A Cyber-Security Strategy for Internationally-dispersed Industrial Networks

Ralf Luis de Moura
Operational Technology Architecture
Vale S.A.
Vitória, Brazil
https://orcid.org/0000-0002-0170-4056

Alexandre Gonzalez
Enterprise Architecture
Vale S.A.
Rio de Janeiro, Brazil
alexandre.gonzalez@vale.com

Virginia N. L. Franqueira
University of Kent
School of Computing
Canterbury, UK
https://orcid.org/0000-0003-1332-9115

Antonio Lemos Maia Neto
Foundation Architecture
Vale S.A.
Belo Horizonte, Brazil
antonio.lemosmaia@vale.com

Gustavo Pessin
ITV- Instituto Tecnológico Vale
Vale S.A.
Ouro Preto, Brazil
gustavo.pessin@itv.org

***Abstract*— Globalization implies geographically dispersed supply chains composed of facilities strategically located in several countries and regions of the world. These structures commonly involve several Operational Technology (OT) and Information Technology (IT) infrastructures and integration to enable accurate and useful information processing. Such integration (also called Cyber-Physical Systems) transforms the industry and facilitates massive data volumes' systematic transformation into valuable information. Security risks posed by such integration may be substantial and, depending on the size of the company, and the number of integration points, dealing with them could easily cost millions of dollars. With the main objective of studying available strategies to manage security risks in companies with dispersed supply chains, this paper reviews international cyber-security standards and regulations and proposes a more comprehensive strategy. The strategy includes IT services, optimized perimeter segregation, and data flow policies among OT and IT networks to balance a high level of protection and cost-effectiveness.**

Keywords—Cyber-Physical Systems, Cyber Security Strategy, Internationally Dispersed Supply Chains

I. INTRODUCTION

The advent of Industry 4.0 instigated a series of digital transformation programs in companies [1] that undoubtedly results in a high level of processes integration into manufacturing, products, and services. Such networks integration of physical and computational components, also called Cyber-Physical Systems (CPS) [2], is transforming the industry. It facilitates the systematic transformation of massive data volumes into valuable information, which allows identification of visible patterns of degradations and inefficiencies, which, in turn, yields to optimal decision-making [3]. CPS also promotes autonomy, reliability, and control without human participation by combining technology and knowledge [4].

A CPS architecture may consist of multiple static/mobile sensors and actuators networks integrated under an intelligent decision system [4]. CPS's essential enabler integrates several Operational Technology (OT) network segments starting at the shop floor up to high-level networks traditionally managed by Information Technology (IT) teams.

Continuous improvements in Information and Communication Technologies (ICT) are increasing connectivity in all industries. On the other hand, advances in Industrial IoT (IIoT) and OT technologies provide the foundation of interconnecting CPS to the world of the Internet.

In the past, Industrial Control Systems (ICS) from OT were implemented using non-routable networks (also called serial networks) that were born with the concept of islands of technology insolated in small subsystems responsible for the partial control of the production process. At that time, security was not a concern. OT networks (or Industrial Networks) were commonly isolated and, to perform an attack, an attacker would have to gain physical access to the network, which reduced the risk of cyber-attacks.

In recent years, the situation has changed completely. There has been a shift from systems based around the interconnection of physical components (e.g. [5], [6],[7]) migrating to the TCP (Transmission Control Protocol)/IP (Internet Protocol) / Ethernet-based networks that offer better real-time monitoring

and security services [8]. In CPS scenarios, however, TCP/IP / Ethernet networks and full integration, cybersecurity risks increase substantially [9], with the increased volume and pervasiveness of data that generate potential vulnerabilities [10].

Cyber-physical attacks have become a global issue for the nation's economy [11]. Organizations and governments have experienced cyber-security incidents that exfiltrate confidential or proprietary data, alter information to cause unexpected or unwanted effects, and harm capital assets [10] with substantial financial impacts [13]. This situation has attracted attention during the last years that emerged discussions regarding which is the best way to integrate CPS, e.g. [16], [15] and [19], including international cyber-security standards and regulations.

Dispersed supply chain structures imply production chains and facilities distributed in different locations [14], including several CPS, OT networks, and integrations points [15]. This situation increases the security vulnerabilities like in network equipment and IT services, which, in turn, requires additional cyber-security infrastructure, such as firewalls and DMZs (Demilitarized Zones), used for adding an extra layer of protection to the network [16]. Depending on the company's size and the number of integration points, the costs to deploy such infrastructures could easily reach millions of dollars.

There are international cyber-security standards and regulations that organizations may use as an excellent source of knowledge to improve their cybersecurity capabilities [24;25;26;27;28;29;30]. However, they do not specifically address the trade-off between cyber-security effectiveness and costs in the dispersed supply chain context. In organizations, the cost is an important variable that needs to be considered and naturally balanced with related risks.

This work's main objective is to propose a cyber-security strategy for companies with Internationally-dispersed supply chains based on international standards and regulations that encompasses a high level of cyber-security and cost-effectiveness.

