DIGITAL TRANSFORMATION IN LOGISTICS AND SUPPLY CHAIN MANAGEMENT

EDITOR Matevž Obrecht

University of Maribor Press

University of Maribor

Faculty of Logistics

Digital Transformation in Logistics and Supply Chain Management

Editor
Matevž Obrecht

January 2026

Title **Digital Transformation in Logistics and Supply Chain Management**

Editor Matevž Obrecht
(University of Maribor, Faculty of Logistics)

Review Benjamin Marcen
(University of Maribor, Faculty of Logistics)

Jure Erjavec
(University of Ljubljana, Faculty of Economics)

Translation Nena Orel Šanko
(University of Maribor, Faculty of Logistics)

Language editing Kirsten Hempkin
(University of Maribor, Faculty of Logistics)

Technical editor Jan Perša
(University of Maribor, University of Maribor Press)

Cover designer Jan Perša
(University of Maribor, University of Maribor Press)

Cover graphic Logistics web, avtor: Gerd Altmann, pixabay.com, 2023

Graphic material Sources are own unless otherwise noted.
The authors and Obrecht (editor), 2026

Published by *Založnik* **University of Maribor**
University of Maribor Press
Slomškov trg 15, 2000 Maribor, Slovenia
https://press.um.si, zalozba@um.si

Issued by *Izdajatelj* **University of Maribor**
Faculty of Logistics
Mariborska cesta 7, 3000 Celje, Slovenia
https://www.fl.um.si, info.fl@um.si

Edition First edition. Translation of the original work from the Slovenian language Obrecht, M. (ur.). (2025). *Digitalna transformacija v logistiki in managementu oskrbovalnih verig*. Univerza v Mariboru, Univerzitetna založba. doi: 10.18690/um.fl.3.2025

Publication type E-book

Available at http://press.um.si/index.php/ump/catalog/book/1070

Published at Maribor, Slovenia, January 2026

Project name Vzpostavitev okolja za izobraževanje zelene in digitalne logistike ter oskrbovalnih verig

Project financier The project is co-financed by the Republic of Slovenia, the Ministry of Higher Education, Science and Innovation, and the European Union -

NextGenerationEU. The project is implemented in accordance with the plan within the development area Smart, Sustainable and Inclusive Growth, component Strengthening Competences, in particular Digital and those required by New Professions and the Green Transition (C3 KS), for the investment measure F. Implementation of pilot projects, the results of which will be the basis for preparing the starting points for the reform of higher education for a green and resilient transition in the S.O Company: project Pilot projects for the renovation of higher education for a green and resilient transition. The project is part of the NOO scheme (Recovery and Resilience Plan)

CIP - Kataložni zapis o publikaciji
Univerzitetna knjižnica Maribor

658.286:004(082)(0.034.2)

DIGITAL transformation in logistics and supply chain management [Elektronski vir] / editor Matevž Obrecht ; [translation Nena Orel Šanko]. - 1st ed. - E-publikacija. - Maribor : University of Maribor, University of Maribor Press, 2026

Način dostopa (URL): https://press.um.si/index.php/ump/catalog/book/1070

ISBN 978-961-299-074-9 (PDF)
doi: 10.18690/um.fl.2.2026
COBISS.SI-ID 255052803

ISBN 978-961-299-074-9 (pdf)

DOI https://doi.org/10.18690/um.fl.2.2026

Price Free copy

For publisher Prof. Dr. Zdravko Kačič,
Rector of University of Maribor

Attribution Obrecht, M. (ed.). (2026). *Digital Transformation in Logistics and Supply Chain Management*. University of Maribor, University of Maribor Press. doi: 10.18690/um.fl.2.2026

University of Maribor Press

Table of Contents

DIGITALIZATION – PLANNING

BORUT JEREB
University of Maribor, Faculty of Logistics, Celje, Slovenia
borut.jereb@um.si

E-business plays a crucial role in the modern digital environment, transforming business practices and opening new possibilities. The model of the e-business value chain is presented, encompassing supporting processes, the value chain, and technological solutions. Additionally, various e-business approaches are addressed, including e-marketing, e-documentation, e-payments, and e-customer management. The importance of information and cyber security in the contemporary business environment is emphasized. Safeguarding the digital landscape becomes crucial, with information security covering the protection of information, while cyber security addresses the protection of digital systems from cyber threats. Both disciplines are essential for maintaining trust and security in e-business. The article concludes with the presentation of IT risk management using the ISO/IEC 27005 standard.

DOI
https://doi.org/10.18690/um.fl.2.2026.1

ISBN
978-961-299-074-9

Keywords:
digitalization,
e-business,
information security,
cyber security,
IT risks

University of Maribor Press

1 Introduction

In the rapidly changing environment of the digital age, electronic business or e-business has emerged as a paradigm that is changing the way organizations conduct their operations and communicate with stakeholders. For businesses, e-business refers to the use of digital technologies and the Internet to simplify and improve various business processes from buying and selling goods and services to managing internal operations and collaborating with partners. In commerce, unlike traditional business models, e-business transcends geographical and time constraints by providing a global platform for trade.

E-business encompasses a wide range of online activities, including e-commerce, e-marketing, e-supply chain management, and e-procurement. The integration of technology not only enables more efficient and cost-effective business practices but also opens up new opportunities for innovation and market adaptation.

Key elements of e-business include establishing an online presence, conducting secure electronic transactions, leveraging data analytics for informed decision-making, and adapting to an ever-changing digital environment. A company's success in an e-business environment depends on its ability to create seamless and engaging customer experiences, to establish trust and security in online transactions, and to leverage insights gleaned from (often massive) data to stay competitive in a dynamically changing marketplace.

As technology continues to advance and change, e-business will play an increasingly important role in shaping the future of business within and between companies – especially when it comes to supply chains. Whether you're a startup or an established multinational, understanding and harnessing the power of e-business is key to succeeding in the digital economy. In doing so, companies must not only overcome technological challenges but also the changing expectations of connecting with digitally savvy employees and customers inside and outside the company.

In the following, we want to guide the reader on a path to becoming able to:

- review and analyze that part of the business in its environment that would make sense to digitize,

- recognize the importance of information and cybersecurity security and be able to plan them in the role of the middle management
- critically evaluate IT risks in the role of the middle management.

2 E-business

E-business is a comprehensive approach to conducting business processes using electronic means. This also applies to the implementation of business processes that support the implementation of logistics processes. E-business encompasses a wide range of activities that leverage digital technologies to optimize operations, improve customer experience, and increase overall business efficiency. E-business also encompasses both the internal and external interactions of organizations and seeks to transform traditional business practices by connecting electronic systems and communication channels. The concept of e-business is changing the way organizations conduct their operations, communicate with customers, and create value. It constitutes a comprehensive shift toward conducting business processes using electronic means, ultimately driving efficiency, innovation, and global reach.

The origins of e-business date back to the early days of the Internet. With the emergence of e-business (e-commerce), the idea of buying and selling products online emerged. However, over time, the idea of e-business has also evolved to encompass a multitude of activities that extend far beyond digital stores.

E-business thus consists of business that relies on information and communication technologies (ICT). Some of the key areas of such business are:

- **E-marketing**: The use of digital channels such as: social media, email marketing, search engine optimization (SEO), and online advertising to promote products or services and reach a wider audience.
- **E-commerce**: As mentioned above, e-commerce is an important part of e-business. It involves the online buying and selling of goods and services and encompasses various business models and platforms.
- **E-customer relationship management (e-CRM)**: The management and nurturing of customer relationships using digital tools and platforms. This includes tracking customer interactions, analyzing data to customize customer experience, and providing effective online customer support.

- **E-Supply Chain Management (e-SCM)**: The use of digital technologies to optimize supply chain processes: from procurement and inventory management to order fulfilment and distribution.
- **E-Procurement**: The use of electronic systems to manage the procurement of goods and services, including supplier selection, order placement, and supplier relationship management.
- **E-Collaboration**: Enabling collaboration between employees and partners through digital platforms, videoconferencing, and cloud-based tools.
- **E-Knowledge Management**: Managing and sharing organizational knowledge electronically to improve decision-making, problem-solving, and innovation.
- **E-Data Analytics and Business Intelligence**: The use of data analytics tools to extract insights from large data sets, enabling data-driven decision-making.
- **E-Payments and Financial Transactions**: Processing electronic payments, online invoicing, and securely managing financial transactions through digital platforms.

The following are some of the benefits that are conditioned by the characteristics of e-business. The key components and impacts of e-business are:

- **Digital transformation:** e-business has accelerated the process of digital transformation across industries. Organizations have moved from traditional businesses to integrated digital ecosystems that streamline processes, improve customer experience, and increase overall efficiency.
- **Global reach:** e-business allows companies to reach a global audience without the constraints of geographical boundaries.
- **Cost-effectiveness:** Digital processes can reduce operational costs such as paper-based documentation and physical infrastructure. We are witnessing new economic models and employment opportunities. Startups and entrepreneurs can enter into and participate in global markets with minimal barriers to entry, which stimulates economic growth.
- **Customer/Partner Focus:** e-business enables personalized interactions, rapid responses, and convenient access to information, which increases customer satisfaction. Customers and/or partners are at the center of (business) operations. With the help of data driven analytics, organizations understand the

desires, behaviors, and needs of customers and partners, which leads to personalized interactions and offerings.

- **Optimized Processes:** Automation of tasks and processes leads to greater efficiency and reduced human error. Automation, integration and digitalization of processes increase operational efficiency. From supply chain management to inventory control and order processing, e-business optimizes resource utilization and reduces costs.
- **Big Data Insights and Data-Driven Decision Making:** e-business generates valuable data that can be analyzed to gain insights into customer behavior, market trends, and business performance.
- **Competitive advantage:** Organizations that adopt e-business strategies are better positioned to adapt to changing market conditions and outperform the competition.
- **Innovation and agility:** E-business fosters an environment of innovation. Organizations quickly adapt to changing market dynamics, introduce new services and products, and test new business models without delay, quickly and in near real time.

Thus, e-business encompasses various aspects of modern business operations that leverage digital technologies to improve efficiency, customer engagement, and overall competitiveness. It is about adopting a holistic approach to managing business in the digital age.

While e-business offers numerous advantages, such as greater reach, cost savings, and convenience, it also has several negative aspects that companies need to consider and address to ensure sustainable and successful online business. This includes investing in robust security measures, efficient logistics management, ensuring compliance with legal regulations, and building customer trust and satisfaction with reliable services and secure transactions.

Some of the key negative aspects of e-business that need to be addressed with particular care in e-business are:

- **Security challenges**: E-business involves the transfer of sensitive data, including financial transactions and personal information. This means that e-business is a target for cyber-attacks such as hacking, phishing, and malware.

Businesses need to invest heavily in cybersecurity to protect data, which can be expensive and complex.

- **Privacy challenge:** With the collection of vast amounts of consumer data, serious privacy concerns arise. Companies need to ensure that they comply with data protection regulations such as GDPR. Failure to comply with these regulations can result in legal consequences and loss of customer trust.
- **Technical issues:** E-business is heavily technology driven. Technical issues such as website downtime, software bugs or slow loading can disrupt business, leading to lost sales and dissatisfied customers.
- **High start-up costs:** Setting up a robust e-business infrastructure can be expensive. This includes the cost of developing a user-friendly website, operating secure payment systems and integrating the necessary back-end systems. These initial investments can be a barrier for small businesses.
- **Intense competition:** In many business segments, the internet has leveled the playing field for companies large and small. Increased competition makes it harder for companies to stand out and attract customers, often requiring significant investments in marketing and differentiation strategies.
- **Logistics challenges:** E-business businesses need to pay extra attention to managing their logistics processes. This includes warehousing, inventory management, shipping, and returns processing. Poor logistics management can lead to delivery delays and increased costs, which negatively impacts customer satisfaction.
- **Technology dependency:** In e-business, businesses are highly dependent on technology, meaning that any technological failure can bring their business to a standstill. Businesses need to have robust IT support and disaster recovery plans in place to mitigate IT risks.
- **Customer trust and satisfaction:** Building trust with customers is more challenging online than in brick-and-mortar stores. Issues such as the inability to physically inspect products before purchase, concerns about payment security, and delays in responding to customer inquiries can all reduce customer satisfaction.
- **Legal and regulatory compliance:** In e-business, businesses must contend with a complex web of regulations that vary by region and industry. These include consumer protection laws, e-business regulations, and international trade laws. Non-compliance can lead to fines and other difficulties in meeting legal norms.

- **Lack of personal interaction:** The lack of personal interaction in e-business makes it difficult to build deeper relationships with customers. Personalized service and the human touch often play a key role in customer loyalty and satisfaction.
- **Returns and refund management:** Managing returns and refunds in e-business can be more complex and expensive than in traditional retail. The process involves handling reverse logistics, restocking, and dealing with possible loss or damage to returned items.
- **Digital divide:** Not all potential customers have equal access to the internet or digital devices, leading to a digital divide. This limits the reach of e-business businesses, especially in regions with low internet penetration or among demographic groups with lower levels of technological literacy.

2.1 E-business model

Figure 2.1 shows the e-business value chain model from Meier & Stormer (2009). The figure shows the three essential components of e-business, which are:

- support processes for implementing e-business,
- e-business value chain,
- technical and technological solutions to support the implementation of e-business.

The supporting processes consist of: strategic planning, organizational and human resources, information and cybersecurity management, control, and cultural diversity management. All of these processes are conditional and related to e-business. We assume that knowledge about these processes is already present or needs to be acquired from management literature.

The value chain consists of seven different approaches, which complement each other. Within each of the aforementioned approaches, it is possible to find other approaches. However, on the left side of this value chain, approaches that require lower inputs, as a rule, also produce lower value results. The further we go to the right, the greater the inputs for the realization of the solution and the greater the expected benefits.

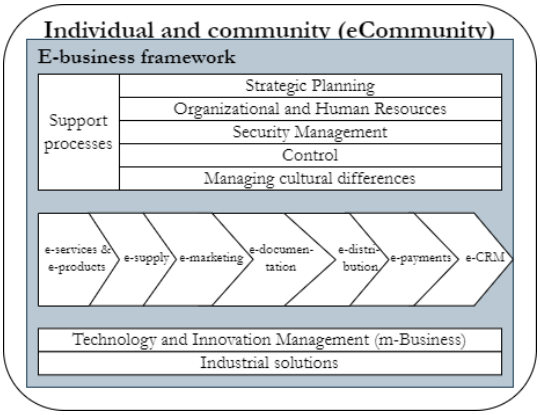


Figure 1.1: E-business model
Source: Summarized by Meier & Stormer, 2009.

In the organization of electronic products and services, the organization is required to find an appropriate form of cooperation using a business model. Such forms of cooperation between organizations and potential buyers range from simple and informative presentation of goods, open markets with goods and their values, to more closed systems where the stakeholders of such a market cooperate with each other.

The next approach in e-business is intended for electronically supported purchasing processes. In principle, there are a number of solutions for e-procurement. Solutions differ from each other depending on whether product and service catalogs for the selection and purchase of products are available on the buyer's side (buy side) or on the supplier's side (sell side). In the third variant (electronic market), a third party provides software solutions and catalogs for purchasing. This allows comparisons and evaluation of products and services. Catalog management presents a special challenge.

E-marketing (or online marketing) works by exploiting market potential and nurturing business relationships through electronic means of obtaining information and communication. Segmenting online »customers« into categories enables the implementation of a diverse marketing process and immediate adaptation of online marketing services. The first successful global example of this type of e-business was Google, with Facebook and others following. With appropriate key indicators, they enable the measurement of the effectiveness of online offers (for example, using a

web browser), can calculate interaction rates (if we say that the other side is an online consumer), encourage online customers to create their (possibly virtual) values, carry out business transactions (online customer) and maintain connections with the customer (online key customer). Of course, in this process, it is necessary to study and analyze the specifics of online advertising.

The next approach deals with the concept of e-documentation. Here, an electronic document is considered a legally valid document. To achieve this, it is necessary to establish trusted centers that register real persons, issue digital certificates and provide a pair of electronic keys for digital signatures. Asymmetric cryptographic procedures using private and public keys are a basic requirement for the use of such certificates and signatures. Electronic documents can be electronically signed on the one hand while digital signature authentication can be performed on the other. Documents can also be appropriately converted into an electronic cryptogram, which protects the document relatively well from unwanted views.

In the case of the electronically supported distribution of a product or service, which can be in physical or electronic form, we encounter the next level of complexity of electronic commerce. If the consumer has a mobile device with an Internet connection at hand for the service, he can take advantage of a time- and location-independent purchase or service (online distribution). Of course, products in electronic form can also be distributed in a classic way - that is, not electronically, since offline distribution on the World Wide Web also has its advantages. In addition, hybrid distribution forms can be presented that combine online distribution with a version of offline distribution. Distribution is only part of the complete supply chain. In e-delivery, it is necessary to coordinate the steps of planning, purchasing, production and delivery of products and services using a reference model.

Electronic payments (e-payments) allow for the payment of small amounts involving only a few cents (picopayment), medium amounts of a few euros (micropayment) and larger amounts (macropayment). To ensure that the transaction costs for picopayments and micropayments are low enough to be worthwhile, methods based on the use of electronic coins have been developed. In addition, there are several accounting and proprietary procedures for electronic payments. In order to ensure the security of electronic payment procedures, cryptographic procedures and digital signatures must be used. For example, the SET (Secure Electronic Transaction)

protocol requires the use of a double signature procedure so that both the order data (regarding the merchant) and the payment methods (regarding the bank) are protected.

