Mehran University Research Journal of Engineering and Technology

https://doi.org/10.22581/muet1982.3202

2024, 43(2) 220-238

Securing industry 5.0 using 6σ CYBERNETIC framework

Lubna Luxmi Dhirani *, Thomas Newe

Department of Electronic and Computer Engineering, University of Limerick, Limerick, Ireland

* Corresponding author: Lubna Luxmi Dhirani, Email: Lubna.luxmi@ul.ie

Received: 13 March 2024, Accepted: 28 March 2024, Published: 01 April 2024

KEYWORDS

Cybersecurity

Industry 5.0

Six Sigma

Standards

Cloud

IT/OT

ABSTRACT

The data-driven digital economy highly relies on immersive and emerging technologies, mass customisation, autonomous systems, and seamless connectivity. Enabling such an Industrial IoT/Industry 5.0 environment requires streamlined and end-to-end transparent methods for insights, visibility, and control. However, it is important to note that its success depends on data security metrics. The recent cyber-attacks in healthcare and industrial infrastructures have led service providers to high-risk scenarios. From supply chain to service delivery, remote functionality variables, enabling a fully connected factory is a major cybersecurity concern as emerging technologies employ different security requirements. To mitigate these risks, strategic, operational, technical, and cybersecurity alignment is a must, where the gaps between the production and process environments must be bridged to achieve the prime goal of a sustainable, secure, and technologically innovative factory. This research provides a systematic approach to bridging Industry 5.0's QoS metrics and security gaps by implementing a Six Sigma (6σ) approach in a manufacturing environment. The approach further maps IT/OT, cloud, and cybersecurity standards, thereby enabling insights, visibility, and control. A healthcare 5.0 use-case is demonstrated to show how a 6σ implementation can improve the QoS metrics, unifying standards to achieve a secure, sustainable, resilient, and high-performance environment.

1. Introduction

Industry 5.0 is expected to fully transform the manufacturing environment as it will enable technological convergence, mass customization, and product and process efficiencies employing emerging technologies (i.e., Cloud, IoTs, AI, Digital Twin, etc.). This technological advancement is anticipated to drive the traditional manufacturing boundaries forming a human-machine-centric manufacturing environment, empowered with remote functionality, powerful machinery, and scalability. In short, the world will be seeing a whole new era of digital transformation and innovation [1, 2, 3]. The Sustainable Development Goals (SDGs) [4] of this technological advancement in the production ecosystem are to achieve sustainability and circular economy goals (that is enabling cascading of products, by-products, and reverse cycles for waste reduction (SDGs 9, 11, 12, and 13). The European Net Zero Industry Act [4] has raised global awareness of the impact of global warming and addressed the strong need to reduce e-waste, energy consumption, excess produce, and resource waste in the manufacturing environment to achieve the net zero target by 2050. At present, the production environment is dealing with issues related to extracting, process, controlling, governing, and mining the enormous amount of data to get desired outcomes. *"The goal for this is to develop advanced*

diagnostics having near-zero error or failure rate for sustainable, mass customized, high-quality manufacturing with human-centered management. This intelligent human-machine collaboration will lead to effective production with minimal training and investments" [5]. Though a concept for mass customization has been set down theoretically but achieving something that involves extremely intricate processes, the information and communication technology (ICT) experts, smart factory entrepreneurs and industrial engineers raise concerns related to the rapid changes in technological architectures used in the production environment can lead to disruption and potential loopholes and mandate an in-depth investigation for prospective adopters [6, 7, 8, 9].

One of the major concerns related to the industry 5.0 environment is cybersecurity. With billions of IoT-based devices transmitting data remotely over the network, it is essential to understand the Information Technology and Operational Technology (IT/OT) convergence issues and cybersecurity blueprint of the production (endpoints, connectivity, cloud, physical infrastructure, and universal machines) ecosystem [3]. To build trust and transparency it is important to address and answer complex security issues such as: (i) providing confidential computing mechanisms, (ii) having strong authentication and verification methods in place for remote devices, (iii) having measures, controls, and technical incident response in place for building both operational and cyber resilience, (iv) cyber preparedness (pen-testing, impact assessment, skills and ability to identify the source of breach and knowing the mean time to recover from different types of potential cyber-attacks), (v) understanding the flow of data and ensuring conformance and convergence between emerging technologies (IT, OT, IoT, cloud, etc.), (vi) cyber laws, policy, standards and regulations in place for protecting the critical infrastructure and people affected from the breaches, (vii) providing assurances/guarantees that the different communications methods and technologies are in harmony (compliant) with each other, etc. These are just a few of the many arising questions and emerging cyber security issues that Industry 5.0 is susceptible to. This paper discusses the implications of evolving cyber threats in Industry 5.0 stemming from a lack of alignment, technological convergence, and standardisation. New regulations (i.e., Cyber Resilience Act, Network and Information Security Directive (NIS 2-D) [9], data security and privacy standards [3, 10, 11, 12, 13] have been enacted for protecting critical infrastructures and different standardisation bodies are working together fostering standards interoperability and bridge the gaps. However, despite of such efforts majority of the projects are still in progress. As the digital ecosystem facilitates seamless and high connectivity, any type of downtime (IT, OT, cloud, 5G/network, etc.) would lead the infrastructure susceptible to operational unavailability. Such QoS metrics would not only impact the production and return on investments but also result in increased costs and poor services. From this vantage point, the actual cost of an IT/OT/cloud downtime is much higher than it is anticipated to be. Referring back to the Cyber Resilience Act and NIS2-D, compliance and conformance with security, and data privacy standards, (i.e. ISO 27001, Cybersecurity Frameworks (NIST CSF 2.0, NIST Risk Management Framework (RMF)), IEC 62443, General Data Protection Regulation (GDPR), Digital Operational Resilience Act (DORA), etc.) [3, 10, 11, 12, 13], ICT regulations and controls have become mandatory for Industry 5.0. These regulations may also require evidence of cross-functioning security standards across the entire production facility. At present, this is one of the biggest challenges to achieve, which is why the authors of this work have considered a Six Sigma (6σ) methodology [14] for achieving alignment, zero waste, gap mitigation, high QoS, sustainable, interoperable and cybersecure Industry 5.0 environment. The paper is structured as follows: Section 2 discusses the scope of Industry 5.0 in healthcare, section 3 elaborates the complexity of cybersecurity service level agreements, section 4 illustrates the usability of 6σ in Industry 5.0 and removing zero waste, section 5 provides a roadmap from transforming from traditional healthcare to healthcare 5.0, the section also introduces the author's designed 6σ CYBERNETIC Framework that aligns and bridges the security, IT/OT and cloud standards gaps in digitally transformed environment. A use-case implementation is provided for a better understanding of the framework and to demonstrate the impact of Six Sigma (6σ) in Industry 5.0. In the end, section 6 concludes the paper.

2. Industry 5.0 For Healthcare

The pandemic has acted as a catalyst for increased use and dependency on technological platforms. It is essential to be proactive and prepared for situations that the future might hold. To facilitate innovative and services, faster and more effective treatments in healthcare, implementations of enabling and emerging technologies will be required. These benefits may also expose healthcare to cybersecurity (i.e., ransomware attacks, data privacy, denial of service, etc.) issues as discussed in Table 1.