II. CHALLENGES OF INTERNATIONALLY-DISPERSED SUPPLY CHAINS

Globalization and international trade imply geographically dispersed supply chains composed of production and facilities strategically located in several countries and regions of the world [14].

Company facilities may support different business capabilities with diverse CPS and IT services. Business capability (BC) is the notion used to describe an enterprise's essential functions [17]. These dispersed and diverse structures commonly involve several OT/IT infrastructures and integration to enable accurate and effective information processing [15].

Typically, each BC has its facilities, CPS, and work process as an independent subsystem inside the enterprise, even if geographically close to other BCs. In this scenario, horizontal integration (among BCs) of networks is not common. However, to maximize opportunities to identify correlated information useful for business needs, vertical integration is essential for data processing and analysis in an integrated way[1] [18], as shown in Figure 1.

[1] Nevertheless, this does not exclude the possibility of data being processed locally; sometimes local processing is necessary due to real-time requirements or latency restrictions.

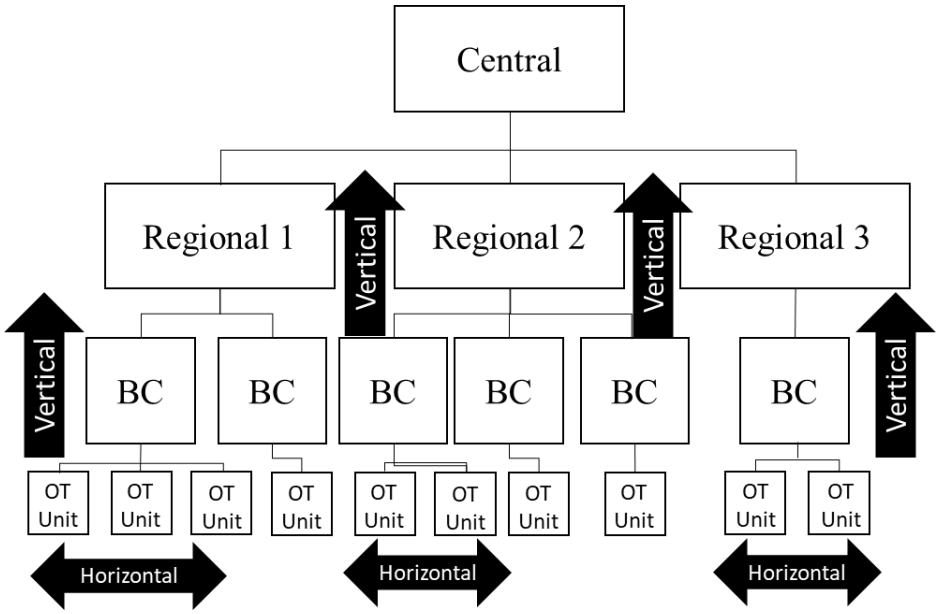

Fig. 1. A dispersed supply chain with different business capabilities

The main challenges posed by the industrial network (vertical) integration of diverse supply chains with multiple BCs distributed across different locations are *(i)* how to reach the desired level of integration without compromising different aspects of cyber-security and *(ii)* how to balance the levels of security, integration in a non-prohibit costs scenario.

III. OT NETWORKS AND VULNERABILITIES

An OT network is an interconnection system of devices used to monitor and control physical equipment in a cyber-physical system [19]. OT networks are most typically composed of several distinct areas, which can be simplified (based on ISA 95[2] [20]) in four network layers [21]: (1) Process and control networks, (2) Supervisory networks, (3) Business operations networks and (4) Business networks (enterprise), as illustrated in Figure 2.

[2] ISA-95 defines a functional hierarchical enterprise and production control system levels [34].

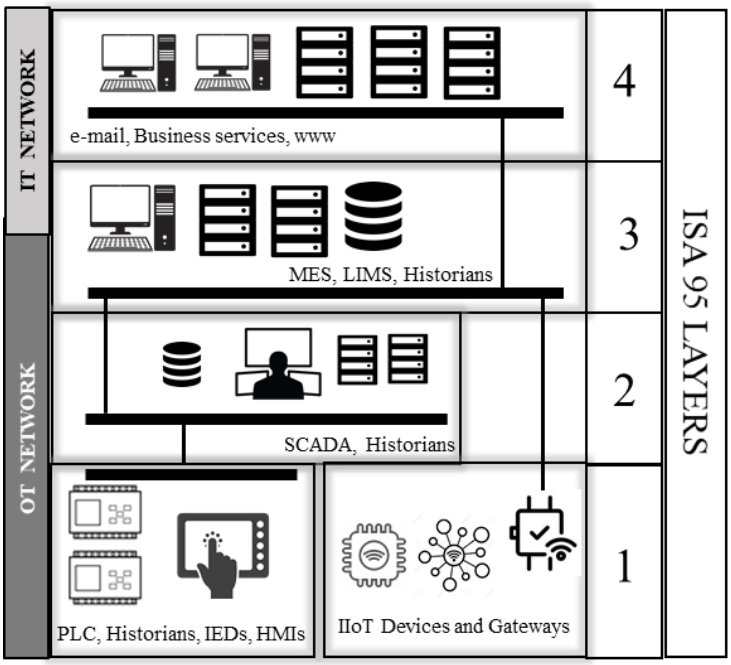

Fig. 2. Network Layers adapted from ISA 95 [34]

