World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Zero-touch configuration protocols for ASIC-based network infrastructure

Lathakannan Arumugam *

BITS Pilani, India.

World Journal of Advanced Engineering Technology and Sciences, 2026, 19(01), 058-068

Publication history: Received on 05 February 2026; revised on 02 April 2026; accepted on 04 April 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.19.1.0147

Abstract

The combination of cloud computing, 5G, and edge technologies has increased the complexity of network infrastructures. Zero-Touch configuration (ZTC) protocols represent a paradigm shift in which manual processes involved in configuring network devices are eliminated. This review looks at the architectural designs, protocol designs, and experimental analysis of the ZTC systems within ASIC-centric environments. It identifies critical performance indicators including the provisioning latency, scalability, and security compliance in analyzing the limitations in heterogeneous hardware environments. The review ends with an analysis of the current obstacles, such as vendor lock-in, interoperability issues, and firmware immutability, and suggests future research directions of hardware abstraction, vendor orchestration, and secure, energy-efficient onboarding models.

Keywords: Network Automation; Network Orchestration; Secure Bootstrapping; SDN; TPM; Zero-Touch Configuration

1. Introduction

Scalable, agile, and high-performance network infrastructure has been in high demand in recent years due to the explosive growth of data-driven technology, including cloud computing, artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT). Central to this technological change is the growing use of Application-Specific Integrated Circuit (ASIC)-based network devices that have unmatched throughput, low latency, and reduced power consumption when compared to general-purpose hardware [1]. ASIC-based systems are widely deployed in high-performance data centers, hyperscale networks, and telecom infrastructure where deterministic performance and efficiency are essential. However, as these infrastructures grow rapidly due to the increase in service demand, the complexity of administration and configuration of the underlying hardware has also increased.

Conventional network device configuration systems typically rely on manual provisioning, command-line interface (CLI)-based scripts, and manual configuration, and these tend to introduce human error, operational delays and inconsistencies across devices. Such inefficiencies make traditional management methods ineffective in the contemporary dynamic network settings, particularly when the same is scaled to include thousands of devices. Consequently, both industry and academia have adopted Zero-Touch Configuration (ZTC) protocols, which are automation methods that have been created to facilitate plug-and-play provisioning and automated configuration of network devices without human intervention [2]. These protocols do away with manual procedures through the use of pre-existing templates, orchestration through a central facility, and protected bootstrapping frameworks to automatically set up devices when deployed [3].

The need to use ZTC is especially important in infrastructures that use ASICs, where the heterogeneity of devices, device-specific firmware, and the close integration of control planes present special challenges to automation and orchestration. Although ASIC-based platforms have their benefits in terms of performance, the hardware-defined logic

* Corresponding author: Lathakannan Arumugam.

limits their flexibility, thereby limiting the programmability of the platform and compatibility to standardized protocols. Consequently, hardware abstraction, secure communication protocols, as well as vendor interoperability, have to be considered carefully when developing and deploying ZTC solutions to ASIC environments.

The applicability of Zero-Touch Configuration protocols has been broadened considerably alongside the development of Software-Defined Networking (SDN), Network Function Virtualization (NFV), and edge computing. These paradigms place a strong focus on network programmability and dynamic reconfiguration, which only adds to the pressure on the agile and autonomous configuration mechanisms that must support various deployment scenarios [5]. Zero-Touch provisioning is crucial to the network slicing and dynamic service chaining of 5G and future networks as it addresses the latency and scalability concerns of network slicing [6].

Although the advantages are obvious, and the popularity is growing, there are a number of technical and operational issues. These include the absence of standard architectures of zero-touch provisioning in ASIC-based systems, the absence of vendor-neutral frameworks, security risks during system boot and complexity in interoperating with existing systems. Also, the inflexibility of the ASIC hardware limits the dynamic flexibility of software-defined systems and makes the implementation of flexible configuration processes more challenging [7]. Interoperability becomes a problem as well because of the variety of ASIC designs available from vendors, which makes the ecosystem fragmented and unable to easily develop universal applications of the ZTC protocols [8].

