MANTECH Publications

Journal of Product Design, Quality Engineering & Technology
Volume 4, Issue 1, January-April 2019

Cybersecurity in Product Design and Quality Systems

Subodh Karthikeyan[1], Shobha M. Kulkarni[2], A. Praveen Kumar[3], Avinash Goyal[4]

Associate Professor[1], Assistant Professor[2]

Department of Mechanical & Manufacturing Systems

Horizon College of Applied Sciences, India

Email ID: *Subodhkarthikeyan29@gmail.com[1], shobhamkulkarni23@rediffmail.com[2], Apraveenkumar90@yahoo.com[3]*

Abstract

With the rapid digitalization of product design processes and quality management systems, cybersecurity has emerged as a critical concern for manufacturing and engineering organizations. Modern product design environments rely heavily on interconnected tools such as computer-aided design (CAD), product lifecycle management (PLM), digital quality management systems (QMS), and cloud-based collaboration platforms. While these technologies improve efficiency, traceability, and innovation, they also introduce new cyber risks that can compromise intellectual property, product integrity, compliance, and customer safety. This paper reviews the role of cybersecurity in product design and quality systems, highlighting key threats, vulnerabilities, and risk factors across the product development lifecycle. The integration of cybersecurity principles into quality management frameworks is discussed, along with standards, best practices, and emerging technologies supporting secure-by-design and quality-by-design approaches. Challenges faced by organizations, particularly small and medium enterprises, are examined. The paper concludes by emphasizing the need for a holistic strategy that aligns cybersecurity with product quality objectives to ensure sustainable and resilient manufacturing systems.

Keywords: *Cybersecurity, Product Design, Quality Management Systems, Secure-by-Design, Digital Manufacturing, Risk Management*

INTRODUCTION

Digital transformation has fundamentally changed the way products are designed, developed, manufactured, and maintained. Product design activities now rely on digital models, simulations, and data-driven decision-making. At the same time, quality systems have evolved from paper-based documentation to integrated digital platforms that manage audits, nonconformities, corrective actions, and compliance data. While these changes have improved speed, accuracy, and collaboration, they have also increased exposure to cybersecurity threats. Cyber incidents in product design and quality systems can lead to severe consequences, including theft of intellectual property, manipulation of design data, falsification of quality records, and non-compliance with regulatory requirements. In safety-critical industries such as automotive, aerospace, medical devices, and consumer electronics, cyberattacks may even result in unsafe products reaching the market. Therefore, cybersecurity is no longer only an information technology issue but a core element of product quality and organizational risk management.

This paper provides a comprehensive review of cybersecurity considerations in product design and quality systems. It explores how cyber risks impact design integrity, quality assurance, and lifecycle management. The paper also discusses frameworks, standards, and practices that help integrate cybersecurity into quality systems, ensuring that products are not only functional and compliant but also secure and trustworthy.

DIGITALIZATION OF PRODUCT DESIGN AND QUALITY SYSTEMS

The digitalization of product design and quality systems has transformed traditional engineering practices into highly connected, data-centric ecosystems. Advances in computing power, networking, and software platforms have enabled organizations to manage complex products across geographically dispersed teams. While these developments improve efficiency, flexibility, and innovation capability, they also introduce new cybersecurity challenges that directly influence product quality and reliability.

Evolution of Product Design Environments

In earlier manufacturing environments, product design activities were largely isolated within organizational boundaries. Design data such as drawings, calculations, and specifications were stored on local servers or even in physical formats. Access was restricted, collaboration was

limited, and cybersecurity risks were relatively low due to minimal connectivity. Changes to designs were slower, but control over information was easier to maintain.

The shift toward digital product development has significantly changed this landscape. Modern design environments rely on advanced tools such as computer-aided design (CAD), computer-aided engineering (CAE), and product lifecycle management (PLM) systems. These tools allow real-time collaboration among designers, analysts, suppliers, and customers. Cloud-based platforms further enable remote access to design data, supporting global development teams and faster product iterations.