The essential difference between OT (layers 1 to 3) and enterprise networks (layer 4) is that OT networks are connected to physical equipment and are used to control and monitor real-world actions (generally in real-time) and conditions usually in a SCADA - Supervisory Control and Data Acquisition environment. Enterprise Networks, in turn, is connected to the Internet to support corporative IT systems. As a result, OT networks have different considerations like service quality, determinism, and real-time data transfers that generally need robust architectures [19].

Industrial networks are mainly used in the direct operation of cyber-physical systems considered "critical infrastructures." According to the HSPD-7 (Homeland Security Presidential Directive Seven) [20], the prioritized vital resources that must be protected from terrorist attacks include electric energy, nuclear energy, chemical, agricultural and pharmaceutical manufacturing, among others [21;20]. Regardless of the application, physical equipment controlled in an industrial network usually implies risks for assets and people's lives involved in the production processes. Therefore, this study considers "critical infrastructures" those that can affect the production process causing financial losses, company reputation, or endanger human lives, independent of the company segment.

When industrial protocols were first conceived, the goal was to provide good performance, emphasizing providing features that would ensure that task constraints over the network would be met; network security was hardly a concern. Over the years, the automation industry has moved away from proprietary standards for communication protocols towards open international standards (TCP/IP). However, in reality, both coexist [22]. That is why a robust integration strategy to avoid compromising the cyber-security aspects becomes a must.

In the past, OT networks were not connected to the enterprise or public networks like the Internet. Today, however, the need to make fast and cost-effective decisions makes up for the necessity of accurate and up-to-date information about the plant and the process that demands an increasing integration level between different OT systems and between OT and business contexts [22]. Such integration transforms the industry and facilitates massive data transformation into accurate, fast, and cost-effective information [3]. However, the benefits come with a cost; integrating such different contexts increases vulnerabilities, threats, and risks. Vulnerabilities may be caused by logical design flaws, implementation errors, or fundamental weakness. In turn, a threat arises when a vulnerability can be exploited, inflicting damage to the system [22].

The three well-known basic security requirements are availability – the ability to keep the resource accessible and available upon demand; integrity – the ability to safeguard the accuracy and completeness

of the resource and confidentiality – guarantee that information is not made available to unauthorized individuals. From the CPS point of view, since an unexpected stop in operation may lead to catastrophic events, the availability is the most critical security requirement in OT networks.

An attacker that successfully exploits vulnerabilities in a CPS might gain access to and, ultimately, control operations jeopardizing assets and human lives. The entry points and attack vectors in an industrial system are different from enterprise-networks. Sometimes even well-established techniques to search for vulnerabilities, such as scanning, have to be avoided in OT networks because of the impact that such techniques may bring the operation.

Typical data flow and information exchange within OT and IT networks integration create connections that can be vulnerable to cyber-attacks. The vulnerabilities include, for example, hacking into a network's asset or server and compromising information; or physical intrusion into a company to gain access to the information or control in the manufacturing processes [10]. Table 1 shows typical attacks and threats on cyber-physical systems [4].

Table 1
Attacks and threats to cyber-physical systems

Point of attack	Damage	Typical attacks
Communication	Remote spying, data; theft of information; eavesdropping; interception of compromising interference signals; software malfunction.	Packet replaying; package spoofing; selective forwarding; Sybil attack.
Actuation	Loss of power supply; tampering with hardware; remote spying; interception of compromising interference signals.	Finite energy attacks; bounded attacks.
Computing	Illegal processing of data; error in use, equipment failure; corruption of data; software malfunction.	Worm; trojan, virus
Sensing	Tampering with hardware; loss of power supply; environment threats; equipment failures; equipment malfunction; disturbance due to radiation.	GPS spoofing; injection of false radar signals; dazzling cameras with light.
Feedback	Control disruption; feedback integrity attack.	Feedback integrity attacks.

The consequences vary widely between different levels of the network and across different points in a supply chain. A cyber-attack can cause, for instance, the loss of integrity by hacking into and altering measurement systems, unavailability in the form of power disruption, unauthorized access to critical information for theft of critical proprietary data or knowhow, unauthorized remote control in industrial equipment, or disruptions to production [10].

IV. INTERNATIONAL CYBER-SECURITY REGULATIONS AND STANDARDS

Several cybersecurity standards and regulations are imposed by governments and organizations, which provide best practices recommendations, sometimes enforcing penalties and fines [21]. This study covers the major standards and regulations that apply to OT networks [23], [21]. The following topics encompass parts of these documentations related to network and services security (the focus of this research).

