Technologies for Industrial Internet of Things (IIoT): Guidelines for Edge Computing Adoption in the Industry

Ralf Luis de Moura[1(✉)], Tiago Monteiro Brasil[2], Ludmilla Bassini Werner[1], Claudio José Barcelos Dal' Col[2], Alexandre Gonzalez[3], and Sajjad Quadri[4]

[1] Vale S.A., Vitória 29990-900, Brazil
{ralf.moura,ludmilla.werner}@vale.com
[2] Vale S.A., Nova Lima 34006-270, Brazil
{Tiago.brasil,claudio.dalcol}@vale.com
[3] Vale S.A., Rio de Janeiro 22250-145, Brazil
alexandre.gonzalez@vale.com
[4] Vale S.A., Toronto M5J2K2, Canada
sajaad.quadri@vale.com

Abstract. The industrial sector is reinventing itself to find improved production processes. Industry 4.0 brings opportunities for growth productivity with the IIoT. There is a range of IIoT-related technologies to manage vast volumes of data that should be stored and processed for the decision-making process. Cloud computing is a reliable option for remote storage and data processing. However, in situations where the requirement is response time, intermittent connectivity, and low latency, edge computing processing is a more suitable option. Any device with computational resources can implement an edge computing capability with functions like gateway and data aggregator capabilities. These devices need to be classified to avoid an uncontrolled proliferation of appliances in the enterprise's environment, which easily create cybersecurity vulnerabilities and transform device management into chaos. This study proposes a taxonomy for edge computing and defines industrial application guidelines as a strategy to facilitate their sustainable implementation.

Keywords: Edge computing · Guidelines · Taxonomy · Industrial Internet of Things

1 Introduction

The Internet of Things (IoT) is considered a new technological paradigm where any device or machine may interact with each other [1]. The Industrial Internet of Things (IIoT) is the application of IoT in the industry. It is part of the Industry 4.0 concepts that transform many segments in enterprises and challenging industries to rethink their production processes on an unprecedented scale. The IIoT emphasizes the idea of consistent

S. Paiva et al. (Eds.): SmartCity360° 2020, LNICST 372, pp. 259–273, 2021.
https://doi.org/10.1007/978-3-030-76063-2_19

digitization, combining the strengths of traditional industry technologies with internet and cloud capabilities [7].

Many IIoT solutions have cloud-based applications as a central computational infrastructure to store and process data generated by different sources. This model assumes the existence of stable connectivity with low latency and acceptable response times for an ever-increasing demand for IIoT data.

The majority of IIoT literature is based on the reactive computing paradigm that data computing starts after the data task is offloaded to the central processing node. However, stringent latency and reliability constraints in networks often are not considered. The high volume and fast velocity of data streams generated by IIoT devices may consume a massive amount of network bandwidth. Since the remote cloud is physically distant from IIoT devices that send application requests and await the results to be processed and generated in the remote cloud, the response time for these requests may not be adequate. This delay can be especially unbearable, considering sensitive IIoT applications [5]. Due to these networks' distributed nature, having computing resources closer to the edge network enables personalized and robust computational services [4].

The concept of edge computing is predicated on moving some computational load to the network edge [3], enabling, for example, processing on-premise, next to where the data is being generated [1].

Several types of devices may process data on-premises. In general, any device with computational capability may receive data from various "things" and process them locally. This situation may provoke the enterprise dissemination of many distinct electronic devices with different characteristics. Its heterogeneity can produce management issues when maintaining and supporting these devices—for example, critical services such as things diagnosis and failure alarms [1].

Cyber-security is another critical point; edge devices, in the IIoT context, interact with various access technologies, such as Wi-Fi, Bluetooth, LoRaWAN, and LTE. It makes the edge infrastructure prone to several cybersecurity attacks. For example, Denial-of-Service (DoS) and Man-in-the-middle attacks, furthermore, attackers could access the information stored in the edge [6]. It shows how imperative it is to create specific rules for adopting adequate edge computing devices, to avoid reliability, management, and cyber-security issues.

There is a growing interest in using IIoT edge computing technologies in various industries [13], but one of the biggest challenges is choosing the right technology for adoption. There are a plethora of edge computing solutions, making their way into the industry [14]; however, the industry has specific technological features that need to be considered before choosing the right technology.