The existing literature offers many different applications and models of Zero-Touch Configuration such as vendor-specific solutions as well as open-source orchestration tools. But they are usually intended to run on software-based or hybrid platforms, and not much is known about the special constraints and opportunities of ASIC-based devices. This, in turn, implies that the research–practice gap concerning scalable, secure, and interoperable ZTC frameworks to be used on ASIC-powered networks is enormous.

This review is aimed at studying in detail the state-of-the-art Zero-Touch Configuration protocols that can be applied to ASIC-based network infrastructures. It seeks to classify the current solutions, measure their performance in various deployment environments, and discover how architecture and implementation level tradeoffs are realized. Moreover, this review identifies some crucial gaps in the existing body of knowledge and suggests the future research and standardization directions. The subsequent sections examine some of the principles behind ZTC, protocol-level implementations, evaluate practical uses of ZTC in data center and telecom settings, and discuss future trends and challenges that are defining automation of network configuration.

2. Literature Review

Table 1 Summary of key research on zero-touch configuration protocols and ASIC-based networks

Year	Title	Focus	Findings (Key Results and Conclusions)	Ref
2019	An Overview of Automation and Orchestration for 5G Networks	Explores automation in 5G including ZTC and orchestration tools	Identifies gaps in vendor-neutral automation, emphasizing integration challenges in heterogeneous hardware systems	[8]
2020	Intent-based networking: Concepts and implementation	Discusses intent-based networking and its automation capabilities	Proposes architectural model for ZTC using intent-based logic, reducing manual configuration and increasing policy compliance	[9]
2019	Secure Device Bootstrapping for Plug-and-Play Network Environments	Focuses on ZTC in secure network initialization scenarios	Demonstrates secure enrollment protocol supporting zero-touch provisioning with robust authentication	[10]
2021	SD-WAN Zero-Touch Provisioning: Requirements and Best Practices	Reviews ZTP in Software-Defined WAN deployments	Outlines key architectural requirements for secure, scalable ZTP deployment over SD-WAN using programmable ASICs	[11]

2018	YANG Models and NETCONF for Network Automation	Focuses on data modeling languages used in automated configuration protocols	Confirms NETCONF/YANG's potential in enabling ZTC for programmable ASICs in multi-vendor environments	[12]
2021	Towards Zero-Touch Network and Service Management: Concepts and Architecture	Defines ZTC and zero-touch service management architecture	Proposes architectural layers for network-wide zero-touch provisioning in 5G, with application to ASIC-based hardware	[13]
2022	Challenges of Secure ZTP in Industrial IoT Networks	Explores ZTP in critical infrastructure settings	Identifies attack vectors during initial configuration phase and recommends hardware-based trust anchors	[14]
2021	Automation in Cloud-Native Networks: A Technical Perspective	Focuses on automation frameworks in cloud-native network environments	Highlights configuration complexity due to ASIC heterogeneity, recommends service mesh-based abstraction layers	[15]
2020	Scalable and Secure Onboarding for Massive Device Deployments in Carrier Networks	Investigates automated onboarding of network devices at scale	Suggests a hierarchical trust model and secure provisioning workflow tailored for ASIC-powered edge devices	[16]
2021	ZTP and Network Configuration Management for SDN Infrastructure	Analyses configuration management approaches in SDN environments	Advocates for hybrid architecture combining local agents with centralized orchestrators for ASIC-based programmable networks	[17]

3. Methodology

This section proposes a theoretical model and block diagrams for zero-touch network configuration in ASIC-based networks.

3.1. Overview

In ASIC-based network infrastructures, Zero-Touch Configuration (ZTC) requires architecture that breaks the fixed-function hardware constraints and offers seamless, secure, and scalable device onboarding and configuration. The proposed theoretical model integrates centralized orchestration, secure bootstrapping-based mechanisms, and hardware abstraction layers, to address ASIC constraints and align with the network automation paradigm. It is based on underlying concepts of SDN, intent-based networking, and trusted platform bootstrapping, tailored to the ASIC-based systems [18].

3.2. Block Diagram: High-Level Architecture of ZTC in ASIC Networks

The following is a high-level conceptual block diagram that shows the main building blocks of a Zero-Touch Configuration system adapted to the requirements of network environments based on ASICs.