- NCSC CAF (National Cyber Security Center - Cyber Security Framework): guidance for organizations responsible for vitally services and activities. CAF is a framework with three objectives and 14 sub-objectives and principles that helps to avoid cyber incidents. It encompasses managing network risks in the supply chain, asset and risk management, resilient networks and systems, security monitoring, and detecting security event discovery [24].
- NIST SP 800-82 (National Institute of Standards and Technology – Special Publication): Encompasses common system topologies, re-targets management, operational, and technical security controls [25].
- NISCC Firewall Deployment Guide (National Infrastructure Security co-ordination center): Guidelines for firewall configuration and deployment in industrial environments [26].

- AGA-12 (America Gas Association): Address retrofitting serial communication and encapsulation/encryption of serial communication channels [27].
- API-1164 Security Standard (American Petroleum Institute): Guidelines physical security, data flow, and network design [28].
- ISO/IEC 27002:2005 (International Standards Organizations): provide less guidance for industrial networks, but it is useful because it maps other security standards. Include asset and configuration management controls and segregation and security controls for network communications [29].
- NERC CIP (North American Electric Reliability Corporations – Critical Infrastructure Protection): Consists of nine separate configuration management controls: security management controls, cyber asset identification, electronic security perimeters, and physical security [30].
- CFATS (Chemical Facilities Anti-Terrorism Standards): Outline controls for security policies, access control, personnel security, awareness, and training [31].
- NRC Regulation 5.71 (Nuclear Regulatory Commission): provides general security requirements of cybersecurity, including a five-zone separation model with one-way communication between zones [32].
- ISA 99 / IEC 62443 (International Society of Automation / International Electrotechnical Commission): Composed two technical reports on control system security. It focuses on security technologies for manufacturing and control systems and addresses the integration security in industrial environments, including requirements, policies, procedures, and best practices [33].

Several international security regulations apply to industrial networks; some are global, some are regional, and some are applicable in all industrial networks, while others only fit specific industrial segment. These cyber-security measures are different but often overlaps security recommendations [21].

V. CYBER-SECURITY STRATEGY

The cyber-security strategy proposed in this work and described in detail in the following sections was mapped according to the most relevant security and compliance requirements extracted from international cybersecurity regulations and standards listed in section IV. These requirements were compiled in three groups [21]: Perimeter and Security Controls; Host Security Controls and Security Monitoring Controls, as shown in Table 2

Table 2
Relevant security requirements

Group	Security Requirement	Description	Regulation / Standard
1. Perimeter and Security Controls	1.1 Electronic Security Perimeter	Construct perimeter at edges using multiple layered defenses.	NIST; ISO/IEC 27002:2005; NRC RG 5.71; CFATS; NERC; API-1164; NCSC CAF; ISA 99 / IEC 62443
	1.2 Network and Perimeter Monitoring	Implement access policies at the perimeter.	CFATS; NERC; NCSC CAF
	1.3 Network Access and Authentication	Implement network access control, central authentication system, directory system, or identity access management (IAM).	ISO/IEC 27002:2005; NRC RG 5.71; CFATS; NERC;
	1.4 Network Perimeter Ports and Services	Include mechanisms to prevent protocols from initiating commands across the perimeter.	NRC RG 5.71; AGA-12

Group	Security Requirement	Description	Regulation / Standard
2. Host Security Controls	2.1 Asset Configuration	Implement configuration management and change control.	NIST; ISO/IEC 27002:2005; NRC RG 5.71; CFATS; NERC
	2.2 Ports and Services	Unnecessary ports and services should be disabled.	NRC RG 5.71; NERC; NISCC
	2.3 Anti-Malware	Use of anti-virus systems to detect and repair.	NIST; ISO/IEC 27002:2005; NRC RG 5.71; CFATS; NERC
	2.4 Authentication	Implement a centralized authentication system.	NIST; ISO/IEC 27002:2005; NRC RG 5.71; CFATS; NERC
3. Security Monitoring Controls	3.1 Asset Configuration	To identify, control, and document all entity or vendor-related changes to hardware and software.	ISO/IEC 27002:2005; NRC RG 5.71; CFATS; NERC; NCSC CAF
	3.2 Documentation	Documentation of assets (assets may be detectable or discoverable using SNMP)	ISO/IEC 27002:2005; NRC RG 5.71; CFATS; NERC
	3.3 Monitoring	Generate alerts from unallowed traffic at the perimeter.	ISO/IEC 27002:2005; NRC RG 5.71; CFATS; NERC; NCSC CAF
	3.4 Authentication	Implement user account and authentication activity log.	NERC.

Compiled from [21;27;28;29;30;31;32;33]

A. Perimeter and Security Controls

Electronic Security Perimeter (1.1)

Construct perimeters and multilayered defenses in a dispersed supply chain requires a specific segregation model. The network segregation may be done using firewalls and DMZs.

