessment in autonomous telecom systems, which for the first time combines dynamic risk analysis based on telemetry and SLAs, taking into account the vulnerabilities of AI/ML components and supply chain threats in 5G/6G infrastructure.
Autonomous telecommunication systems (Autonomous Networks (AN) is a key trend in the development of 5G and 6G networks. Modern networks already use virtualization (NFV), software-defined networks (SDN), and network slicing to improve operational efficiency [1]. The transition to AN means that network management, optimization, and decision-making are increasingly performed by machine learning (AI) algorithms and intelligent orchestration , minimizing human intervention [2].

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

Growing automation, especially the active implementation of AI-oriented control modules, expands the attack surface and creates new critical threats:

1. Attacks on orchestration systems (MANO/SDN controllers) and virtualized network functions (VNF).

2. Targeted attacks aimed at manipulating SLA policies or network slices. A compromised policy can instantly propagate an error or malicious effect to critical services.

data poisoning poisoning) and adversarial attacks (adversarial ML), which undermine the robustness of autonomous decisions.

4. The importance of threats associated with malicious updates, vulnerable VNF images, and untrusted third- party components , which can become the initial point of compromise, is increasing.

5. In autonomous networks, the damage from attacks is amplified: automation accelerates the propagation of configuration errors, and an attack on a single control component can affect dozens of network slices.

Therefore, protecting AI requires new approaches to threat modeling. Classic frameworks must be supplemented with: security analysis of AI models, verification of orchestration integrity, and continuous monitoring of network behavior [3].

Risk assessment in future networks is becoming a dynamic task that depends not only on traditional parameters (confidentiality, integrity, availability), but also on the robustness of decision-making algorithms and the quality of the data on which the autonomous network is trained.

Autonomous telecommunications systems rely on a distributed and virtualized architecture, where control functions and service logic are implemented in software, often on an edge /MEC platform. In such an environment, critical assets can be grouped into layers reflecting their role in ensuring network security, resilience, and manageability:

1. Physical infrastructure. Base stations, switches, servers, optical channels, and edge platforms. Threats include physical sabotage, radio interference , and attacks on intelligent equipment components (e.g., O-RUs).

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

2. Control and orchestration plane . SDN controllers, MANOs, slice managers , and autoconfiguration systems . Compromise gives the attacker complete control over network policies and slices.
3. Virtualized network functions and service plane. VNFs / CNFs , 5G/6G core functions, traffic routing. Key risks: container/image vulnerability exploitation, cross-slice side channels.
4. Data and AI components. Telemetry, policies, training datasets , ML models (traffic prediction, QoS optimization , anomaly detection). Threats: data poisoning, adversarial attacks, model incapacitation.
software updates . Hardware and VNF vendors, CI/CD, and firmware delivery mechanisms. Risks associated with the introduction of untrusted code and attacks on dependent components [4].
System security requires consistent control across all levels, from physical infrastructure to AI components, as a vulnerability in a single element can be exploited to quickly and widely disrupt network operations through automated processes.

Table 1 - Classification of assets and corresponding risk areas

Asset class	Examples	Key threats	Potential consequences
Physical infrastructure	RU/DU/BBU, MEC nodes, data centers	Sabotage, channel hijacking, and side-channel attacks on equipment	Violation of accessibility, degradation of coverage
Orchestration and management	SDN controllers, MANO, slice orchestrators	Privilege escalation, API compromise, policy substitution	Loss of control over the network and SLA, massive failures
Virtualized network functions	VNF/CNF of the kernel and services	Container vulnerabilities, cross-slice attacks	Traffic hijacking, privacy violation
AI/ML components	Autoconfiguration models , telemetry data	Data poisoning, adversarial input, model drift	Incorrect network decisions, hidden attacker control
Supply chain	Firmware, VNF images, libraries	Malware injection , supply-chain attacks	Mass spread of infection during updates

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

Autonomous telecom systems inherit the traditional threats of communication networks, but simultaneously acquire new risks arising from virtualization, orchestration, and the use of AI. Therefore, threat modeling requires combining classical approaches (focused on network components and interfaces) with methods that consider the dynamic behavior of systems and the vulnerabilities of machine learning models.

STRIDE, attack frameworks trees and data flow analysis (DFD) are used to identify threats related to the integrity and controllability of SDN controllers, NFV functions, and orchestration APIs [3].

MITRE ATT&CK approach for Telecom allows classifying real attack scenarios on network components and their behavioral indicators [5].

Autonomization introduces threats related to :

- data poisoning , adversarial attacks on input data and models;
autoconfiguration mechanisms ;
- violation of the integrity of edge /MEC telemetry;
- dynamic propagation of the error throughout the network.

These threats have been recorded and studied in scientific papers [6,7].