This study proposes an edge computing taxonomy and defines rules for their adoption in each category previously defined here. It assumes that edge devices need to be appropriately classified, and rules should be created before the industry's adoption. Device standardization is useful to avoid the proliferation of mixed solutions, simplify the management, and mitigate cyber-security attacks, facilitating these devices' adoption.

2 Industrial Internet of Things

Internet of Things – IoT can be considered as a "… group of infrastructures, interconnecting connected objects and allowing their management, data mining and the access to data they generate" where connected objects are "sensor(s) and/or actuator(s) carrying out a specific function that can communicate with other equipment" [8]. The Industrial Internet of Things (IIoT) is the application of these technologies in manufacturing [5]. IIoT can be considered a physical network of things, objects, or devices for sensing and remote control, in an industrial context, that allowing greater integration between the physical and cyber world [5].

Boyes et al. [9] conceptualize the Industrial Internet of Things as "a system comprising networked smart objects, cyber-physical assets, associated generic information technologies and optional cloud or edge computing platforms, which enable real-time, intelligent, and autonomous access, collection, analysis, communications, and exchange of process, product or service information, within the industrial environment, to optimize overall production value."

The use of these technologies results in generating huge volumes of data to be stored, processed, and presented in a friendly and interpretable way [6]. This large amount of data requires information technology services with diverse and sufficient capacity to support the growing demand, typically offered by cloud computing services [10].

Cloud computing is an internet-based computing paradigm that provides on-demand services through a configurable set of computing resources [5]. The Cloud computing platform delivers virtually endless capabilities and services that meet the various IIoT demands [8, 9]. However, cloud computing may not always be the best strategy for industrial applications, and sometimes, the computing needs to be performed closer to the source of the data to improve the service delivered [18].

IIoT combines the application of machine-to-machine communication and smart machines capable of delivering data that can be used for future analysis. IIoT requires the application of several connectivity options due to the diversity of scenarios with varied requirements in remote locations related to physical distance, latency/jitter, infrastructure, installation environments, and energy consumption [7]. These features demand on-premises devices and particular communication protocols to provide robustness and redundancy, considering that remote locations typically do not have the proper communication infrastructure [10].

One technology that should be adopted by the industry is edge computing, in some situations replacing cloud-based applications due to the network dependency and latency. Real-time and near real-time systems need fast response time, for example, when applied in industrial equipment. However, the application of these devices imposes challenges that need to be adequately addressed.

3 Challenges in Edge Computing

Although the term edge computing is relatively new in the context of IIoT, its function has been known and applied for many years, and it can be found in almost every segment of human activity [23]. It is a variation of distributed computing [25] applied in the industry

through distributed control systems in which the process intelligence takes place closer to the factory floor. Generally, any equipment that does any processing close to the origin point of data can be considered edge computing.

ARC Advisory Group [14] defines the Industrial IoT edge as the place where physical devices, assets, machines, processes, and applications intersect with internet-enabled portions of the architecture. Industrial IoT edge devices provide input to, and may receive output from, industrial internet-enabled systems, applications, and services but reside outside of clouds and local data centers.

Koustabh and Datta [2] defines Edge Computing as "The delivery of computing capabilities to the logical extremes of a network to improve the performance, operating cost, and reliability of applications and services." Gartner defines edge computing as "solutions that facilitate data processing at or near the source of data generation" [3].

Edge computing refers to enabling technologies that allow computation to be performed at the edge of the network. It is any computing and network resources located between the data sources and the central storage and processing unit, such as a cloud data center [1]. An edge device can perform computing offloading, data storage, data aggregation, data filtering, caching, and processing and distribute requests and delivery services [1, 7, 10].

Edge computing is one of the IIoT devices that most interact with other devices [10]. The implementation of edge computing devices can bring several advantages, such as network traffic reduction, faster response rate, and lower network connection reliability [24].

An edge computing device can be responsible for consolidating data from multiple sources and forwarding it to a central storage and processing unit. Local processing, such as advanced analysis, can also be performed on the edge device. It is also responsible for handling outages, storage, and data forwarding. Additionally, it enables the orchestration of other devices from different vendors using different protocols [7, 10]. Those tasks at the edge of the network introduce risks and become a challenge for industry adoption.