To meet the electronic security perimeter requirements and reduce costs with multiples infrastructures services simultaneously, the diverse regions where a company has operations and facilities should implement a regional DMZ that may offer services to local networks that support its business capabilities. One Central DMZ should be implemented to host services that may be offered in a centralized way, as given in Figure 3.

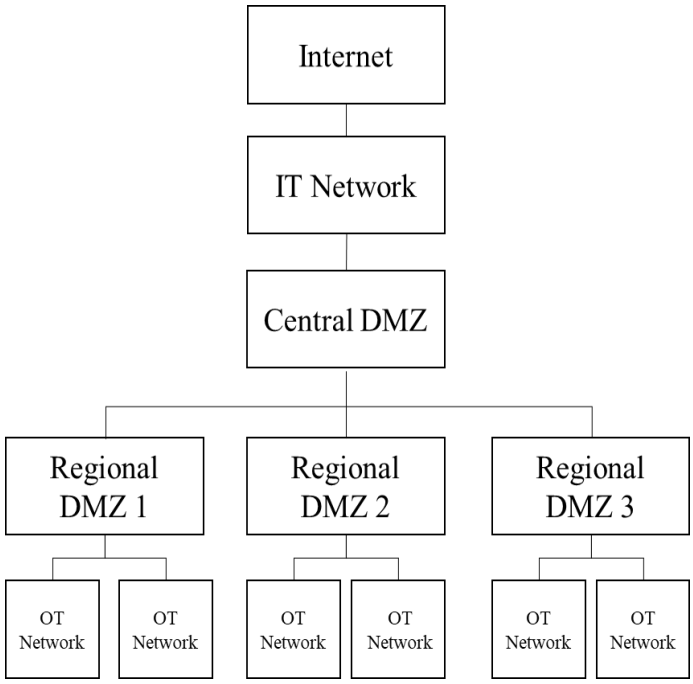

Fig. 3. Network segmentation framework

The segregation strategy is first by geographically, second by business capability, creating a hierarchical structure centered on a single Central DMZ. This segregation model's main objective is to reduce the number of services infrastructures by offering them as centralized as possible. The option to be centralized or not depends on the service's data flow rules and latency requirements.

The strategy behind centralization is to reduce the need to create local infrastructures. Services can be offered centrally, lower the need for local infrastructures, and lower the cost of implementing and maintaining these services. In dispersed supply chain companies, this strategy may be very advantageous.

The communication may be done between OT's networks and the Regional DMZs and between Regional DMZs and Central DMZ. Direct communication between two OTs or two Regional DMZs (general horizontal communication) is not allowed (this need is unusual), but it may be implemented using Regional DMZ or Central DMZ as an intermediary.

Figure 4 details the network segregation and data flow strategy. Bidirectional (inbound and outbound) data flow is allowed only in the adjacent enclave. Only outbound data flow is allowed in the enclave, not adjacent (outbound from more secure enclave) limited to one jump. For example, Layer 1, in industrial networks, may only communicate with Layer 3 with outbound traffic, Layer 2 may communicate with Regional DMZ only with outbound traffic, and communication between Layer 1 and Regional DMZ is not allowed.

IIoT enclaves may be created to support smart devices and sensors that do not belong to the OT infrastructures (e.g., environmental sensors).

In some situations, Regional DMZs can be used as Regional IIoT DMZs when smart devices are located near them. However, the data must flow to the IT network through the Central DMZ and not Central IIoT DMZ in this context.

The Internet DMZ is the only way out to the Internet through the IT Network; in some cases, it is possible to connect the Central IIoT DMZ direct to the Internet DMZ, for example, when using smart sensors in public network infrastructures (4G, 5G, etc.). However, the use of private APNs (Access Point Name) should be privileged. This strategy allows the data flow from any CPS (IIoT or OT) to the IT network, and all data may be centralized in a data hub or data lake, compromising cybersecurity aspects as little as possible.