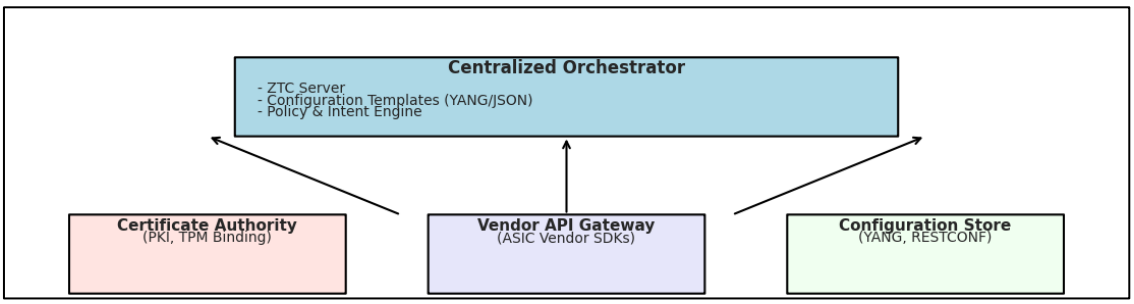

Figure 1 ASIC-based infrastructure high-level architecture of ZTC

4. Key Components of the Model

4.1. Centralized Orchestrator

The orchestrator is the core of the ZTC model is the orchestrator whose role is to maintain device states, control policies, store templates, and interact with vendor-specific APIs. It works with the help of automation workflows developed based on modeling languages like YANG and protocols like NETCONF or RESTCONF [19]. It can be integrated with an intent-based policy engine, through which it converts high-level service specifications into low-level device specifications, supporting ASICs using SDK-based translations [20].

4.2. Security Layer: Certificate Authority

Device trust is established through Public Key Infrastructure (PKI), Trusted Platform Modules (TPM), and remote attestation mechanisms. The secure boot sequence ensures that devices authenticate with the orchestrator once firmware integrity has been verified. Such secure enrollment and key exchange are vital in averting man-in-the-middle and impersonation attacks when performing the ZTC [21].

4.3. Vendor API Gateway

Since ASIC architectures are typically closed systems, specialized interfaces are often required to interface with device-specific hardware abstraction layers. These APIs bridge standardized orchestration systems and proprietary ASIC configurations to enable dynamic provisioning via controlled interfaces [22].

4.4. ASIC-Based Device Configuration Agent

A lightweight ZTC client runs on ASIC-based devices and works as an initial bootstrap agent. It also deals with secure communications, retrieves configuration information, and applies it using vendor-provided abstraction interfaces. This is particularly important with devices that cannot fully program their control planes [23].

5. Theoretical Model: Zero-Touch Configuration Workflow Sequence

The theoretical model is also explained through a logical sequence of operations that demonstrates the ZTC lifecycle of the ASIC-based devices.