In e-Customer Relationship Management, the focus shifts from the products themselves to customer management. In addition to the usual key financial indicators, what becomes especially important is that customers, buyers or stakeholders in general need to be captured and evaluated. Relevant data is stored in a customer data warehouse, which allows for a comprehensive analysis of customer behavior. In addition to analytical customer relationship management, we also use multi-channel management, which presents a special challenge, as it is necessary to evaluate different communication channels with customers and determine which ones are suitable for use. This e-business approach requires the highest investment in implementation but can also provide the highest returns. These returns can be measured in money or in other ways - for example, in knowledge of behavior. Recently, great efforts have been made in the EU especially to limit the collection of data/information on individuals (customers) by both individual companies and other organizations (for example, intelligence services).

3 Information and cybersecurity

Securing the digital landscape in a rapidly changing digital age, where information and data are at the heart of modern operations, means that information security and cybersecurity have become crucial. These two intertwined disciplines are designed to ensure the availability, integrity and confidentiality of digital information and protect individuals, organizations and societies from the expanding world of cyber threats (Jereb, 2019). The following presents the general importance of cybersecurity in the light of planning and implementing business digitization.

Information security encompasses the strategies, practices, and technologies implemented to protect information from unauthorized access, use, disclosure, interference, alteration, or destruction. It involves a holistic approach that encompasses people, processes, and technology. The most important key aspects of information security include:

- **availability:** ensuring that information and services are accessible and usable when needed,
- **integrity:** maintaining the accuracy and trustworthiness of data by preventing unauthorized changes,
- **confidentiality:** ensuring that information is accessible only to authorized individuals or entities,
- **authentication and authorization:** verifying the identity of users and assigning the appropriate level of access,
- **data encryption:** converting data into an unreadable format to prevent unauthorized access,
- **risk/vulnerability management:** identifying and addressing vulnerabilities that attackers could exploit,
- **employee training:** educating employees about security best practices and potential risks.

Cybersecurity focuses on protecting digital systems, networks, and devices from cyber threats. These threats encompass a wide range of malicious activities, including hacking, malware, ransomware, fraud, and more. Key elements of cybersecurity include:

- **Network Security:** Protecting computer networks from unauthorized access, data breaches, and other cyberattacks,
- **Endpoint Security:** Securing individual devices (computers, smartphones, IoT devices) from malware and other cyberthreats,
- **Incident Response:** Developing strategies to effectively respond to cyber incidents and reduce their impact,
- **Threat Intelligence:** Collecting and analyzing information about emerging threats to anticipate and mitigate attacks,
- **Security Audit and Monitoring:** Regularly assessing and monitoring systems for signs of intrusions or suspicious activity,
- **Cybersecurity Policies and Procedures:** Creating guidelines and protocols to ensure consistent and effective security measures.

In today's world, with interconnected organizations of all types and sizes, the importance of information security and cybersecurity cannot be overstated.

Cyberattacks have the potential to disrupt critical infrastructure, compromise personal data, and harm national security. The challenges in these areas are constantly evolving due to the increasing sophistication of cybercriminals, rapid advances in technology, and the ever-increasing number of attack vectors.

In addressing information and cybersecurity, we face challenges that we try to overcome with some generally accepted strategies to ensure a secure digital environment. The most important of these strategies are proactive and comprehensive approaches that organizations and individuals must adopt, including:

- **Education and training:** Continuous training and awareness programs are essential to empower individuals to identify and respond to cyber threats,
- **Advanced technologies: Strategies** such as artificial intelligence and machine learning are used to detect/prevent cyber threats in real time,
- **Collaboration:** Sharing information and communicating threats and best practices between organizations (including governments) to strengthen shared cybersecurity,
- **Rules and compliance:** Adhering to cybersecurity regulations and standards to improve data protection and privacy,
- **Resilience planning:** Developing incident response and disaster recovery plans to reduce the impact of cyber incidents.

A more detailed description of ensuring security against IT threats and attacks is presented in the chapter on information and computer security.

4 IT risk and investment management

When establishing a security management system, organizations must ensure systematic risk management, which must be consistent with the needs, policies and environment in which the organization operates. Ultimately, the management of individual (operational, IT, exchange rate, etc.) risks must be consistent with the management of all risks that the organization faces. Security policies relate to the timely and effective management of risks in areas where and when necessary. It is a process that must be established and, once established, continuously implemented and supplemented.

IT risk management is a key component of overall risk management in an organization. It involves identifying, assessing and mitigating risks associated with information technology to ensure the availability, confidentiality and integrity of information and systems. The key aspects of IT risk management are presented in Figure 1.2. They are summarized in ISO/IEC 27005:2022 (*ISO/IEC 27005*, 2022), which is a standard that describes the risk management process and its activities to ensure information security.

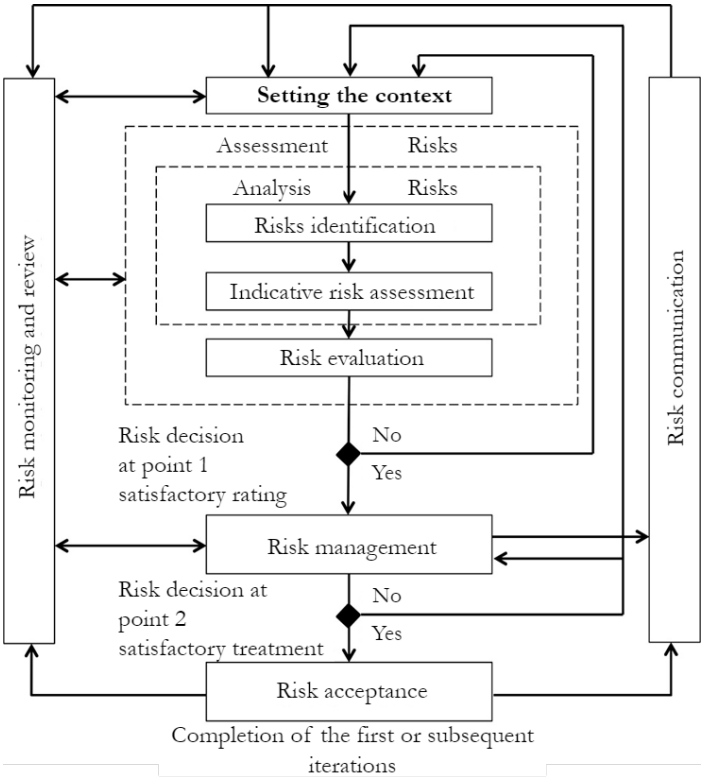


Figure 1.2: Information risk management activities
Source: (Jereb, 2019).

The highest management level of the organization must be responsible for implementing the information security policy and security system. In doing so, it implements the information risk management process in a way that considers the criterion of damage reduction. A very rough estimate is that when ensuring the availability, integrity and confidentiality of information, it takes into account the

business impact of a potential security incident on the business and the realistic probability of an information incident occurring (Jereb, 2019).

Since it is not practical to completely avoid risks, or eliminate them completely, we need to come to terms with them and learn to manage them. When managing risks, organizational leaders make decisions according to the following options:

- the risk needs to be reduced,
- the risk is accepted without additional action,
- the risk is avoided,
- the risk is transferred to contractual or third parties.

Information risk management according to ISO 27005 consists of the following activities, which are also shown in Figure 2.2 (*ISO/IEC 27005*, 2022):

- **Setting the** context in which we try to define the risk management framework.
- **Risk assessment:** where we try to evaluate the level of risk. This set contains two activities:
    - **risk analysis**, which is again divided into:
        - **risk identification,**
        - **risk assessment framework,**
    - **risk evaluation**,
- **Risk management:** where appropriate measures must be taken to avoid, reduce, transfer or accept risks as they are at a given moment.
- **Risk acceptance:** we decide to take measures related to risks and determine responsibility for identifying risks with justifications.
- **Risk communication:** where we ensure that there is a continuous high-quality exchange of information between all interested publics and risk managers about the existence, nature, form, probability, severity, acceptability and similar risk factors.
- **Monitoring and review:** where risks and their factors are monitored and reviewed to detect any changes within the organization and maintain a comprehensive view of the risk.

The practical application of ISO/IEC 27005 across industries is key to ensuring robust IT risk management. Some hypothetical case studies or examples of how ISO/IEC 27005 could be applied across industries are as follows:

- Financial sector:
  - Scenario: A financial institution or company implementing financial processes wants to improve its information security risk management processes.
  - Application: ISO/IEC 27005 can be implemented to systematically identify and assess risks associated with customer data, financial transactions, and regulatory compliance. The institution can then implement tailored risk management strategies to protect sensitive information and ensure compliance with financial regulations.
- Healthcare sector:
  - Scenario: A hospital is concerned about the security of medical records and medical data.
  - Application: ISO/IEC 27005 provides a framework for conducting a risk assessment of the confidentiality, integrity, and availability of health data. The hospital can use it to identify vulnerabilities, assess potential breaches, and implement measures to protect patient data.
- Manufacturing sector:
  - Scenario: A manufacturing company seeks to secure its intellectual property and production processes.
  - Application: ISO/IEC 27005 can help assess the risks associated with intellectual property theft, supply chain disruptions, and operational disruptions. The company can implement risk mitigation strategies to protect critical assets and ensure the continuity of production processes.
- Information Technology (IT) Services:
  - Scenario: An IT service provider wants to demonstrate to its customers its commitment to information security.
  - Application: ISO/IEC 27005 can be used to comprehensively assess the risks in its IT service portfolio. By identifying and managing the risks associated with data breaches, service disruptions and cyber

threats, the company can strengthen its credibility and demonstrate to its customers its commitment to information security.

- Government agencies:
  - Scenario: A government agency responsible for citizen data wants to strengthen its security measures.
  - Application: ISO/IEC 27005 can guide the agency in assessing the risks associated with the confidentiality of citizen data and the availability of critical services. The agency can develop and implement risk management plans to ensure the secure handling of cross-border information.
- Retail:
  - Scenario: A retailer is concerned about the security of customer payment data.
  - Application: ISO/IEC 27005 can help a retailer identify risks associated with payment processing, point-of-sale systems, and online transactions. By implementing security controls and regularly assessing risks, a company can build customer trust and protect financial transactions.

In any case, it is crucial to tailor the use of ISO/IEC 27005 to the specific IT risks and industry requirements. This includes understanding the unique assets, threats and vulnerabilities relevant to each sector and implementing effective strategies to manage IT risks and mitigate potential negative impacts.

References

ISO/IEC 27005:2022—Information security, cybersecurity and privacy protection—Guidance on managing information security risks (Version 4). (2022). [International standard]. https://www.iso.org/standard/80585.html

Jereb, B. (2019). *Informatika in informacijska varnost: Repetitorij*. Univerza v Mariboru, Fakulteta za logistiko. https://doi.org/10.18690/978-961-286-251-0

Meier, A., & Stormer, H. (2009). *eBusiness and eCommerce: Managing the Digital Value Chain*. Springer. https://www.abebooks.com/9783540893271/eBusiness-eCommerce-Managing-Digital-Value-354089327X/plp

DIGITALIZATION – IMPLEMENTATION

BORUT JEREB
University of Maribor, Faculty of Logistics, Celje, Slovenia
borut.jereb@um.si

Software is intangible, and its creation is still associated with individuals in the digitization of processes. As software has become highly complex, organizations developing and using it face new opportunities and challenges throughout its entire life cycle. ISO/IEC 12207:2011 is a standard that provides a framework for describing the life cycle of software systems based on an interdisciplinary approach. The software life cycle encompasses processes from conception to development or acquisition, through testing, deployment, maintenance, and eventual retirement. Understanding the life cycle helps all stakeholders establish systematic and organized management of software-related work, which is crucial for improving quality and reducing issues in the digitization of business processes. Software quality, crucial for user satisfaction, is reflected in functionality, reliability, performance, usability, maintainability, portability, security, and scalability. ISO/IEC 25010:2017 is a standard defining a comprehensive quality model, enabling the assessment and improvement of software.

DOI
https://doi.org/10.18690/um.fl.2.2026.2

ISBN
978-961-299-074-9

Keywords:
digitalization, software lifecycle, software quality, ISO/IEC 12207, ISO/IEC 25010

University of Maribor Press

1 Introduction

Software consists of a set of instructions used to perform specific tasks on computers. Software is a key component of modern computer systems. It is intangible, meaning that it does not have a physical presence like hardware. In the vast majority of cases, its creation is still associated with an individual (human) or individuals working on a joint project to digitize a process.

Software improves our daily lives and drives technological progress. This can be for work, entertainment, communication or information retrieval. Software plays a central role in the usability of computers and digital devices, enabling the automation of various processes, increasing efficiency and reducing manual labor.

The complexity of software has reached a very high level. As a result, while organizations that create and use software systems are gaining new opportunities on the one hand, they are also on the other hand facing greater challenges. These challenges exist throughout the entire system life cycle and at all levels. ISO/IEC 12207 is a standard that provides a common process framework for describing the life cycle of systems based on an interdisciplinary approach.

The software development life cycle consists of various processes, such as: development, testing, deployment, and decommissioning. The cycle can be iterative, meaning that the phases are not always sequential. For example, developers can return to the planning phase if they encounter problems during implementation. It is important to be aware of and familiar with the software life cycle because this knowledge helps us ensure that software is developed in a systematic and organized manner. This is a prerequisite for improving software quality and reducing the number of problems in all processes of its life cycle.

Software quality is a key aspect of any software development process. It refers to the level of excellence or fitness for purpose of a software product. Software quality is crucial because it directly impacts user satisfaction, reliability, and the overall success of the process being digitized. By focusing on functionality, reliability, performance, usability, maintainability, portability, security, and scalability, developers can deliver reliable software products that meet user expectations and business requirements. Regular testing, user feedback, and quality metrics help ensure continuous

improvement and maintain high standards of software quality. Quality software has high value.

Software quality is therefore crucial in the implementation of all (business) processes, as it ensures that software products meet user expectations and thus provides new value through the digitalization of business. Organizations rely on established standards and frameworks to effectively achieve and assess software quality.

The ISO/IEC 25000 family of standards, also known as the SQuaRE (Software Quality Requirements and Evaluation) series, provides a comprehensive and internationally recognized set of guidelines for software quality management. The ISO/IEC 25000 series includes standards and technical reports that address various aspects of software quality characteristics, including quality models, evaluation procedures, and measurement methods.

ISO/IEC 25010 serves as the foundational standard in a series that defines a comprehensive quality model and a set of quality characteristics. Quality characteristics include functionality, reliability, usability, efficiency, maintainability, and portability. By tracking these characteristics, organizations can assess, measure, and improve the quality of their software products. This framework also provides a systematic approach that enables organizations to define quality requirements and evaluation criteria and select appropriate evaluation techniques.

Because such standards promote consistency and comparability in software quality assessment, they enable effective communication between stakeholders. They help improve decision-making processes, enable effective risk management (including costs), enhance customer satisfaction, and encourage continuous improvement. They enable organizations to achieve greater transparency, reliability, and interoperability in their digitized business processes.

Quality is thus integrated into all software lifecycles in phases such as (among other things):

- **Planning**: Quality aspects should be included in project planning to ensure that quality objectives are met.

- **Testing:** Thorough testing at various stages of the lifecycle ensures that quality standards are maintained.
- **Feedback loops:** Regular feedback from users and stakeholders helps to identify and address quality issues.
- **Continuous improvement:** The software lifecycle includes continuous improvement measures that ensure that quality standards evolve in line with changing needs and technologies.

Both, software life cycle and software quality, are related fields where quality assurance practices are embedded throughout the entire life cycle to ensure reliability, functionality, and high quality of software.

2 Software Lifecycle and ISO/IEC 12207:2017

ISO/IEC 12207:2017 is a standard that is used for the entire life cycle of software systems, products and services, including conceptualization, development, production, use, support and retirement, and for their delivery, either within or outside an organization (*ISO/IEC/IEEE 12207*, 2017). The life cycle processes in this document can be applied concurrently, iteratively and recursively to its component parts.

There is a wide diversity of software in terms of purpose, scope, complexity, size, innovation, adaptability, quantity, locations, life span and development. The standard supports this diversity and does not limit it. It applies to single software systems that are written for a single and unique solution, to software systems for wide commercial or public distribution, and to flexible software systems. It also applies to completely stand-alone software systems and to software systems that are embedded and integrated into other, larger, more complex and comprehensive systems.

Software systems, as covered by this standard, are human-made, and created and used to provide products or services in specific environments for the benefit of users and other stakeholders. Software systems may include the following system elements: hardware, software, data, people, processes (e.g., procedures for providing services to users), procedures (e.g., instructions for operators), objects, services,

materials, and naturally occurring entities. Depending on the user, the software systems considered are products or services.

The perception and definition of a particular software system, its architecture, and its system elements depend on the interests and responsibilities of the stakeholders. A system of interest to one stakeholder may be viewed as a system element within a system of interest to another stakeholder. Furthermore, a system of interest may be viewed as part of the environment for a system of interest to another stakeholder.

The ISO/IEC 12207:2017 standard is used by many organizations and industries worldwide that are involved in the development, maintenance and management of software. The main groups that use this standard are:

- **Informatics and Information Technology**: This standard is most used in the IT industry, where organizations develop software solutions, applications, systems, and services. This includes both large companies that develop software solutions for the public and specialized IT companies.
- **Telecommunications:** The telecommunications industry often uses ISO/IEC 12207 to develop software used in networks and communication devices.
- **Automotive:** The automotive industry uses this standard to develop embedded software in cars, including engine control, safety systems, and infotainment solutions.
- **Healthcare:** In the healthcare industry, the standard is used to develop software for medical devices, electronic health records, and other information systems.
- **Military:** Military organizations use this standard to develop and maintain software for military systems, including intelligence, communication, and control systems.
- **Financial industry:** In the financial industry, this standard is used to develop software for financial transactions, banking systems, and asset management.
- **Aerospace:** The aerospace industry uses this standard to develop software for aircraft, satellites, and space missions.
- **Energy and other industrial sectors:** This standard can also be used in industrial sectors such as: manufacturing, energy, and others; for the development of software for process control and automation.