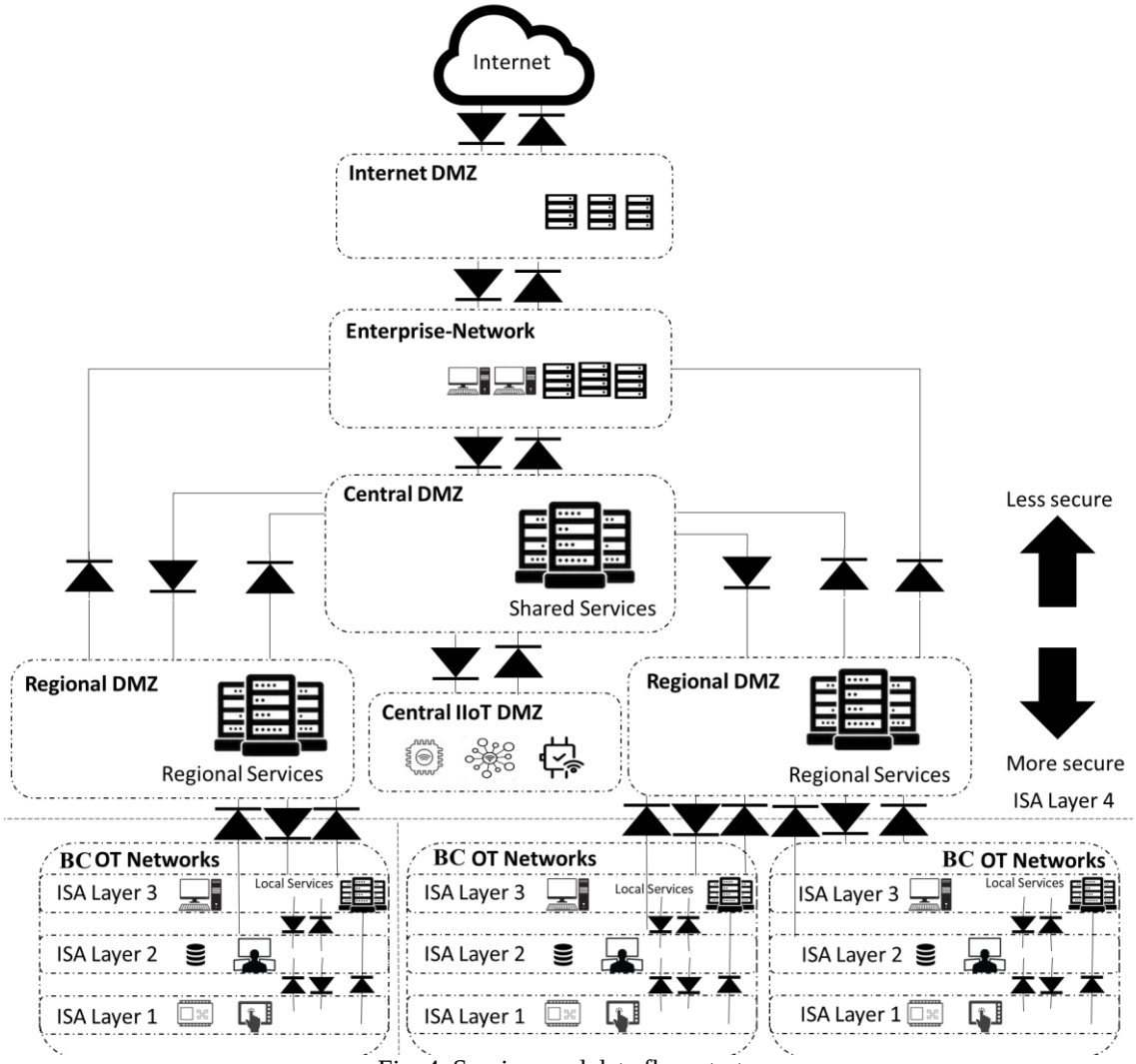

Fig. 4. Services and data flow strategy

Network and Perimeter Monitoring (1.2)

In order to meet requirement 1.3, all inbound network traffic should be monitored by an IPS (Intrusion Prevent System) or IDS (Intrusion Detection System) depending on the feasibility. OT networks are sensitive to traditional scanning technics and an IPS, for example, uses intrusive scans that may cause unavailability to the production processes. In general, IPS should be used to monitor traffic near to the IT network (layer 4) and IDS in low-level industrial networks (layers 1,2, and 3).

Network Access and Authentication (1.3)

The Central DMZ should host a centralized IAM (Identity Access Management) or directory services that may have regional DMZs if necessary. Single sign-on in OT services from IT Zones or in IT services from OT zones is not allowed, and it is necessary for the implementation of distinct multi-factor authentication (MFA).

Network Perimeter Ports and Services (1.4)

Unnecessary perimeters (among DMZs) port and services should be disabled. Only necessary traffic between networks must be allowed.

B. Host Security Controls

Asset Configuration (2.1)

A configuration management system should control asset configuration and changes. The requirement (2.1) may be made possible through a configuration management software known as CMDB (Configuration Management Database). CMDB is a database that contains all relevant information about the hardware and software components used in a specific perimeter. This service may be hosted at Central DMZ and support all OT network layers. CMDB may compare security configurations against authorized configuration files and monitor changes. To manage changes in low-level assets (Layers 1 and 2), it is suggested to implement backup and versioning (V&B) tools that integrate with equipment such as PLCs (Programmable Logic Controllers) and HMIs (Human-Machine Interfaces), for example, and the use of agnostic software tools is recommended.

Any code changes must be previously authorized by an approval flow, implemented through a change management tool. This condition can be audited via the V&B tool.

OT patch management should be performed separated from IT patch distribution systems due to the critical differences between IT and OT environments. OT systems have different life-cycles, and generally, they do not homologate patches in the same velocity that IT systems. It is important to obtain risk-free patches so that adequate testing and verification of them should be performed before implementation.