Edge computing requires further research work to comprehend all potential benefits [23] and limitations. From the industry perspective, some key concerns need to be addressed to enable a sustainable implementation, like, for example, device management [15], reliability [17], security, and privacy protection [13].

3.1 Management Concerns

Some edge devices provide little or no visibility into their state and composition, including the identity of any external services and systems they interact with, and little or no access to their software and configuration. Their proliferation may difficult to access, managing, and monitoring those devices. This challenge can generate some issue that should be addressed [15]:

- Lack of management features: The administrator may not be able to fully manage an edge device, including firmware, operating systems, and applications.
- Complexity regarding management at scale: An edge device may not support standardized mechanisms for centralized management.

- Wide variety of software to manage: Extensive variety of software used by edge devices, including firmware, standard, and real-time operating systems, and applications, can complicate software management tasks such as configuration and patch management.
- Lack of inventory capabilities: Edge devices included in the IIoT technology environment may not be inventoried, registered, and otherwise provisioned via regular IT processes. **Sample Heading (Third Level).** Only two levels of headings should be numbered. Lower level headings remain unnumbered; they are formatted as run-in headings.

3.2 Reliability Concerns

IoT devices are usually not designed to be used in unpredictable and variated industrial environments [17]. Unlike traditional IoT devices, IIoT devices are generally used in harsh environments exposed to dust, electromagnetic noise, humidity under a wide variety of temperatures, along with other physical risks raising concerns regarding reliability and unexpected or premature failures.

Edge computing devices often employ embedded systems, variability in circuit parameters due to the nature of the manufacturing process, signal integrity issues arising from internal and external noise sources, and accelerated aging of the devices are essential categories of reliability concerns facing embedded design systems hardware [16].

3.3 Cyber-Security Concerns

According to NIST SP 800-37 [13], cybersecurity risk and privacy risk are related but distinct concepts. For privacy, the risk is "a measure of the extent to which a potential circumstance or event threatens an entity, and typically is a function of (i) the adverse impact or magnitude of the harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." For cybersecurity, the risk is about threats—the exploitation of vulnerabilities by threat actors to compromise device or data confidentiality, integrity, or availability.

As an IIoT device, Edge computing generally faces the same types of cybersecurity risks compared to conventional IT devices [11]. Edge devices interact with the physical world through the IIoT sensor data. In the physical world, effective IIoT data management is essential to mitigate physical attacks on sensor technology. Such attacks are usually performed through wireless signals [11, 12].

Edge computing can contribute to the aggregation of data collected by many sources used for future decision-making. When misused, these capabilities can affect the decision-making process or lead to revel private information. Edge devices with IIoT actuators can make changes to physical systems and thus affect the physical world. In a worst-case scenario, a compromise could allow an attacker to use an IIoT actuator to endanger human safety, damage or destroy equipment and facilities, or cause major operational disruptions [11, 12].

Edge network interfaces often enable remote access to physical systems. It may put the physical systems accessible through the IoT devices at much higher risk. Another

important aspect is the operational requirements that devices must meet in various environments and use cases. Many devices must comply with stringent requirements for performance, reliability, resilience, safety, and other objectives. These requirements may be at odds with cybersecurity and privacy rules [11].

4 Challenges in Edge Computing

Edge computing is usually treated generically as if all edge devices perform the same function. However, this is not a reality in all use cases. The capabilities of edge computing devices range from event filtering to complex-event processing or batch processing, and more specialized edge computing devices can act as gateways or data aggregators [20].

4.1 IIoT Edge Gateway Data Capture

The first category of edge computing devices is Gateway Data Capture. Edge Gateway Data Capture (EGDC) provides connectivity for other IIoT devices, usually using wireless non-IP network protocols like LoRaWAN (Long Range Wide Area Network), Zigbee or, even IP networks like Wi-Fi. It works as a data aggregator from many sources and as a single point of store and forward.

Scripts can be created using high-level languages, python, for example, to execute during the receiving data process. These scripts can perform basic data filtering or basic data processing. EGDCs commonly are placed between network zones, for example, an access zone and another zone with internet connectivity, as showed in Fig. 1.