ISO/IEC 12207:2017 is used in all areas where software development is crucial to the functioning of organizations and where it is necessary to ensure quality management of the entire software life cycle from concept to termination. Thus, it includes, among others (*ISO/IEC/IEEE 12207*, 2017):

- **Development**: addresses the processes and activities involved in software development from initial concept and requirements definition to design, coding, testing, and implementation.
- **Maintenance:** addresses the processes and activities associated with maintaining and improving existing software systems.
- **Delivery:** includes processes for acquiring software from external suppliers or providing software to external customers.
- **Quality Assurance:** defines processes for ensuring software quality throughout its life cycle.
- **Process Improvement:** provides a basis for evaluating and improving processes that help organizations improve their software development and maintenance processes throughout their life cycle.
- **Negotiation Guide:** provides guidelines for forming agreements between customers and suppliers regarding software processes and activities.
- **Different Life Cycle Models:** supports different software life cycle models, including iterative, incremental, and classical approaches.

Also, a standard can be used in one or more ways. If the criterion is a scope, it can be used on the page (*ISO/IEC/IEEE 12207*, 2017):

- **Organizations** - to help establish the desired process environment.
- **Projects** - to help select, structure and use elements of the established environment to deliver products and services.
- **Clients and** suppliers - to help develop agreements on processes and activities.
- **Process auditors** - as a reference process model for use in conducting process audits that can be used to support organizational process improvements.

Its purpose is to provide a standardized framework for software life cycle processes and as such serves several key purposes (*ISO/IEC/IEEE 12207*, 2017):

- **Process standardization**: ISO/IEC 12207 aims to standardize software development processes and to make them consistent and repeatable across organizations and projects. This standard helps establish a common language and set of practices for software engineering.
- **Quality assurance:** Promotes the quality of software and services by defining processes and activities that ensure that software meets specified requirements and standards. By following the guidelines in ISO/IEC 12207, organizations can improve the quality of their software.
- **Risk reduction:** The standard helps reduce the risks associated with software development and maintenance by providing a structured approach. It helps identify and mitigate potential problems early in the software lifecycle.
- **Lifecycle management:** ISO/IEC 12207 covers the entire software lifecycle from concept and requirements through to design, development, testing, implementation and maintenance to retirement. It provides a comprehensive approach to managing software throughout its life.
- **Interoperability:** By providing a common framework, the standard facilitates interoperability between different software components and systems developed by different organizations. It ensures that software can work together smoothly.
- **Alignment with stakeholder requirements:** ISO/IEC 12207 emphasizes the importance of understanding and aligning software development with stakeholder requirements. This helps ensure that software products meet the expectations and requirements of users and other relevant parties.
- **Process improvement:** The standard can be used as a basis for process review and improvement. Organizations can use it to identify areas where they can improve their software development processes.
- **International compatibility:** ISO/IEC 12207 is an international standard, making it applicable and recognized worldwide. This global recognition can be particularly beneficial for organizations that participate in international collaborations or offer software to a global market.

2.1 Processes of the ISO/IEC 12207:2017 standard

Each process in this document is described in terms of the following characteristics:

- **the process name** represents the scope of the entire process,

- **the purpose** describes the goals of the process,
- **the outcomes** express the tangible results expected from the successful implementation of the process,
- **the activities** are groups of related tasks in the process,
- **the tasks** are requirements, recommendations, or permitted actions intended to support the achievement of outcomes.

The standard groups the processes that can be performed during the software system life cycle into four process groups. Each life cycle process in these groups is described in terms of its purpose and desired outcomes, with a set of related activities and tasks that can be performed to achieve these outcomes. The four process groups and the processes included in each group are shown in Figure 2.1.

The process groups are as follows (Figure 2.1) (*ISO/IEC/IEEE 12207*, 2017):

- **Negotiation/Contracting Processes:** Organizations are producers and users of software systems. One organization (as the client) may engage another organization (as the supplier) for products or services. This is accomplished with agreements (or contracts). The latter enables both clients and suppliers to realize value and support their organizations' business strategies. Negotiation processes are organizational processes that are used beyond the scope of the project life cycle, as well as during the project life cycle. Typically, organizations operate simultaneously or sequentially as both clients and suppliers of software systems. Negotiation processes can be used less formally when the client and supplier are within the same organization. They can also be used within an organization to agree on the responsibilities of the organization, the project, and technical functions.
- **Project organization processes:** These processes are concerned with providing resources that ensure that a project meets the needs and expectations of the organization's stakeholders. They are usually focused on the strategic level of managing and improving the organization's business or operations. They do this by providing and allocating resources and by managing risks in competitive or uncertain situations. They are usually used outside the scope of the project life cycle but can also be used during the project life cycle. They establish the environment in which projects are implemented. The organization: defines the processes and life cycle models used by projects; establishes, redirects or cancels

projects; provides the necessary resources, including people and financial resources; and establishes and monitors quality criteria for software systems and other products that are the result of development for internal and external customers. Project organization processes create a business image for many organizations and imply commercial and profit motives. They are equally important for non-profit organizations, as they are also accountable. They are accountable for resources and face risks in their activities.

- **Technical process management:** In this management field, we are concerned with managing the resources and means for the implementation of technical processes that are available to us and are usually assigned by the management layer of the organization. By using them, we achieve the fulfillment of agreements that the organization or organizations have entered. Technical management processes relate to the technical implementation of projects, in particular, planning in terms of costs, time frames and objectives, checking actions to ensure compliance with plans and performance criteria, and identifying and selecting actions to eliminate deficiencies or delays. These processes are used to establish and implement technical plans for the project, manage information within a team of technical personnel, assess technical progress against plans for a software system, products or services, control technical tasks until completion, and assist in decision-making. Typically, several projects will coexist in any organization. Technical management processes can be used and implemented at the corporate level to meet requirements and needs at the level of the entire organization.
- **Technical processes:** These processes transform stakeholder needs into a product or service. By using the product or managing the service, technical processes provide the capabilities needed whenever and wherever to meet the requirements (and ensure satisfaction) of stakeholders. Technical processes are used to create and use a software system either in the form of a model or as a product that is operationally useful. Technical processes are used at any level in the hierarchy of the software system structure and at any stage in the life cycle.

In addition to the intended processes, additional processes can be defined that prove necessary and useful for an organization. The order of the subchapters in which the processes are defined in the standard does not determine the order in which the processes are implemented during the system life cycle or any of its phases.

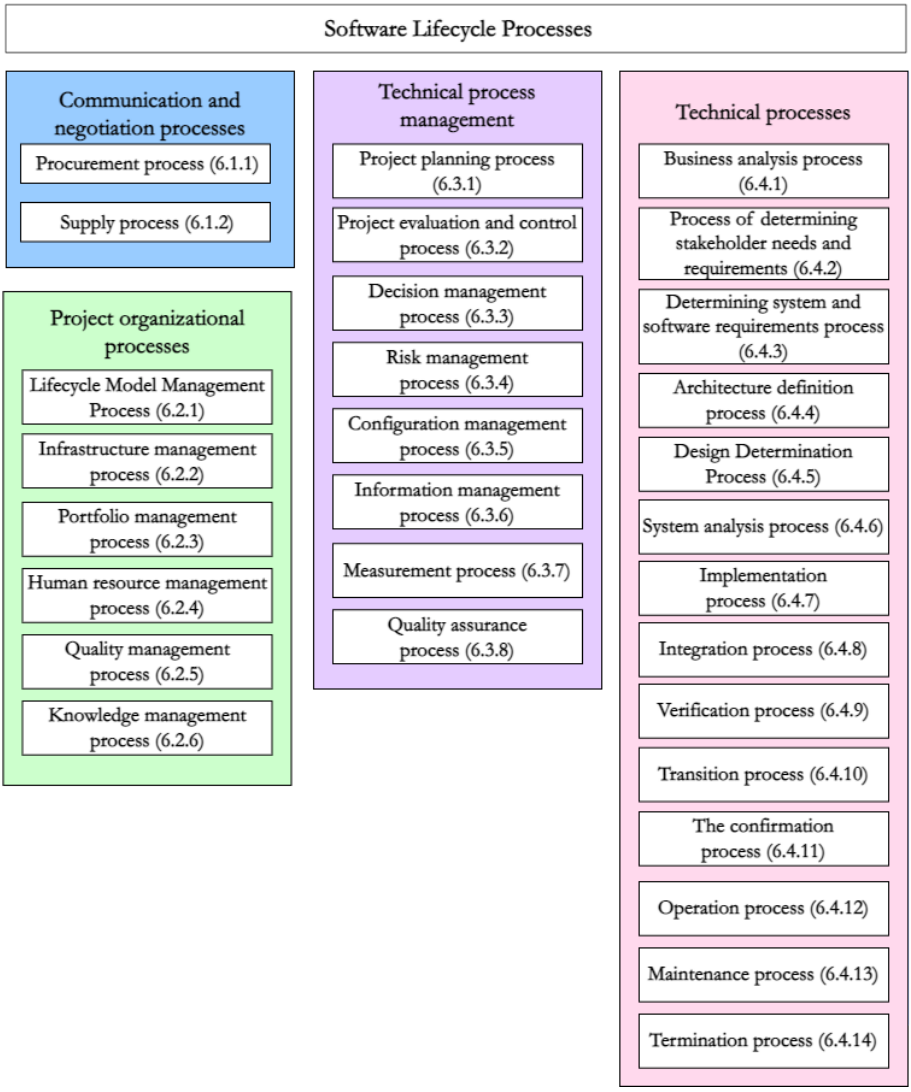


Figure 2.1: Processes and process groups according to ISO/IEC 12207:2017
Source: Summarized by (ISO/IEC/IEEE 12207, 2017).

3 Model for software quality requirements and assessment ISO/IEC 25010:2011

ISO/IEC 25010 is part of the ISO/IEC 250xx family of standards, also known as SQuaRE (Software Quality Requirements and Evaluation) (*ISO/IEC 25010*, 2011). ISO/IEC 25000 is the foundational standard that provides a comprehensive

framework for software quality assessment and management. SQuaRE was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to provide a structured and consistent approach to software quality assessment. This approach helps organizations understand, define, and assess the quality of their software products and make decisions about improvements and optimizations. The entire family of standards establishes quality models, defines quality attributes, and defines quality requirements for software products. These models and attributes serve as tools for assessing and measuring various aspects of software quality. It is used by software development organizations and other stakeholders to assess, communicate, and improve the quality of software products. By following the guidelines and principles set forth in these standards, organizations can improve the quality of their software products, ultimately leading to increased customer satisfaction and successful software implementations. The basic SQuaRE reference model is shown in Figure 2.2.

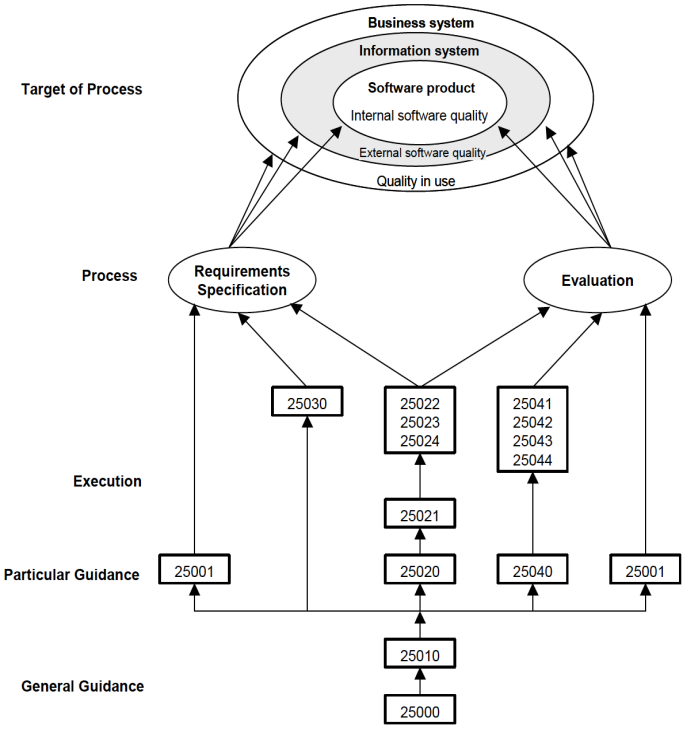


Figure 2.2: SQuaRE Software Quality Standards Family Reference Model
Source: (*ISO/IEC 25010*, 2011).

ISO/IEC 25010 provides a detailed quality model with specific characteristics and sub-characteristics for assessing the quality of a software product. ISO/IEC 25000 and ISO/IEC 25010 are related standards but they perform different tasks within the broader SQuaRE series. Thus, ISO/IEC 25000 is an informative standard that introduces broader concepts and structures for assessing software quality. At the same time, ISO/IEC 25010 is a normative standard that clearly defines the quality model and criteria for assessing the quality of a software product. The key differences between ISO/IEC 25000 and ISO/IEC 25010 are presented in Table 2.1 (*ISO/IEC 25010*, 2011).

Table 2.1: Key differences between ISO/IEC 25000 and ISO/IEC 25010

	ISO/IEC 25000	ISO/IEC 25010
Scope and purpose	the core standard in the SQuaRE series, provides a framework for the requirements and evaluation of software product quality, defines general concepts, terms and principles related to software quality management, introduces quality models and metrics used to assess software quality and guides users to other specific standards in the series, including ISO/IEC 25010.	a specific standard within the SQuaRE series that defines a comprehensive quality model, highlights quality characteristics and sub-characteristics that can be used to assess and measure the quality of a software product, delves into various aspects of software quality, providing specific criteria for evaluating software.
Content	is an informative standard that introduces the software product quality framework, the overall structure of quality characteristics and sub-characteristics, acts as a guiding document for understanding software quality assessment within the SQuaRE series.	a normative standard with specific requirements, intended for direct use in assessing software quality, defines eight basic quality characteristics and their sub-characteristics (accuracy, consistency, efficiency).
Use	is primarily used to provide an overview of software quality management and to direct users to other relevant standards in the SQuaRE series, sets the context and terminology for quality models and metrics for assessing software quality.	is used directly for assessing the quality of a software product, serves as a reference for practitioners who wish to assess and measure the quality characteristics of a software product, guides the selection of relevant quality characteristics and sub-characteristics for assessment according to the specific needs and objectives of the assessment

Source: (ISO/IEC 25010, 2011)

The model described in ISO 25010:2011 assumes (*ISO/IEC 25010*, 2011):

- **a quality model** that encompasses eight main quality characteristics, each representing a key aspect of software quality:

  - Functional suitability: all the capabilities in which the software provides the necessary functions to meet specified needs.
  - Operating efficiency: the ability of the software to perform within expected time frames and with expected use of other IT resources, response times, and data transfer.
  - Compatibility: ability of software to work with other systems, software, or hardware.
  - Usability: ease of use of the software and the user experience.
  - Reliability: ability of software to maintain its level of performance under specified conditions over a specified period of time.
  - Security: ability of software to protect data and functionality from unauthorized access and damage.
  - Durability: effort required to implement changes, correct errors, or adapt the software to changes.
  - Portability: ease with which software can be transferred from one environment to another.
- **Sub-characteristics:** each of the characteristics listed above is broken down into specific sub-characteristics, which makes it easier to assess and focus on specific areas of quality assessment.
- **Quality requirements:** includes a set of quality requirements that can specify the desired level of each quality characteristic and sub-characteristic for a specific software product.
- **Quality in use:** emphasizes the importance of quality assessment on the part of end users who ascertain the quality of the software during actual use.

Figures 2.3 and 2.4 show the set of characteristics and sub-characteristics of software quality as defined by the ISO/IEC 25010:2011 quality assessment model.

The quality of a software product can be assessed by measuring internal properties (usually static measurements of intermediate products), by measuring external properties (usually measuring the behavior of the code during execution), or by measuring quality properties in use (when the product is in actual or simulated use). See Figure 2.1 and Figure 2.5.

(Sub)Characteristic
Functional suitability
Functional completeness
Functional correctness
Functional appropriateness
Performance efficiency
Time behaviour
Resource utilization
Capacity
Compatibility
Co-existence
Interoperability
Usability
Appropriateness recognizability
Learnability
Operability
User error protection
User interface aesthetics
Accessibility

Reliability
Maturity
Availability
Fault tolerance
Recoverability
Security
Confidentiality
Integrity
Non-repudiation
Accountability
Authenticity
Maintainability
Modularity
Reusability
Analysability
Modifiability
Testability
Portability
Adaptability
Installability
Replaceability

Figure 2.3: Software quality characteristics and sub-characteristics according to ISO/IEC 25010:2011

Source: (ISO/IEC 25010, 2011).

Effectiveness
Efficiency
Satisfaction
Usefulness
Trust
Pleasure
Comfort
Freedom from risk
Economic risk mitigation
Health and safety risk mitigation
Environmental risk mitigation
Context coverage
Context completeness
Flexibility

Figure 2.4: Characteristics and sub-characteristics of quality in the use of software according to ISO/IEC

Source: (ISO/IEC 25010, 2011).