Table 1

Security challenges in Industry 5.0 for healthcare

Title	Year	Overview	Challenges
[13]	2024	Provides a high-level overview of the IT/OT security posture of an Industrial IoT (IIoT) environment. It also introduces the CYBER INTEL framework that enables identifying, assessing, and mitigating cyber threat vectors that the ICS/OT networks are susceptible to. The framework further assists in building compliance and aligns with the regulatory and statutory components essential for building cyber resilience.	Emerging cyber threats, IT/OT risk mitigation, auditing, compliance, cyber resilience, cyber laws.
[15]	2023	Demonstrates various cyber-attacks in Healthcare-IoT (H-IoT) impacting the security and privacy domains. The research also provides potential risk mitigation strategies in H-IoT using AI/ML techniques.	Healthcare-IoT, security and privacy issues in IoT devices, novel attacks.
[16]	2023	Presents the privacy and security issues related to technological use in healthcare.	IoT vulnerabilities, security and privacy issues in healthcare-IoT.
[17]	2022	Addresses cybersecurity concerns related to secure communication, connectivity, and storing healthcare data. It also mentions the lack of standardization and acceptable benchmarking policies in Industry 5.0 that arise with implementing emerging technologies.	Cybersecurity standards, governance, risk and control
[18]	2022	Mentions the scope of Internet of Healthcare Things (IoHT) devices for observing, processing, storing, and communicating personal information. Data privacy and protection issues (i.e., data leakage, conflicts in laws, using sub-standard devices, lack of understanding, and unavailability of dedicated local regulatory bodies are addressed. The article draws awareness towards the escalating need for appropriate regulatory frameworks. It also analyses regulatory issues in IoHT devices concerning healthcare data privacy and compliance.	Cyber Law (data governance, regulatory and compliance frameworks), privacy issues in protecting healthcare data.
[19]	2022	Addresses *"the impact of cyber threats in healthcare and employs an Advanced Encryption Standard (AES) as a protective measure for mitigating health-based organizations"* [18].	Cyberattack surface, system vulnerabilities, protecting healthcare data.
[20]	2021	Highlights the increase in cyber security vulnerabilities that arise by connecting the cyber-physical production systems (CPPS) and factory floor. A risk-based assessment is developed on the system vulnerability of a CPPS. *"A use case requirement and performed a simulated approach by launching a cyber-attack and measuring the causal effect to identify implications on human worker safety"* [19].	Increased attack surface, compromised nodes, secure communications, occupational safety.
[3]	2021	This work enables an understanding of IT/OT cybersecurity standards, and convergence, and provides a roadmap for mapping and implementing the right types and levels of security standards and strategies for securing machine-to-machine communications in IIoT.	Data security, IT/OT Cybersecurity standards and risk assessment, IoT-M2M communication.
[21]	2021	Discusses the cybersecurity challenges (i.e., systematic security validation, supply-chain risks, E2E security, incident response, etc.) in autonomous vehicles.	Cybersecurity, standards, AI, autonomous vehicles, data security.
[22]	2021	Mentions the scope and usability of Internet of Medical Things (IoMT) in smart health monitoring systems around the world enabled by Industry 5.0 technology and 5G/6G networks supporting cost-efficient sensors and devices to collect a wide range of health data and transfer it through wireless networks in real-time. This leads to the remote real-time monitoring of health data through various IoMT devices remotely. The data produced from many patients on a daily basis must be secured and ensure privacy/trust. The research proposes a three-level/tier healthcare network integrated with blockchain and interplanetary file system (IPFS) for securely exchanging data.	Data privacy, data security (confidentiality, integrity, and availability), IoT security, communication security.
[23]	2020	Elaborates on challenges associated with establishing governance, risk, and control in Industry 5.0. It also mentions Horizon 2020 ECHOs ongoing work of designing a governance model for a cybersecurity network and the needs/objectives to prioritise these regulations.	Data governance, risk and control.
[24]	2020	Refers to potential issues that arise as an outcome of increased connectivity. Seamless cyber and physical connectivity in the production environment enlarges the attack surface. The paper provides a cyber manufacturing system security testbed, developed for examining	Increased threat surface, malicious actors, digital forensic and intrusion detection.

		cyber-physical intrusions and validating the detection methods in the cyber manufacturing ecosystem.	
[25]	2020	This paper discusses various aspects of data security from an Industry 4.0 cloud perspective and provides insights into the security and regulatory issues that arise out of it.	Data security, regulations, cloud standards, alignment.

Industry 5.0 facilitates the seamless integration of cyber and physical domains within manufacturing ecosystems, however, with the increased connectivity in a plant and/or between plants this widens the cyber-physical system attack surface for potential exploitation [3, 15, 16, 17] causing enormous damages to the manufacturing system [18, 19, 20, 21, 22, 23, 24, 25]. It is just a matter of time before the IoT turns into Ransomware of Things (RoT) [26], the advanced connectivity and denser network infrastructure create new openings for probable exploitation. Remote locking of intelligent devices or factory buildings being abused for extortion, manipulation of building automated systems (i.e., controlling the Heating Ventilation, and Air Conditioning (HVAC) could serve as a basis for new cybercrime schemes). The cost associated with these types of risks and vulnerabilities is extremely high. These lessons have been learned with the recent ransomware attacks on healthcare facilities, and critical infrastructures (i.e., water facilities, smart grid, etc.) [13, 27, 28, 29]. Such cyber threats are classified as cyber terrorism, as the malicious hackers intend to create operational disruption at the industrial or government levels and impact human lives. Sadly, due to the lack of appropriate cyber laws, governance, risk, and control, these threats have been increasing with every passing day.

Regulations fail to mitigate geopolitical cyber risk and shock scenarios as production facilities based in different jurisdictions have to comply with different regulations (i.e., GDPR, HIPAA, etc.) [30, 31, 32], this leads to a wide gap open in terms of securing the flow and mediums of data. This is why there is a pressing need for implementing data security controls to mitigate these gaps. With 80-85% of successful cyber-attacks (malware, ransomware, phishing, etc.) occurring due to human error, there is still a lot to do in terms of securing the wide attack surface [33]. Deploying secure, vigilant, and resilient data needs must be established, for providing a digital footprint (real-time insights and visibility of the productions' cyber threat surface) when where intelligent devices are employed in the environment. Applying the same level of security for all devices will allow quick detection of malicious nodes/devices [24, 25, 26, 27, 28, 29, 30, 31, 32, 33], however, this strategy may not be workable in scenarios where certain types of devices have higher priority of security than the rest (e.g., maritime facilities, nuclear). Manufacturing sectors are progressively implementing security standards, controls, multi-factor authentication, and Zero Trust (ZT) [34] models for both their IT/OT and cloud domains. However, if authorized personnel make such an unintentional/accidental human error, that may lead to a massive breach. The impact, cost, and reputation damage that such breaches cause would be huge in terms of financial and operational aspects and could only be limited/mitigated by employing stronger security measures (i.e., network segmentation, damage control, critical zone isolation, data security controls, encryption, pseudonymization, etc.) and using an effective and informed cybersecurity strategy. The authors previous research in [3] highlights different Industrial cyber breaches over the past 15 years and provides a roadmap for unifying standards in the Smart Manufacturing space/domain. The work done in [3] is extended and mapped across the Six Sigma (6σ) approach to develop a sustainable, human-centric, resilient factory as shown in Fig. 1.

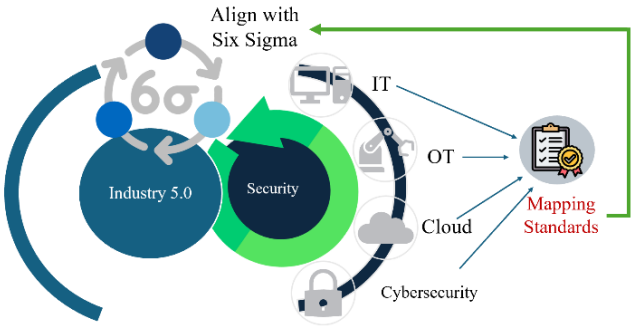


Fig. 1. Concept of Developing a Sustainable, Human-Centric Resilient Smart Factory

3. Cybersecurity Service Level Agreement

Disruptive technologies provided by separate vendors are subject to different security controls and conformance standards. The requirements identified as part of the cybersecurity strategy are often missed and not met. Cybersecurity Service Level Agreements (SLAs) [35] are a way to make sure that the promised services are delivered and reduce the cyber risk exposure for the manufacturer. If at any stage the QoS availability/reliability parameters are not met or there is a breach, cyber-SLAs provide a basis for post-incident legal combat. The cyber-SLAs are aligned with the data security (confidentiality, integrity, and

availability (CIA) triad) and can be measured based on QoS metrics (e.g., (i) the percentage of failed/successful cyber incidents on sensitive data by intruders, unauthorized persons or devices, (ii) log analysis, (iii) number of failed/successful login attempts leading to tampered data, etc.). Such metrics can assist in implementing conformance and controls across the environment. In cybersecurity, there are various QoS metrics such as incident containment, remediation, patching cadence, third-party risk, downtime, cost-per-incident, cyber preparedness, Mean Time to Detect (MTTD), security rating, etc. [36]. However, in this research the authors align and map the following selected metrics: (i) availability (uptime, force majeure, scheduled downtime), (ii) quality of service (mean time to recover), (iii) security (access management, governance, risk and control, data integrity, mean-time to recover, etc., (iv) and cost efficiency from a resource provisioning, return on investment and total cost of ownership perspective as shown in Appendix A. These metrics were chosen based on the scope of this research. The authors suggest aligning and mapping the cyber and cloud SLAs first because the industry 5.0 ecosystem needs to function universally across the production facility. As an example, if the cloud suffers a downtime/QoS issue, that would compromise the availability metric and lead to operation disruption, similarly, the same situation will happen if there is a cyber breach, hence the availability metric needs to be mapped across both cloud and cyber SLAs. Availability is a significant security metric and is the core component for building operational and cyber resilience within a smart manufacturing environment. To achieve this goal of a secure, sustainable, and innovatively aligned environment, the cloud, IT, OT, and cyber security standards must be aligned across a single framework. The next section deep-dives and builds an understanding of how Six Sigma could foster in realizing this goal, bridging the QoS issues and standardisation gaps.