Another major development is the adoption of digital twins and simulation-driven design. Digital twins replicate physical products and processes in virtual environments, allowing continuous testing, optimization, and performance monitoring. These models rely on continuous data exchange across systems and stakeholders, increasing dependency on secure data communication channels. Any unauthorized modification to digital twin data can lead to incorrect design decisions and flawed physical products.

While collaborative and distributed design environments accelerate innovation and reduce time-to-market, they also expand the attack surface for cyber threats. Design files may pass through multiple networks, devices, and organizations, each with different security maturity levels. Unauthorized access to CAD or PLM systems can result in intellectual property theft, loss of competitive advantage, or intentional design manipulation. Malware embedded in design software or plugins may remain undetected for long periods, affecting multiple projects simultaneously.

Supplier integration adds another layer of complexity. Many organizations allow suppliers direct access to design platforms for co-development and customization. If a supplier's system is compromised, attackers may gain indirect access to the core design environment. In such interconnected ecosystems, a single security breach can quickly propagate across the design network, affecting multiple products and product lines. As a result, cybersecurity has become a fundamental requirement for maintaining design integrity and consistency.

Digital Quality Management Systems

Quality management systems have undergone a similar digital transformation. Traditional QMS relied heavily on paper-based records, manual approvals, and periodic audits. Although these systems were slow and prone to human error, they offered a certain level of security due to limited accessibility. Digital QMS platforms now centralize quality data and automate quality processes across the organization.

Modern digital QMS manage a wide range of quality-related information, including inspection results, nonconformance reports, deviation handling, corrective and preventive actions (CAPA), supplier quality data, and audit records. These systems support compliance with international standards such as ISO 9001, as well as industry-specific regulations in sectors like automotive, aerospace, and medical devices. Digital workflows improve traceability, accountability, and real-time visibility of quality performance.

However, the effectiveness of digital QMS depends heavily on the integrity, availability, and confidentiality of stored data. Any unauthorized alteration of inspection records or audit findings can lead to incorrect quality decisions and potential regulatory violations. Loss of quality data due to cyber incidents such as ransomware attacks may disrupt certification audits and damage organizational credibility.

Integration of QMS with enterprise systems such as enterprise resource planning (ERP), manufacturing execution systems (MES), and PLM platforms further increases system complexity. These integrations enable seamless data flow from design to production and quality assurance, supporting closed-loop quality management. At the same time, they create multiple interfaces where data may be exposed to cyber risks. Weak authentication mechanisms, insecure APIs, or misconfigured access controls can allow unauthorized users to modify or extract sensitive quality information.

In highly regulated industries, digital QMS data serves as legal evidence of compliance. Cybersecurity incidents affecting QMS can therefore have legal and financial consequences beyond operational disruption. Ensuring secure access, robust audit trails, and tamper-resistant records becomes essential for maintaining trust in quality systems.

Overall, digitalization has enhanced the capability and responsiveness of both product design and quality management systems. However, without adequate cybersecurity controls, these digital advantages can quickly turn into sources of risk. Cybersecurity thus acts as a key enabler of reliable, transparent, and trustworthy digital quality management in modern product development environments.

CYBERSECURITY THREATS IN PRODUCT DESIGN AND QUALITY SYSTEMS

As product design and quality systems become increasingly digital and interconnected, they are exposed to a wide range of cybersecurity threats. Unlike traditional information systems, these environments handle highly sensitive technical data that directly influences product performance, safety, and regulatory compliance. Cyber incidents in this context do not only result in data loss but can also lead to physical product failures and long-term damage to organizational credibility.

Intellectual Property Theft

Product design data is among the most valuable assets of manufacturing organizations. CAD models, design calculations, material specifications, and process parameters represent years of research, experimentation, and financial investment. Cyberattacks targeting this information are therefore often motivated by economic gain rather than simple system disruption.