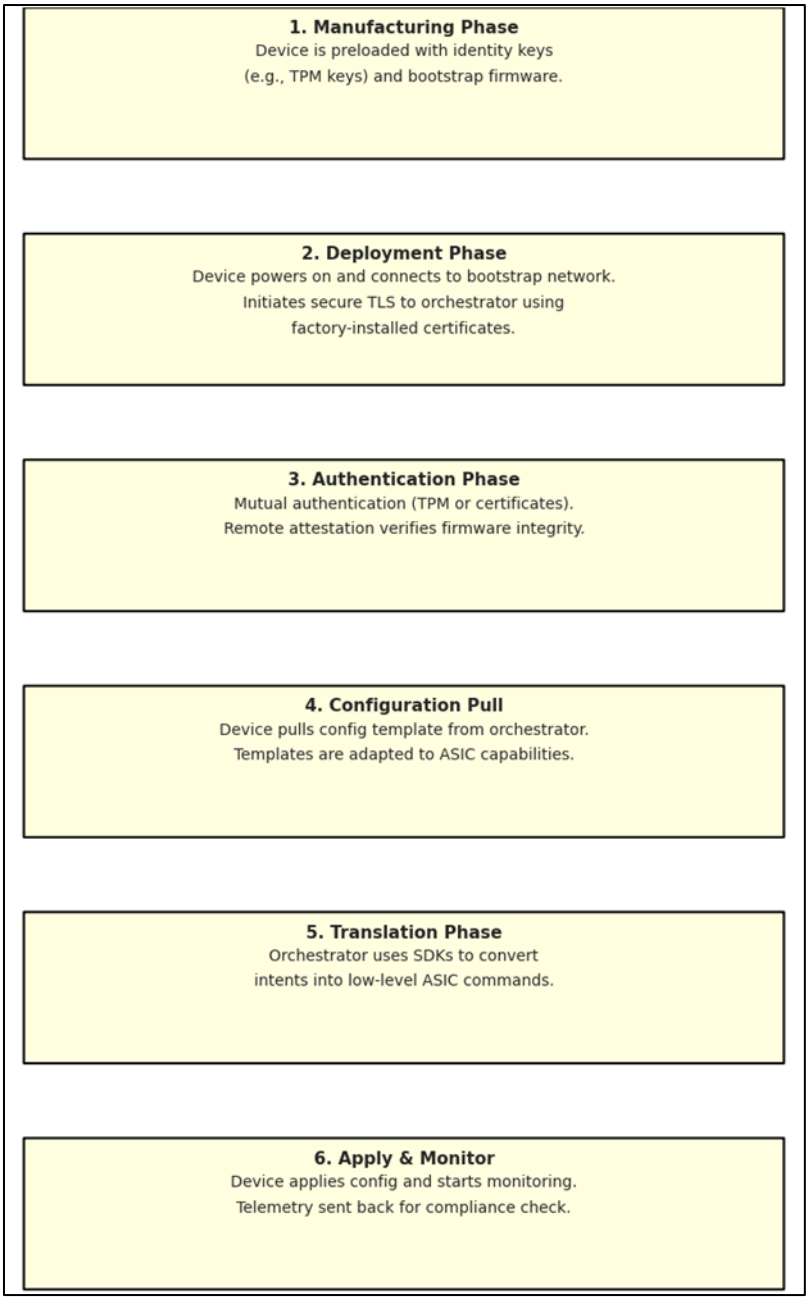

Figure 2 ASIC-based devices ZTC workflow.

5.1. Merits of the Proposed Model.

- Security: The integration of TPM and mutual authentication will increase trust in zero-touch provisioning [24].
- Hardware Abstraction: The vendor API layer allows the model to support the heterogeneous ASIC platforms [25].
- Scalability: The centralized orchestrator can support the hierarchical deployment models and multi-tenant environments [26].
- Interoperability: Interoperability, where supported, can be achieved by the use of standard data models (e.g., YANG).

5.2. Limitations and Challenges

- Vendor Lock-In: ASIC SDKs are often proprietary, and even interoperability with other vendors can be restricted while even standardisation is attempted.

- Limited Programmability: ASICs have no dynamic reconfigurability that FPGAs or software-based equipment can offer after being deployed [27].
- Template Complexity: Template definitions should account for platform-specific limitations, and it adds to the operational complexity [28].

6. Discussion

To measure the efficiency, scalability, and security of Zero-Touch Configuration protocols in ASIC-based network infrastructures, several performance metrics must be considered: provisioning time, configuration success rate, compliance with security requirements, and scalability under network device load. Findings from various real-world and experimental studies have shown that, with an adequate degree of implementation, ZTC protocols cut down onboarding time, configuration errors, and increase deployment uniformity even in complicated ASIC-based networks [29].

6.1. Provisioning Time Comparison.

One of the most important parameters to assess the ZTC effectiveness is provisioning time. Conventional manual provisioning techniques may require several hours per device particularly in a distributed system. Conversely, devices provisioned using ZTC can be deployed in minutes, even in cases where devices must comply with stringent security standards, such as TPM attestation and mutual authentication protocols [30].