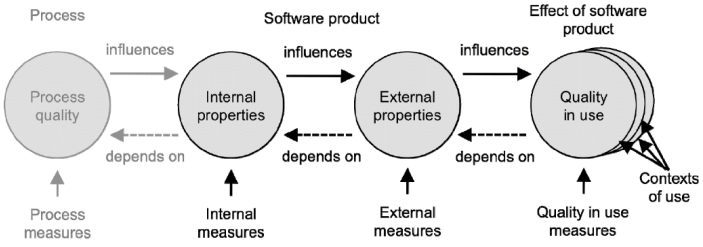


Figure 2.5: Software Quality Lifecycle

Source: (ISO/IEC 25010, 2011).

4 Comment on the applicability of both standards

The ISO/IEC 12207 and ISO/IEC 25010 standards play a key role in the digitalization of logistics processes, as they provide a structure and guidelines for the effective management of software development and its quality assurance. The following is a brief critical evaluation of their importance in the context of the digitalization of logistics processes.

ISO/IEC 12207 defines standard processes for software lifecycle management. This standard is important for the digitalization of logistics processes for the following reasons:

- **Structured approach to software development:** ISO/IEC 12207 provides a structured framework for planning, developing, maintaining and managing software. In the context of digital logistics, this means that companies can effectively plan and implement digital solutions that are reliable and compliant with best practices.
- **Managing complexity:** Logistics processes are complex and involve many actors and technologies. ISO/IEC 12207 helps manage this complexity by clearly defining processes, responsibilities and activities throughout the software lifecycle.
- **Reducing risks:** By providing clear guidelines for software development and maintenance, the standard helps reduce the risks associated with software errors, which is particularly important in logistics, where errors can cause significant financial losses and supply chain disruptions.
- **Increasing compliance and standardization:** Using ISO/IEC 12207 ensures that software development processes are consistent and standardized. This is crucial for the interoperability of different systems and technologies used in digitalized logistics processes.

ISO/IEC 25010 defines a software quality model that includes various quality characteristics such as: functionality, efficiency, reliability, usability and other indicators. Its importance in the digitalization of logistics processes is mainly as follows:

- **Quality measurement:** ISO/IEC 25010 enables the precise measurement and evaluation of software quality. In logistics, where accuracy and reliability are crucial, companies can use this standard to ensure that digital solutions meet high quality standards.
- **User experience improvement:** Software quality has a significant impact on the user experience. ISO/IEC 25010 helps design software that is easy to use, efficient and tailored to the needs of users in logistics processes.
- **Reliability and maintainability:** Reliability and maintainability are key quality characteristics in logistics, where system failures or outages can cause serious disruptions. ISO/IEC 25010 helps ensure that software solutions are reliable and easy to maintain.
- **Decision support:** The standard provides clear criteria for assessing software quality, which can help management decide whether to implement new digital solutions or improve existing systems.

One criticism of both standards is that they impose additional costs and resource requirements. Small and medium-sized logistics companies may not have the resources to fully implement these standards. In addition, they may be too complex and difficult to understand and implement for some environments, which can be a barrier for companies that do not have specialized knowledge and experience in systems engineering and software quality.

The ISO/IEC 12207 and ISO/IEC 25010 standards are important aids in the digitalization of logistics processes, as they provide a structured approach to software development and quality assurance. Their use can improve the efficiency, reliability and quality of digital solutions in logistics. However, companies must be mindful of the costs, resources and flexibility associated with implementing these standards and be aware of the potential challenges and limitations they may bring.

References

ISO/IEC 25010:2011–Systems and software engineering–Systems and software Quality Requirements and Evaluation (SQuaRE) –System and software quality models (Version 1). (2011). https://www.iso.org/standard/35733.html

ISO/IEC/IEEE 12207:2017–Systems and software engineering–Software life cycle processes (Version 1). (2017). https://www.iso.org/standard/63712.html

Information and Computer Literacy

Nena Orel Šanko
University of Maribor, Faculty of Logistics, Celje, Slovenia
nena.orel@um.si

Today, information and computer security are extremely important for several reasons. Digitalisation has enabled a massive flow of data and information through computer networks, where information is often sensitive in nature, including financial data, personal identities, and business secrets. It is imperative to protect information from unauthorised access and misuse. In today's digital world, a lot of infrastructure is connected to computer networks, such as schools, hospitals, and transportation systems. Attacks on these systems can lead to significant financial or material damage and jeopardise people's lives. Hence, it is crucial to ensure systems' security and resiliency against cyber-attacks, which have become increasingly common, sophisticated, and exploit vulnerabilities to steal data, spy, and cause harm. Thus, constant upgrading of security measures and raising awareness among people are essential. Therefore, information and computer security are of paramount importance for safeguarding privacy, economic stability, and national security in the modern digital world.

DOI
https://doi.org/10.18690/um.fl.2.2026.3

ISBN
978-961-299-074-9

Keywords:
information security,
computer security,
data,
information

University of Maribor Press

1 Introduction

Information and computer security have become fundamental issues in today's digital age, where data and information have become valuable resources that drive both private and business environments. With the rapid development of technology and constant connectivity via the Internet, data protection has become crucial, as new threats have emerged that threaten both individuals and organizations. Security breaches such as identity theft, hacker attacks and loss of sensitive information may result in serious consequences that can cause irreparable damage on both a personal and business level. Therefore, ensuring information and data protection is a key task today, which ultimately protects our privacy, financial stability and business competitiveness.

At the beginning, it should be made clear that the existence and operations of every organization depend on information technology (hereinafter: IT) resources, without which logistics processes and supply chain systems cannot (smoothly) operate (Jereb, 2017). These include (Kajba et al., 2023): information, applications (or software), infrastructure, intangible assets, and people. IT resources are available for implementation in various IT processes (Jereb, 2017), and we can understand them as investments in these processes, where the appropriate level of protection is also important (Jereb et al., 2016). We can also argue that these four IT resources are the foundation of every technology, constituting four interdependent, co-determining and equally important components (Kabanda, 2019).

For each of the IT resources, it is also necessary to ensure the IT requirements that were already mentioned in the chapter "Digitalization – Planning". According to the Control Objectives for Information and related Technology, there are seven business requirements or information criteria for IT resources (IT Governance Institute, 2007):

- effectiveness – refers to information relevant to the business process that is part of that business process and its timely provision, correctness, consistency and usability,
- efficiency – refers to providing information with optimal use of resources,
- confidentiality – refers to protecting sensitive information from disclosure,

- integrity – refers to the accuracy and completeness of information and its validity in accordance with business value and expectations,
- availability – refers to information that must be available when needed in business processes and the protection of necessary resources and related capabilities,
- compliance – addresses compliance with laws, regulations and contractual agreements (externally defined business criteria, internal policies) that apply to the business process in question,
- reliability – refers to providing management with appropriate information to manage the organization and carry out its responsibilities for confidentiality and governance.

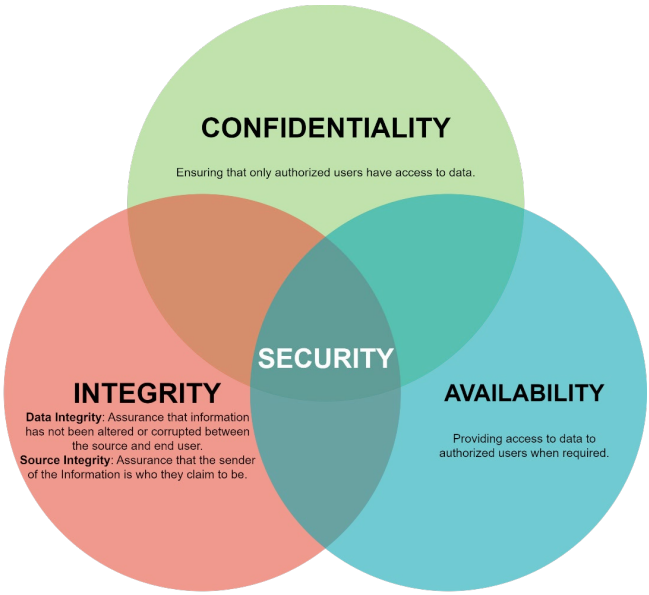


Figure 3.1: The CIA Triad
Source: own.

Informatics, from a security perspective, primarily requires that information is available, complete and confidential to the extent necessary to implement and support business processes. In the case of logistics, this means ensuring the availability, completeness and confidentiality of information so that the right products or services can be provided in the right quantity and quality, delivered to the right place and at the right time (Kajba & Jereb, 2021). These three requirements

(availability, completeness and confidentiality) also make up the CIA Triad (Figure 1.1), where (Kemmerer, 2003):

- confidentiality ensures that sensitive information is not disclosed to unauthorized recipients,
- integrity ensures that data and programs are modified or destroyed only in a specific and authorized manner,
- availability ensures that IT resources will be available whenever an authorized user needs them.

2 Types of Security and Threats Related to IT Operations

The chapter "Digitalization – Planning" outlined the general importance of information and cybersecurity, describing the key elements of cybersecurity and proactive and comprehensive approaches. The following is a detailed description of the various types of security and IT threats.

2.1 Types of security related to IT operations

It is necessary to introduce the types of security related to IT operations: information security, IT security, cybersecurity, computer security and network security.

Information Security (InfoSec) encompasses the tools and procedures that organizations use to protect information and prevent unauthorized access to business or personal information, including policy settings that prevent unauthorized people from accessing business or personal data. InfoSec is a growing and evolving field that covers many aspects from network security testing, auditing, and infrastructure. It protects sensitive data from unauthorized activities, including viewing, modifying, recording and any disruption or destruction. The main goal is to ensure the security and privacy of critical organizational data, such as: customer account details, financial data or intellectual property. Organizations must allocate resources to ensure information and data security and be prepared to detect, respond to, and proactively prevent attacks such as: phishing, malware, viruses, malicious insiders, and ransomware ('Information Security: The Ultimate Guide', n.d.).

Information Technology Security (IT security) describes precautions taken to protect computers and networks from unauthorized access. Procedures and processes are designed to prevent data theft or disruption of information systems. High-quality IT security focuses on protecting data integrity, maintaining the confidentiality of information stored on a network, ensuring that data and information are accessible to authorized personnel, verifying the authenticity of users attempting to access computer networks, and enabling secure messaging across networks for users (The Upwork Team, 2021).

While both IT security and cyber security focus on protecting customer data, they take slightly different approaches. IT security refers to a broader understanding of security, exploring the steps to protect business data, including physical data and information in internal systems. Cyber security focuses more on the threats an organization may encounter over the Internet when information and data are transmitted digitally or otherwise used online (The Upwork Team, 2021). Cyber security encompasses a set of tools, policies, security concepts, security measures, guidelines, risk management approaches, actions, training, best practices, assurances, and technologies that can be used to protect the cyber environment and the assets of the organization and its users (Von Solms & Van Niekerk, 2013).

Computer security generally focuses on protecting computer systems from unauthorized access and use. Computer security professionals work to establish best practices for computer security, which include managing computer and network security and creating a culture focused on security within the organization. There are several types of computer security that affect different elements of an organization's physical and digital infrastructure. As a result, there are a wide variety types of security that professionals need to focus on, including (The Upwork Team, 2021; 'What Is Computer Security?', 2022):

- application security – describes the steps developers take when building an application to ensure user security and reduce vulnerabilities in the application (this type of security involves analyzing the application code to find potential weaknesses),
- information security,

- network security – protects an organization's digital infrastructure and prevents security incidents on computer networks so that users can work without interruption,
- internet security – protects browsers and information in applications that use the Internet. Firewalls and similar types of protection that only allow authorized users to access protected areas are considered internet security services,
- cloud security – ensures that users connecting through cloud applications remain protected and uses systems such as cloud-based unified threat management (UTM) to maintain secure cloud connections,
- operational security – describes the practices and analysis used in routine activities to find potential vulnerabilities that hackers can exploit. The goal is to see regular actions from the perspective of a bad actor and identify where they can take advantage,
- endpoint Security – with the number of devices used in an organization (mobile phones, tablets, laptops, and computers), endpoint security focuses on protecting these system endpoints and includes protecting devices from malware infection.

Each of these types of computer security includes multiple components, which makes them a specialized field in their own right. ('What Is Computer Security?', 2022). The aforementioned CIA triangle has been the industry standard for computer security since the development of the mainframe[1] (Whitman & Mattord, 2011).

Understanding the difference between IT security and network security lies in understanding the different uses of data. IT security focuses on all data managed by an organization, while network security focuses on network systems and protecting them from intrusions and data attacks. Security service providers often protect the infrastructure that enables organizations to collaborate electronically (The Upwork Team, 2021).

[1] Mainframe - at their core, "mainframes" are high-performance computers with large amounts of memory and data processors that process billions of simple calculations and transactions in real time (IBM, n.d.).

2.2 Types of IT threats

Before we continue with types of hacks, it is necessary to mention the types of IT security threats (The Upwork Team, 2021):

- cybercrime – involves the targeting or use of computers or computer systems to commit crimes (identity theft or extortion) for some type of financial reward,
- cyberattacks – large-scale digital attacks that can disable an entire computer system or multiple computer systems (attacks may use malware or ransomware) to achieve the goal of obtaining information about millions of users or carrying out a denial of service (DoS) attack,
- cyberterrorism – uses the tools and methods of cybercrime and attacks to attempt to target the critical infrastructure of countries or otherwise harm countries and cause fear through unauthorized access to communications infrastructure.

3 Malicious software

A common term for malicious software is also malicious code or "malware". Every year, businesses are flooded with malware attacks, caused by the ever-increasing communication capabilities of computers and phones. A characteristic of all forms of malware is that their existence is unwanted, unknown or hostile to the attacked user who receives these programs. Twenty years ago, malicious code spread exclusively via floppy disks that users transferred from computer to computer. With the increase in communication capabilities, the prevalence of malicious code has also increased. Today, pests like to spread via files, e-mail, instant messaging systems and websites (Šepec, 2018).

Malware exploits security vulnerabilities in operating systems and applications to spread infections. The successful penetration of malicious code is a result of the inadequacy of traditional defense tools, which operate primarily reactively. Antivirus and antispyware programs are most successful in combating attacks. When a new type of malware appears on the Internet, it can spread unhindered until antivirus vendors analyze the attack and create a suitable “vaccine.” Properly configured firewalls could play a vital role in this fight; however, most users do not even know what a firewall is.

3.1 Types of malware

Malware appears as an auxiliary or main means of execution in many cybercrime crimes and is defined as harmful programs especially adapted for attacks (damage) on information systems, networks or data (Šepec, 2018). In today's information age, in which the possibility of profiling individuals is relatively common and interference with the information privacy of individuals has reached the highest level in history, spyware is anything but an innocent collection of codes. Malicious codes, which dominate criminal acts, and through which a variety of methods can be implemented, cause various disruptions, damage and serious obstruction of information systems and e-data. A characteristic of all forms of malware programs is that their existence is unwanted, unknown or hostile to the attacked user who receives these programs (Šepec, 2018).

When cybercriminals plan to attack computer networks and systems, they have a variety of tools at their disposal. There are several types of malicious attacks that organizations should be aware of when developing their cybersecurity and IT security strategies. Some of the types of malware are presented below: viruses, worms, Trojan horses, spyware, adware, ransomware, and (distributed) denial of service.

3.1.1 Viruses

The word VIRUS stands for »Vital Information Resource under Siege« (Maity & Dey, 2021). While all types of malwares are often considered viruses, viruses are only one form of malware, and not all types are viruses. A virus is a computer program that was originally written for entertainment but today mainly causes incalculable damage to information systems.

The term virus is used in computer jargon in the same way as self-replicating biological viruses – a virus is a program or code that automatically spreads to other files it encounters and performs malicious tasks, such as displaying simple message windows or destroying data. A virus can be described as a program that infects various media and changes the operation of a computer or network (Šepec, 2018). Or as a self-replicating program that can “infect” other programs by altering them or their environment, so that a call to the 'infected' program means a call to a possibly

modified and, in most cases, functionally similar copy of the virus (Horton & Seberry, 1997).

Viruses need user assistance to activate and spread, which happens when you click on a specific file, launch a specific program, or click on a link. When an infected file is opened, the virus spreads and can infect other programs, the boot sector of the hard disk, its partition, or a document. Once activated, it also starts spreading to other files or through other communication channels. A computer system can become infected even if the infected program is not launched, as some viruses spread while copying themselves. Viruses cannot infect a computer if we only view websites – infection occurs only if we allow online programs to run. It is good to know that viruses are not only present in stolen or cracked programs; due to carelessness, they can also appear in legal programs. Some viruses also spread via e-mail without attachments because of software errors (Šepec, 2018).

Viruses usually reside in individual executable programs on an infected computer, which increases the size of the program. The contents of the screen of the infected computer suddenly begin to change, individual parts of the screen may move, and various images or inscriptions may also appear, such as: "Your computer is now infected." The infected computer may request different passwords and codes or otherwise change typical commands sent via the keyboard or mouse. The computer's performance is also slowed down (this does not mean that every slow computer is also infected with a virus). Most viruses are designed to destroy the computer or data (Šepec, 2018).

Every virus has the following components (Šepec, 2018):

- infection: the part of the program that enables the virus to spread,
- payload: represents the main activity of the virus and is designed to perform specific functions, such as deleting, modifying and configuring data and installing software for remote access,
- trigger function: defines a time or event and executes a supporting component of the program.

3.1.2 Worms

Viruses differ from worms in that their launch requires action from the recipient in the form of program execution, with the user executing the virus file themselves (opening an email attachment, clicking on the executable file with the mouse). Worms exploit vulnerabilities in operating systems (for example: Windows and Linux) and do not require any action from the victim (Šepec, 2018).

