# A Zero-Trust Framework for Industrial Internet of Things

Adel Atieh
*Faculty of Engineering and IT*
*University of Technology, Sydney (UTS)*
Sydney, Australia
adel.atieh@student.uts.edu.au

Priyadarsi Nanda
*Faculty of Engineering and IT*
*University of Technology, Sydney (UTS)*
Sydney, Australia
priyadarsi.nanda@uts.edu.au

Manoranjan Mohanty
*Faculty of Science*
*University of Technology, Sydney (UTS)*
Sydney, Australia
manoranjan.mohanty@uts.edu.au

*Abstract*— **Interactions between different types of systems from various environments are increasing continuously due to the nature of business and commercial requirements. All of these interactions require a level of trust given for each system in order to enable essential operations and functions. Traditional trust models and frameworks implemented in different environments define static levels of trust given to users and systems. This includes the Defence-in-depth security model that is typically implemented in industrial control systems (ICS) environments. While this model and other security models provide an outstanding level of restriction and security if implemented correctly, they can still allow unauthorised access to sensitive data through compromised trust devices. Industrial Internet of Things (IIoT) solutions are actively being deployed in different sectors. Despite the criticality of the environments IIoT solutions serve, these solutions require more integrated connectivity that ICS environment due to cloud connectivity. This research paper proposes a zero-trust framework for IIoT and explores how this framework could mitigate the existing risks within IIoT solutions. Moreover, this research paper proposes a zero-trust anatomy for IIoT and explores the potential performance and/or complexity overhead resulted from the use of this model.**

***Keywords— Zero-Trust, Industrial Control Systems (ICS), Industrial Internet of Things (IIoT), Internet of Things (IoT), Critical Infrastructures, Defence-in-Depth.***

## I. Introduction

Digitisation of assets has been the central focus of various industries in the past decade as data became the core of our everyday life. Specifically, a huge interest in digitising industrial assets was clear by the Industry 4.0 initiative [1]. Due to this, the Industrial IoT (IIoT) model started to be utilized widely across organizations to enhance monitoring and connectivity between organization assets [2]. IIoT involves the replacement of currently deployed Industrial Control Systems (ICS) environments with smarter and more interactive devices to communicate with next-generation IT systems. ICS environments are deployed in critical infrastructures serving multiple sectors. In Australia and other Commonwealth governments, critical infrastructures are defined as [3]:

*'Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security'.*

In order to properly segregate and secure critical infrastructures, the US Department of Homeland Security (DHS) has defined a zoned architecture with trust levels assigned to each zone defining the access and authorisation levels for resources [4]. This is built upon the security defence in depth model. Defence in Depth model aims to assist in the reduction of compromise surface area and/or breach impact to the organisation [5]. The main assumption in this model is entities contained within these zones are always trusted with respect to the devices in the zones and in zones with lower security levels [6]. Therefore, the use of security zoning can allow malicious actors to traverse defences and move laterally within trusted zones easily as the compromised device will always keep its trust level. This research paper proposes a zero-trust framework to mitigate the risks related to trust given to internal and third-party resources within IIoT solution. This research paper examines the potential performance and complexity overhead added as a result of using zero-trust.

The remaining of this paper is organized into six sections. Section 2 provides an overview on IIoT architectures, trust and zero-trust frameworks. Section 3 explains and discusses the existing issues with various trust evaluation models and existing proposed zero-trust frameworks along with our research questions. Section 4 provides an in-depth explanation of our proposed zero-trust framework and the trust evaluation process for IIoT solutions. Section 5 describes the experimental setup and implementation of the proposed zero-trust framework for an IIoT lab and compares its performance and complexity to a standard IIoT lab setup. Section 5 also provides a threat model for the proposed zero-trust framework implementation. Section 6 provides an analysis of the observed results and the impact of these results on IIoT environments. Finally, Section 7 draws conclusions from the results and outcomes on the use of zero-trust in IIoT solution and discusses future work and potential improvements.