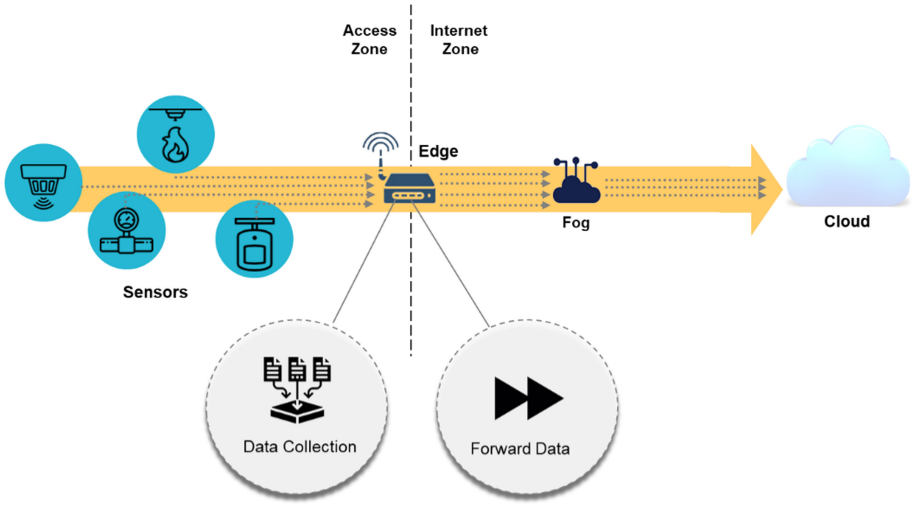

Fig. 1. IIoT gateway data capture.

These devices' primary role is data collection, usually working as a translator between access network protocols and internet protocols. Eventually, these devices can

act as a local database, storing data locally when the internet connection is unavailable and forwarding data when the connection is available.

4.2 IIoT Edge Data Processing

The second category of edge computing devices is Edge Data Processing. Edge Data Processing (EDP) is a specialized device that enables a first pass data filtering, making it possible to reduce the amount of data transmitted, running batch processing, stream analytics [7, 22], and data cleaning [2], as shown at Fig. 2.

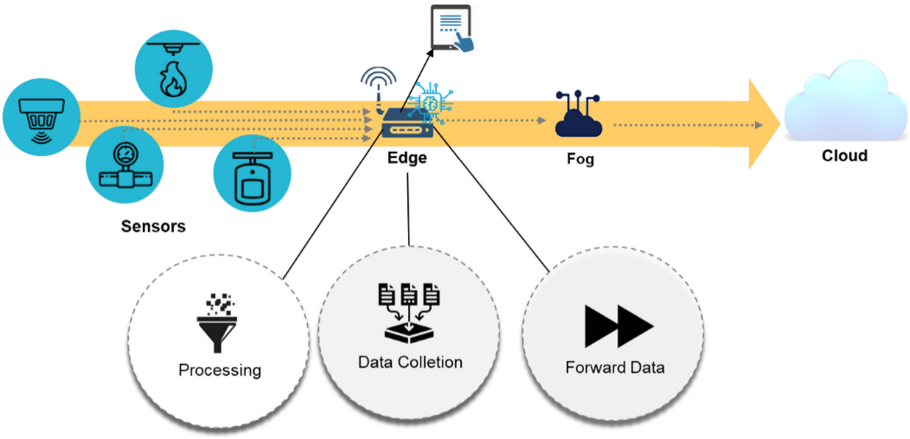

Fig. 2. IIoT gateway data processing.

The fundamental difference between Edge Gateway Data Capture and Edge Data Processing is the role that it plays in the data life cycle. For Edge Data Processing, sophisticated computational models are usually embedded and self-sufficient to the point of performing all complex processing functions locally as batch processing or stream analytics. After the processing, the row data is still needed in the cloud, but only to update the computational models' quality.

Those devices can sometimes manipulate physical variables, acting in equipment or triggering alarms. In some situations, Edge Data processing allows human interaction through human-machine interfaces (HMI), using screens, tablets, or mobile phones, for example [21].

Those two types of devices require different attention points, as they have different functions and characteristics (Table 1).