Attackers may exploit vulnerabilities in CAD, CAE, or PLM platforms, particularly when these systems are accessed through cloud environments or remote connections. Insecure file-sharing practices, weak authentication mechanisms, and outdated software versions increase the likelihood of unauthorized access. Once obtained, stolen design data can be used to create counterfeit products, reduce competitors' development costs, or undermine market advantage. Intellectual property theft is especially damaging in industries with short product life cycles, where early access to design information can significantly impact market share. In some cases, organizations may remain unaware of the theft until similar products appear in the market. The lack of visibility makes such attacks difficult to detect and respond to in a timely manner.

Data Manipulation and Integrity Attacks

While data theft focuses on confidentiality, integrity attacks target the accuracy and reliability of design and quality data. In these attacks, malicious actors intentionally alter information

without necessarily removing it from the system. Modified tolerances, incorrect material grades, or altered testing parameters can compromise product functionality and safety.

Integrity attacks are particularly dangerous because they may bypass traditional security and quality controls. Small changes in design values may not trigger immediate alarms or deviations, especially in complex systems with numerous variables. As a result, defective products may progress through development and manufacturing stages without detection.

In quality systems, manipulated inspection records or falsified test results can create a false sense of compliance. This may lead to products being released to the market without meeting regulatory or customer requirements. In safety-critical applications, such undetected changes can have serious consequences, including equipment failure, recalls, or safety incidents. The delayed nature of detection makes root cause analysis more difficult and costly.

Supply Chain Cyber Risks

Modern product development relies heavily on collaboration with suppliers, contractors, and service providers. Design data, quality requirements, and compliance documentation are often shared across organizational boundaries. While this improves efficiency and flexibility, it also increases exposure to cyber risks originating outside the organization's direct control.

A supplier with weak cybersecurity practices can become an entry point for attackers. Compromised supplier design files, infected software updates, or falsified quality certificates can easily propagate through integrated systems. In some cases, attackers deliberately target smaller suppliers, knowing that they often lack robust security controls.

Supply chain cyber risks are particularly challenging to manage due to limited visibility and varying security maturity levels among partners. Even if the primary organization maintains strong cybersecurity measures, vulnerabilities in the extended supply chain can undermine overall product quality and trust. Ensuring secure data exchange and verifying the authenticity of supplier-provided information are therefore critical quality concerns.

Ransomware and System Disruption

Ransomware attacks have emerged as one of the most disruptive cybersecurity threats to digital

design and quality systems. These attacks typically involve encrypting critical data and demanding payment in exchange for restoration of access. When design databases, PLM platforms, or QMS systems are affected, normal operations may come to a complete halt.

Disruption of design activities can delay product development schedules and increase costs. Similarly, the unavailability of QMS data can interrupt audits, production approvals, and regulatory submissions. In highly competitive markets, even short delays can result in missed opportunities and loss of customer confidence.

Beyond operational impact, ransomware incidents can damage an organization's reputation, especially if sensitive design or quality data is exposed. Recovery efforts often require significant resources, including system restoration, data validation, and process requalification. These activities divert attention from innovation and continuous improvement, further affecting long-term performance.

CYBERSECURITY AS A QUALITY ATTRIBUTE

Quality in manufacturing and product development has traditionally been associated with attributes such as functionality, performance, reliability, safety, durability, and compliance with standards and regulations. These attributes focus primarily on physical and functional aspects of the product. However, as products and quality systems become increasingly digital and interconnected, cybersecurity has emerged as an equally important dimension of quality.

In digital environments, a product that meets all functional requirements but is vulnerable to cyber threats cannot be considered fully fit for use. Cybersecurity weaknesses can compromise product behavior, expose sensitive customer data, or allow unauthorized control of connected products. From the customer's perspective, security failures often translate directly into quality failures, even if the product performs well under normal operating conditions. As a result, cybersecurity must be recognized as an intrinsic quality attribute rather than a separate technical concern.

Regulatory bodies and industry stakeholders are also beginning to treat cybersecurity as part of product quality and safety. In sectors such as automotive, medical devices, and industrial equipment, cyber vulnerabilities may lead to non-compliance, recalls, or legal liabilities.