## II. Literature Review

### A. IIoT Architecture

Industrial environments are built to communicate measure certain physical aspects in real world environments with field sensors and actuators. These environments are broken down into process control cells that consist of a set of systems that function and communicate together to perform certain process. IIoT environments are typically broken down into the following 4 subsystem layers [7]:

- Sensing/Actuating layer: this layer is responsible for collecting environment and operations data and sending it to the control layer. In addition, this layer can receive command signals from operators via the control layer to adjust and modify its mechanical and physical processes.
- Controller Layer: this layer is responsible for collecting and controlling field sensors and actuators.

- Gateway Subsystems Layer: This layer connects the control layer and some field sensor devices to management systems utilised by operators and to the IIoT Cloud platform layer.
- IIoT Cloud Layer: This layer performs analysis on the collected data from IIoT devices and presents dashboards and reports to the business.

### B. *Trust*

Trust has been defined as entities belief in the reliability and honesty of the behaviour of another entity. Trust is modelled in each environment for each node describing the trustworthiness. Trust is formed using the following attributes [8, 9]:

- **Reputation**: formed by intel generated by previous and historical interactions with other entities. This includes but not limited to case-studies, customer references in addition to historical bad and good events associated
- **Recommendations**: forms an indirect trust relationship with an entity by a trusted third party.
- **Sensor & behavioural data**: this attribute is formed by collecting data from different assets in an environment. This includes but not limited to authentication information, network and system logs and device health information.

Using these attributes, trust can be defined as the following:

$$reputation \times recommendations \times behaviour = trust \quad (1)$$

### C. *Zero-Trust*

The zero-trust concept was first presented in 2004 by Jericho Forum [10] to the expanding utilisation of cloud computing along with the increase of mobility in IT. This has introduced private networks and systems to various uncontrolled dynamic environment that are vulnerable to various threats. Zero-Trust consists of a series of theories and concepts that aims to lower the likelihood of unnecessary access in the network. This is done by enforcing continuous authentication and authorisation per access request made by devices [11]. The zero-trust model treats all hosts as if they are in compromised networks [6].

## III. Current State of Research & Research Questions

Zero-Trust is still a new concept that's still being explored and examined by multiple organisations and security vendors around the world. There are still new models and frameworks that are being developed that follow the zero-trust principles. Paper [12] proposed a novel explicit zero trust methodology enabled by a network architecture which utilises steganography to embed authentication tokens in TCP requests. Paper [13] also proposed a dynamic trust model that utilises fuzzy logic to derive the trust value of cloud services and address the issue of uncertainty. One of the main zero trust architectures proposed in the industry is Google Zero Trust approach called BeyondCorp. BeyondCorp defines the different controls used to implement zero trust in Enterprise environments [14,15]. Paper [16] proposed a zero-trust solution for a university environment while paper [17] proposed a zero-trust framework for healthcare. In addition, NASA proposed a zero-trust architecture that could suit their environments and facilities [18]. These solutions cover networks and environments that follow enterprise standards, and they utilise score-based trust evaluation approach.

However, these proposed solutions and models do not cover IIoT environments as these environments are mainly based on machine-to-machine data communications. In this research paper, we are proposing a score-based zero-trust model for IIoT environments. The proposed model will be catering for the nature of industrial systems to apply necessary restriction while minimising its impact on the functionality and operation of IIoT solutions. Throughout our paper, the following research questions will be covered:

1. How can zero-trust be implemented for IIoT environments?
2. How can zero-trust improve the security of IIoT environments?
3. Does zero-trust affect the performance and/or complexity of the solution?

## IV. Proposed Zero-Trust Framework for IIoT

### A. *Zero-Trust Architecture*

The proposed Zero-Trust architecture consists of three functional layers that are responsible to organise and enforce policies on the data flow between systems. Various security controls are implemented and integrated together at each layer using different methods and interfaces. Figure 1 shows the following three layers included in our architecture:

- **Data Layer**: this layer is responsible for sending data between devices. This layer is where the IIoT edge devices reside that need to communicate with the cloud IIoT platform resource servers. This layer includes multiple Policy Enforcement Points (PEP) that are controlled and driven by the control layer. The PEP is responsible for managing the connection between a subject and a target resource.
- **Control Layer**: this layer is responsible for configuring and managing access to the resources. Access requests are made through the control plan after authenticating and authorising the device(s) and user(s). This layer includes the Policy Admin (PA) of the solution. The responsibility of the PA is to allow and/or stop communication between the entities and works with the PE to enforce the appropriate action. The Zero-Trust (ZT) engine acts as the PA which communicates with PE and the PEP(s).
- **Security Analytics Layer**: this layer includes The Policy Engine (PE) of the solution. PE is the main engine responsible for granting, denying or revoking access for a subject to a resource. All the decisions made by the PE is logged for auditing and future evaluation purposes. This layer is also responsible for enriching the control layer with data that can allow the ZT engine to take appropriate actions dynamically based on dynamic trust management.