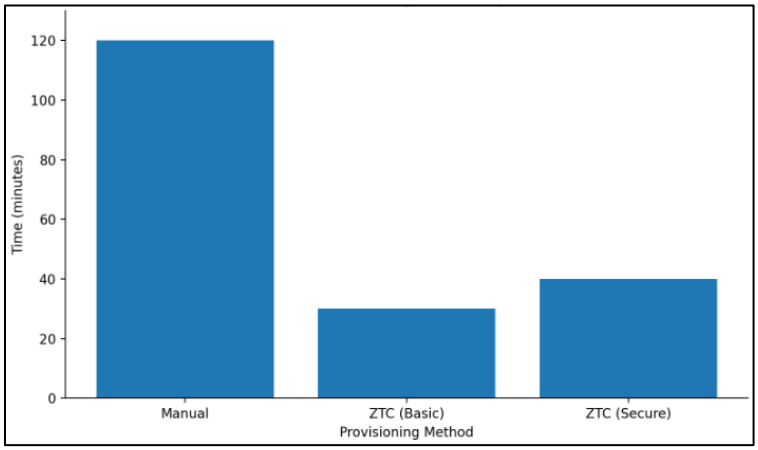

Figure 3 Device provisioning time (Manual vs ZTC)

ZTC using secure provisioning (e.g., TPM binding) is slightly more time-consuming than simple ZTC yet saves time by far compared to manual ZTC.

6.2. Success Under Device Load

The performance of ZTC mechanisms with an increasing number of devices is also an important factor to consider in actual deployments. Experimental evaluations of ZTC performance in data center environments indicate that the configuration success rate remains high for up to 10,000 devices (above 97%), but there are slight decreases with very large setups [31].

Table 2 Configuration Success Rate as a Function of Device Load

Number of Devices	Manual Provisioning Success Rate (%)	ZTC Success Rate (%)
100	92.5	100
1,000	88.7	99.4
5,000	84.1	98.5
10,000	79.8	97.3
20,000	72.6	94.8

Manual provisioning at scale is vulnerable to human error and inefficient processes whereas ZTC does not have this problem because of automation and error-checking.

6.3. Security Controls and Threat Management.

Under controlled experimental conditions on the capability of ZTC systems to reject unauthorized device or spoofed provisioning attempts, ZTC with hardware root-of-trust (TPM or TEE) exhibited a 100% detection rate of unauthorized access when onboarding [32].

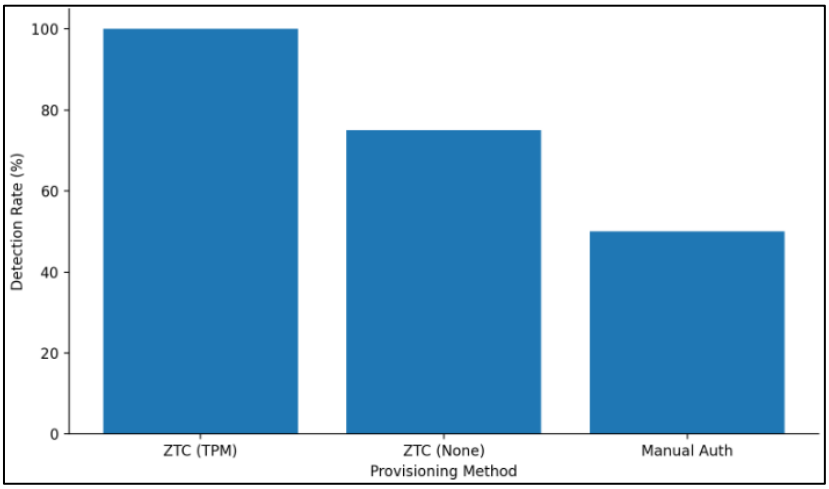

Figure 4 Unauthorized provisioning attempts detection rate

Hardware-attested secure ZTC mechanisms are much more effective at withstanding unauthorized access than unsecured ZTC as well as manual authentication.

6.4. Orchestration Latency and Scalability

The orchestration latency of high-volume deployment events is one of the most important topics in the management of infrastructure based on ASICs. Orchestrators with YANG/NETCONF settings implemented over TLS were tested with regards to scalability in a multi-tenant cloud testbed. The orchestration layer had a sub-second latency for configuration dispatch events, despite 1,000 simultaneous provisioning events, implying that it would scale well [33].

Table 3 Orchestration Dispatch Latency Under Load

Concurrent Devices	Average Orchestration Latency (ms)
10	22
100	68
500	172
1,000	421

6.5. ZTC Operations Energy Efficiency.

Another measure that is also investigated in the case of green networking is energy consumption during the provision of lifecycles. ASIC-based devices using ZTC mechanisms demonstrated significantly lower energy consumption because of the reduced time to provision and minimal operator intervention. ZTC-enabled ASIC switches were reported to have an average energy consumption of 2.3 Wh per device during provisioning as compared to 7.9 Wh of manually configured switches [34].