Quality systems that fail to address cybersecurity risks may therefore fall short of meeting evolving regulatory and market expectations.

Integrating cybersecurity into quality thinking requires a fundamental shift in organizational mindset. Traditionally, security controls were implemented after product development, often as corrective actions in response to incidents. In contrast, modern quality approaches emphasize prevention over detection. Cybersecurity controls should be incorporated from the earliest stages of product design, process planning, and quality system development. This proactive approach reduces the likelihood of vulnerabilities being introduced into products and processes.

The concept of secure-by-design aligns closely with established quality principles such as defect prevention and right-first-time design. By identifying potential cyber risks during design reviews, risk assessments, and failure mode analyses, organizations can implement appropriate controls before products are released. This reduces dependency on inspections, patches, and reactive fixes, which are often costly and less effective.

Continuous improvement also plays a key role in treating cybersecurity as a quality attribute. Cyber threats evolve over time, and security measures must be regularly reviewed and updated. Integrating cybersecurity metrics into quality performance indicators allows organizations to monitor security effectiveness alongside traditional quality measures. Lessons learned from cyber incidents can be analyzed using established quality tools such as root cause analysis and corrective action processes.

Ultimately, recognizing cybersecurity as a quality attribute strengthens the overall quality management system. It ensures that products are not only functional and compliant at the time of release but remain safe, reliable, and trustworthy throughout their lifecycle. This integrated view supports long-term customer satisfaction, regulatory confidence, and sustainable product development in an increasingly digital manufacturing environment.

INTEGRATION OF CYBERSECURITY WITH QUALITY MANAGEMENT SYSTEMS

The increasing reliance on digital tools in product development requires cybersecurity to be

closely integrated with quality management systems rather than treated as a separate technical function. Quality management systems provide structured processes for planning, execution, monitoring, and improvement, making them well suited to manage cybersecurity-related risks. Integrating cybersecurity within QMS frameworks helps ensure that security considerations are consistently applied across the product lifecycle and aligned with organizational quality objectives.

Secure-by-Design and Quality-by-Design

Secure-by-design is based on the principle that cybersecurity requirements should be defined and implemented during the earliest stages of product development. Instead of reacting to vulnerabilities after product release, security controls are embedded into product architecture, design tools, and development workflows. This approach reduces the likelihood of critical vulnerabilities being introduced and minimizes the cost of later corrective actions.

Quality-by-design follows a similar philosophy, emphasizing the prevention of defects through systematic process planning and control. Rather than relying heavily on inspection and testing, quality-by-design focuses on understanding process variability and designing robust processes that consistently produce acceptable outcomes. When secure-by-design and quality-by-design are combined, cybersecurity becomes an integral part of overall product quality.

In practice, this integration means that cybersecurity requirements are treated as quality requirements. Design inputs may include access control needs, data protection criteria, and secure communication protocols. Design reviews can evaluate both functional performance and security robustness. By embedding cybersecurity into established quality planning activities, organizations can ensure that security is not overlooked or deprioritized under schedule or cost pressures.

Risk-Based Thinking

Risk-based thinking is a central principle of modern quality management standards and provides a natural framework for integrating cybersecurity. Rather than applying uniform controls across all processes, risk-based thinking encourages organizations to identify, assess, and prioritize risks based on their potential impact.

Cyber risks should be explicitly included in design risk assessments and process evaluations. Tools such as failure mode and effects analysis (FMEA) can be extended to consider cybersecurity-related failure modes, such as unauthorized access, data manipulation, or system unavailability. The severity, occurrence, and detectability of these risks can be evaluated in relation to product quality, safety, and compliance.

By incorporating cyber risks into existing quality risk management tools, organizations can prioritize security controls where they matter most. For example, design data related to safety-critical components may require stronger access restrictions and validation controls compared to non-critical information. This targeted approach improves efficiency while maintaining adequate protection.