Some features are shared between the two types of devices, such as Basic Data Filtering, Storage and Forward, and Basic Data Processing, but others are different, generating different recommendations.

Table 1. Edge computing characteristics

Characteristics	EDP	EDGC
It is usually placed between network zones	No	Yes
Multiples protocols	No	Yes
Basic data filtering	Yes	Yes
Storage and forward	Yes	Yes
Basic data processing	Yes	Yes
Human machine interface	Yes	No
Embedded computational model	Yes	No
Complex data processing	Yes	No
Stream analytics	Yes	No
Data cleaning	Yes	No
Batch processing	Yes	No
Act on physical variables	Yes	No

5 Rules for Edge Computing

After the classification of the devices, it is necessary to establish rules for their adoption. Some rules are generic to adhering to both taxonomies, and some are specific to each type of edge. The rules are defined according to the concerns previously aborded: Management, Reliability, and Cybersecurity.

5.1 IIoT Edge Data Processing

With the proliferation of edge devices, it is essential to have a centralized management capability preferred to maintain all devices' control. For centralized processing to be implemented, each edge device must implement specific functions. Edge devices should enable remote management, including manipulating maintenance, monitoring, and inventory information [15].

For maintenance, the device should have the ability to:

- Upload firmware or operating system and to track the status of remote software/firmware update.
- Update applications or embedded code.

For monitoring, the device should have the ability to:

- Remotely collect health information.
- Real-time tracking of the physical location.
- Remotely collect diagnostic and error information.

For an inventory, the device should have the ability to:

- Provide information about hardware, versions, model, manufacturer.
- Provide information about time in operation, time on.

For EGDC-type devices, these features can be implemented through all protocols that the device has available, wireless or not. EDGC-type devices can also deliver information regarding other devices (things) to which they are connected to extend the same management functions. The device can be integrated into a centralized and agnostic device management system by supporting all management functions.

5.2 Reliability Rules

Tolerant electronics, as well as long life survivability, are critical capabilities required for IIoT. Approaches to harsh environments focus on component level robustness, and hardening should be considered. Moreover, the product can be designed to adapt to the changing use of environments to maintain target reliability.

Edge computing devices should be adequately designed with redundancy implemented that includes characteristics that mitigate environmental effects [16]:

- Edge devices should incorporate power optimizations and deploy techniques such as dynamic voltage scaling.
- Edge devices should use circuit techniques that generate less noise, improving circuit noise immunity, or suppressing noise without circuit modification.
- Redundancy should be provided for the edge device's subparts prone to failure.
- Industrial protection certification (water and dust resistance).
- Edge devices in IIoT networks are constrained many times. The computing capabilities should be enough for the processing suitable for the required processing load.

Harsh areas with difficult accessibility to IIoT Edge devices are very demanding on the lifespan of devices. Reliability characteristics should be present in both edge-type devices, but some of them can be relaxed if the device is installed in a location with external physical protection (panel, for example). By supporting all reliability rules, devices can be better prepared to support their tasks.

5.3 Cyber-Security Rules

To mitigate the risks of attacks on edge devices, specific rules needed to be established. By working with multiple protocols, Edge Gateway Data Capture devices may be more vulnerable to cyber-attacks. Communication protocols on access networks must be secure to prevent an attacker from taking control of an edge device or subtracting or modifying data.

Special attention needs to be given to EDP-type devices that act directly on physical variables. Devices of this type cannot be allowed to be invaded and manipulated by attackers.

Cyber-security topics should be addressed to cover fundamental security principles: for confidentiality to ensure only the data proprietor can access the edge computing information. For integrity, to assure the proper and steady transmission of data to the accredited device without unauthorized modification of the data. For availability to assure the authorized party manages to access the edge services for access control and authentication to ensure that an individual device's identification is accredited [24].

In general, an edge computing device should have:

- A registration process.
- An initial provisioning process regarding software, components, and configurations.
- Authentication mechanisms.
- Encryption mechanisms.
- A decommissioning strategy, including revocation of access, certificates, and deletion of sensitive data
- Control and restrict access to devices individually or in a group.

Device management systems implemented through the management rules can assist in the cybersecurity requirements since real-time monitoring can allow for halting attempts at hacking quickly.