4. Six Sigma (6σ) – Understanding the Scope of Lean Standards And 6σ In Industry 5.0

One of the questions arising at this stage would be why Six Sigma (6σ) approach is being implemented and how it relates to Industry 5.0's promising vision. Well, 6σ is a strategic, structured quality standard tool that uses statistical process control (SPC) and problem-solving techniques in cross-functional processes [37, 38]. As shown in Fig. 2 earlier, one of the objectives of this research is to align and implement 6σ across the smart factory enabling interoperability. 6σ is a widely adopted standard in the manufacturing environment for mitigating gaps and achieving the highest quality conformance (QC) metrics (i.e., define, measure, analyse, improve, and control, as shown in Fig. 2), producing zero defect products 99.99966% of the time (permitting 3.4 defects per million opportunities (DPMO)) [37, 38, 39]. This not only improves the overall QoS but also provides insights, visibility, and control and reduces unnecessary/conformance-based costs in production. Having objectives to deliver a highly sustainable, edge-cutting human-centric, resilient factory and meeting the objectives of an agile, efficient, automated, and zero waste production environment, this is how 6σ fits in the scope of this research as it aligns to meet the vision of Industry 5.0 (healthcare, production, supply-chain) environment.

Fig. 2. Six Sigma in Industry 5.0

4.1 Comparing (6σ) and Lean

6σ and Lean share common grounds as they both seek to eliminate waste and increase the efficiency of a system as much as possible. 6σ's five-step approach "DMAIC" is data-driven and well-equipped to reduce waste and improve and monitor the supply-chain performance manufacturing, whereas lean fully focuses on waste reduction delivering maximum value to customers with the least amount of investment. The implementation and impact of Lean in IIoT have been discussed in terms of return on investment (ROI) perspective [14], however [37] states that Lean works best when it is aligned with 6σ, because as a standalone it does not focus entirely on the manufacturing aspects, instead on different business facets. The 6σ approach enables the production environment to mitigate defects, overproduction, and waiting (process bottlenecks, downtime), efficiently and effectively use human resources, transportation, inventory, and motion, and manage issues related to extra-processing. 6σ can be combined with lean to produce desired outcomes, however, in this research, we focus solely on 6σ as it fully aligns with Industry 5.0's vision.

4.2 Comparing (6σ) and Lean

6σ is based on the principles of "Kaizen" which means continuous improvement, and so is Industry 5.0. Based on the self-driving, self-learning variables used in the factory, the production is continuously working towards precise resourcing and continuous improvement variables. Agile flexibility allows a digital factory to adapt the manufacturing schedule changes with the least intervention and increase the production uptime and yield (by reducing scheduling/product changeovers that would enable flexible scheduling). 6σ reduces the costs by improving the QoS which results in better ROI, these features are the epicentre of a digital transformation, in order to achieve a long-term and sustainable impact. A futuristic factory may only expand physically if it is enabled to support the production lifecycle in a collaborated and orchestrated method.

The Kesaya Supply chain attack that affected a chain of supermarkets globally, VMware cloud vulnerabilities, and Microsoft's zero-time patch, exploitations are just handpicked examples that demonstrate the growing cyber threat landscape [40]. For Industry 5.0 to succeed it is essential to have a clear vision and roadmap for the factory of the future and establish a path for both IT and OT convergence addressing the enterprise's entire function/connectivity beyond the manufacturing process itself, including all open standards and protocols. As smart data is the most valuable operational asset in today's time, it should be securely handled. Deploying 6σ assists the production environment in analysing and presenting data legitimately to the stakeholders, similarly, a digital factory must be enabled to provide plant metrics (i.e., overall equipment effectiveness (OEE) = Availability x Performance x Quality) [39] for understanding the full potential of the production environment), predictive monitoring/metrics such as machine health, life predictions, and failure diagnosis. If at any stage the environment faces unavailability issues due to cloud downtime, cyber-attack (Denial of Service (DoS), or data manipulation), this will impact the performance and quality metrics (CoQ) leading to a poor OEE. This is why it is essential to mitigate cybersecurity risks and threats in the Industrial environment.

4.3 Aligning Cybersecurity with 6σ

As discussed in section 2 and 3, cybersecurity SLAs' QoS metrics (availability, reliability, etc.) are measurable and able to present the current state of QoS performance metrics in terms of score/threshold/impact factor. These types of QoS parameters have also been implemented in Information Security (IT, cloud, and network) services. The 6σ technique facilitates in improving the QoS considerations using different techniques, these techniques (voice of customer, critical to quality drivers, failure mode effects analysis, house of quality, etc.) have previously been implemented and aligned in the Business Cloud IT (BCIT) environment [37, 41]. However, in this research, the authors extend the Six Sigma BCIT Framework in the context of Industry 5.0 for securely mitigating cyber risk in the environment.

Standards implementation has always been crucial in the Industrial environment (healthcare, agriculture, etc.) as they ensure the safety, security, quality, and reliability of the products and services provided. Standards enable the industry to measure the maturity of the technical and business processes. In conventional enterprises, manufacturing standards applied to only the production domain whereas Information security or operational standards applied to the IT and OT domains, but as everything is converged (processes are no more exclusive) these standards must be mapped together as well. In the past, Information Security Standards (i.e. ISO 27001, Control Objectives for Information and Related Technologies (COBIT), Information Technology Infrastructure Library (ITIL), etc.) [3, 37] have been employed as a stand-alone and in situations where different standards were adapted, they were not mapped. This is why several critical infrastructures, manufacturing, and fintech industries have suffered breaches recently. The professional standards bodies have now realised the importance of interoperable standards and gap analysis, which is why working groups have been formed [3, 42] to aid the process of mapping different standards.

Cybersecurity, IT, OT standards, frameworks (i.e., NIST CSF 2.0, NIST RMF, ISO 27001, IEC 62443, etc.) [3, 11, 12, 13, 43] and controls have processes similar to 6σ for identifying, analysing, detecting, protecting, responding and recovering. The scope of these standard processes is to mitigate infrastructure IT/OT security risks. As the primary role of both standards (6σ and cybersecurity) is to improve the overall QoS, reduce defects/waste, and continuously monitor, improve, and control the ecosystem, it is evident that both standards have the same objectives and process methods and be aligned and implemented in any Industry 5.0.

4.4 6σ Business Cloud IT (BCIT) Framework

To understand how the authors have extended the 6σ BCIT Framework, it is essential to learn the core concepts of the framework itself. The existing cloud

standards lacked versatility and did not focus on the impact of cloud QoS metrics on the business services. Cloud Service Level Agreement (SLA) is the only way that provide assurances that cloud vendors will deliver the promised services and enterprise-level requirements. Under circumstances where cloud services are violated or fall below the promised levels, the SLA contract enters a termination phase. Each application running over the cloud platform is subject to a different SLA, the complexity of the existing cloud offering increases with different cloud models (i.e., public, private, hybrid, multi-cloud, etc.) [41, 44] and architectures. Over the last few years cloud standardization bodies have been keenly working on bridging standards gaps in cloud, for example, the NIST SP 500-332 [45] provides a brief overview of the roles of different cloud actors (vendors, end-users, auditors, etc.) enact, technical and service description, and ways for easing the cloud adoption barriers. Whereas the IEEE P2302 *"Standards for Cloud Federation"* [46] is working side with NIST 800-332 for mapping the standard; but that is a work in progress. At present, considering the federated cloud setups, there are no standards fully designed yet that could grant absolute interoperability and uniform governance. Even the EU-funded H-Cloud project [47] recently indicated major data security and regulatory challenges that may impact digitally transformed IIoT. Comprehensive research on cloud economics and enterprise strategy [48] also presented the levels at which cloud SLAs failed to meet the promised services and have not been aligned with the IT or business strategy. These issues have led to security breaches and operational disruption (failure, performance issues, and downtime) at unplanned times. As a result, the cloud tenants face poor returns on investment, contract breaches, inability to design and develop products and services timely. As per the cloud vendor SLA this is not considered a violation and no credit/compensation is provided for the undelivered services. It is now obvious that the vendors holding standards accreditations can suffer QoS issues and breaches as they are not being assessed and evaluated from a strategic business perspective.