Ports and Services (2.2)

Unnecessary host ports and services should be disabled, maintaining only the ports and services necessary for its function.

Anti-Malware (2.3)

An anti-virus system should be implemented for malicious code prevention. The placement strategy of anti-virus services depends on the data flow needs. They can be hosted in a centralized way only if it does not disregard the inbound/outbound traffic rules. It is necessary to ensure that the anti-virus software is up to date and uses the most current malware detection signatures. An important point of attention is that equipment and devices that support the industrial system sometimes are sensitive to anti-virus software, which may require testing and verification performed before implementation.

Authentication (2.4)

The centralized direct services or IAM (already discussed in sections 1.3) cover requirement 2.4-Implement a centralized authentication system.

C. Security Monitoring Controls

Asset Configuration and documentation (3.1 and 3.2)

The CMDB tool may meet the requirement 3.1 and 3.2 (as discussed at requirement 2.1). All changes in OT assets are monitored and controlled in real-time through SNMP (Simple Network Management Protocol) or agents installed at the equipment.

Monitoring (3.3)

Monitoring tools should be implemented to generate alerts that typically involve traffic at the perimeter (denied or not). Most of the perimeter devices (Firewall, IPS, IDS) can be part of the monitoring process, but specific monitoring software may be used.

The user account and authentication activity log should be implemented in IAM or directory service infrastructure (req. 2.4).

Table 3 consolidates all services that should be implemented to meet all requirements described in Table 2.

Table 3
Security services/strategy

Group	Security Requirement	Service / Strategy
1. Perimeter and Security Controls	1.1 Electronic Security Perimeter	DMZ strategy
	1.2 Network and Perimeter Monitoring	IDS, IPS
	1.3 Network Access and Authentication	IAM, Directory services, MFA
	1.4 Network Perimeter Ports and Services	DMZ strategy
2. Host Security Controls	2.1 Asset Configuration	CMDB, Patch management
	2.2 Ports and Services	DMZ
	2.3 Anti-Malware	Anti-virus
	2.4 Authentication	IAM, Directory services, MFA
3. Security Monitoring Controls	3.1 Asset Configuration	CMDB, V&B, and change management tools
	3.2 Documentation	CMDB
	3.3 Monitoring	V&B, Monitoring software, firewall, IDS, IPS
	3.4 Authentication	IAM, Directory services

VI. CONCLUSION

This paper aimed to define an appropriate strategy to manage security risks in companies with dispersed supply chains. Dispersed supply chains imply facilities and chains of production strategically located in several regions scattered across the world. These dispersed facilities may deliver many business capabilities that generate local OT and IT infrastructures.

Creating local infrastructures for all listed services may be unfeasible depending on the business' size, diversity, and dispersion. The greater the number of local infrastructures, the greater the need for integration, and the higher the cost of implementation. Additionally, it may increase the security vulnerabilities that need to be addressed.

The cost-effective network services segregation strategy proposed in this paper tries to centralize as many services as possible to ensure that all international standards and regulations requirements are covered and simultaneously reduce the implementations and maintenance costs, compromising cyber-security aspects as little as possible. Therefore, creating an integrated network, which, in turn, provides a holistic system for monitoring and controlling the physical world through the collection, processing, and analysis of data generated by the company's OT and IT as a whole.

REFERENCES

[1] Moura, R., Ceotto, L., Gonzalez, A. Industrial IoT and Advanced Analytics Framework: an approach for the Mining Industry (2017). 2017 International Conference on Computational Science and Computational Intelligence (CSCI). Las Vegas, 2017, pp.1308-1314, doi: 10.1109/CSCI.2017.228.

[2] Griffor, E. R., Greer, C., Wollman, D. A., & Burns, M. J. (2017). Framework for cyber-physical systems: Volume 1, overview (No. Special Publication (NIST SP)-1500-201).

[3] Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. Computers in Industry, (100), 212-223, doi: 10.1016/j.compind.2018.04.017.

[4] Lee, J., Ardakani, H. D., Yang, S., & Bagheri, B. (2015). Industrial big data analytics and cyber-physical systems for future maintenance & service innovation. Procedia Cirp, (38), 3-7, doi: 10.1016/j.procir.2015.08.026.

[5] Bellagente, P., Ferrari, P., Flammini, A., Rinaldi, S., & Sisinni, E. (2016). Enabling PROFINET devices to work in IoT: Characterization and requirements. In 2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings, 1-6.

[6] Andrews, S. Kevin; Rajavarman, V. N.; Ramamoorthy, S. (2018). Implementing an Iot Vehicular Diagnostics System Under a Rtos Environment Over Ethernet IP. Medico-Legal Update, 18(1), 548-554.

[7] Lavrov, K. G. et al. (2018). Development of FOUNDATION TM Fieldbus technology for coke oven plants. Coke and Chemistry, 61(7), 270-273, doi: 10.3103/S1068364X18070049.