By supporting all cyber-security rules, devices can be less vulnerable. These requirements are necessary for both edge computing devices, especially to EGDC-type due to the multiple options of connection and to EDP-type devices that manipulate physical variables.

5.4 IIoT Computing Placement Strategy

An IIoT edge device should be appropriately positioned in network infrastructure, and its data flow should be segregated to prevent mixing it with the TI data flow. This guidance is necessary for two main reasons, the first for security, preventing an attacker from taking over a smart device, or even the edge computing device to gain access to the corporate network. The second reason is related to the use of the corporate network only for traditional IT services, avoiding an overload or improper use of the infrastructure.

For economic reasons, the physical IT infrastructure, in some situations, may be used for IIoT data flow, but it should be logically segregated. Figure 3 shows an example of network segregation, using a DMZ as an intermediate zone between data collection at the source and the final destination of data in the cloud or an on-premises database. DMZ is the first line of defense to protect the internal infrastructure from external threats [26]. The figure shows a typical EGDC device; however, positioning can be applied to any type of edge computing device.

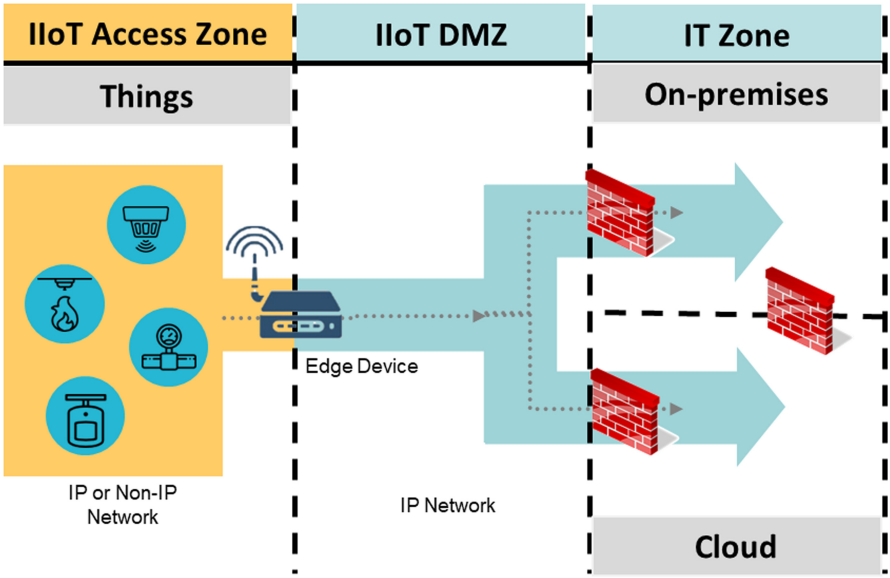

Fig. 3. IIoT edge placement

6 Study Case of Edge Computing Devices

Two case studies are presented in this section to illustrate the edge computing devices rules comprehensively. First, it was analyzed an EGDC-type device that uses LoraWAN protocol. Second, an EDP-type device for local data processing.

Both devices are available in the market and are considered relevant, and they can be easily acquired for IIoT applications. The manufacturers' names will not be revealed; only each one's main characteristics will be addressed.

6.1 IIoT Edge Gateway Data Capture

The EGDC-type device is part of the global Long-Range Radio fixed network to provide an M2M connectivity link between low power end-point and Internet access. The EGDC-type device has the following general characteristics:

- CPU Module, which includes: Power management, CPU, Memories and, GNSS receiver (GPS)
- WAN Module
- Backup battery
- 4G modem
- LoRa module
- Ethernet or GPRS/EDGE/HSPA/CDMA/LTE
- The unlicensed band (ISM)
- Ingress protection IP66 / EN 60529

- The antenna interface: single (omnidirectional), dual (space diversity or dual-polarization), or tri (sectorization).

Table 2 consolidates the analysis for the EDGC-type device considering the Edge computing rules.