The 6σ BCIT Framework [37] enables cloud tenants to mitigate QoS issues in cross-functional processes and provide proactive risk assessment and risk mitigation. A use-case example implementing 6σ BCIT Framework is presented here. Cloud tenant enterprises require a pre-emptive approach before migrating services to the hybrid cloud environment. A Cloud SLA with 99.9% availability implies to 9 hours of agreed downtime/year. A clear SLA may outline the accountability of the tenant/vendor, the acceptable performance metrics, a description of the applications and services covered under the agreement, procedures for monitoring service levels, and a schedule for the remediation of outages. Since Cloud SLAs are the only method to control the cloud QoS, the terms defined play a huge role in the success of cloud deployment. The factors precisely affecting the cloud services are [48]: quality (i.e., timeliness, cost of poor quality, audits, non-conformance costs, rework, etc.), availability (i.e., downtime/uptime, scalability, reliability, etc.) and responsibilities which differ based on cloud vendor and tenant roles (i.e., service assurance (SA), SA period, SA granularity, Service guarantee, Service recognition, Service violation measurement, and reporting). The roles of these metrics are detailed in [41, 49, 50]. If such a service breach occurs at a peak processing hour, the tenant's services are compromised but as per the SLA the breach is justified, leading the tenant to vendor lock-in situation. As each process in the example use-case was treated differently, it affected the enterprise's QoS (failure to identify faults, defects, and errors incurred). When the cloud outage took place, the enterprise was significantly affected but there was no way to assess/calculate or improve the fault domain since each process was assessed independently instead of a single unit. The historic trend of cloud tenants adopting cloud services has been based on low IT, operational, and maintenance costs with the appropriate computational needs and services. Around 40-60% of the computational-based costs are reduced with cloud setups in comparison to on-premises technical support where maintenance, deployment, integration, and in-direct costs may contribute to the overall cost [50]. Considering the scope, and strategic preparedness, there are several vulnerabilities that the hybrid cloud architectural blueprint is susceptible to. The recent VMware vulnerabilities have exposed the widespread threat landscape that is hard to control using exclusively cloud standards.

6σ BCIT Framework [37] provides a roadmap to align and map business, cloud, and IT Security metrics, strategy, and SLA QoS metrics. This is something that cloud standards failed to deliver at both quality and security levels. The risk impact also shifted from unknown risks to known risks, which made assessing and measuring the potential parameters possible. Fig. 3 demonstrates the interdependencies and need for interoperable standards and cross-functional business processes in Industry 5.0 for developing a sustainable, innovative and disruptive production environment.

Fig. 3. Cross-Functional Standards in Industry 5.0

5. Traditional Healthcare to Precision Healthcare 5.0

This section presents an Industry 5.0 healthcare use case implementing the extended version of 6σ BCIT Framework [37] that will be referred to as "6σ CYBERNETIC Framework" (6σ CYBERsecurity busiNEss oT iT Cloud Framework). The real-world healthcare 5.0 (use-case/case study) "Jay", its real-name has been pseudonymized due to confidentiality and data protection (see Fig. 4). Jay is a medium-to-large facility based in Ireland (Europe), using cloud-based services for technological aspects supporting the healthcare facility. The reason to migrate IT service to the cloud was based on the expected ROI, high volume of health/patient data processing per day, convenience, and patient retention. Jay Healthcare adopted cloud services to lower the IT and operational/maintenance costs. As per the facility's records, the IT-based costs were lowered by 50-60% in comparison to traditional in-house data processing, cloud costs were reduced by choosing a long-term contract with reserved instance type (r4) based on upfront billing, provided discounts in comparison to on-demand and on-spot instances. Regardless of using cloud services, healthcare has been struggling with resource optimization, integration of new and legacy systems, manual systems, cybersecurity data breaches, high turn-around time, lack of control, alignment, lost customers, and poor services.

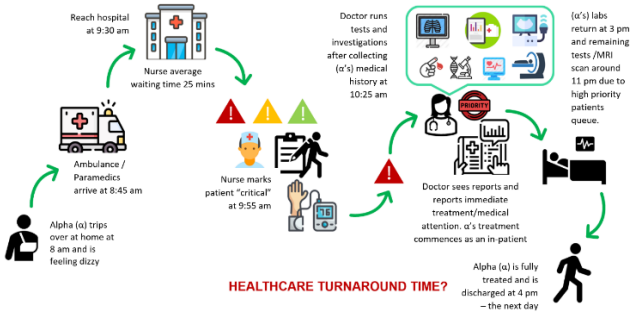


Fig. 4. Jay Healthcare 5.0

Fig. 4 presents the Jay use-case in which (α) suffers an injury at 8 am and his treatment starts at 11:45 pm. As (α) was considered a high priority patient the turnaround time was 32 hours. The lag for average patients would be even longer. On average there were 200 emergency cases per day with only 20 treated and 5 discharged the same day. Calculating the yield on the day (α) was hospitalised.

$$\text{Yield} = \text{Out/In} = (20+5)/200 = 0.125 < 1\ \sigma \qquad (1)$$

The yield [39] benchmarks Jay QoS lesser than 1σ, the overall healthcare facility requires secure, technical, innovative, and digital transformation to improve and reach the 6σ benchmark as shown in the fishbone diagram (see Fig. 5).

Fig. 5. Jay Fishbone: Cause and Effect in Healthcare 5.0

Fishbone is a 6σ tool used for identifying root causes of QoS faults/defects and their impact on the healthcare Industry. In the current times where there have been various cyber breaches in hospitals across the world, with the increased use of IoT-based applications and devices, this industry is considered to have a complicated and complex ecosystem (see Fig. 6).

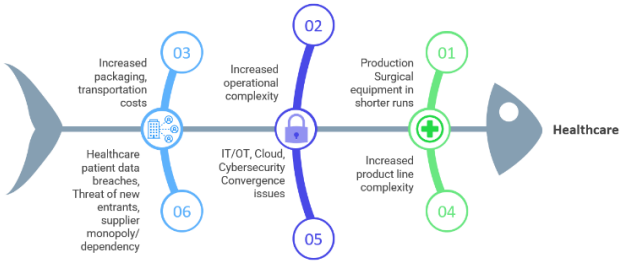


Fig. 6. Complexities In the Global Healthcare Ecosystem

To digitally transform Jay to Jay 5.0, it must demonstrate a strategic, streamlined, operational, cost-effective, aligned, and secure environment. To deliver such a healthcare 5.0 facility, the 6σ CYBERNETIC Framework is implemented using the following steps.

1. Root cause analysis [39] is applied to identify and assess the cause of defects/faults (as shown in Fig. 6).
2. Voice of the customer (VOC) [37, 39] assists in mapping Jay 5.0's business strategy with the end-users/patients' feedback. Based on that weightage and yield it was apparent that the cross-functional processes required attention, as they had a direct impact on the patient's experience at the facility (e.g., cheaper = reduced cost, faster = resource provisioning, scalability, backup up strategy, etc., better = compliance, security, availability, resilience, etc.).
3. The Critical to Quality (CTQ) tree (see Appendix A) underlines the issues/defects addressed in VOC and provides a roadmap to improve the critical to quality drivers, map processes, and set achievable goals so that the QoS metrics could be evaluated [37, 39]. For a better understanding, some of the issues related to Cloud, IT, and OT have been presented in Appendix A. At each stage of the framework, the authors have aligned the Business and cloud IT/OT strategy.
4. The project plan that provided the Plan Do Check Act (PDCA) [37, 39] objectives, supported the consistency of implementation (timelines) and the evaluated progress in sprints.
5. Based on the yield the sigma level was known (1σ), however FIT Sigma [39] was applied to identify the difference between the actual and anticipated QoS, Field Pass Yield (FPY) metrics, and the loss incurred due to poor quality.

Table. 2 presents the transition of Jay's existing cloud, IT/OT, cybersecurity service levels, and strategy that exhibit a void at the analysis and improvement levels leading to vendor lock-in situations. Cyber standards do have processes for analysing and improving the environment, but gap analysis exists which can be mitigated using the 6σ CYBERNETIC Framework.