Compromising MANO, SDN controllers, or slice managers is one of the most dangerous scenarios, as an attacker gains the ability to impact SLAs and the availability of critical services across multiple slices [8]. Supply-chain risks are further exacerbated by malicious VNF images and the introduction of vulnerable equipment.

Table 2 - Applicability of threat models to key components of autonomous telecom systems

Network component	Recommended Threat Model	Threats taken into account
SDN/MANO orchestration	STRIDE, attack trees, MITER ATT&CK	Privilege escalation, policy substitution, API compromise
Virtualized network functions (VNF/CNF)	DFD, CVSS + ATT&CK	Cross-slice attacks, side channels
MEC/ edge platform	Behavioral threat modeling	Telemetry attacks, resource manipulation
ML models and data	Adversarial ML frameworks (FGSM, PGD), data provenance	Data poisoning , model drift
Supply chain	Threat modeling By chain supplies (SBOM)	Malicious updates, bookmarks

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

Risk assessment in autonomous telecom systems requires a combination of standard information security management approaches with methods focused on dynamic orchestration and AI components.

Classical international standards, NIST Risk Management The Responsible Management Framework (RMF) and ISO/IEC 27005 provide a common methodological basis for asset identification, threat analysis, and the definition of protective measures [9, 10]. However, in the context of 5G/6G and MEC, continuous risk assessment based on telemetry and network behavioral indicators is required. Network management automation leads to an acceleration of incident development, which makes it important to apply dynamic and quantitative methods, in particular attack chain analysis, MITRE ATT&CK, and SLA impact monitoring. Risk assessment of AI components, including model robustness testing, data integrity monitoring, and model drift management, deserves special attention. Thus, an integrated approach combining static vulnerability assessment and dynamic assessment of the consequences of autoconfigurations and ML algorithm decisions is required.

Table 3 - Application of risk assessment methodologies to stand-alone telecom components

Methodology / Framework	Strengths	Limitations of autonomy	Scope of application
NIST RMF	Full risk management lifecycle; link to controls	Doesn't take ML and runtime dynamics into account sufficiently	Basic network architecture
ISO/IEC 27005	ISMS Compatibility; Formalism in Threat Analysis	Focus on static systems	Corporate operator security
MITRE ATT&CK for Telecom	Real-life attack scenarios	Requires constant updating and telemetry	Network and orchestration plane
Quantitative risk + SLA impact	Assessing the impact on services	Insufficient historical data	Network slicing , MEC
Adversarial ML testing / Data provenance	Considers training and telemetry risks	Requires expertise and computing resources	AI control, self-optimization

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

Key Recommendations:

1. Integrate RMF and ISO 27005 with SLA monitoring and orchestration behavior (runtime risk evaluation).
2. Include risk assessment of ML modules in the standard certification and acceptance testing process.
3. Apply MITRE ATT&CK for Telecom for scenario analysis of control and slicing attacks .
4. Use SBOM and supply chain control as mandatory elements of risk analysis .
5. Develop automation risk scoring based on MEC/ edge telemetry .

Ensuring the resilience of autonomous telecommunications systems requires a multi-layered and continuous risk assessment process that combines traditional auditing with dynamic network behavior monitoring. The proposed architecture is based on three key principles:

1. Multi-level threat modeling. This principle involves the integration of static and scenario-based analysis methods:

- STRIDE (component and interface analysis) and DFD (data flow diagrams);
- MITRE ATT&CK for Telecom for scenario analysis of complex attacks targeting orchestration systems and network slicing.

2. Integrating AI/ML risk assessment. Since autonomy is based on AI, risk assessment should include testing of the algorithms themselves:

- tests of model stability (Adversarial Evaluation) to check the behavior when manipulating data;
- monitoring of model drift and control of data origin (Data Provenance) to ensure the quality and reliability of training datasets .

3. Continuous monitoring and runtime risk scoring . A shift from periodic auditing to continuous monitoring is required:

- telemetry analysis to assess impact on SLA in real time;
- automatic detection of anomalies in management policies and supply chain control (using SBOM – Software Bill of Materials and certifications).

To implement this approach, new dynamic components are integrated into the RMF/ISO 27005 network process:

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

Table 4 - Critical assets and threats in autonomous networks (AN)

Element	Purpose
Policy Security Gateway	Validates the integrity and authorization of management commands (MANO/SDN), preventing the implementation of malicious policies.
AI Trust & Validation Layer	Monitors data and machine learning models, ensuring their reliability before deploying autonomous solutions.
Adaptive Risk Dashboard	Automatically updates the network risk level based on current SLA metrics and attack indicators.
Supply Chain Security Manager	Validates VNF/MEC artifacts and images before deploying them to production.

This approach therefore helps limit the spread of attacks (e.g., by automatically blocking or rolling back malicious configurations). It is expected to reduce the mean time to repair (MTTR) of incidents, reduce the likelihood of cross-slice compromise, and increase trust in autonomous AI components of the network.