Risk-based thinking also supports proactive decision-making. Emerging cyber threats can be monitored and assessed as part of management review processes, allowing organizations to adjust controls before incidents occur. In this way, cybersecurity becomes part of the continuous improvement cycle rather than a reactive response to failures.

Documentation and Traceability

Documentation and traceability are fundamental elements of effective quality management systems. Digital QMS platforms provide structured mechanisms to record design decisions, changes, approvals, and quality actions throughout the product lifecycle. These records are essential for demonstrating compliance, supporting audits, and enabling root cause analysis.

Cybersecurity controls play a critical role in protecting the integrity and reliability of QMS documentation. Access management ensures that only authorized personnel can create, modify, or approve quality records. Digital signatures and approval workflows help verify the authenticity of design changes and quality decisions. Audit trails provide visibility into who accessed or altered records and when those actions occurred.

Tamper-resistant documentation is particularly important in regulated industries, where quality records may be reviewed by external auditors or regulatory authorities. Any compromise in data integrity can undermine confidence in the entire quality system. By integrating cybersecurity measures into QMS documentation practices, organizations can strengthen trust

in their records and processes.

Furthermore, secure documentation supports continuous improvement. Reliable data allows quality teams to analyze trends, identify recurring issues, and implement effective corrective actions. When cybersecurity incidents are documented and managed through the same QMS processes used for quality issues, organizations can apply familiar improvement tools and methodologies, reinforcing a unified approach to quality and security management.

STANDARDS AND FRAMEWORKS SUPPORTING CYBERSECURITY

The growing importance of cybersecurity in product design and quality systems has led to the development and adoption of several international standards and frameworks. These standards provide structured guidance for managing cyber risks, protecting sensitive information, and ensuring consistent implementation of security controls across organizational processes. When aligned with quality management principles, they help organizations embed cybersecurity into everyday design and quality activities.

One of the most widely recognized standards in this domain is ISO/IEC 27001, which focuses on establishing, implementing, and maintaining an information security management system (ISMS). The standard adopts a systematic and risk-based approach to managing information security, covering areas such as access control, asset management, incident response, and continuous improvement. For organizations involved in product design, ISO/IEC 27001 provides a foundation for protecting design data, quality records, and intellectual property throughout their lifecycle.

ISO 9001, on the other hand, emphasizes quality management through process control, customer focus, and risk-based thinking. Although it does not explicitly address cybersecurity, many of its requirements are directly relevant to managing cyber risks. Clauses related to risk assessment, documented information, control of changes, and performance evaluation can be extended to include cybersecurity considerations. By integrating ISO/IEC 27001 controls within an ISO 9001-based QMS, organizations can ensure that security risks are treated with the same rigor as traditional quality risks.

In addition to these general management system standards, several industry-specific

frameworks address cybersecurity in greater detail. In the automotive sector, cybersecurity standards focus on protecting vehicle electronics, software, and communication systems from cyber threats. These standards recognize that cyber vulnerabilities can directly impact product safety and reliability. Similarly, standards for industrial automation and control systems address security risks associated with connected machinery, sensors, and manufacturing networks.

Such sector-specific standards are particularly important because they consider the operational context of products and processes. They address real-world threats such as unauthorized access to control systems, manipulation of operational parameters, and disruption of production processes. When applied alongside quality standards, they help ensure that cybersecurity measures are practical, relevant, and aligned with product and process requirements.

Alignment between cybersecurity and quality standards offers several advantages. It reduces duplication of effort by allowing organizations to use common processes for risk assessment, documentation, auditing, and management review. Instead of treating cybersecurity as a standalone technical issue handled only by IT departments, it becomes part of the overall management system involving design, quality, operations, and leadership.

Integrated frameworks also support better communication and accountability across functions. Quality managers, design engineers, and cybersecurity specialists can work within a shared structure, using common terminology and objectives. This integrated approach improves consistency, reduces gaps in control, and enhances organizational resilience.
Overall, standards and frameworks play a critical role in supporting the effective integration of cybersecurity into product design and quality systems. When properly aligned, they provide a structured and scalable approach to managing cyber risks while reinforcing core quality principles such as prevention, traceability, and continuous improvement.