Table 2

Comparison of 6σ and well-known cloud, IT, OT standards

	Six Sigma (6σ)	Cloud, IT, OT well-known standards and service providers
Define	Scope, root cause analysis, planning, VOC	Service level defined
Measure	Process map	Service level agreement
Analyse	Qualitative, Quantitative (mapping Business, IT, OT, and Cybersecurity frameworks) analysing of the QoS metrics	X
Improve	Process improvement metrics (using above mentioned mapped framework)	X
Control	FMEA – Evaluating performance with the unified framework approach and seeing if the QoS metrics are better than the former. Assists in implementing data security, regulatory, privacy and compliance across Jay 5.0.	Service level agreement violations, penalties, negotiations, data breaches

6. Unified standards mapping and alignment to improve cross-functional processes.
7. PERT (Program Evaluation and Review Technique) critical path method (CPM) [51, 52].
8. Jay's business adjusted risk (BAR) was <1, post alignment Jay 5.0's BAR was 2. Similarly, the Failure Mode Effect Analysis (FMEA) also showed an improvement in QoS metrics.
9. The House of Quality (HoQ) [39] helped in mapping and benchmarking the services, and healthcare operations to the identified QoS requirements.
10. Besides this diverse qualitative and quantitative frameworks (i.e., Balanced Scorecard, Strengths Weaknesses Opportunities and Threats (SWOT), PESTLE), cybersecurity, IT, OT, and Cloud Standards (i.e., NIST RMF, ISO 27001, Cloud Controls Matrix (CCM), ITIL, NIST SP Trusted Cloud, IEC 62443, MITRE ATT&CK, etc.) [3, 37, 42, 53] were applied for aligning and achieving the vision of a strategic, secure, technology enabled, sustainable Jay healthcare 5.0 (see Table 3).

The table also sheds light on why aligning and mapping standards is essential. Business continuity is one of the most important features, but the majority of the security and cloud standards do not map the cybersecurity strategy with the business strategy, and this is how the 6σ CYBERNETIC Framework brings together different standards under the same roof to deliver an Industry 5.0 strategic vision.

- X represents fully mapped
- Φ represents partially mapped
- The unmarked boxes represent no mapping at all
- The red boxes state that the mentioned processes and standards are not mapped, hence leaving the environment vulnerable to various security issues
- The blue boxes highlight little or no implementation in critical processes (i.e., business continuity) provided by security standard bodies. Previously standards were not seen from a business perspective, and this is why they lack versatility. Every potential breach has the potential to cause an enterprise to halt, therefore it is essential to look into the dimensions as 6σ CYBERNETIC Framework does

Table 3

Standards illustrating different parameters of cloud, IT, OT, cybersecurity and business continuity [3, 54, 55]

	NERC CIP [54] mapped to NIST CSF [12]	GDPR [30] mapped to NIST CSF 2.0 [12]	HIPAA [31]	BPI-CPNI [55]	NIST 800-53A RMF mapped to NIST CSF [12]	NIST 1800-19 Trusted Cloud [53]	NIST 800-207 [34]	NIST 800-82	NIST 800-100	NIST 800-48, 800-97 [55]	ISO 27001	IEC 62443	IEC 61784	MITRE ATT&CK [56] [57]	One M2M	CCMV 3.0.1 [37]
Identity and access control	X	ID.AM3, ID.AM-4	Φ	X	X	X		X			X	ID. AM 1-5		X	X	X
Asset classification and control	X				X	X			X		X			X		Φ
Business Continuity Management	ID.BE-3 Not mapped				Φ						Φ					Φ
Governance (legal, regulatory, risk, environmental an operational requirements are understood)	ID.GV-3, ID GV-4	ID.GV-3 (mapped) **ID.GV-4 (Not mapped)**			Controls mapped against ID.GV 1-4, ID.RM 1-3	d										
Risk management strategy, supply chain risk management	ID-RM-3. ID.SC-4, ID.SC-5		Φ		Controls mapped against ID.RM 1-3											

Information protection processes and procedures, protective technology	PR.IP-2, PR.PT-5		Φ		Control mapped against (PR. C 1-7, PR.AT 1-5, PR.DS 1-8, PR.IP 1-12, PR.MA 1-2, PR.PT 1-5)									Φ		
Anomalies and events	DE.AE-1 (Anomalies and Events)	DE.AE-4, DE.CM-7	Φ		Controls mapped against DE.AE 1-5, DE.CM 1-8, DE.DP 1-5)									X		
IT/OT convergence								X				X		Φ	X	
IT/OT characteristics, cybersecurity threat and vulnerabilities								X				X		X		
IT/OT security controls (management, operational, technical)								X				X	X		X	
Multi-connections to IT/OT networks	Φ			X											X	
Secure network architecture	Φ			X	X							X			X	
Patch management strategies	X			X	X	X		X							X	
Physical and environmental security	X										X					
Physical and				X				X								

logical demilitarized zone (DMZ)																
Remote access, identity and access management	X		X	X	X	X									X	
Zero Trust Policy					Φ		X									
Cybersecurity strategy					Φ						X					
Standards interfaces between different networks	X												X		X	
Logical segmentations on virtual LANs								X				X				
Physical segmentations				X								X				
Securing wireless networks										X		X	X		X	
Securing autonomous networks																
Cloud Security		PR.DS-1, PR.DS-2,														
PKI															X	
Data security, privacy		PR.DS-5., PR.DS.6	Φ		Φ											
Resiliency (incident response and recovery), vulnerability management, respond, mitigate	RC.CO-2, RC.CO-3	PR.IP-10, PR.IP-12, , RS.RP-1, RS.CO-1, RS.MI-3, RS-IM1, RC-CO3	Φ		RS.RP-1, RS.CO 1-5, RS.AN 1-5, Rs. MI 1-3, RS. IM 1-2, RC.RP 1, RC.IM 1-2, RC.CO 1-3)											
E2E encryption												X				

Table. 4 presents existing cybersecurity standards related to securely transferring healthcare data [58]. It is evident from below that number of standards are not equipped to support the required security measures for healthcare 5.0 and this is where the 6σ CYBERNETIC framework does the needful.

Table 4

Existing Cybersecurity Standards related to healthcare [58]

Cybersecurity Standards	Transferring Healthcare Data
ISO/IEC 15443 (Security assurance) [59, 60]	
ISO/IEC 15816 (Information security for access control) [61]	
ISO/IEC 19790 (Security requirements for cryptographic modules) [62]	•
ISO/IEC 20008 (anonymous digital signatures), ISO/IEC 2009 (anonymous entity authentication) [63, 64, 65, 66, 67]	
ISO/IEC 20889 (privacy aspect) [68]	•
ISO/IEC 27035 (ISIM) [69, 70]	
ISO/IEC 27036 (Information Security for Supplier Information) [71, 72, 73]	
ISO/IEC CD 27099 (Public Key Infrastructure) [74]	
ISO/IEC 29147 and 30111 (Vulnerability disclosure and management) [75, 76]	
ISO/IEC DIS 23264-1 (Redaction of authenticated data) [77]	
ETSI DTS/CYBER-0013 (TS 103 485) – Privacy assurance and verification [78]	
ETSI DTS/CYBER 0014 (TS 103 486) – Identity management and discovery for IoT [79]	

Walking through the Jay healthcare 5.0's use-case: QoS, IT/OT, cloud, and cyber resilience post 6σ CYBERNETIC framework implementation using the same (α) example.

1. (α) has access to the Jay 5.0s smart app that provides real-time information on the number of patients and wait time.
2. As soon as (α) checks in the hospital at 9:30am, a token is issued using his app barcode ID, the average wait time is provided (25 mins) but as (α) arrived via ambulance, his wait time was reduced 10 mins based on emergency basis. A screen in the waiting area shows the list/no of patients in the queue and that (α) is next in line to be seen. Having seen the real-time information, reduces stress and panic situations among patients and they do not have to visit the check-in counter over and over again for queries (VOC).
3. Based on the check-in and paramedic history gathered in the ambulance, the nurse pulls out (α's) previous health records and has all the required information related to drug reactions, previous tests, medical history, etc. While the nurse checks (α's) vitals (blood pressure, fever) to ensure (α's) rank in the priority queue, a flag/alert is generated on the health management system which in return provides relevant doctors Rota and availability. This enables efficient human resourcing, the nurse assigns (α) to a doctor. The maximum waiting time is reduced to 10-20 minutes (9:40-9:50 am).
4. Jay 5.0 implements the medical risk adjustment approach (RAA) [80] that enables healthcare to identify patients with higher risks, complications, etc. The risk adjustment approach is aligned with the health management system. Using healthcare analytics, a risk score with the patient's background records/information is provided to the nurse.
5. (α's) is moved to the specific ward and is familiar with the estimated time to be seen by a doctor (max. 30 mins). As (α's) medical samples were collected by paramedics at 8:45 am, and deposited at the lab on arrival, (α's) reports will be ready 12:30 pm. The doctor sees (α) at 10:20 am for an initial assessment/examination, the doctor has concerns, checks RAA data, and books priority availability for an MRI that is max. 2 hours. (α's) lab and MRI scan report results are updated on the health information systems at 12:30pm. The investigations show a concussion and (α's) is booked in as an in-patient for further investigations and treatment.
6. The total time it took for (α's) to be seen is 4 hours and 30 minutes (8am - 12:30), whereas the same process took 15 hours and 30 minutes (8am to 11:30pm). Aligning and mapping the disruptive technologies helped Jay in improving healthcare outcomes (i.e., timely treatment of all patients, identifying high-risk patients and providing swift care as soon as possible, reduced wait times for diagnostic tests, examining more patients per day, improved (effective and efficient) resourcing).