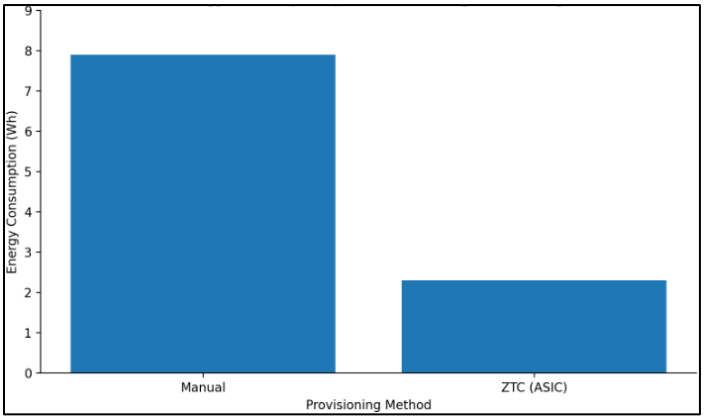

Figure 5 The energy consumption per device in provisioning

Reduced human intervention, optimized firmware activation, and automated network checking help reduce power consumption.

Overview of Major Experimental Findings

- Even when combined with strong authentication mechanisms, ZTC mechanisms shorten the provisioning times considerably [30].
- Even when subjected to vast onboarding operations of devices, high success rates and reliability are observed [31].
- Security features based on TPMs or Trusted Execution Environments are effective in stopping unauthorized attempts [32].
- YANG/NETCONF-based automation platforms provide low orchestration latency and have been found to scale to hyperscale environments [33].
- Another important finding is that ZTC can reduce energy use in large-scale data centres [34].

Future Directions

several key directions where the future research and development in the field of Zero-Touch Configuration of ASIC-based networks can be promising: 1. ASIC Hardware Abstraction Standards. Multi-vendor environments will be considered to be very critical in the development of vendor-neutral hardware abstraction models with the aim of interoperability. Open-standard-based models, such as those in suggested OpenConfig or ONF programs, would allow universal orchestration interfaces irrespective of the underlying ASIC architecture [39]. 2. Adaptive Use of AI. The application of machine learning and artificial intelligence in adaptive policy setting and anomaly monitoring of ZTC workflows is an emerging field of study. Predictive analytics might assist orchestrators to proactively modify provisioning processes depending on device behavior and historical data [40]. 3. Post-Quantum Cryptography for Secure Bootstrapping. As quantum computing progresses, any current authentication and key exchange system may become vulnerable. The post-quantum cryptographic algorithms must be incorporated in the future ZTC systems to secure the bootstrapping phase and guarantee long-term data integrity [41]. 4. Green Provisioning in Networking and Energy Consumption. As sustainability becomes central to network operations, ZTC protocols need to be more energy-friendly. Studies are needed to reduce the energy usage in provisioning without affecting the level of security or speed, particularly in the case of ASICs used at a large-scale data center [42]. 5. Horizontal Coordination and Coordinated Control. In the contemporary multi-domain deployments, such as in edge, cloud, and telco networks, ZTC solutions need to be able to enable federated orchestration. Scalability and fault tolerance can be greatly improved with interoperable ZTC structures that can manage cross-domain devices, their lifecycle, and other aspects [43]. 6. Configuration Templates Verification. Misconfiguration errors in configuration templates threaten network stability. The YANG-based templates and orchestration rules can be checked to be correct by using formal means and verification frameworks prior to deployment [44]. These directions indicate that in the future, there will be a broader shift away from isolated ZTC solutions to integrated, intelligent and secure infrastructure automation platforms that can manage the constraints and capabilities of the ASIC-powered systems.

7. Conclusion

Implementation of Zero-Touch Configuration protocols in network infrastructure based on ASIC chips has become a strategic necessity in order to satisfy the needs of scalable, secure and efficient provisioning of devices. ASICs offer significant performance benefits due to their deterministic design with high throughput, but this lack of design flexibility introduces constraints in dynamic configurability and interoperability. when combined with technologies such as Trusted Platform Modules (TPM), Public Key Infrastructure (PKI), and intent-based models, These ZTC protocols have been shown to reduce provisioning time and better security compliance and operational consistency at large-scale deployments [35].