TECHNOLOGIES ENABLING CYBERSECURE DESIGN AND QUALITY SYSTEMS

Access Control and Identity Management

Role-based access control ensures that users can only access relevant design and quality data. Strong authentication mechanisms reduce the risk of unauthorized access.

Encryption and Data Protection

Encryption of design files, quality records, and data transmissions protects sensitive information from interception or tampering. This is especially important in cloud-based environments.

Monitoring and Incident Response

Continuous monitoring of system activity helps detect unusual behavior and potential breaches. Integration with QMS processes allows cybersecurity incidents to be treated similarly to quality incidents, with root cause analysis and corrective actions.

Table 1: Cybersecurity Risks Across Product Lifecycle Stages

Product Lifecycle Stage	Key Cyber Risks	Impact on Quality
Concept & Design	IP theft, data manipulation	Incorrect specifications
Development & Testing	Malware, unauthorized changes	Invalid test results
Manufacturing	System disruption	Process deviations
Distribution & Service	Data breaches	Loss of customer trust

CHALLENGES IN IMPLEMENTATION

Despite growing awareness, many organizations struggle to integrate cybersecurity into product design and quality systems. Limited expertise, budget constraints, and cultural resistance are common barriers. Small and medium enterprises often lack dedicated cybersecurity teams and rely on basic controls that may not be sufficient.

Another challenge is balancing security with usability. Overly restrictive controls can slow down design activities and discourage collaboration. Therefore, organizations must carefully design security measures that support, rather than hinder, quality objectives.

FUTURE TRENDS

Emerging technologies such as artificial intelligence, blockchain, and digital twins offer new opportunities to enhance cybersecurity in product design and quality systems. AI-based monitoring can detect anomalies in design data, while blockchain can improve traceability and trust in quality records. However, these technologies also introduce new risks and require

careful governance.

Regulatory expectations related to product cybersecurity are also increasing. Organizations that proactively integrate cybersecurity into quality systems will be better positioned to meet future compliance requirements and customer expectations.

CONCLUSION

Cybersecurity has become an essential component of product design and quality management systems in the digital era. As design and quality processes become more interconnected and data-driven, the potential impact of cyber threats on product integrity, safety, and compliance increases significantly. This paper has highlighted key cybersecurity risks across the product lifecycle and emphasized the importance of integrating security principles into quality management practices.

By adopting secure-by-design and risk-based approaches, organizations can align cybersecurity with traditional quality objectives. Standards, technologies, and continuous improvement practices provide a structured path for implementation. While challenges remain, particularly for smaller organizations, the integration of cybersecurity into product design and quality systems is no longer optional. It is a critical requirement for delivering reliable, compliant, and trustworthy products in an increasingly digital and connected world.

REFERENCES

1. ISO 9001:2015, *Quality Management Systems – Requirements*, International Organization for Standardization.
2. ISO/IEC 27001:2022, *Information Security Management Systems*, International Organization for Standardization.
3. Boyes, H., *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2015.
4. Stouffer, K., Pillitteri, V., *Guide to Industrial Control Systems Security*, NIST Special Publication 800-82.
5. McKinsey & Company, *Cybersecurity in Manufacturing and Product Development*, Industry Report, 2020.
6. IEC 62443, *Industrial Communication Networks – IT Security for Networks and*

Systems, IEC.

7. Kshetri, N., "Cybersecurity and Supply Chain Risk Management," *Journal of Business Strategy*, 2018.
8. Juran, J.M., Godfrey, A.B., *Juran's Quality Handbook*, McGraw-Hill, 2010.
9. ENISA, *Cybersecurity Challenges in Manufacturing*, European Union Agency for Cybersecurity, 2019.
10. Lee, J., Bagheri, B., Kao, H.A., "A Cyber-Physical Systems Architecture for Industry 4.0," *Manufacturing Letters*, 2015.