### B. *IIoT Trust Evaluation*

To evaluate the trust of systems in IIoT environments, our proposed zero-trust framework uses a scoring-based trust evaluation approach.

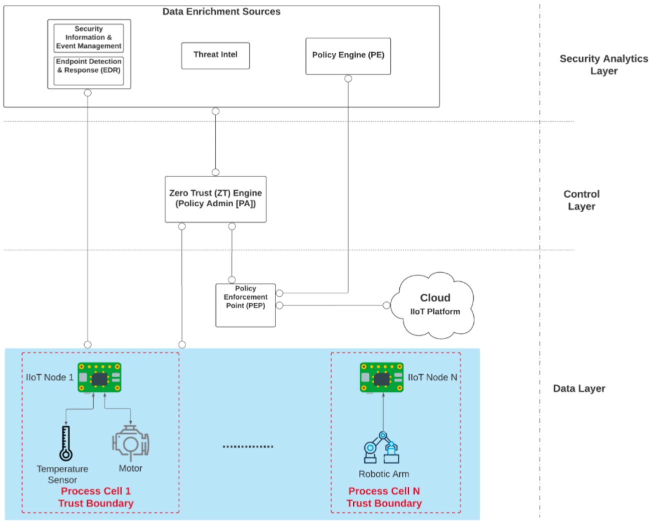

Figure 1: The proposed zero-trust architecture

The trust criteria we chose to be used for this trust evaluation approach are divided into the following three categories:

- Device-based criteria (operation, cell, zone/are): evaluation criteria based on the values collected from the IIoT client related to hardware and the programming of the device consisting of:
  - Serial Number
  - GPS Location
  - Zone
  - Process Cell ID
- Network-based criteria: data related to the networking configuration of the device consisting of:
  - IP Address
  - MAC Address
  - GPS
- Security based criteria: authentication credentials and behavioural data used to authenticate and authorise devices dynamically. This consists of:
  - Security Alerts
  - Threat Intel
  - Behavior-based

### *1) Trust Access Grant Levels*

Each IIoT client will need to authenticate and provide their attributes in order to gain a level of access into the environment. The total trust score is calculated by summing all the trust scores of each of the valid attributes provided by the IIoT client. Based on the total trust score, IIoT clients will be granted an access level. There are three different access grant levels that can be given to an IIoT client when they authenticate in our framework:

- **Full Access grant**: authorised access to resources in the environment with full permissions based on the IIoT client role. IIoT devices with full access grant are able to send I/O read/write control signals to field devices and send metrics to the central IIoT cloud platform. It will also be accessible by IT administrators and the security incident response team for management and to respond to threats when required.
- **Partial Access grant**: IIoT devices with partial access will report their metrics and status to the IIoT platform and will be accessible by the engineering team. However, they will not be able to send write signals to field devices to prevent the possibility of an attacker disrupting and/or modifying the process logic of these systems.
- **Limited Access grant**: IIoT devices with limited access will not report their status and metrics to the IIoT platform. It will only be accessible by central management.

Table 1 shows the access permissions given to an IIoT device per access grant level. Our scoring-based approach is implemented by adding a trust score for each authorisation process performed. Table 2 shows a breakdown of the proposed trust score thresholds per access grant level. **The minimum total trust score required to gain access to the required resource is 55 with the maximum score being 100 and minimum being 0.** The total score is calculated based on the sum of the trust attributes used when authenticating and authorising the subject entity and is affected by the security events that are associated with that entity.