[8] Mejías, A., Herrera, R., Márquez, M., Calderón, A., González, I., & Andújar, J. (2017). Easy handling of sensors and actuators over TCP/IP networks by open source hardware/software. Sensors, 17(1), 94, doi: :10.3390/s17010094.

[9] Ponomarev, S., & Atkison, T. (2015). Industrial control system network intrusion detection by telemetry analysis. IEEE Transactions on Dependable and Secure Computing, 13(2), 252-260, doi: 10.1109/TDSC.2015.2443793 .

[10] Hutchins, M. J., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W., & Dornfeld, D. (2015). Framework for identifying cybersecurity risks in manufacturing. Procedia Manufacturing, (1), 47-63, doi: 10.1016/j.promfg.2015.09.060.

[11] Shukla, M., Johnson, S. D. & P. Jones, Does the NIS implementation strategy effectively address cyber security risks in the UK?, (2019). 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, United Kingdom, 2019, pp. 1-11. doi: 10.1109/CyberSecPODS.2019.8884963.

[12] Ahmad, F., Adnane, A., Franqueira, V., Kurugollu, F., & Liu, L. (2018). Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies. Sensors, 18(11), 4040, doi: :10.3390/s18114040 .

[13] Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31, doi: 10.19101/IJACR.2016.623006.

[14] Lorentz, H., Töyli, J., Solakivi, T., Hälinen, H. M., & Ojala, L. (2012). Effects of geographic dispersion on intra-firm supply chain performance. Supply Chain Management: An International Journal, 17(6), 611-626, doi: 10.1108/13598541211269229.

[15] Turkulainen, V., Roh, J., Whipple, J. M., & Swink, M. (2017). Managing internal supply chain integration: integration mechanisms and requirements. Journal of Business Logistics, 38(4), 290-309, doi: 10.1111/jbl.12165.

[16] Dadheech, K., Choudhary, A. & Bhatia, G., "De-Militarized Zone: A Next Level to Network Security," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, 2018, pp.595-600. doi: 10.1109/ICICCT.2018.8473328.

[17] Zdravkovic, J., Stirna, J., Henkel, M., & Grabis, J. (2013, June). Modeling business capabilities and context-dependent delivery by cloud services. In International Conference on Advanced Information Systems Engineering (pp. 369-383). Springer, Berlin, Heidelberg.

[18] Miloslavskaya, N., & Tolstoy, A. (2016). Big data, fast data and data lake concepts. Procedia Computer Science, 88, 300-305, doi: : 10.1016/j.procs.2016.07.439.

[19] Galloway, B., & Hancke, G. P. (2012). Introduction to industrial control networks. IEEE Communications Surveys & Tutorials, 15(2), 860-880.

[20] House, W. (2006). Homeland Security Presidential Directive 7 (HSPD-7): "Critical Infrastructure Identification, Prioritization, and Protection,".

[21] Knapp, E. D., & Langill, J. T. (2014). Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Syngress.

[22] Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. Computers & Security, 25(7), 498-506, doi:10.1016/j.cose.2006.03.001.

[23] Dzung, D., Naedele, M., Von Hoff, T. P., & Crevatin, M. (2005). Security for industrial communication systems. Proceedings of the IEEE, 93(6), 1152-1177.

[24] Chandia, R., Gonzalez, J., Kilpatrick, T., Papa, M., & Shenoi, S. (2007, March). Security strategies for SCADA networks. In International Conference on Critical Infrastructure Protection (pp. 117-131). Springer, Boston, MA.

[25] NCSC. National Cyber Security Centre – Cyber Assessment Framework (CAF) (2019). Available in: https://www.ncsc.gov.uk/collection/caf. Access in: 12/08/2019.

[26] Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. NIST special publication, 800(82), 16-16.

[27] Byres, E., Karsch, J., & Carter, J. (2005). NISCC good practice guide on firewall deployment for SCADA and process control networks. National Infrastructure Security Co-Ordination Centre, 2.

[28] Hadley, M. D., Huston, K. A., & Edgar, T. W. (2007). AGA-12, Part 2 performance test results. Pacific Northwest National Laboratories.

[29] API Standard 1164, "Pipeline SCADA Security," September 2004.

[30] ISO/IEC 27002:2005, "Information technology - Code of practice for information security management," June 2005 (Redesignation of ISO/IEC 17799:2005).

[31] NERC Standard CIP-002 through -009, "Cyber Security," June 2006 [http://www.nerc.com/files/Reliability_Standards_Complete_Set_21Jul08.pdf].

[32] De la Rosa, D. M. (2011). Chemical Facilities Anti Terrorism Standards Overview (No. SAND2011-2764C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

[33] US Nuclear Regulatory Commission. (2010). Cyber security programs for nuclear facilities. US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.

[34] IEC 62443, Industrial communication networks - Network and system security, IE C Std., many parts, closely related to ISA 99 Stds.
[35] ISA-95 Enterprise Control Systems. www.isa-95.com. Accessed 13 Jan 2020.