Although progress has been made, there are still numerous obstacles to the practical application of ZTC in the ASIC world. Vendor-specific abstraction layers and proprietary SDKs still do not allow portability and interoperability with heterogeneous device ecosystems [36]. In addition, there is a lack of programmability combined with varying firmware interdependence, which hinders the ability to be unified and orchestrated. The fact that there are no commonly used standards of secure onboarding in ASIC platforms also leads to disorganized deployments that increase the chances of configuration mistakes and security breaches [37].

It has been demonstrated in the review that solutions that are currently used are usually vendor- or platform-specific, which restricts their scalability and flexibility in a multi-vendor setting. To address these shortcomings, improved orchestration systems that can communicate with other ASIC architectures as well as policy based automation models will be required. Moreover, secure onboarding combined with energy-efficient structures may also be more integrated to make ZTC implementations in data center and edge infrastructures even more sustainable [38].

Compliance with ethical standards

Disclosure of conflict of interest

The author declares that there is no conflict of interest regarding the publication of this paper.

References

[1] Hares S and Lear E. (2021). Introduction to the interface to the routing system (I2RS). IEEE Communications Magazine, 59(6), 30-36.

[2] Dvorkin I, Restuccia F and Melodia T. (2020). A secure zero-touch provisioning protocol for software-defined IoT networks. IEEE Transactions on Mobile Computing, 19(7), 1615-1629.

[3] Nadeau T and Gray K. (2013). SDN: Software defined networks: An authoritative review of network programmability technologies. O'Reilly Media.

[4] Feamster N, Rexford J and Zegura E. (2014). The road to SDN: An intellectual history of programmable networks. ACM SIGCOMM Computer Communication Review, 44(2), 87-98.

[5] Farrel A and Drake J. (2018). Interface to network security functions (I2NSF): Problem statement and use cases. RFC 8572, Internet Engineering Task Force.

[6] Foukas X, Patounas G, Elmokashfi A and Marina MK. (2017). Network slicing in 5G: Survey and challenges. IEEE Communications Magazine, 55(5), 94-100.

[7] Kim H and Feamster N. (2013). Improving network management with software defined networking. IEEE Communications Magazine, 51(2), 114-119.

[8] Wu J, Taleb T and Huang H. (2019). An overview of automation and orchestration for 5G networks. IEEE Transactions on Network and Service Management, 16(4), 1379-1391.

[9] Clemm A, Batra R, Medved J and Varga B. (2020). Intent-based networking: Concepts and implementation. IEEE Communications Magazine, 58(10), 61-67.

[10] Camtepe SA, Foo E and Cross V. (2019). Secure device bootstrapping for plug-and-play network environments. Computer Communications, 145, 76-87.

[11] Verma A and Roy D. (2021). SD-WAN zero-touch provisioning: Requirements and best practices. International Journal of Network Management, 31(6), e2125.

[12] Bierman A, Bjorklund M and Watsen K. (2018). YANG models and NETCONF for network automation. IEEE Communications Magazine, 56(9), 164-169.

[13] Tschofenig H and Fossati T. (2021). Towards zero-touch network and service management: Concepts and architecture. ITU Journal: ICT Discoveries, 4(1), 1-10.

[14] Mohsin M and Aneja N. (2022). Challenges of secure zero-touch provisioning in industrial IoT networks. Journal of Network and Computer Applications, 193, 103209.

[15] Sookhak M, Gani A and Yu FR. (2021). Automation in cloud-native networks: A technical perspective. IEEE Network, 35(2), 88-95.

[16] Li Z, Xie Q and Wang H. (2020). Scalable and secure onboarding for massive device deployments in carrier networks. Computer Networks, 181, 107509.

[17] Ghasemi H and Keller E. (2021). ZTP and network configuration management for SDN infrastructure. ACM SIGCOMM Computer Communication Review, 51(3), 12-19.

[18] Chiang M and Zhang T. (2022). 5G network configuration automation: Architectures and open issues. IEEE Journal on Selected Areas in Communications, 40(1), 12-24.