TABLE I: Access Permissions per Access Grant Level

| **Access Grant Level** | **Field Device** | **Same Cell Device** | **Engineering Team** | **Cloud IIoT Platform** |
|---|---|---|---|---|
| Full Access | ✓ | ✓ | ✓ | ✓ |
| Partial Access | | | ✓ | ✓ |
| Limited Access | | | ✓ | |

TABLE II: Access Grant Trust Threshold Scores

| **Access Grant Level** | **Threshold** |
|---|---|
| Full Access | ≥ 55 |
| Partial Access | ≥ 25 |
| Limited Access | ≤ 25 |

### *2) Trust Attribute Evaluation*

These attributes have been chosen accordingly to create a security profile of systems that suits the nature and basis of IIoT environments. The table below describes the scores given to each attribute. Table 3 shows the proposed trust scores given to each trust attribute.

TABLE III: Access Grant Trust Threshold Scores

| **No.** | **Attribute** | **Acronym** | **Trust Score** | **Type** | **Requirem ent** |
|---|---|---|---|---|---|
| 1 | Serial Number | SN | 15 | Device | Optional |
| 2 | Industrial Zone | IND | 15 | Device | Mandatory |
| 3 | Process Cell ID | PRC | 15 | Device | Mandatory |
| 4 | IP Address | IP | 25 | Network | Mandatory |
| 5 | MAC Address | MAC | 15 | Network | Optional |
| 6 | GPS Location | GPS | 15 | Network | Optional |

### 3) *Security Event Trust Score*

The breakdown of these trust thresholds has been established focusing on mandatory attributes to get the full access to the environment. If some of mandatory attributes are not provided, then a device cannot be authorised. Optional attributes can assist the agent in gaining a higher trust score and hence higher access level. However, when a security event occurs then the trust score is decreased and hence the access level may decrease. Table 4 describes the security events and their associated trust score.

TABLE IV: Access Grant Trust Threshold Scores

| No. | Event | Acronym | Trust Score |
|---|---|---|---|
| 1 | Security Alert - Low | SEC-L | -10 |
| 2 | Security Alert - Medium | SEC-M | -30 |
| 3 | Security Alert - High | SEC-H | -50 |
| 4 | Threat Intel | TI | -25 |
| 5 | Behaviour | B | -15 |

Using our framework and the proposed trust scores, the resultant trust score for an entity is calculated through this formula:

$$T_{Attribute} + T_{SecurityEvent} = T_{Entity} \quad (2)$$

- $T_{Attribute}$: The total sum of the used attribute scores
- $T_{SecurityEvent}$: The total sum of the detected security events
- $T_{Entity}$: Resultant entity trust score

## V. Experimental Implementation & Threat Modelling

The main objective of this experimental implementation is to **measure and compare the latency between the proposed zero-trust solution and a standard IIoT solution**. The solution implementation examined the functionality of the experimental design and recorded the results observed from the following tests:

- Lab Design
- Performance Testing
- Results

### A. *Lab Design*

#### 1) *Zero-Trust IIoT Lab Design*

The lab implementation consists of three functional layers that are responsible to organise and enforce policies in our lab:

- Data Layer: Wazuh agents are installed on these edge devices in order to facilitate logging of events and send it to the Security Analytics Layer for analysis and detection. NGNIX is used as PEP to allow or drop traffic based on the authorisation and trust levels of the data flow sent to the cloud IIoT Platform.
- Control Layer: The ZT was implemented with SOAR capabilities to dynamically apply traffic enforcement policies. SOAR capabilities are implemented with different combinations of Python3 scripts and servers running Flask to receive various data input feeds.
- Security Analytics Layers: This layer is the main support layer for the control layer that feeds multiple types of security events. This includes the following feeds:
  - Identity Governance: Keycloak is the Policy engine which will act as the authorisation server for this environment.
  - Endpoint Detection and response: Wazuh is the chosen EDR system for this solution.
  - Threat Intelligence: the chosen threat intel platforms are as follows:
    - Alienvault OTX
    - VirusTotal (VT)

#### 2) *IIoT Standard Solution Lab Design*

The cloud lab design will only have direct data flow between the IIoT client and the IIoT platform server in the cloud. The implementation of the cloud lab is quite similar to the Zero-Trust lab design except for the security layers applied in the Zero-Trust lab.