Thus, a worm is an independent program that can spread copies of itself or parts of itself to other computers, usually over network connections, and these copies are fully functional independent programs that can either spread further and/or communicate with the parent worm (for example, to report the results of a calculation) (Horton & Seberry, 1997). They often attack important systems and websites. In the case of worms, the most noticeable consequence is increased network traffic.

Similar to viruses, worms are self-replicating programs that most often spread uncontrollably across a computer system, the Internet, and other networks (Šepec, 2018). However, compared to viruses, they are somewhat more intelligent, as they are able to automatically find suitable targets for infection and spread without user assistance, as they use errors in operating systems and programs (Bhargava et al., 2022). They are usually very successful in spreading, as computer users do not install the necessary security systems. Like viruses, worms carry a "payload" that allows them to control the infected computer, delete files, or steal personal information and data. In 2004, a worm called Blaster infected more than 100,000 computers in just five hours. Another worm, called Mydoom, is perhaps the worst malicious program in history, as it caused more than $38 billion in damage in 2004 (Paulo, 2022).

3.1.3 Trojan horse

A Trojan horse is incapable of self-replication. A characteristic of Trojan horses is that they often contain some innocent function (for example, displaying the time and weather on the desktop of a computer system) (Šepec, 2018), a small and harmful part of some original, generally useful program. Unlike a computer virus (which attaches itself to another program by any of a number of methods), a Trojan horse is a standalone program and may have user functions for the user (Horton & Seberry, 1997).

A Trojan horse can easily be presented as a seemingly innocent file downloaded from the Internet as a Word or PDF document attached to an email (Bhargava et al., 2022). When this generic program is installed, a Trojan horse is also installed with it, allowing the attacker to take over the computer. Although this type of malware does not replicate, it can perform several harmful activities. Behind the primary program are so-called "trap doors" that allow the author of the Trojan horse to perform a specific function (access the user's information system, retrieve files from the system, or install malicious code on the system). They work similarly to viruses, as they require some prior action from the victim in the form of running an executable file, visiting a website, or opening a seemingly innocent file containing the Trojan horse code. The main purpose of Trojan horses is to create and steal identities in connection with achieving financial gain (Šepec, 2018).

3.1.4 Spyware, adware and ransomware

Spyware and adware are major nuisances in the computer world. Both are types of malicious software and differ from viruses and worms in that they cannot spread from one computer system to another.

Spyware is a general term for various types of malicious software that controls the operation of information systems in a certain way and collects personal data (Šepec, 2018). It is a set of code that is installed on a computer system and acts as a spy, focusing on the activities of the system owner and collecting all information that it accesses without authorization (Maity & Dey, 2021). Spyware is installed on a computer while browsing the Internet and it exploits security flaws in the web browser to infect the computer. It can take various forms, from free programs, screen savers, to various toolbars, and even file sharing programs. One of the popular tricks of criminals is to redirect your browser to unwanted websites, which allows attackers to commit additional crimes. The purpose of spyware is not to destroy, damage or disrupt data and systems but to collect various information about the user (their habits and behavior, remembering and recording passwords and other confidential information) through websites, social networks and online stores, which is then reported back to a central source for either legal or illegal purposes (Šepec, 2018).

Adware collects data about users and their online habits and sends its findings to various agencies, which bombard users with ads and spam. Adware can constantly display pop-ups, which significantly slows down the computer (Šepec, 2018).

Ransomware is a self-explanatory term – programs hold critical information "hostage" to receive a ransom. The consequences can include data loss or unauthorized distribution of data to the public, affecting the future operations of an organization (Šepec, 2018), its reputation, or the reputation of an individual. Today, most ransomware occurs as a result of a computer worm that can spread from one system to the next and across networks without user intervention (Bhargava et al., 2022). Ransomware can target all industry sectors, with some more vulnerable than others. For example, in 2021, legal, manufacturing, financial, and human resources services (Cyberreason, 2022) were most affected by ransomware (Fedor, 2022).

3.1.5 Denial of Service

Denial of Service (hereinafter: DoS) is a type of cyberattack in which criminals make a specific network inaccessible to users and gain access to a computer system to collect personal information. The attack originates from a single system or network. It is an attempt by attackers to prevent a legitimate user of a service from using that service. A DoS attack can be carried out through (Šepec, 2018):

- disabling network routers that allow access to the Internet of the attacked information system. Wireless access points are reprogrammed to no longer provide a wireless Internet connection to the attacked IT systems,
- sending a mass of e-mail messages (mail bombing), which overloads the e-mail server,
- programs that constantly reproduce or other types of viral code that attack the information system.

Distributed Denial of Service (hereinafter: DDoS) is coordinated across multiple information systems, each sending a portion of the data to carry out the attack simultaneously from multiple attack points. It is a distributed denial of service of an information system. The attacker can attack multiple slave systems (slaves), which are controlled by control systems (masters). Attacks are often carried out on a significantly larger scale with multiple slave systems (Šepec, 2018).

4 Measures to protect against IT threats

The saying »prevention is better than cure« also applies when we talk about information and computer security. In today's highly digitalized and connected world, both individuals and companies are exposed to various dangers at every turn, which is why it is important to know how to protect ourselves from IT threats and malicious software. Various strategies and methods primarily follow the process of preventing, detecting or sensing and responding (Kemmerer, 2003) to IT threats. Cybersecurity is primarily concerned with protecting IT resources (information, applications or software, infrastructure, intangible assets and people) from unauthorized disclosure, modification or destruction. In this way, the IT requirements of the CIA triangle (availability, integrity and confidentiality) are ensured.

Information and computer security are key topics that need to be addressed and implemented in any company to ensure the protection of internal assets and intellectual property (McFadzean et al., 2011). Most companies (as well as individuals) operate online, as it enables real-time connectivity and communication (Chen et al., 2010). There are various ways in which a company can protect itself from IT threats and attacks. In certain cases, a financial investment is also required, which depends on the method and level of protection. First and foremost, it is necessary to educate and train people on appropriate behavior in cyberspace, since in most cases it is people who are responsible for the attack in the first place (opening inappropriate pages, clicking on web links or attachments). The subchapters cover some measures on how a company can protect its IT resources with the help of employees from IT threats and attacks. The same measures can also be used in the case of a physical individual to protect personal devices.

4.1 Creating passwords

Every user account and some applications require a password. Many people choose simple passwords, usually including their place of residence or birthplace, birthdays, children's or pets' names, and the like. Dictionary words are also often used in passwords. This is not a good idea, as they are easy to guess and relatively short. When attackers try to gain access to accounts, they use brute-force attacks, where they use software to "check" dictionaries and try a large number of different passwords, hoping that one of them will be correct (Kaspersky, 2023b).

The recommended password length is also being extended every year, with a minimum requirement of at least eight characters. Longer passwords are always better than short ones – the more characters there are, the longer it will take to "crack" the password or determine it. One additional character (letter, number or symbol) can extend the time to crack a password by months or even years. Therefore, it is always better to create passwords longer than the minimum required. It is recommended to use passwords with at least 12 characters. It is necessary to combine uppercase and lowercase letters, numbers and symbols. Of course, we must also pay attention to the order, as it is increasingly common for passwords to consist of (in this order): one uppercase letter, a set of lowercase letters, a set of numbers and one or two symbols. Therefore, the use of "salting and peppering" passwords is very important (The Upwork Team, 2021), which involves the random use of a mixture of uppercase and lowercase letters, numbers, and symbols, which greatly increases the level of difficulty and extends the time it takes to crack a password.

Due to overload, people tend to be lazy and overly-relaxed when creating online accounts, which is why we often use one password for multiple accounts, which is not recommended at all. When we use one password for multiple accounts or devices, attackers can access all these accounts and the data in them in the event of unauthorized access or hacking. However, if we have a different password for each account and device, only one account is at risk, and the others are not. This way, our data is more secure and protected from IT threats and attacks.

4.2 Computer network protection

Protecting IT infrastructure and applications or software, and consequently information and people in the company, can be achieved in various ways. Table 4.1 presents a set of preventive measures that a company can use to protect the aforementioned IT resources and their description.

Table 4.1: Preventive measures to protect against IT threats

Measure	Description
Installing IT security frameworks	IT security frameworks describe documented and mutually understood policies that dictate sensitive information management in an organization.
Creating a whitelist of applications	Based on the list of allowed applications, the company can determine which applications are allowed to be installed and/or run on company devices.

Measure	Description
Using antivirus software	It enables the maintenance of "clean" computers and operating systems by regularly checking, detecting, preventing and removing various malicious software.
Firewalls	A firewall sets rules that govern data traffic and controls the entry and exit of data and other devices into and out of the computer.
Using a network intrusion detection system (NIDS)	A network intrusion detection system (NIDS) works similarly to antivirus software and a firewall; it monitors traffic flowing into and out of various devices connected to the network and checks for malicious activities or unauthorized access and notifies the network owner.
Implementing multi-factor authentication	Information and data security can be ensured based on multi-level authentication, required for access to sensitive information. In this case, it can be a combination of entering different passwords received via different devices (phone and computer) or accounts (email, phone number).
Using encryption	Asymmetric encryption protects sensitive information that is transmitted from one device to another, either over the Internet or other devices. A document or file is encrypted (created as ciphertext) using a public key and then decrypted (changed back to plaintext) using a private key.
Using a virtual private network (VPN)	A virtual private network (VPN) is a way to create a private place on the Internet that helps users create a secure connection and encrypt data sent over the network. VPN is often included in antivirus software.
Using honeypots	"Honeypots" are artificially created targets that contain useless information. While attackers unknowingly try to access honeypots, important information and files on the computer are protected.
Performing a vulnerability assessment and penetration test	Performing a vulnerability assessment involves looking for potential problems in a network or system that could allow unauthorized external access. Vulnerabilities are discovered and their severity is determined with priority for resolution. The latter is done by attempting to access the network or system from the outside, with the help of ethical hackers.

Source: (Chen et al., 2010; The Upwork Team, 2021; Vacca, 2013)

5 Conclusion

In 2020, an average of 360,000 new malicious files were discovered (Kaspersky, 2023a), and every year their authors become more innovative. New types of malicious code are emerging that can exploit security vulnerabilities in operating systems, antivirus programs and firewalls. The most common malicious codes that dominate criminal acts, in which various methods are implemented, are disruption, damage and severe obstruction of information systems and electronic data (Šepec, 2018).

The Internet has become the most common place for viruses to spread. Malicious software can be hidden in anything downloaded from websites, and without a proper security system, it can cause a lot of damage. Due to the rapid growth of email, attachments have become the most common reason for the spread of computer

viruses. It is important to note that there are many different types of malware, which are improving, multiplying, and appearing in new forms or variations almost every day.

Therefore, information and computer security of companies must also include protection against social engineering, such as various forms of phishing (including smishing and vishing), as attackers often target the human factor as the weakest link in the security chain. Phishing attacks, where attackers pose as trusted entities to obtain sensitive data or access to systems, are particularly dangerous in logistics due to the complex and branched supply chains. Employees may receive fake emails urging them to reveal passwords, credit card numbers or other confidential company information, which can lead to serious security incidents and business disruption. Therefore, it is crucial that companies conduct regular training and awareness-raising among employees on how to recognize phishing attempts and implement security measures that reduce the risk of such attacks.

In the context of the digitalization of logistics, information and computer security play a key role in ensuring the smooth and secure operation of logistics processes. Digitalization brings many benefits, such as increased efficiency, better traceability of shipments and optimization of inventories, but at the same time it exposes companies to IT threats and attacks. Cyberattacks such as system intrusion, data theft or ransomware attacks can cause serious disruption in supply chains, leading to delays, financial losses, and general damage to the reputation of companies. Therefore, it is imperative that companies invest in information and computer security through the appropriate solutions and measures presented within this chapter.

Information security in logistics, in addition to the above, also refers to the protection of confidential data, such as information about customers, transactions, suppliers and business partners, and others. Effective data management is essential for maintaining trust between business partners and end users. Compliance with legislation and data protection standards, such as GDPR and ISO 27001, is an important aspect of information security, ensuring that companies operate in accordance with legal requirements and best practices. Security policies and procedures, including regular security reviews and risk assessments, are essential in preventing security incidents and mitigating risks in the digitalization of logistics.

References

Bhargava, P., Choudhary, R., & Gupta, A. (2022, May). A Review Study on Computer Virus. *World Journal of Research and Review (WJRR)*, *14*(5), 39–44.

Chen, R.-S., Chung, Y.-M., & Tsai, C.-H. (2010). A study of the performance evaluation of a network intrusion detection system. *Asian Journal on Quality*, *11*(1), 28–38. https://doi.org/10.1108/15982681011051804

Cyberreason. (2022). *Ransomware: The True Cost to Business—A Global Study on Ransomware Business Impact*. https://www.cybereason.com/hubfs/dam/collateral/reports/Ransomware-The-True-Cost-to-Business-2022.pdf

Fedor, O. (2022, November 3). *93 Must-Know Ransomware Statistics [2023]*. Antivirus Guide. https://www.antivirusguide.com/cybersecurity/ransomware-statistics/?gclid=Cj0KCQjwi46iBhDyARIsAE3nVrYtrwBey_1ErcYLO6UBJVk3as7CfdxsGKVcHVkKJfM_Mcyvk92IlH0aAr3WEALw_wcB

Horton, J., & Seberry, J. (1997). *Computer Viruses—An Introduction. 19, 1*, 122–131. https://documents.uow.edu.au/~jennie/WEBPDF/1997_09.pdf

IBM. (n.d.). *What is a mainframe?* IBM. Retrieved 4 October 2023, from https://www.ibm.com/topics/mainframe

Information Security: The Ultimate Guide. (n.d.). *Imperva*. Retrieved 3 October 2023, from https://www.imperva.com/learn/data-security/information-security-infosec/

IT Governance Institute. (2007). *COBIT 4.1: Framework, control objectives, management guidelines, maturity models*. IT Governance Institute.

Jereb, B. (2017). Mastering logistics investment management. *Transformations in Business and Economics*, *16*, 100–120.

Jereb, B., Cvahte Ojsteršek, T., & Rosi, B. (2016). *Governance of Investments in Logistics* (pp. 236–247). https://doi.org/10.4018/978-1-5225-0001-8.ch011

Kabanda, G. (2019). *Trends in Information Technology Management*.

Kajba, M., & Jereb, B. (2021). *Three Crucial Years of IT Trends in Logistics*. 187–198. https://www.elibrary.ru/item.asp?id=46600879&pff=1

Kajba, M., Jereb, B., & Obrecht, M. (2023). Considering IT Trends for Modelling Investments in Supply Chains by Prioritising Digital Twins. *Processes*, *11*(1), Article 1. https://doi.org/10.3390/pr11010262

Kaspersky. (2023a, May 18). *The number of new malicious files detected every day increases by 5.2% to 360,000 in 2020*. Www.Kaspersky.Com. https://www.kaspersky.com/about/press-releases/2020_the-number-of-new-malicious-files-detected-every-day-increases-by-52-to-360000-in-2020

Kaspersky. (2023b, June 30). *Brute Force Attack: Definition and Examples*. Www.Kaspersky.Com. https://www.kaspersky.com/resource-center/definitions/brute-force-attack

Kemmerer, R. A. (2003). Cybersecurity. *25th International Conference on Software Engineering, 2003. Proceedings.*, 705–715. https://doi.org/10.1109/ICSE.2003.1201257

Maity, S., & Dey, D. (2021). Computer Virus Attacks. *La Pensée*, *51*(3), 585–594. https://doi.org/10.6084/m9.figshare.19258763.v1

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2011). Information Assurance and Corporate Strategy: A Delphi Study of Choices, Challenges, and Developments for the Future. *Information Systems Management*, *28*(2), 102–129. https://doi.org/10.1080/10580530.2011.562127

Paulo. (2022, December 21). *Top 10 most dangerous computer viruses of all time*. Dynamic Solutions Group. https://www.dsolutionsgroup.com/top-10-most-dangerous-malware-of-all-time/

Šepec, M. (2018). Kibernetski kriminal: Kazniva dejanja in kazenskopravna analiza. In *Univerzitetna založba Univerze v Mariboru*. Univerzitetna založba Univerze v Mariboru. https://press.um.si/index.php/ump/catalog/book/335

The Upwork Team. (2021, June 8). *What Is IT Security? Examples and Best Practices for 2024*. https://www.upwork.com/resources/it-security

Vacca, J. R. (2013). *Cyber Security and IT Infrastructure Protection*. Syngress.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

What Is Computer Security? (And Why It's Important). (2022, August 23). *Berkeley Boot Camps*. https://bootcamp.berkeley.edu/blog/what-is-computer-security/

Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security* (4th edition). http://almuhammadi.com/sultan/sec_books/Whitman.pdf

Business Information Systems

Bojan Rupnik
University of Maribor, Faculty of Logistics, Celje, Slovenia
bojan.rupnik@um.si

Information systems have become an indispensable cornerstone of modern business operations, facilitating data management, process optimization, and informed decision-making. This abstract explores the pivotal role of information systems in business, with a specific focus on the pervasive influence of Enterprise Resource Planning (ERP) systems. ERP systems serve as integrated platforms that harmonize various business functions, streamlining processes and unifying data into a single, accessible repository. They empower organizations by providing centralized, real-time data, which aids in efficient resource allocation, cost reduction, and enhanced customer service. ERP systems are invaluable in driving cross-functional insights, fostering improved communication and collaboration, and ensuring data security and compliance. Moreover, these systems are a catalyst for strategic planning, offering the capacity for data-driven decision-making, predictive analytics, and long-term goal alignment. In essence, information systems, especially ERP, have revolutionized the way businesses operate, adapting to the ever-changing landscape of the digital age and serving as a cornerstone for achieving operational excellence and competitive advantage.