Calculating the yield on the day (α) was hospitalised, as the average time to see patient reduced (15h 30m – 4h 30m = 11h), that has potentially increased the possibility of treating more patients per day.

$$\text{Yield} = \text{Out/In} = (25\text{x}11)/200 = 1.375 > 6\sigma \quad (2)$$

Besides this, the 6σ CYBERNETIC Framework resolved several other problems related to business-integrated technologies, data conformance, and disseminating valuable information from different

new and legacy equipment used in Jay 5.0. The availability of real-time data/status through the app gave the patients a proactive approach as they knew the wait time, update, and possibility of being treated on the same day. As the app showed the patient's number in the queue, the patient could decide either to visit Jay 5.0 or visit another healthcare facility where he/she could be assessed and treated sooner. Understanding the patterns of patients on certain times, days, and months of the year facilitated Jay 5.0 in forecasting resources, demand fluctuations, and staff capacity required at what time. Such critical key performance indicators enable in improvement QoS across all processes (see Fig. 7 and 8). The 6σ CYBERNETIC Framework enabled the authors to continuously assess the QoS metrics mentioned in section 2 and also provided added capabilities to (i) precisely identify, calculate, and assess the impacts of cyber incidents, (ii) mapping trust architectures and digital identities across the ecosystem, (iii) real-time operational management, log analysis, threat intelligence (iv) resilience, conformance and control.

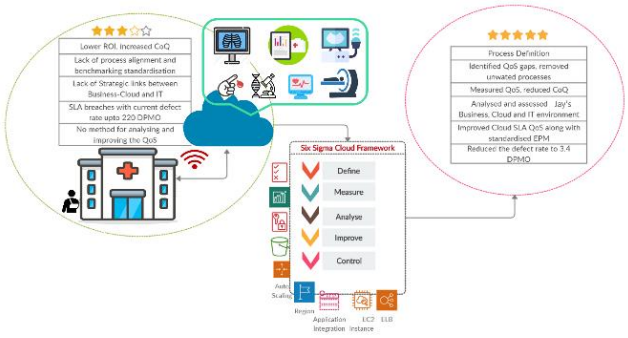


Fig. 7. Jay Healthcare 5.0

Various "what-if" scenarios could be developed for proactively planning/premediating different situations facilitating continuous improvement in Jay 5.0. Jay's healthcare transformation from a traditional to precision healthcare 5.0 involved migrating systems from stand-alone to a fully connected and sustainable ecosystem that could anticipate and respond to changes, predict and mitigate risks and disruptions swiftly. This also facilitated centralised and real-time access to critical data, streamlining automated core processes, and increased capability to collaborate within the healthcare infrastructure and external environments.

This allowed Jai 5.0's processes to: gain access to the key process (inventory, supply chain, etc.) data effectively, provide increased visibility across supply relationships and the entire healthcare life cycle from predicting the demand, and requirements to delivering services, reducing downtime, fully connecting the healthcare's virtual supply teams in the network, enabling combined value creation and effective decision-making by providing an operational environment for multi-healthcare alliance on shared business processes in the supply chain.

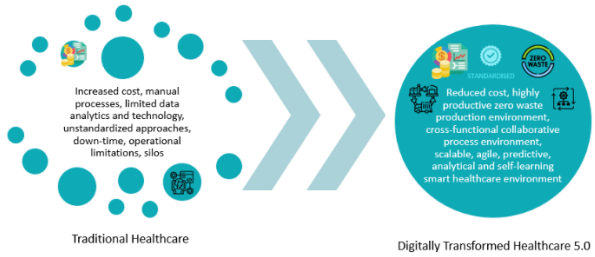


Fig. 8. Digitally Transformed Jay Healthcare 5.0

6. Conclusion

The emerging technologies have enabled the data-driven digital economy, however, to sustain and build resilience within the ecosystem it is essential to align, assess, and protect the interconnected and interdependent technologies from the novel cyber threat landscape. This paper provides a roadmap to mitigate the emerging cybersecurity issues that Industry 5.0 may be susceptible to. The authors designed "6σ CYBERNETIC Framework" (6σ CYBERsecurity busiNEss oT iT Cloud Framework) maps and bridges the gap between the cloud, IT, OT, cybersecurity, and business standards leading to a sustainable and cutting-edge Industry 5.0 environment. A Healthcare 5.0 use case (Jay 5.0) has been presented to demonstrate the efficacy and impact of the 6σ CYBERNETIC framework. It also demonstrates the alignment between business, cloud, IT/OT and cyber, cybersecurity measures and strategy as a single process, reducing costs, operational and cloud waste.

7. References

[1] S. Zardari, N. Nisar, Z. Fatima and L. L. Dhirani, "IoT – assets taxonomy, threats assessment and potential solutions," 2023 Global Conference on Wireless and Optical Technologies (GCWOT), Malaga, Spain, 2023, pp. 1-8, doi: 10.1109/GCWOT57803.2023.10064657.

[2] Y. Lu, H. Zheng, S. Chand, W. Xia, Z. Liu, X. Xu, L. Wang, Z. Qin, and J. Bao, "Outlook on human-centric manufacturing towards industry 5.0," Journal of Manufacturing Systems, vol. 62, pp. 612-627, 2022, doi: 10.1016/j.jmsy.2022.02.001.

[3] L. L. Dhirani, E. Armstrong, and T. Newe, "Industrial IoT, cyber threats, and standards landscape: evaluation and roadmap," Sensors, vol. 21, no. 11, pp. 3901, 2021, doi: 10.3390/s21113901.

[4] "The net-zero industry act: accelerating the transition to climate neutrality". Sustainability. [Online]. Available: https://single-market-economy.ec.europa.eu/industry/sustainability/net-zero-industry-act_en. [Accessed: 13-Feb-2024].

[5] A. Frank, L. Dalenogare, and N. Ayala, "Industry 4.0 technologies: Implementation patterns in manufacturing companies," International Journal of Production Economics, vol. 210, pp. 15-26, 2019, doi: 10.1016/j.ijpe.2019.01.004.

[6] K. A. Demir, G. Döven, and B. Sezen, "Industry 5.0 and human-robot co-working," Procedia Computer Science, vol. 158, pp. 688-695, 2019, doi: 10.1016/j.procs.2019.09.104.

[7] S. Nahavandi, "Industry 5.0—A human-centric solution," Sustainability, vol. 11, pp. 4371, 2019, doi: 10.3390/su11164371.

[8] V. Özdemir and N. Hekim, "Birth of industry 5.0: Making sense of big data with artificial intelligence, the internet of things and next generation technology policy," Omics, J. Integrative Biology, vol. 22, no. 1, pp. 65-76, 2018, doi: 10.1089/omi.2017.0194.

[9] D. Paschek, A. Mocan, and A. Draghici, "Industry 5.0-The expected impact of next industrial revolution," Proc. Thriving Future Educ., Ind., Bus., Soc., Proc. Make Learn TIIM Int. Conf., 2019, pp. 15-17.

[10] "EU cyber resilience act," Shaping Europe's digital future. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. [Accessed: 2-Mar-2024].

[11] "ISO/IEC 27001 Standard – information security management systems," ISO. [Online]. Available: https://www.iso.org/standard/54534.html. [Accessed: 1-Mar-2024].

[12] "Cybersecurity framework," NIST. [Online]. Available: https://www.nist.gov/system/files/documents/2022/10/03/NIST_CSF_update_Fact_Sheet.pdf. [Accessed: 2-Mar-2024].