Table 2. Rules applied to an EDGC-type device

Rules	Meet the rule
Management rules	
It can upload the firmware or operating system and track the status of remote software/firmware update	Yes
It can update applications or embedded code	Yes
It can have remotely collected health information	Yes
Real-time tracking of the physical location	Yes
It can have remotely collected diagnostic and error information	Yes
Provide information about hardware, versions, model, manufacturer	Yes
Provide information about time in operation	Yes
Reliability rules	
Incorporate power optimizations and deploy techniques such as dynamic voltage scaling	Yes
Use circuit techniques that generate less noise, improving circuit noise immunity, or suppressing noise without circuit modification	Yes
It has redundancy	Yes
Industrial protection certification	Yes
Processing capacity	Yes
Cybersecurity rules	
It has a registration process	Yes
It has an initial provisioning process regarding software, components, and configurations	Yes
It has authentication mechanisms	Yes
It has encryption mechanisms	Yes
It has a decommissioning strategy, including revocation of access, certificates, and deletion of sensitive data	Yes
Control and restrict access to devices individually or in a group	Yes

The EGDC-type device meets all defined rules regarding management, cybersecurity, and reliability and is ready to be applied in the industry context.

6.2 IIoT Edge Data Processing

The EDP-type device is a small computer-implemented in a single board that can use an operating system like Linux or Windows IoT. The device is mostly used in IoT applications due to its flexibility and low cost. The software can be developed installed to manage data from other devices. The EDP-type device has the following general characteristics:

- CPU: Quad-core 64-bit ARM Cortex A53 clocked at 1.2 GHz.
- Memory: 1 GB SDRAM
- Network: 10/100 Mbps Ethernet and 802.11n Wireless LAN.

Table 3 consolidates the analysis for the EDP-type device considering the Edge computing rules.

Table 3. Rules applied to an EDP-type device

Rules	Meet the rule
Management rules	
It can upload the firmware or operating system and track the status of remote software/firmware update	Yes
It can update applications or embedded code	Yes
It can have remotely collected health information	Yes
Real-time tracking of the physical location	No
It can have remotely collected diagnostic and error information	Yes
Provide information about hardware, versions, model, manufacturer	Yes
Provide information about time in operation	Yes
Reliability rules	
Incorporate power optimizations and deploy techniques such as dynamic voltage scaling	No
Use circuit techniques that generate less noise, improving circuit noise immunity, or suppressing noise without circuit modification	No
It has redundancy	No
Industrial protection certification	No
Processing capacity	Yes
Cybersecurity rules	
It has a registration process	Yes
It has an initial provisioning process regarding software, components, and configurations	Yes
It has authentication mechanisms	Yes
It has encryption mechanisms	Yes
It has a decommissioning strategy, including revocation of access, certificates, and deletion of sensitive data	Yes
Control and restrict access to devices individually or in a group	Yes

The EDP-type device does not meet all rules regarding reliability and management in the real-time tracking location. This device can only be applied in particular situations in which adequate physical/electric protection. A hardening process is necessary to reduce its vulnerability. In order to mitigate the absence of location tracking, this edge device should be used only in stationary applications.

7 Conclusion

Edge computing devices are pervasive and increasing their presence in industrial operations. To make an edge function, a device needs to have computational and communication capabilities obtained in countless ways with many devices. This context provides the risk of uncontrolled spread of devices that are not fully prepared to operate in industrial environments and can lead to human life and cybersecurity.

These devices must follow some minimum rules to be appropriately adopted in the industry. Standardization and attention to particular prerequisites can be the difference between a sustainable implementation and chaos.

This study established criteria for identifying two types of Edge devices used in the industry in the context of IIoT, called Edge Gateway Data Capture and Edge Data Processing.

Both types of devices have specific functions and characteristics that make them more adapted to certain data capture and data processing functions. However, both need to have specific characteristics that make them more suitable for industrial adoption, given factors such as reliability, management, and cyber-security. By establishing and following these rules, the industry can better prepare for the fourth industrial revolution's consequences.