DOI
https://doi.org/10.18690/um.fl.2.2026.4

ISBN
978-961-299-074-9

Keywords:
ERP systems, information support, information flow, ERP selection and implementation

University of Maribor Press

1 Introduction

The modern business world is based on information. With the development of technology, new solutions for individual business processes are constantly emerging. The integration of new technologies enables better overview, faster control, greater reliability, and security (as well as risks) of processes. Depending on the scope of business, small companies can still manage their business with basic computer tools, but as the scope increases, the transition to more complex information systems is inevitable. The concept of information systems is very broad and can describe both individual solutions for certain business segments and comprehensive centralized systems that connect various subsystems. The amount of information and data exchange used in business has also increased tremendously recently. The connectivity of systems within the company and with business partners is no longer a competitive advantage but can often be a condition for business existence. While classic (paper) communication is still present in many aspects of business, digitalization is steadily replacing it.

In this chapter, we present basic business information systems, their importance for business operations, and integrated solutions for comprehensive business process management.

2 Business Information Systems Overview

When we talk about information systems, we can divide them in different ways according to their purpose. Each information system is intended to perform a specific business process or part of a process, and often different information systems are integrated and complement each other when managing processes. In general, modern business information systems can be divided into areas of application:

- Enterprise resource planning (ERP) systems are usually an integrated solution that includes functionalities for managing key business processes:
  - Supply Chain Management system (SCM).
  - Production planning and management.
  - Human resource management.
  - Finance and accounting.

    - Inventory management.
- Sales systems:
    - Customer Relationship Management (CRM).
    - Sales and marketing.
    - E-business and online sales.
- Business Intelligence and Data Analytics Systems:
    - Databases and Data Mining Systems.
    - Business Intelligence Systems (BI).
- Document systems.
- Process management systems:
    - Manufacturing Execution System (MES).
    - Process control system (PCS).
    - Warehouse management systems (WMS).
    - Transport management systems.
- Advanced Planning and Scheduling system (APS).

Depending on the various solutions, many of the listed systems can be combined into one comprehensive control system – ERP.

3 Overview of ERP systems

The beginnings of business automation date back to the 1960s and 1970s, when the first Material Resource Planning (MRP) systems appeared, which were used to plan material inventories and production. With development, these systems evolved into MRP II, adding functionalities to manage additional processes or resources, such as finance or accounting and human resources, for a more comprehensive view of business operations.

In the early 1990s, existing systems developed into today's established ERP systems, with the core idea being to integrate all major business processes into a comprehensive system.

The share of ERP systems in companies has continued to increase, so that today it is impossible to imagine operating without such systems in larger companies.

Further development of ERP systems initially aimed at developing user interfaces (access via a web browser), but recently there has been a shift to cloud solutions, where functionalities are accessible on external servers, thus transferring the cost of hardware and maintenance to the ERP service provider.

In the current period, we are mainly witnessing integration with other technologies, such as: Internet of Things (IoT), mobile devices, etc., and especially the inclusion of machine learning and artificial intelligence for the automation of routine tasks and predictive analytics.

Alongside general development, some ERP solutions are focused on the specifics of individual areas, such as healthcare, manufacturing, services, etc.

While different ERP implementations may offer different services, they can be broadly divided according to the type of installation and the type of license:

- **Local installation** – information systems are installed on the company's own information infrastructure. This allows for greater control and flexibility of the system but establishing and maintaining the necessary infrastructure can be costly, depending on the specific needs. Greater security is also a clear advantage, since confidential data is located within the company.
- **Cloud solution** – ERP system providers can also offer this as a service, with the system installed on the ERP service provider's infrastructure. Given that the costs of the hardware are covered by the provider, this can be a more affordable option for many companies. However, this option may result in potential risks for the interception of confidential data. Due to greater flexibility, this approach may be more suitable for small and medium-sized or rapidly changing companies.
- **Open-source solutions** allow greater control over the system, as they can largely adapt the operation to their needs. From a cost perspective, open-source solutions can also be free and costs arise mainly in maintenance and support. The latter is often carried out through a community of users in open-source solutions. Independence from the ERP system provider can also play an important role in this and insight into the code allows for transparency of operation. The weakness is often a limited set of functionalities, and adapting to requirements can incur significant costs. Integration problems are also usually

more common in open-source solutions. Shifting support to communities may mean less up-to-date and reliable support compared to proprietary options.

- **Proprietary solutions** mostly provide a larger set of functionalities already adapted to individual industries. Support is provided by the provider itself, which can be an important factor for many companies. Integration with other systems is also usually simpler with proprietary ERPs. The disadvantages are mainly higher acquisition and maintenance costs, dependence on the selected provider and, compared to open-source solutions, there is a greater possibility that the company will have to adapt its operations to the selected system instead of adapting the ERP system to its operations.

4 Selection and implementation of ERP systems

There are many factors to consider when choosing an ERP system for your business. The first and foremost is the cost of implementing the system, which can include:

- software acquisition cost,
- hardware acquisition cost,
- software and hardware maintenance cost,
- support services cost,
- implementation cost and others.

The implementation costs are certainly not the only factor that needs to be taken into account. In the selection process, it is first necessary to identify all the requirements arising from business processes and to establish criteria and evaluate their priorities. Equally crucial is the duration of the ERP solution implementation.

In the next step, a market survey is carried out based on the given requirements, in which the compliance of existing systems with these requirements is checked. After the selection of potential candidates, negotiations with ERP solution providers follow.

In addition to costs, other important criteria are (Alanbay, 2005):

- adaptability,
- implementation capability,

- maintenance,
- responsiveness to real-time changes,
- user experience,
- system requirements,
- support and training services,
- data and configuration backup,
- reporting and analytics tools,
- supplier reliability,
- integration capability with other systems,
- financing flexibility.

Given the diversity of requirements, it makes sense to use a multi-parameter decision-making method such as AHP (Podvezko, 2009). In this case, it is necessary to classify the criteria according to their impact or importance for business.

ERP system implementation is a demanding process in which business processes are adapted to the use of the system (Pelphrey, 2015). The steps involved in implementation are:

1. **Project plan:** within which the project team with representatives of individual departments determine the following: goals and performance requirements, a plan of essential tasks, deadlines and necessary resources, identification of possible pitfalls in the transition to ERP. In addition to end users, consultants from the ERP solution provider also participate in the plan.
2. **System plan and configuration:** allows the selected ERP system to be adapted to the specifics of individual company processes, if possible. In many cases, it is also necessary to adjust the ERP solution process. Individual system modules are set up to operate within departments by configuring properties, procedures and reports. In this section, data structures or databases are also established and integration with other systems is performed.
3. **Data transfer:** makes up another key element in the transition to an ERP system. In this section, it is necessary to clean up existing data and prepare a transfer plan to the ERP system database. During the transfer, it is necessary to ensure accuracy and integrity and data validation.

4. **Employee training** should be carried out before the actual transition to ERP. Plans are established for different users and their expected roles. It is crucial for training that employees raise any concerns that could affect the implementation of processes.
5. **Testing** is crucial for validating the functionality and effectiveness of ERP systems. This usually includes unit testing, integration testing and testing of the entire system. The goal is to detect any errors and deficiencies that then need to be fixed.
6. **The launch of the tested** and validated system marks the transition from the existing to the ERP system and a transition plan is also required here. The correct operation and effectiveness of the system are recorded and user support is particularly significant during this step.
7. **Completion of implementation and optimization** is the final phase in the transition to ERP operations. This involves assessing the effectiveness of the system, checking the success of the implementation project and identifying any problems. Depending on the identified needs, there is the possibility of implementing additional functionalities. Upon completion of the transition, maintenance and support procedures are also established.

There are various approaches to implementing ERP systems and the one a company chooses depends on the size of the company, industry, available resources, deadlines, and individual needs. The most common implementation approaches are:

- **Big Bang approach** in which ERP is implemented in all departments at once. The advantages of this approach are rapid implementation and immediate access to the system; however, the latter can pose a risk of disruption to business processes, especially in the case of incomplete or unsuccessful implementation.
- **Phased approach** involves the gradual implementation of individual functionalities or in groups. This approach also allows for gradual adaptation of the system (or process), thereby reducing the risk of major disruptions. This approach is generally more time-consuming and can lead to integration problems between individual functions.
- **Parallel implementation** assumes that the newly established ERP operates in parallel with the existing (old) system until efficient operation is ensured. This approach requires more resources for the operation of the redundant system but this greatly reduces the risk of interruptions.

- **The modular approach** assumes the establishment of each module, one by one, similar to the phased approach. The main difference is the emphasis on the introduction of individual functionalities in the phased approach, while in the modular approach, functionalities are established as part of individual modules. In this case, more important modules are given priority, and an easier overview of the implementation process is enabled. Even with the modular approach, problems can arise with the integration of individual functionalities, as they can be deeply intertwined between modules.
- **Unified implementation** is an approach in which each business unit or department establishes the ERP independently. This reduces the likelihood of interruption of other departments but may cause discrepancies in the intertwined processes of individual departments.

5 Basic processes and management in ERP

In this chapter, we will provide examples of typical business processes managed by ERP systems.

Within the sales module, ERP systems (Figure 4.1) enable, among other things:

- Contact management:
  - capturing and managing contacts (leads),
  - forwarding contacts to salespeople for communication planning,
  - recording communication with potential customers.
- Opportunity management:
  - converting contacts (potential customers) into likely customers,
  - recording the sales flow,
  - estimating expected sales values based on the probability of a successful opportunity.
- Management of offers and preliminary invoices:
  - creating invoices for products or services,
  - creating quotes and sales orders,
  - adding key information about quotes.
- Sales order processing:
  - converting confirmed pro forma invoices into sales orders,

  - determining order details (products, quantities, prices, discounts, etc.),
  - checking stocks and delivery times.
- Customer management:
  - managing customer data,
  - monitoring purchases and communications of individual customers,
  - categorizing customers according to criteria.
- Price management:
  - determining product pricing structures,
  - determining discounts based on purchase quantity, promotions, etc.,
  - ensuring price consistency across various sales channels.
- Invoicing:
  - issuing invoices to customers,
  - linking sales orders to deliveries,
  - including tax information and payment terms.
- Payment processing:
  - recording customer payments,
  - supporting payment methods (transfers, credit cards, etc.),
  - payment automation.
- Analytics and reporting.
- Sales forecasting.
- Integration with inventory management, finance and CRM modules.

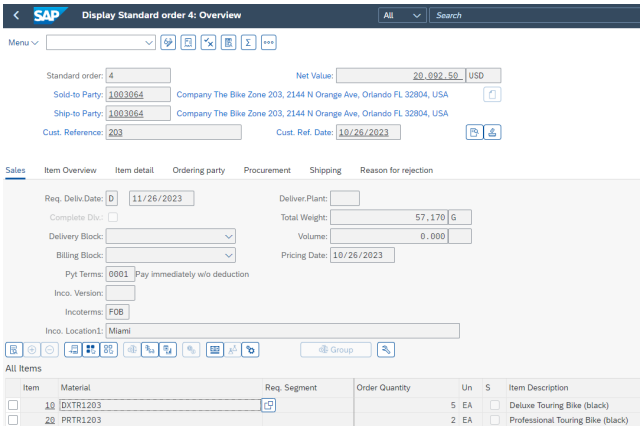


Figure 4.1: Example of a sales order in SAP

Source: own.

The basic processes performed within the production module are:

- Bill of materials management (BOM) (Figure 4.2):
  - creation of bills of materials for individual products,
  - definition of relationships and structures between individual product components.
- Routing and work center management:
  - defining production routes, product manufacturing sequence,
  - determining work centers and resources required for the production process.
- Production planning:
  - creating production schedules based on demand forecasts, existing sales orders or other requirements,
  - optimizing sorting to balance resource usage and meet deadlines.
- Materials planning:
  - calculating and planning the required materials/raw materials for production,
  - ensuring enough raw materials and components for production needs.
- Work order management:
  - creating and managing work orders for production,
  - monitoring the status of work orders against the production plan.
- Capacity planning:
  - assessing and managing the capacity of work centers, resources and machines,
  - preventing overloading or low utilization of production resources.
- Production activity management:
  - monitoring and recording production activities in the production hall,
  - capturing production data, resource utilization and machines in real time.
- Quality control:
  - establishing measures to check product quality,
  - carrying out quality assurance inspections.

- Inventory management:
  - updating inventory in real time as raw materials and components are used and finished products are manufactured,
  - picking and inventory management based on orders.
- Integration with inventory management, finance, and warehouse system modules.

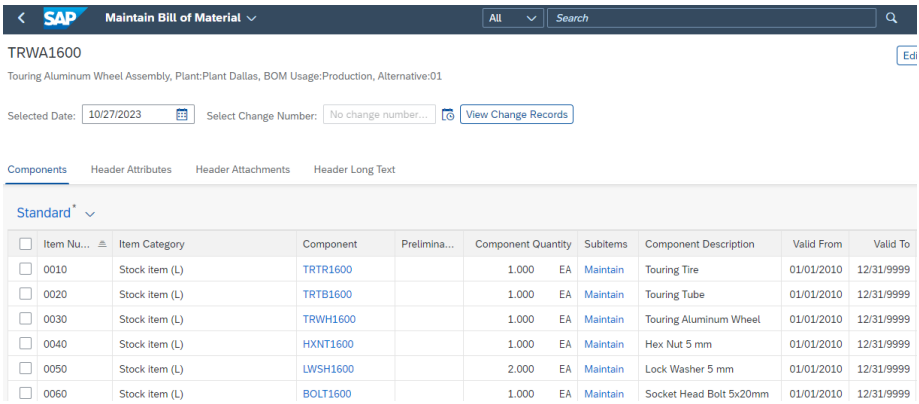


Figure 4.2: Example of BOM for a product in the SAP system
Source: own.

As part of human resource management, ERP supports:

Employee data management (Figure 4.3):

- employee database,
- capturing and updating personal data,
- maintaining profiles and histories.

Recruitment and candidate monitoring:

- creating jobs and hiring,
- monitoring applications,
- organizing interviews and assessing candidates.

Employee appraisal:

- setting performance expectations,
- conducting employee performance appraisals,
- monitoring employee performance.

Attendance recording:

- recording arrivals and departures,
- monitoring absences/vacations/sick leave,
- generating attendance reports for payroll.

Payroll:

- calculating and paying salaries,
- deducting taxes and benefits,
- generating payroll.

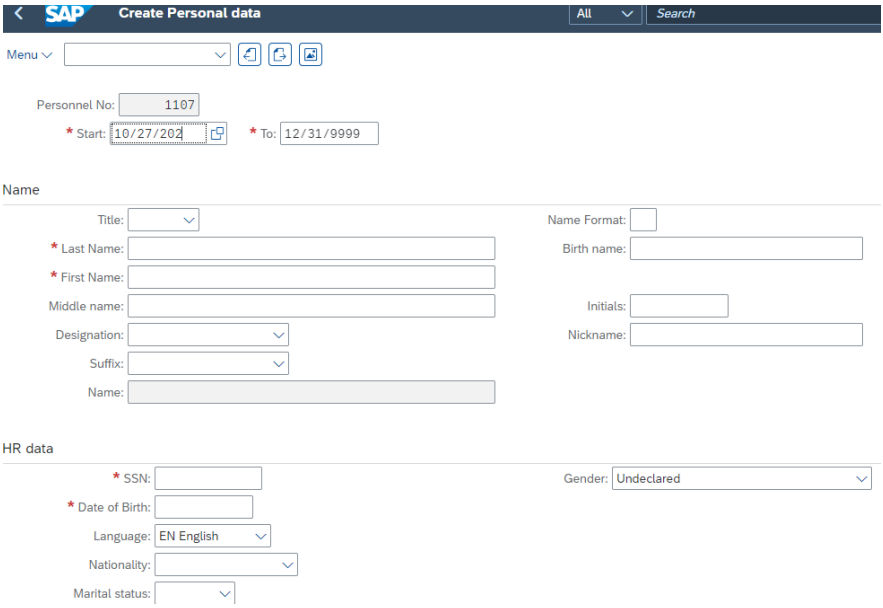


Figure 5.3: Example of entry for a new employee in the SAP system
Source: own.

The main tasks supported by ERP in procurement are:

Supplier management:

- maintaining supplier data, contacts, business history,
- evaluating and categorizing suppliers based on reliability, costs, and service quality.

Search for suppliers and requests for offers:

- finding possible suppliers for products or services,
- creating requests for quotes (request for quotation) and their management,
- assessment and comparison of quotes.

Procurement:

- making purchases based on needs,
- determining products or services and quantities,
- preparing resources and authorizations.

Purchase order:

- creating and approving purchase orders to selected suppliers,
- determining details (quantities, prices, payment and delivery terms),
- forwarding the purchase order to the provider and internal services for approval.

Defining approval procedures:

- determining approval stakeholders,
- determining approval responsibilities and directing approvals,
- ensuring compliance with business process procedures.

Supplier Negotiations and Contract Management:

- leading negotiations to achieve favorable terms,

- creating and managing contracts with suppliers,
- monitoring contract implementation and renewal.

Product Receiving and Inspection:

- recording products received from suppliers,
- reviewing quality and compliance with requirements,
- updating inventory and finances.

Accounting:

- checking the consistency of invoices and received shipments,
- confirming prices, quantities and terms,
- confirming invoices and payments.