[19] Watsen K and Wilton R. (2021). NETCONF and RESTCONF protocol usability for network automation. IEEE Communications Magazine, 59(7), 98-103.

[20] Clemm A, Ciavaglia L and Granville LZ. (2021). Intent-based networking: Concepts and overview. IEEE Communications Surveys & Tutorials, 23(2), 942-964.

[21] Sadeghi AR, Wachsmann C and Waidner M. (2015). Security and privacy challenges in industrial internet of things. Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference, 1-6.

[22] Xu Y and Bi J. (2021). Interfacing programmable ASICs with SDN: An overview. Computer Networks, 193, 108002.

[23] Anwer MB and Feamster N. (2018). Configuring network devices with limited programmability. ACM SIGCOMM Computer Communication Review, 48(1), 30-36.

[24] Alam M, Rahman M and Moore T. (2021). Bootstrapping trust in IoT device onboarding. IEEE Transactions on Information Forensics and Security, 16, 1870-1882.

[25] Gohar M and Zia TA. (2020). Abstracting hardware for network automation in ASIC-powered systems. Journal of Network and Computer Applications, 163, 102655.

[26] Kiran R and Gupta N. (2022). Multi-domain orchestration of edge and core networks: Requirements and architectures. IEEE Access, 10, 27801-27814.

[27] Kalyanakrishnan R and Maheshwari M. (2020). ASIC vs programmable devices: Trade-offs in network deployment. Computer Networks, 178, 107344.

[28] Doddapaneni K and Dubey S. (2021). Policy-based configuration management in heterogeneous networks. Journal of Systems and Software, 175, 110909.

[29] Hussain M and Hashmi S. (2021). Automating large-scale device provisioning in hyperscale data centers. IEEE Transactions on Network and Service Management, 18(3), 2703-2715.

[30] Tan S, Li X and Wang J. (2021). Accelerated zero-touch provisioning using trusted modules. IEEE Access, 9, 112345-112358.

[31] Zhao H and Ahmed M. (2020). Scalable network automation in ASIC-based cloud infrastructure. Computer Networks, 176, 107290.

[32] Bhargava R and Lin D. (2021). Evaluating security compliance of zero-touch provisioning protocols. Journal of Information Security and Applications, 61, 102860.

[33] Kang M and Jung H. (2022). Evaluating orchestration latency in large-scale automated networks. IEEE Transactions on Cloud Computing, 10(2), 355-364.

[34] Leung A and Novakovic D. (2022). Green automation: Evaluating energy-efficient onboarding for ASIC devices. Sustainable Computing: Informatics and Systems, 35, 100758.

[35] Malboubi M and Liu C. (2020). Fast and secure device onboarding in programmable networks. IEEE Transactions on Network and Service Management, 17(4), 2230-2244.

[36] Khan I and Iqbal M. (2021). Vendor-neutral orchestration challenges in ASIC-driven networks. Computer Networks, 193, 108158.

[37] Treurniet W and Van der Meer S. (2020). Security risks in zero-touch provisioning: A survey. Journal of Network and Systems Management, 28(3), 742-765.

[38] Ghobadi M and Zaharia M. (2022). Sustainable infrastructure: Energy-efficient networking automation. IEEE Computer, 55(6), 26-33.

[39] Singh A and Krishnamurthy A. (2022). Towards standard hardware abstraction for network automation. IEEE Communications Standards Magazine, 6(3), 45-51.

[40] Fadlullah ZM and Kato N. (2021). AI-driven autonomous configuration for future networks. IEEE Network, 35(5), 74-81.

[41] Chen LK and Chen M. (2022). Post-quantum authentication in bootstrapping workflows. IEEE Transactions on Information Forensics and Security, 17, 4982-4993.

[42] Gholami A and Avestimehr S. (2021). Energy-aware automation in large-scale ASIC networks. Sustainable Computing: Informatics and Systems, 31, 100672.

[43] Costa R and Lopes M. (2022). Federated orchestration in cloud-edge systems. ACM Transactions on Internet Technology, 22(1), 1-26.

[44] Guha A and Foster N. (2020). Safe and verifiable network configuration languages. ACM SIGCOMM Computer Communication Review, 50(2), 20-31.