### B. *Implementation*

In our experimental set-up we used ThingsBoard as the IoT platform. A Raspberry Pi 3 model B+ board is used as the IIoT client which runs a Python Script to communicate with the ThingsBoard servers. The network connectivity was established via 2.4GHz wireless LAN using Wi-Fi (≈ 72 Mbps). Google Cloud was chosen for the cloud setup. We have chosen australia-southeast1-a as the Google Cloud zone which is located in Sydney, Australia in order to get the optimum latency between our IIoT device and our cloud IIoT platform. The internet bandwidth used for connecting the IIoT client and the cloud setup was as follows:

- Download ≈ 50 Mbps
- Upload ≈ 14 Mbps

### 5.3 Performance Testing

In order to perform appropriate Performance testing to our solution, we compare the number of hops and the total latency for both deployments. As the standard cloud lab setup has less hops and interactions required to verify and authorise IIoT device, we expect a lower latency from cloud lab setup than the zero-trust lab. The following measurements are performed:

**Systems interaction analysis** is performed by analysing the number of interactions required to send IIoT data from the IIoT client to the cloud IIoT server. The following interactions for successful transfer of data from a IIoT client to cloud IIoT server are required:

1. *IIoT client → NGINX reverse proxy (PEP)*
2. *NGINX reverse proxy (PEP) → ZT-Engine (PA)*
3. *Verification Request*
   a) *ZT-Engine (PA) → Keycloak server (PE)*
   b) *ZT-Engine (PA) → EDR*
4. *Valid Verification Response*
   a) *Keycloak server (PE) → ZT-Engine (PA)*
   b) *EDR → ZT-Engine (PA)*
5. *NGINX reverse proxy (PEP) → Google Cloud Firewall*
6. *Google Cloud Firewall → ThingsBoard Server (Cloud IIoT Server)*

On the other hand, the following interactions to send data from the IIoT client to the cloud IIoT server using the standard cloud IIoT lab requires only the following interaction:

1. *IIoT client → Google Cloud Firewall*
2. *Google Cloud Firewall → ThingsBoard Server (Cloud IIoT platform)*

**Latency measurement** is performed by sending IIoT data from the IIoT client to the cloud IIoT server utilising both lab setups to measure and comparing their latencies. To measure the latency of both lab setups, we have sent 25 IIoT data packets from the IIoT client to the cloud using the zero-trust lab and the cloud lab setup. We observed that the cloud lab setup had a lower latency than the zero-trust lab. Table 5 summarises the results observed from our analysis and tests.

TABLE V: Performance Testing Results Summary

| **Metrics** | **Zero-Trust Lab** | **IIoT Cloud Lab** |
|---|---|---|
| No. of hops | 5 | 1 |
| No. of interactions | 8 | 2 |
| Min. latency (ms) | 96.0102 | 36.9999 |
| Max. latency (ms) | 401.3401 | 50.9200 |
| Avg. latency (ms) | 142.9972 | 44.0488 |

## VI. Analysis

As expected from the performance testing, the zero-trust lab had higher latency than the standard IIoT cloud lab. The major factor here is the long verification process required to authorise the IIoT device traffic the cloud IIoT server. In addition to the performance overhead, it is clear that the proposed zero-trust framework introduces more complexities due to the increased number of systems and integrations. Increasing complexity increases the likelihood of errors and issues occurring in the environment which likely can have a severe impact on critical infrastructures. From a security perspective, the zero-trust lab provides the capability required to respond to threats and apply restrictions dynamically based on the dynamic trust score of an asset in the environment. However, as the trust is defined solely based on defined attributes and security events, there will always be a chance of false positives occurring. In order to enhance the zero-trust applied actions, **machine learning and Artificial Intelligence (A.I.) with fog computing** would be the complementary factors to improve the accuracy and results of this framework.

## VII. Conclusion

The convergence of IT and critical industrial environments is becoming more apparent as the need for advanced technologies and integrations increases. IIoT is one of the key enablers that can introduce the need for this convergence to occur and become a core technology ecosystem. Zero-trust is one of the new concepts that being frameworks that are being studied and explored in various avenues. As discussed in our paper, further work is needed to improve the performance and reduce the complexity of the trust evaluation and authorisation process of zero-trust for IIoT. This can be achieved potentially by the use of fog computing to reduce the latency and change the trust evaluation process of the framework. In addition, the utilisation of machine learning and/or deep learning within the zero-trust framework may assist in improving the accuracy of the trust evaluation and hence the response to threats targeting IIoT environments.