In all activities, the connection between actual events and the information flow that accompanies these events is essential. For every activity in business, there must be a connection between actual and information flow. Each activity performed must be recorded or confirmed in the ERP system, and the ERP also specifies which activities must be performed.

Just as actual material flows, performed services and other activities are stored in the ERP system in real time, for example, when a shipment is dispatched (and the activity is confirmed), inventories are recalculated.

ERP systems with central operation ensure that each department has up-to-date data available and only those that individual participants in the process are allowed to access.

Since there is usually interdependence in the activities of individual departments, data consistency is also important in ERP systems. This way, a production plan can be created based on confirmed sales orders and purchase orders for the necessary raw materials can be created.

An additional advantage that ERP systems offer here is the automation of processes. For example, a sales order can be automatically created after an order is confirmed, or a production plan can be created based on the orders. Of course, confirmation by an authorized employee in the relevant department is still required at key stages.

6 Systems integration

Depending on the type, companies can use an ERP system as a standalone tool, but in many cases, integration with others is required. Figure 5.4 shows an example of automation levels and systems. ERP systems here constitute the top management level that oversees the operation of the entire business.

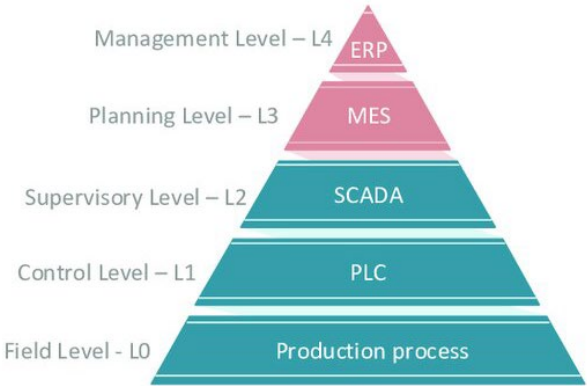


Figure 5.4: Automation according to ANSI/ISA-95
Source: (Pospisil et al., 2021).

Support systems are set up according to the level of use. Thus, at the lowest level, we are talking about the production process at machine level. Programmable Logic Controller (PLC) systems enable the control or management of individual machines and are the basis for production automation. Supervisory Control and Data Acquisition (SCADA) systems are responsible for monitoring events, which collect and display data from devices and sensors and enable remote management. Manufacturing Execution System (MES) systems manage and control production. With a PLC connection, it provides deep insight into the execution of the process and ensures the continuous exchange of data on production orders, inventories, quality checks and other key production indicators in real time.

The design of ERP systems must be compatible with other existing system solutions, which is why horizontal integration is also necessary in many cases. This can include connectivity with user software, such as office solutions, communication applications, etc. Above all, appropriate sharing of data and access to it between individual departments is essential. In horizontal integration, it is necessary to carefully plan operations based on business processes.

7 Conclusion

ERP and their support systems are of key importance for today's businesses, as they no longer offer a competitive advantage but are indispensable for successful operation. By integrating such systems, it is possible to provide not only information support for business processes but also their implementation with a high level of automation. It is precisely the automation of frequent routine activities that helps to increase the efficiency of business activities. Unified access enables a high level of transparency and thus also increases the reliability of processes and often, by reducing human influence, also reduces the likelihood of errors. Given extensive data or information support, the systems enable advanced business analyses and decision-making support at the operational, tactical and strategic levels.

References

Alanbay, O. (2005). *ERP Selection Using Expert Choice Software*. 10. https://doi.org/10.13033/isahp.y2005.030

Pelphrey, M. W. (2015). *Directing the ERP Implementation: A Best Practice Guide to Avoiding Program Failure Traps While Tuning System Performance* (1st ed.). CRC Press. https://www.routledge.com/Directing-the-ERP-Implementation-A-Best-Practice-Guide-to-Avoiding-Program-Failure-Traps-While-Tuning-System-Performance/Pelphrey/p/book/9781482248418

Podvezko, V. (2009). Application of AHP technique. *Journal of Business Economics and Management - J BUS ECON MANAG*, *10*(2), 181–189. https://doi.org/10.3846/1611-1699.2009.10.181-189

Pospisil, O., Blazek, P., Kuchar, K., Fujdiak, R., & Misurec, J. (2021). Application Perspective on Cybersecurity Testbed for Industrial Control Systems. *Sensors*, *21*(23), Article 23. https://doi.org/10.3390/s21238119

Simulations in Decision Making

Bojan Rupnik
University of Maribor, Faculty of Logistics, Celje, Slovenia
bojan.rupnik@um.si

DOI
https://doi.org/10.18690/um.fl.2.2026.5

ISBN
978-961-299-074-9

Keywords:
simulations, discrete event simulation, digital twin, material flow, queuing systems

Logistical, production, transportation, and all related issues in the industry follow similar processes, with time being the crucial factor. While some processes can be relatively easily analysed due to their simplicity, the more interconnected the processes are, the more challenging it becomes to describe them accurately using traditional analytical approaches. Simulations, in this regard, provide a deeper insight into the flow of such processes. They enable the analysis of efficiency, shortcomings, and, most importantly, allow for the examination of existing systems under different conditions without interfering with their operation. Besides having a good understanding of the processes, data support is crucial for simulation. This support can involve the recording of historical data and predicting future events with possible alternative scenarios. By enabling real-time data logging during process execution and providing the data to an active simulation that processes it in real-time, a digital twin can be created. Within the scope of this subject, participants familiarize themselves with server systems, queuing systems, discrete event simulations, and the tools that support them, along with examples of their application in manufacturing, logistics, and transportation scenarios.

University of Maribor Press

1 Introduction

With simulations, we try to map real-world events into a mathematical or computer model, with which we can repeat these events, change them, and observe how they behave under different conditions. Most areas of the business world can be analyzed with simulations, such as material flows in production plants or warehouses, simulations of transport flows, information or financial flows. Simulations are therefore used not only for the analysis of such systems, but also for optimization - especially when systems are too computationally complex to be optimized in a timely manner using classical optimization methods.

Depending on the type of problems we are solving and the purpose of optimization, there are several different simulation approaches:

- 3D/real-time simulations (e.g. pilot training simulations),
- system dynamics (simulations of complex, comprehensive systems),
- agent simulation (observing people, entities interacting in space and time),
- discrete event simulation.

The latter approach is at the forefront of this work. Discrete event simulations allow for the description of any systems where individual events influence the further behavior of the events. The method itself is fundamentally simple. The entire system is designed with states that are changed only by events at predetermined times. Unlike continuous simulations, the state is always unchanged between individual events, regardless of the elapsed time. Events can be defined in advance (e.g., expected customer arrivals), or they can generate new events themselves.

2 Process modeling and simulation

Regardless of the field, all processes include a time component. Thus, based on behavior, we observe what is happening in a particular system and how long something takes. Here we can consider input flows, such as customer arrivals to the store, duration of purchase, waiting in front of the cash register. This example can be mapped to many others, where we talk about inputs, processing and finally output from the system.

2.1 Server Systems and Queues

A basic example (Figure 5.1) of a server system (Thomopoulos, 2012) includes a queue in which entities wait for processing and a server that processes these tasks, and the operation of the system depends on the server's processing capacity, the intensity of task arrivals and the capacity of the queue. Depending on the nature of the simulation, entities can represent tasks, packages, customers, information, workpieces or practically any element that affects the events within the simulation.

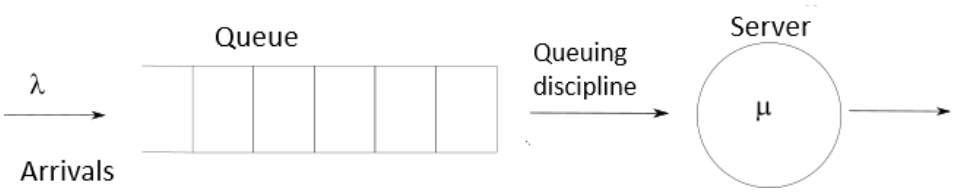


Figure 5.1: Basic server system with queue
Source: own.

The arrival rate determines how often entities arrive in the queue. In general, the arrival rate can be given as:

$$\lambda = \frac{N}{T} \tag{1}$$

where λ is the intensity, N the number of arrivals and T the time interval of arrivals.

According to the process, each entity is placed in a queue from which it is forwarded to the server, if it is available. In the case of multiple waiting entities, the selection of the next one to be forwarded can be done using different approaches:

- FIFO (First-in, First-out) approach, where each task is submitted to the server in the order in which it arrives.
- LIFO (Last-in, Fast-out) approach, where the last task to enter the queue is submitted to the server first.
- Priority queues allow for priority treatment to be set for certain tasks or groups of tasks. Thus, entities with higher priorities are submitted to the server before those with lower ones.

- Random approach determines a random entity in the queue.

Depending on the intensity of arrivals and the availability of the server, the entities in the queue can accumulate, decrease or wait in the queue for an average uniform amount of time. In system modeling, the latter variant is usually sought, as it allows for stable systems.

In addition to the intensity of arrivals, a key factor is also the service rate μ, which is given by the number of entities that the server can process per unit of time. The service rate is thus given as the reciprocal of the service time.

$$\mu = \frac{1}{S} \tag{2}$$

S represents the service time. Like arrivals, service time can also be subject to randomness. Thus, we distinguish service speeds into:

- deterministic,
- stochastic.

In some cases, the service time is constant and known in advance, while in others it depends on factors and is random. The modeling of service times is usually appropriate for exponential or normal distributions, depending on the type of process.

The presented model (Figure 5.2) allows for the simulation of a very basic process with one queue and one server. However, imitating real-world cases requires the construction of more complex networks, where each building block can have multiple inputs and outputs. Depending on the complexity of the case we want to model, complex models can be created where the flow is influenced not only by the connections between the building blocks, but also by the rules for sorting by individual, conditionally determined arrivals and by the serving rules. It is therefore sensible to model and simulate such cases in appropriate dedicated tools.

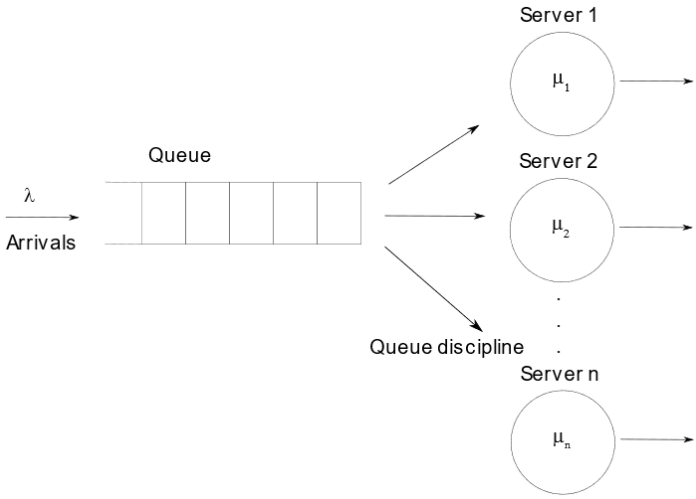


Figure 5.2: Server system with multiple servers
Source: own.

Kendall's notation is used to describe the main characteristics of queueing systems (Bolch et al., 2006). The basic notation is in the following form:

$$A/B/c/K/m/Q \tag{3}$$

where represents:

A – arrival time distribution,
B – service time distribution,
c – number of servers,
K – queue capacity,
m – population size,
Q – service strategy.

The values thus taken by components A and B are:

- M – exponential distribution,
- D – deterministic distribution,
- E – Erlang distribution,
- G – general distribution.

The number of servers c p specifies how many servers can be used to perform parallel services.

Capacity K determines the maximum number of clients in the system, both in the queues and on the server, while m represents the expected number of clients. The previously mentioned server strategies (FIFO, LIFO) determine how entities are delivered from the queues.

2.2 Discrete event simulation

While queueing systems are primarily an abstract representation, a more advanced approach is needed to model more complex systems. Discrete event simulations (Fishman, 2002) are one of the most widely used approaches, alongside e.g. system dynamics or agent simulation. They are commonly used in simulating problems in manufacturing, healthcare, transportation and logistics, energy systems, supply chains, and related fields.

Queuing systems assume a straightforward flow between arrivals and processing. In discrete event modeling, in addition to the entities, queues, and servers themselves, characteristics, rules, resources, and events are also considered. As part of the simulation, a list of all events and their expected time are built based on the model. An event represents any change in the system, such as a customer entering a queue, the start or end of processing a product on a machine, or a change in the properties of an entity. Each event changes the state of the simulated system.

The simulation is performed in simulation time, which does not run in real time, but discretely skips the times between individual events. Individual events can also create new events, which are also placed in the list of future events, which can cause some already planned events to be postponed.

During the simulation itself, statistics on queues, server utilization, throughput and other parameters are recorded, which can be used to provide an appropriate analysis of simulated systems.

Two more key elements in the implementation of simulations are verification and validation. Verification checks the correctness of individual implemented functionalities, calculation formulas, logic. Validation checks how well the model imitates the real system. For this purpose, the simulation results are compared with the expected behavior of the real system, which is obtained from measurements or expert assessment. Verification and validation are repetitive processes that lead to greater accuracy and reliability of the created model. Sensitivity analysis can also be used to assess areas of uncertainty.

2.3 Modeling simulation parameters

The methods of modeling the input parameters of the simulation depend on the type of simulated system and the available data. In this, a good understanding of the processes based on which it is possible to model the material flow is required in the first phase. Thus, it is necessary to identify all the factors (processes or parameters) that can affect the behavior of the system, such as:

Entities and their properties – what are the key elements of the simulation, how can their properties affect the material flow (entities with different properties have different flows through the network, for example).

Simulation objects – any building blocks of the simulation tool that affect the state of the system – sources, sinks, servers or processors, queues, objects for combining or uncombining entities, objects for changing entity properties, event generators.

Material flow – connections between all objects from or to which entities can move. In this case, it is necessary to carefully determine the conditions for redirection from individual objects to successors.

Input intensities – the example given at the beginning of the chapter is just one of the options for modeling inputs. When modeling inputs from real systems, we can use:

- Deterministic values – in systems where quantities and times are well-defined (e.g. train schedules, meeting schedules, etc.).

- Dynamic arrivals – input loads can depend on various factors such as the number of vehicles during rush hour.
- Fitting to statistical distributions – when we have appropriate data available, input loads can be modeled by fitting to statistical distributions.
- Historical data – where we have records of events in the systems (e.g. MES systems), we can perform an analysis by fitting to statistical distributions.
- Expert estimates – in the absence of records, the assessment of the behavior of individual building blocks can be estimated based on the empirical assessments of experts.
- Random values – randomness is a key element of simulations. In arrival modeling, random values are used within appropriate ranges or random values are generated according to appropriate distributions.
- Sensitivity analysis - input parameters can be varied to assess how the system behaves under different initial settings under certain assumptions.
- Service speeds – obtaining service speeds is like input intensities. It is often possible to obtain service speeds from knowledge of process durations such as production machine specifications, transport speeds, etc.

Regardless of which approach is used, it is necessary to carefully examine all selected parameters (model validation) depending on the modeled system.

2.4 Random values

The generation of random values is one of the fundamental concepts in simulations, which is why we dedicate a chapter to it. Generating a random number (L'Ecuyer, 2007) is a mathematically simple operation, but if approached incorrectly, it can lead to the appearance of patterns. The appearance of patterns in the generation of random numbers can lead to inappropriate behavior of the simulation, as unwanted dependencies may appear in the simulation flow, which would otherwise not be expected in a real system.

Computer systems for generating random values use pseudo-random number generators, where the calculation of the random value is performed by a function with an input variable. An example of a simple linear congruence generator is given by the formula:

$$X_{n+1} = (aX_n + c)\%m \tag{4}$$

Here they represent:

X_n- generator seed,
a – multiplier – determines the period and quality of randomness,
c – increment – sequence shift for greater variety of generated numbers,
m – divisor – determines the range of generated numbers.

The properties of the sequence of random numbers generated by such a generator depend on the choice of given parameters. The purpose of generators is to create as much entropy or unpredictability of states as possible, so the choice of seed is also important. When using the same seed, the function will always generate the same sequence of pseudo-random values. Depending on the needs, this may be desirable, such as when implementing different configurations with the same initial inputs or for verification. In most cases, however, it is desirable to disperse the random values as much as possible. In such cases, it makes sense to choose the generator seed as randomly as possible, for example from the current processor time when generating the random value. A linear congruence generator generates integers on the interval $[0, m-1]$, but often the generation of real numbers on the interval $[0,1]$, is desired, mainly for the purpose of normalizing the values. For this purpose, the new number is divided by m.

In modeling most real-world problems, the intensity of arrivals occurs randomly, but this randomness can usually be limited. The intensity of arrivals is thus often modeled by distributions where the arrivals are independent and follow each other at equal intervals on average. Modeling of real-world random processes is often done using the Poisson distribution:

$$P(X = k) = \frac{(\lambda^k e^{-\lambda})}{k!} \tag{5}$$

where ($P(X = k)$ is the probability of occurrence of k events, λ is the average intensity of arrivals in the time interval, and k is the number of events for which we want to find the probability. The Poisson distribution is useful in describing events such as:

- modeling customer arrivals to a store over a certain period of time,
- analysis of the number of production defects,
- forecasting the number of accidents on a section within a time period,
- arrivals of e-mail messages.

Modeling of input flows or service speeds is performed by fitting to statistical distributions (Johnson, 1987), such as Poisson or normal. These can be determined using statistical tests, histogram shape estimation, least squares, and other approaches. Once the process distributions are known, they can be used to generate random events that follow the same statistical characteristics as the systems under study.