[13] H. Meagher, L. L. Dhirani, "Cyber-resilience, principles, and practices," Cybersecurity Vigilance and Security Engineering of Internet of Everything. Internet of Things. In: K.N. Qureshi, K., T. Newe, G. Jeon, A. Chehri, Eds. Springer, Cham, 2024. doi: 10.1007/978-3-031-45162-1_4

[14] D. Romero, P. Gaiardelli, D. Powell, T. Wuest, and M. Thürer, "Digital lean cyber-physical production systems: the emergence of digital lean manufacturing and the significance of digital waste," Advances in Production Management Systems. Production Management for Data-Driven, Intelligent, Collaborative, and Sustainable Manufacturing. APMS 2018. IFIP Advances in Information and Communication Technology, vol 535, I. Moon, G. Lee, J. Park, D. Kiritsis, & G. von Cieminski, Eds. Springer, Cham, 2018. doi: 10.1007/978-3-319-99704-9_2

[15] M. A. Khatun, S. F. Memon, C. Eising and L. L. Dhirani, "Machine learning for healthcare-iot security: a review and risk mitigation," IEEE Access, vol. 11, pp. 145869-145896, 2023, doi: 10.1109/ACCESS.2023.3346320.

[16] M., Sharma, R. Sehrawat, S. Luthra, T. Daim, & D. Bakry, "Moving towards industry 5.0 in the pharmaceutical manufacturing sector: challenges and solutions for germany," IEEE Transactions on Engineering Management, pp. 1-18, 2024. doi: 10.1109/tem.2022.3143466

[17] J. Shahid, R. Ahmad, A.K. Kiani, T. Ahmad, S. Saeed, and A.M. Almuhaideb, "Data protection and privacy of the internet of healthcare things (IoHTs)," Appl. Sci., vol. 12, no. 4, art. no. 1927, 2022. doi: 10.3390/app12041927.

[18] S. Thomas and L. Ngalamou, "The impact of cybersecurity on healthcare," Proceedings of the Future Technologies Conference (FTC) 2021, vol. 2, K. Arai, Ed. Cham: Springer, 2022, pp. 680-689. doi: 10.1007/978-3-030-89880-9_50.

[19] A. Khalid, Z. Khan, M. Idrees, P. Kirisci, Z. Ghrairi, K. Thoben, and J. Pannek, "Understanding vulnerabilities in cyber-physical production systems," International Journal of Computer Integrated Manufacturing, vol. 35, pp. 569-582, 2021, doi: 10.1080/0951192X.2021.1992656.

[20] "Cybersecurity challenges in the uptake of artificial intelligence in autonomous driving," ENISA, 11-Feb-2021. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving. [Accessed: 24-Feb-2024].

[21] A. Mehbodniya, R. Neware, S. Vyas, M. Kumar, P. Ngulube, and S. Ray, "Blockchain and IPFS integrated framework in bilevel fog-cloud network for security and privacy of iomt devices," Computational and Mathematical Methods in Medicine, vol. 2021, no. 7727685, 2021, doi: 10.1155/2021/7727685.

[22] T. Tagarev, "Governance of collaborative networked organisations: stakeholder requirements," IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020, doi: 10.1109/DESSERT50317.2020.9125029.

[23] M. Wu, J. Song, S. Sharma, J. Di, B. He, Z. Wang, J. Zhang, L.W. Lin, E.A. Greaney, and Y. Moon, "Development of testbed for cyber-manufacturing security issues," International Journal Of Computer Integrated Manufacturing, vol. 33, no. 3, pp. 302-320, 2020, doi: 10.1080/0951192x.2020.1736711.

[24] L. L. Dhirani and T. Newe, "Hybrid cloud SLAs for industry 4.0: bridging the Gap," Annals of Emerging Technologies in Computing, vol. 4, pp. 41-60, 2020, doi: 10.33166/AETiC.2020.05.003.

[25] E. K. Karpunina, "From Digital Development of Economy to Society 5.0: Why We Should Remember about Security Risks?" VISION 2025: Education Excellence And Management Of Innovations Through Sustainable Economic Competitive Advantage, 2019, pp. 3678-3687.

[26] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: evolution, mitigation and prevention," Egyptian Informatics Journal, vol. 22, no. 1, pp. 105–117, 2021, doi: 10.1016/j.eij.2020.05.003.

[27] "French hospital ransomware attack," CyberNews, 2022. [Online]. Available: https://cybernews.com/news/french-hospital-ransomware-attack/. [Accessed: 30-Jan-2024].

[28] "Conti cyberattack on the HSE." [Online]. Available: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf. [Accessed: 30-Jan-2024].

[29] "Cyberattacks cripple dozens of U.S. hospitals," AJN, American Journal of Nursing, vol. 121, pp. 18, 2021, doi: 10.1097/01.NAJ.0000734084.73803.d3.

[30] "GDPR," GDPR.eu, 2023. [Online]. Available: https://gdpr.eu/. [Accessed: 11-Feb-2024].

[31] "HIPAA," U.S. Department of Health and Human Services, 2023. [Online]. Available: https://www.hhs.gov/. [Accessed: 11-Feb-2024].

[32] "Directive on measures for a high common level of cybersecurity across the Union (NIS2 directive)," Shaping Europe's digital future. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis-directive. [Accessed: 11-Feb-2024].

[33] M. Alsharif, S. Mishra, and M. AlShehri, "Impact of human vulnerabilities on cybersecurity," Computer Systems Science and Engineering, vol. 40, pp. 1153-1166, 2022. doi: 10.32604/csse.2022.019938

[34] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," NIST special publication 800-207, 2020. doi: 10.6028/NIST.SP.800-207

[35] Y. Nugraha and A. Martin, "Cybersecurity service level agreements: understanding government data confidentiality requirements," Journal of Cybersecurity, vol. 8, no. 1, Jan. 2022. doi:10.1093/cybsec/tyac004

[36] A. T. Tunggal. "14 cybersecurity metrics + KPIs you must track in 2024," Lean Six Sigma Online Certification & Training at Purdue University, 22-Jan-2024. [Online]. Available: https://www.upguard.com/blog/cybersecurity-metrics [Accessed: 20-Mar-2024].

[37] L. L. Dhirani. "Six sigma based novel approach in resolving hybrid cloud computing qos and sla-based issues in heterogenous cloud environment," Thesis.

[38] S. Tissir, A. Cherrafi, A. Chiarini, S. Elfezazi, and S. Bag, “Lean six sigma and industry 4.0 combination: scoping review and perspectives,” Total Quality Management & Business Excellence, vol. 34, no. 3-4, pp. 261-290, Mar. 2022. doi: 10.1080/14783363.2022.2043740

[39] R. Basu, “Implementing six sigma and lean: a practical guide to tools and techniques,” Elsevier Butterworth-Heinemann, 2009.

[40] “3 security lessons learned from the Kaseya ransomware attack,” Urgent Comms, 29-Jun-2023. [Online]. Available: https://urgentcomm.com/2021/11/02/3-security-lessons-learned-from-the-kaseya-ransomware-attack/ [Accessed 17-Feb-2024].

[41] L. L. Dhirani, T., Newe, and S. Nizamani, “Hybrid cloud computing QoS glitches,” 2018 5th International Multi-Topic ICT Conference (IMTIC), Apr. 2018. doi: 10.1109/imtic.2018.8467224

[42] L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, T. Newe, “Ethical dilemmas and privacy issues in emerging technologies: a review,” Sensors, vol. 23, pp. 1151, 2023, doi: 10.3390/s23031151.

[43] I. T. L. Computer Security Division, “About the RMF - NIST risk management framework: CSRC,” CSRC. [Online]. Available: https://csrc.nist.gov/projects/risk-management/about-rmf. [Accessed: 20-Feb-2024].

[44] L. L. Dhirani, T. Newe and S. Nizamani, “Federated hybrid clouds service level agreements and legal issues,” Advances in Intelligent Systems and Computing, 2018, vol. 471, pp. 471-486, doi: 10.1007/978-981-13-1165-9_44.

[45] “NIST technical series publications.” [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-332.pdf. [Accessed: 20-Feb-2024].

[46] R.. Bohn, M. Michel. “Standards for cloud federation”. [Online]. Available: https://ieeecs-media.computer.org/media/membership/StandardsCloudFed_RBMM_03162021.pdf. [Accessed: 20-Feb-2024].

[47] “Horizon cloud – the forum for strategy focused cloud stakeholders,” [Online]. Available: https://cordis.europa.eu/project/id/871920/reporting. [Accessed: 20-Feb-2024].

[48] L. L. Dhirani, T. Newe and S. Nizamani, “Cloud economics and enterprise strategy: a bird eye's view,” International Journal of Engineering & Technology, vol. 7, no. 3, pp. 360-367, 2018, doi: 10.14419/ijet.v7i4.15.21386.

[49] F. Soliman, “Business transformation and sustainability through cloud system implementation,” IGI Global, 2015.