## References

[1] Australian Government - Department of Industry, Science, Energy and Resources, 2018, Industry 4.0, viewed 20/03/2021, https://www.industry.gov.au/funding-and- incentives/industry-40.

[2] Libow, E., Indurkhya, G., Kreger, H., Hahn, T., Niblett, P., Mike Edwards, Wallace, T.S.S., Luthra, T., Menon, R., Schalk, K., Koupman, E., Daly, G., Flaherty, R., Noller, D. & Kiradjiev, P. 2016, The IBM Advantage for Implementing the CSCC Cloud Customer Reference Architecture for Internet of Things (IoT), IBM.

[3] Critical Infrastructure Centre Australia 2018, Critical Infrastructure Centre Com- pliance Strategy.

[4] DHS 2016, Recommended Practice: Improving Industrial Control System Cyber- security with Defense-in-Depth Strategies, National Cybersecurity and Communi- cations Integration Center Industrial Control Systems Cyber Emergency Response Team.

[5] Amoroso, E. 2018, An overview of the OT/ICS landscape for cyber profes- sionals, viewed 1/25/2020, https://www.helpnetsecurity.com/2018/07/13/ot-ics- landscape/.

[6] Gilman, E. & Barth, D. 2017, 'Chapter 1. Zero Trust Fundamentals', Zero Trust Networks, O'Reilly Media, Inc.

[7] Figueroa-Lorenzo, S., An˜orga, J. & Arrizabalaga, S. 2020, 'A Survey of IIoT Protocols: A Measure of Vulnerability Risk Analysis Based on CVSS', ACM Comput. Surv., vol. 53, no. 2, p. Article 44.

[8] English, C., Nixon, P., Terzis, S., McGettrick, A. & Lowe, H. 2002, 'Dynamic trust models for ubiquitous computing environments'.

[9] Momani, M., Challa, S. & Aboura, K. 2007, 'Modelling trust in wireless sensor net- works from the sensor reliability prospective', Innovative algorithms and techniques in automation, industrial electronics and telecommunications, pp. 317-21.

[10] Bleech, N., Yelland, G., Purser, S., Greenham, S., Tully, S., Walsh, J., Gracey, D., Dorey, P., Yeomans, A., Seccombe, A., Dobson, I. & Lacey, D. 2005, Visioning White Paper What is Jericho Forum?, Jericho Forum.

[11] McClure, D., Death, D., Henley, J., Flick, J., Hernandez, S., Jacobs, D., Harris, D., McKelvey, E., Lamoureaux, J., Harrison, J., Frazier, S., Kovac, S., Gates, T., How- ell, M. & Karkenny, M. 2019, Zero Trust Cybersecurity Current Trends, American Council for Technology-Industry Advisory Council (ACT-IAC).

[12] DeCusatis, C., Liengtiraphan, P., Sager, A. & Pinelli, M. 2016, 'Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authenti- cation', 2016 IEEE International Conference on Smart Cloud (SmartCloud), pp. 5-10.

[13] Selvaraj, A. & Sundararajan, S. 2017, 'Evidence-Based Trust Evaluation System for Cloud Services Using Fuzzy Logic', International Journal of Fuzzy Systems, vol. 19, no. 2, pp. 329-37.

[14] Ward, R. & Beyer, B. 2014, 'Beyondcorp: A new approach to enterprise security'.

[15] Osborn,B.,McWilliams,J.,Beyer,B.&Saltonstall,M.2016,'BeyondCorp :Design to deployment at Google'.

[16] Lukaseder, T., Halter, M. & Kargl, F., 2020. Context-based Access Control and Trust Scores in Zero Trust Campus Networks. In: Reinhardt, D., Langweg, H., Witt, B. C. & Fischer, M. (Hrsg.), SICHERHEIT 2020. Bonn: Gesellschaft fu¨r Informatik e.V.. (S. 53-66). DOI: 10.18420/sicherheit2020 04

[17] 22. Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H. & Zhai, Y. 2021, 'A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture', IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10248-63.

[18] 23. Kay, D. 2019, Planning for a Zero Trust Architecture Target State, Cybersecu- rity Standards, Architecture and Engineering, Federal CIO Zero Trust Architecture Summit.