References

1. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge computing: vision and challenges. IEEE Internet Things J. **3**(5), 637–646 (2016)
2. Koustabh, D., Datta, S.K.: Comparison of edge computing implementations: fog computing, cloudlet, and mobile edge computing. In: Global Internet of Things Summit (GIoTS), pp. 1–6. IEEE, Geneva (2017)
3. Blesson, V., et al.: Challenges and opportunities in edge computing. In: 2016 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, New York (2016)
4. Mohammed, E.S., Bennis, M., Saad, W.: Proactive edge computing in latency-constrained fog networks. In: 2017 European Conference on Networks and Communications (EuCNC). IEEE, Oulu (2017)
5. Fan, O., Ansari, N.: Application-aware workload allocation for edge computing-based IoT. IEEE Internet Things J. **5**(3), 2146–2153 (2018)
6. Shirazi, S.N., et al.: The extended cloud: review and analysis of mobile edge computing and fog from a security and resilience perspective. IEEE J. Sel. Areas Commun. **35**(11), 2586–2595 (2017)
7. Moura, R.L., Ceotto, L.D.L.F., Gonzalez, A.: Industrial IoT and advanced analytics framework: an approach for the mining industry. In: 2017 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 1308–1314. IEEE Xplore, Las Vegas (2017)

8. Dorsemaine, B., et al.: Internet of Things: a definition and taxonomy. In: NGMAST 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, pp. 72–77. IEEE, Cambridge (2015)
9. Boyes, H., et al.: The industrial Internet of Things (IIoT): an analysis framework. Comput. Ind. **101**, 1–12 (2018)
10. Moura, R.L., et al.: Industrial Internet of Things (IIoT) platforms-an evaluation model. In: 2018 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 1002–1009. IEEE, Las Vegas (2018)
11. Boeckl, K., et al.: Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks. US Department of Commerce, National Institute of Standards and Technology (2019)
12. Megas, K., Fagan, M.: Subject: NISTIR 8259, core cybersecurity feature baseline for securable IoT devices: a starting point for IoT device manufacturers (2019)
13. Ross, R.S., et al.: Guide for the security certification and accreditation of federal information systems. No. Special Publication (NIST SP)-800–37 (2004)
14. Polsonetti, C.: Industrial Edge 2.0. https://www.arcweb.com/blog/industrial-iot-edge-20. Accessed 03 May 2020
15. Moura, R.L., et al.: Industrial Internet of Things: device management architecture proposal. In: 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, pp. 1174–1178 (2019)
16. Narayanan, V., Xie, Y.: Reliability concerns in embedded system designs. Computer **39**(1), 118–120 (2006)
17. Ahmad, M.: Reliability models for the Internet of Things: a paradigm shift. In: 2014 IEEE International Symposium on Software Reliability Engineering Workshops, Naples, pp. 52–59. IEEE, Washington DC (2014)
18. Varghese, B., et al.: Challenges and opportunities in edge computing. In: 2016 IEEE International Conference on Smart Cloud (SmartCloud). IEEE (2016)
19. Van der Meulen, R.: What edge computing means for infrastructure and operations leaders. https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/. Accessed 05 Nov 2020
20. Wang, T., et al.: Big data cleaning based on mobile edge computing in industrial sensor-cloud. IEEE Trans. Ind. Inform. **16**, 1321–1329 (2019)
21. Liang, B., et al.: Mobile edge computing. Key technologies for 5G wireless systems, vol. 16, no. 3, pp. 1397–1411 (2017)
22. Calo, S.B., Touna, M., Verma, D.C., Cullen, A.: Edge computing architecture for applying AI to IoT. In: IEEE International Conference on Big Data (Big Data), pp. 3012–3016. IEEE (2017)
23. Stankovski, S., et al.: Using micro/mini PLC/PAC in the edge computing architecture. In: 19th International Symposium INFOTEH-JAHORINA (INFOTEH), pp. 1–4. IEEE, Jahorina (2020)
24. Mocnej, J., et al.: Impact of edge computing paradigm on energy consumption in IoT. IFAC-PapersOnLine **51**(6), 162–167 (2018)
25. Alrowaily, M., Lu, Z.: Secure edge computing in IoT systems: review and case studies. In: IEEE/ACM Symposium on Edge Computing (SEC), pp. 440–444. Virtual (2018)
26. El-Sayed, H., et al.: Edge of things: the big picture on the integration of edge, IoT and the cloud in a distributed computing environment. IEEE Access **6**, 1706–1717 (2017)
27. Dadheech, K., Choudhary, A., Bhatia, G.: De-militarized zone: a next level to network security. In: Second International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 595–600. IEEE, Coimbatore (2018)