[50] L. L. Dhirani, T. Newe and S. Nizamani, “Can IoT escape cloud QoS and cost pitfalls,” 2018 12th International Conference on Sensing Technology (ICST), 2018, pp. 1-5, doi: 10.1109/ICSensT.2018.8603570.

[51] Y. B. Suryono, H. Hasbullah, “Analysis Of new production line project improvement through critical path method (Cpm), design structure matrix (DSM) and program evaluation and review (Pert),” Journal of Industrial Engineering & Management Research, vol. 1, no. 4, pp. 9-17, 2020, doi: 10.7777/jiemar.v1i4.97.

[52] A. Stupina, O. Antamoshkina, I. Ruiga, L. Korpacheva, E. Kovzunova, “Building the strategy for innovative development of industrial enterprises based on network planning methods,” IOP Conference Series: Materials Science and Engineering, vol. 1047, pp. 012039, 2021, doi: 10.1088/1757-899X/1047/1/012039.

[53] M. Bartock, D. Dodson, M. Souppaya, D. Carroll, R. Masten, G. Scinta, P. Massis, H. Prafullchandra, J. Malnar, H. Singh, R. Ghandi, L. Storey, R. Yeluri, T. Shea, M. Dalton, R. Weber, K. Scarfone, A. Dukes, J. Haskins, C. Phoenix, and B. Swarts, “Trusted cloud: security practice guide for vmware hybrid cloud infrastructure as a service (iaas) environments,” CSRC, 20-Apr-2022. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/1800-19/final. [Accessed: 22-Feb-2024].

[54] "Reliability and security guidelines," NERC. [Online]. Available: https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx [Accessed: 22-Feb-2024].

[55] S. Ali, T. Al Balushi, Z. Nadir and O. K. Hussain, "Cyber security for cyber physical systems," Springer, Berlin/Heidelberg, Germany, 2018, vol. 768, pp. 11-33, doi: 10.1007/978-3-319-75880-0.

[56] "MITRE ATT&CK Techniques Mapped to Data Sources," [Online]. Available on: https://attack.mitre.org/docs/attack_roadmap_2019.pdf [Accessed: 22-Feb-2024].

[57] "Mitre ATT&CK®," MITRE ATT&CK®. [Online]. Available: https://attack.mitre.org/. [Accessed: 22-Feb-2024].

[58] "D8.2 project standards matrix - cybersec4europe." [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2020/09/CS4E-D8.2-Project-Standards-Matrix-v1.1.pdf. [Accessed: 23-Feb-2024].

[59] "ISO/IEC TR 15443-1:2012," ISO, 09-Jul-2018. [Online]. Available: https://www.iso.org/standard/59138.html. [Accessed: 23-Feb-2024].

[60] "ISO/IEC TR 15443-2:2012," ISO, 09-Jul-2018. [Online]. Available: https://www.iso.org/standard/59140.html. [Accessed: 24-Feb-2024].

[61] "ISO/IEC 15816:2002," ISO, 06-Nov-2018. [Online]. Available: https://www.iso.org/standard/29139.html. [Accessed: 24-Feb-2024].

[62] "ISO/IEC 19790:2012," ISO, 01-Nov-2015. [Online]. Available: https://www.iso.org/standard/52906.html. [Accessed: 24-Feb-2024].

[63] "ISO/IEC 20008-1:2013," ISO, 05-Jun-2019. [Online]. Available: https://www.iso.org/standard/57018.html. [Accessed: 26-Feb-2024].

[64] "ISO/IEC 20008-2:2013," ISO, 01-Dec-2017. [Online]. Available: https://www.iso.org/standard/56916.html. [Accessed: 26-Feb-2024].

[65] "ISO/IEC 20009-1:2013," ISO, 05-Jun-2019. [Online]. Available: https://www.iso.org/standard/57079.html. [Accessed: 26-Feb-2024].

[66] "ISO/IEC 20009-2:2013," ISO, 05-Jun-2019. [Online]. Available: https://www.iso.org/standard/56913.html. [Accessed: 26-Feb-2024].

[67] "ISO/IEC 20009-4:2017," ISO, 03-Dec-2022. [Online]. Available: https://www.iso.org/standard/64288.html. [Accessed: 27-Feb-2024].

[68] "ISO/IEC 20889:2018," ISO, 06-Nov-2018. [Online]. Available: https://www.iso.org/standard/69373.html. [Accessed: 27-Feb-2024].

[69] "ISO/IEC 27035-1:2016," ISO, 13-Feb-2023. [Online]. Available: https://www.iso.org/standard/60803.html. [Accessed: 27-Feb-2024].

[70] "ISO/IEC 27035-2:2016," ISO, 13-Feb-2023. [Online]. Available: https://www.iso.org/standard/62071.html. [Accessed: 28-Feb-2024].

[71] "ISO/IEC 27036-1:2014," ISO, 09-Sep-2021. [Online]. Available: https://www.iso.org/standard/59648.html. [Accessed: 28-Feb-2024].

[72] "ISO/IEC 27036-2:2014," ISO, 15-Jun-2022. [Online]. Available: https://www.iso.org/standard/59680.html. [Accessed: 28-Feb-2024].

[73] "ISO/IEC 27036-3:2013," ISO, 19-Apr-2021. [Online]. Available: https://www.iso.org/standard/59688.html. [Accessed: 29-Feb-2024].

[74] "ISO/IEC 27099:2022," ISO, 08-Jul-2022. [Online]. Available: https://www.iso.org/standard/56590.html. [Accessed: 29-Feb-2024].

[75] "ISO/IEC 29147:2018," ISO, 23-Oct-2018. [Online]. Available: https://www.iso.org/standard/72311.html. [Accessed: 29-Feb-2024].

[76] "ISO/IEC 30111:2019," ISO, 01-Oct-2019. [Online]. Available: https://www.iso.org/standard/69725.html. [Accessed: 1-Mar-2024].

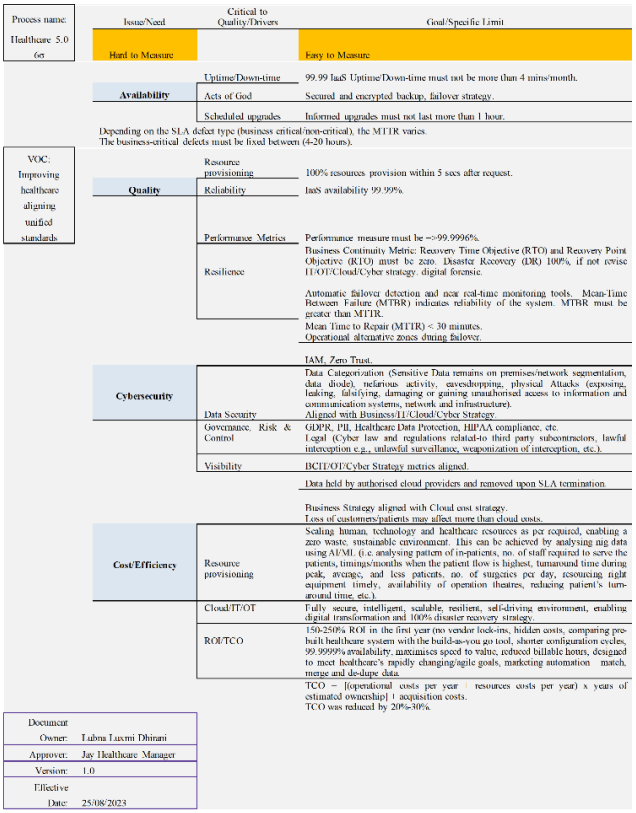
[77] "ISO/IEC 23264-1:2021," ISO, 18-Mar-2021. [Online]. Available: https://www.iso.org/standard/78341.html. [Accessed: 1-Mar-2024].

[78] “ETSI TS 103 485 V1.1.1,” 08-2020. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103400_103499/103485/01.01.01_60/ts_103485v010101p.pdf. [Accessed: 1-Mar-2024].

[79] “ETSI standards on consumer IoT security: EN 303 645 and TS 103 701,” 18-Dec-2020. [Online]. Available: https://www.enisa.europa.eu/events/ENISA-CCC/ccc-conference-slides/speaker-jasperpandza-giselameister.pdf. [Accessed: 1-Mar-2024].

[80] “HHS-operated risk adjustment technical paper on possible model changes,” U.S. Department of Health and Human Services, 2021. Available: https://www.cms.gov/files/document/2021-ra-technical-paper.pdf [Accessed: 1-Mar-2024].

Appendix A



Jay’s CTQ Tree