One of the most critical scenarios for standalone telecom networks is a supply chain attack on virtualized network functions. Let's consider a simplified but realistic case.

Attack scenario: An attacker injects a malicious component into a VNF image distributed via a third-party vendor's CI/CD. The image is automatically delivered and deployed to the telecom operator's MEC nodes using a trusted update automation policy. Once activated, the malicious module gains access to the MANO orchestration API and surreptitiously alters resource allocation policies for several network slices, reducing the priority of a critical service (e.g., emergency services communications). Telemetry manipulation prevents the ML-based management model from correctly detecting anomalies. This results in quality of service (QoS) degradation, SLA violations, and possible shutdown of part of the infrastructure supporting public safety. The escalation of such an incident can be prevented by applying elements of the proposed integrated approach:

- checking signatures of artifacts and SBOM when updating VNF images;

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

- runtime certification of MEC nodes;
- behavioral analysis of orchestration APIs to identify hidden policy changes;
- validation of ML component decisions when detecting drift anomalies.

This case highlights that the risks in autonomous networks are largely related to the fact that the compromise of a single element can be instantly scaled by automation mechanisms.

Therefore, to successfully manage cyber risks in autonomous telecommunications systems (ANs), operators and regulators should focus on the following key strategies.

For telecom operators:

1. Adaptation of frameworks . Transition from periodic audits to continuous risk assessment cycles based on NIST RMF/ISO 27005.
2. Integration of AI validation . Incorporation of machine learning model validation (ML validation) into the risk assessment process.
3. Implementation of threat modeling (threat modelling) as a mandatory practice in the early stages of developing new features, especially for orchestration systems and network slicing.
4. Developing internal expertise in Adversarial ML to regularly test the robustness of algorithms and models that control the network.

Requirements for suppliers:

1. Requiring suppliers to provide SBOM (Software Bill of Materials), the use of signed images (for VNF/CNF) and the provision of provable (auditable) product safety test reports.

For regulators and consortia:

1. Define minimum mandatory security, audit, and certification requirements for network slice orchestrators and managers. This will ensure a basic level of trust and manageability for critical AN components.

Autonomous telecom systems improve efficiency but simultaneously change the nature of risk: automation lowers the threshold for scalable attacks and increases the importance of protecting orchestration , supply chains, and AI components .

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

The solution: an integrated, multi-layered approach to threat modeling and risk assessment that combines recognized standards (NIST/ISO/EBIOS) with new practices for ML and continuous monitoring. Only this can ensure an acceptable level of security and resilience for future 5G/6G networks.

References

1. Hetzel Z., Bisson O., Ponce J., Jha S., Dussan M. Autonomous Networks in 5G: Architecture and Challenges // IEEE Network. - 2023. - DOI: 10.1109/MNET.001.2300035
2. Talli G., Polese M. AI-Driven Autonomous Networks // arXiv preprint. - 2022. - Mode access : https://arxiv.org/abs/2212.01556 (date appeals : 2 7 .10.2025).
3. Sharma S., Chatzimisios P., Bera S., Mukherjee M. Security Management in Future Autonomous Networks // IEEE Communications Surveys & Tutorials. - 2022. - DOI: 10.1109/COMST.2022.3184448.
4. Mota J., Asensio A., García M., Gomes T., Dias J. Improving 5G Network Slicing Security with AI Mechanisms // Sensors. - 2025. - T. 25. - No. 13 . - Art. 3940. - Access mode: https :// www . mdpi . com /1424-8220/25/13/3940 (date of access: 10/27/2025).
5. MITRE ATT & CK ® for Telecommunications . - 2024. - Access mode: https :// attack . mitre . org / technologies / telecommunications / (accessed: 10/28/2025).
6. Abbas N., Zhang J., Taherkordi A., Skeie T. Security for AI-Enabled 5G and Beyond // IEEE Journal on Selected Areas in Communications. - 2023. - DOI: 10.1109/JSAC.2023.3260812.
7. Ullah R., Kong L., Zhang Z., He Q., Lu Z. Security of MEC Systems in 5G Networks // IEEE Access. - 2021. - DOI: 10.1109/ACCESS.2021.3080291.
8. Dias J., Asensio A., Mota J., Gomes T. 5G Network Slicing Security: Threats and Solutions // Sensors. - 2024. - T. 24. - No. 2. - Art . 503. - DOI: 10.3390/s24020503.
9. NIST. Risk Management Framework (RMF). - 2022. - Mode access : https://csrc.nist.gov/projects/risk-management (date accesses : 10/29/2025).

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 01, Issue 09, December, 2025
Website: usajournals.org

10. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection - Guidance on information security risk management. - Geneva: ISO, 2022. - 98 p.