An example of calculating randomly generated values according to a Poisson distribution with mean λ is shown in the following procedure:

$$
\begin{aligned}
&\boldsymbol{function}\ Poisson(\lambda)\\
&L = e^{-\lambda}\\
&k \leftarrow 0\\
&p \leftarrow 1\\
&\boldsymbol{while}\ (p > L)\ \textbf{do}\\
&k \leftarrow k + 1\\
&p = p * rand()\\
&\textbf{end}\\
&Poisson = k
\end{aligned}
$$

Pseudocode 1: Poisson random value generator

3 Simulation example

For a simulation example, let's take a store where customers enter, search for products for different lengths of time, and finally purchase them at the checkout. Let's define the system properties:

- 5 customers enter on average per minute,
- number of cashiers: 5,
- average purchase duration: 15 min,

– the transaction at the checkout takes an average of 5 minutes.

According to Kendall's notation, a basic server system could be described by:

$$M/M/5/30/3000/FIFO \tag{6}$$

assuming exponential customer arrivals and service, 5 cash registers, an estimated store capacity of 30 customers, and a total number of customers rounded to 3000 (estimated for one business day). We choose FIFO as the serving strategy, meaning that customers are served according to their arrival (and purchase) time.

The input parameter here represents the average arrival time between two consecutive customers. Assuming that customer arrivals are a Poisson process, we can model random arrival times as follows:

$$t_i = \frac{-\ln rnd()}{\lambda} \tag{7}$$

Table 1: Example of randomly determined arrivals according to an exponential distribution

	Random time [s]	Next arrival [s]
1	0,010422473	0,625348364
2	0,44356782	27,23941755
3	0,047033142	30,06140609
4	0,561568412	63,7555108
5	0,416494108	88,74515728
6	0,083158277	93,73465391
7	0,023527478	95,14630261
8	0,052567808	98,30037111
9	0,130142537	106,1089233
10	0,055501926	109,4390389
11	0,010422473	144,9275279
12	0,44356782	152,8945772
	…	…

Source: own

The given simulation example can be analyzed with server systems with queues, but the complexity increases with each added element. Therefore, it is advisable to use appropriate simulation tools for such problems. Simulation tools cannot be expected to produce simulation results that are completely consistent with theoretical calculations due to rounding errors and randomness, but with a well-designed simulation model, the results should come close to theoretical calculations.

From the given simulation example, we can quickly see that the system is not sustainable; with an average number of 5 customers per minute and 5 cash registers with a service speed of 5 minutes. The shopping time here represents an example that customers perform simultaneously. If we were to use Kendall's notation to describe only this part, we could describe it as a process, which can be simplified as:

$$M/M/\infty \tag{8}$$

because when shopping, each customer makes their own purchase and does not even need to enter the queue. Therefore, this segment can be considered unlimited (each customer has their own immediately available server). Customer arrivals represent arrivals as generated, and for the service speed, we consider an average of 15 minutes per customer according to the given parameters. After making a purchase, customers enter the queue (or queues in front of individual cash registers). In a concrete simulation, we should of course take into account various factors, such as working hours, breaks and snacks, loads at different times during the day, etc.

The presented example can be modeled in simulation tools (Figure 5.3) and avoids the multitude of calculations involved in increasing the complexity of server systems with queues.

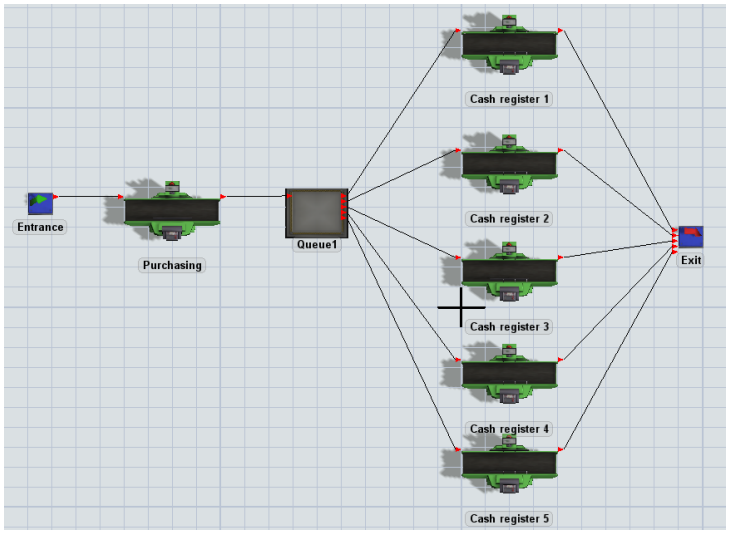


Figure 5.3: Trade simulation model in FlexSim

Source: own.

Since the given example is unstable (constantly growing queue and constant occupancy of the cash registers), let's check how we could change the system to be sustainable. We can mainly use two approaches. We can add additional cash registers or replace them with faster ones. For this scenario, we leave all settings and characteristics the same, only we speed up the cash registers by a factor of 5 (still according to an exponential distribution).

The goal of each simulation is to determine the capabilities of the modeled system, which includes various characteristics. In this case, we focus on the size of the queue (Figure 2.4) and the waiting times in it (Figure 2.5) and the utilization of the cash registers (Figure 2.6).

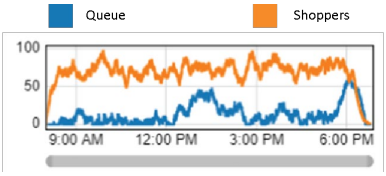


Figure 2.4: Queue length
Source: own.

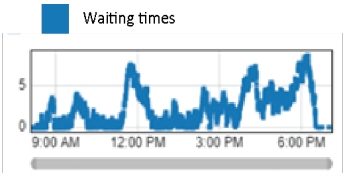


Figure 2.5: Waiting times in the queue
Source: own.

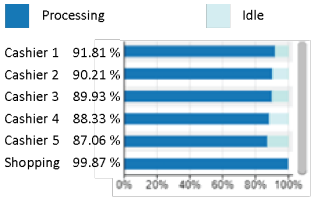


Figure 2.6: Cash register utilization
Source: own.

The simulation results show a (relatively) stable system with changed characteristics, as we do not have constantly increasing queues and waiting times. In simulations of complex systems, it is often necessary to find solutions that avoid bottlenecks and unused resources.

7 Conclusion

The presented example shows only a fraction of the capabilities that simulations offer. The great usefulness of simulations is especially evident in the study of complex systems, where seemingly unrelated parameters are involved. Thus,

simulations are used in logistics, finance, information, production, or in fact any related field. In the field of logistics, simulations represent a cost-effective approach to the analysis of production processes, transport routes and routing, traffic patterns, etc. By changing the parameters of the simulation or simulation scenarios, it is possible to observe complex systems from different perspectives, which enables effective decision-making based on rational analyses.

Performing simulations allows a cost-effective approach to the analysis of complex systems without the need to interrupt processes. In today's technological systems, there is an increasing integration of various solutions, from ERP, MES, PLC, SCADA systems and others. While such systems mainly record and can also largely manage processes, simulation represents an alternative option for optimization by comparing alternatives and supporting decision-making. Recently, digital twins have come to the fore, providing a comprehensive insight into various company processes. Digital twins capture the events of a company's processes in real time from sensors, machines, devices and other sources (Internet of Things) and build a virtual representation based on them. Simulations performed on a virtual image of a real system provide a deeper insight into operations and business and represent added value in business decision-making at all levels.

References

Bolch, G., Greiner, S., Meer, H. de, & Trivedi, K. S. (2006). *Queueing Networks and Markov Chains: Modeling and Performance Evaluation with Computer Science Applications, 2nd Edition | Wiley* (2nd ed.). John Wiley & Sons. https://www.wiley.com/en-us/Queueing+Networks+and+Markov+Chains%3A+Modeling+and+Performance+Evaluation+with+Computer+Science+Applications%2C+2nd+Edition-p-9780471565253

Fishman, G. (2002). Discrete-event Simulation: Modeling, Programming, and Analysis. In *J. Artificial Societies and Social Simulation* (Vol. 5). https://doi.org/10.1007/978-1-4757-3552-9

Johnson, M. E. (1987). *Multivariate Statistical Simulation: A Guide to Selecting and Generating Continuous Multivariate Distributions* (1st edition). Wiley.

L'Ecuyer, P. (2007). Random Number Generation. In *Springer Handbooks of Computational Statistics* (pp. 93–137). https://doi.org/10.1002/9780470172445.ch4

Thomopoulos, N. T. (2012). *Fundamentals of Queuing Systems: Statistical Methods for Analyzing Queuing Models*. Springer Science & Business Media.

AUTONOMOUS VEHICLES IN INTRALOGISTICS

DARKO HERCOG,[1] PRIMOŽ BENCAK[2]

[1] University of Maribor, Faculty of Electrical Engineering and Computer Science, Maribor, Slovenia
darko.hercog@um.si
[2] University of Maribor, Faculty of Logistics, Celje, Slovenia
primoz.bencak1@um.si

Automated guided and autonomous vehicles are increasingly used in intralogistics processes to transport goods or support order picking. The publication provides a brief overview of the areas of automated and autonomous vehicles, their differences, and potential applications in intralogistics. The reader is introduced to the basic theory of the operation of autonomous mobile robots' (sub)systems (drive, sensors, localization, and navigation). For ease of understanding, web links to videos are added, which support the theory with a practical demonstration. Finally, in an example of the autonomous mobile robot MiR100, the operation of the mobile robot and its functions are presented.

DOI
https://doi.org/10.18690/um.fl.2.2026.6

ISBN
978-961-299-074-9

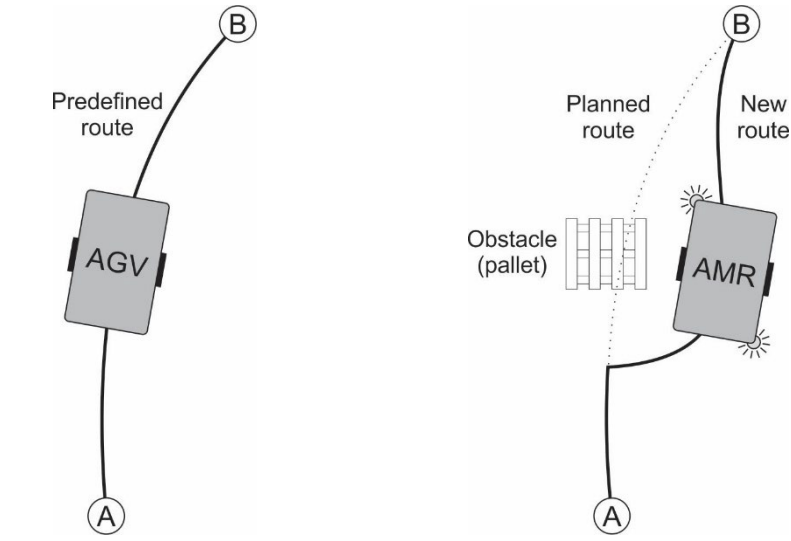
Keywords:
autonomous vehicles, autonomous mobile robots, AMR, automated guided vehicles, AGV, intralogistics

University of Maribor Press

1 Introduction

Autonomous and automated guided vehicles enable the autonomous transport of various loads within production or logistics processes. Automated guided vehicles, for which the abbreviation AGV is used, have been present on the market for quite some time; the first such vehicle was manufactured in 1950. AGVs follow fixed and pre-marked paths (Figure 1.1-a), whereby various systems are used to mark the path, such as tracking wires or magnetic strips. The vehicle recognizes the marked path with the help of installed sensors and then follows this path with the help of a drive and control system. In addition, these vehicles also contain sensors for detecting the presence of obstacles on the marked path. In the event of a detected obstacle, the vehicle must stop and wait for the obstacle to be removed (Figure 1.1-a). AGVs represent a simple and affordable solution for autonomous internal transport, as they are based on simple detection, processing, and decision-making systems. However, these vehicles have several disadvantages, namely: (1) they follow fixed and predetermined routes, (2) in the event of an unexpected obstacle on the way, the vehicles stop, (3) the operation of the vehicles requires a change in infrastructure and later also maintenance of this infrastructure, etc. Despite the disadvantages, these vehicles are widely used in industry today, namely for less complex cargo transport from one location to another.

Less than a decade ago, newer vehicles began to appear on the market, for which the term autonomous mobile robots or the abbreviation AMR is used. These vehicles have a certain level of intelligence and can make decisions independently when they encounter new or unforeseen situations. AMRs perform localization and navigation using sensors and advanced algorithms, and a loaded map or a map of the space in which they perform transport tasks (Siegwart, Nourbakhsh, & Scaramuzza, 2011). AMRs contain numerous sensor systems, among which safety laser scanners are particularly important. As a result, they can operate near people and other dynamic obstacles, and are also able to drive through doors, corridors, and use elevators. With built-in sensors and sophisticated software and hardware, they detect objects in their immediate surroundings and, using advanced algorithms, independently calculate the optimal route to the destination. In the event of a detected obstacle on the intended route, these vehicles independently find an alternative route and continue to deliver the cargo to the target location (Figure 6.1-b). In the following, the term autonomous vehicles will also be used for AMR vehicles, and automatic vehicles for AGV vehicles.



(a) Automated guided vehicle **(b) Autonomous mobile robot**

Figure 6.1: The path of an automatically guided (left) and autonomous vehicle (right)
Source: own.

Due to their many positive attributes, sales of AMRs are growing rapidly. Annual sales currently amount to over 3 billion US dollars and are expected to grow to over 10 billion in the next five years (6.2).

Autonomous vehicles are adaptable, as they adapt to changes in the environment. They can be programmed and adapted to perform various tasks relatively easily. Automated vehicles, on the other hand, are designed for predefined routes and tasks, and are therefore less adaptable to changes in the environment. Changing their routes or tasks requires changing the physical infrastructure. The introduction of autonomous vehicles includes mapping or creating a map of the space in which the vehicle will operate, configuring the vehicle, and programming transport tasks. The introduction of these vehicles does not require the installation of physical routes or any other interventions in the existing infrastructure. When introducing automated vehicles, however, it is necessary to adapt the environment and install tracking paths, which can be quite time-consuming and expensive. Autonomous vehicles are suitable for performing tasks in dynamic environments, such as warehouses or manufacturing plants, where vehicles move near people, equipment, and other obstacles. Automated vehicles, on the other hand, are used in transport processes,

where routes are precisely defined in advance and, generally, do not change over time. Autonomous vehicles are considered more cost-effective in the long term, as they require less investment in infrastructure and can adapt to changing needs.

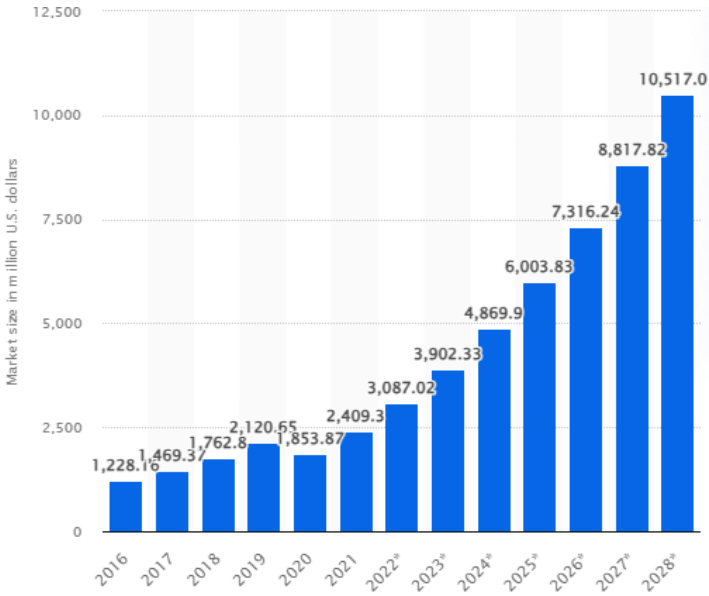


Figure 6.2: Global AMR Market Size from 2016 to 2021 with Forecast to 2028
Source: (Statista., 2023)

1.1 Vehicle types

There are many different types of autonomous and AGV on the market, including (Wikipedija, 2023)

- Pallet Trucks: These vehicles are primarily used for transporting pallets and do not contain a mechanism for automatic loading/unloading of loads. The vehicles only contain a mechanism that allows pallets to be raised and lowered within a range of a few centimeters.
- Fork Trucks: These are equipped with forks and are primarily used for the independent transport of loads on pallets. They are used in transport where there is a height difference between loading and unloading. This type of vehicle is one of the more expensive vehicles.

- Towing Trucks: These vehicles are designed to tow passive trolleys or trailers loaded with various loads. They are often used in production processes to supply assembly lines with the necessary material.
- Unit Load vehicles are designed to transport various loads, such as pallets, crates, or containers. The vehicles have a platform that includes a mechanism for lifting/lowering the load, powered/unpowered transport rollers, belt conveyors, etc.
- Light Load vehicles are vehicles with a load capacity of up to 500 kg. They are used to transport lighter objects, such as boxes, baskets, or other materials.
- Specialized Trucks: These vehicles are adapted to specific applications, such as transporting in clean rooms, hazardous substances in chemical plants, etc.

Table 6.1 summarizes links to YouTube videos showing different types of vehicles. The videos can be accessed by clicking on the YouTube icon. If the link does not work, the video can be searched on YouTube using the relevant keywords.

Table 6.1: Examples of different types of autonomous and automated guided vehicles

Type of vehicle	Video	Keywords
Pallet trucks	▶	Nipper B.V., Nipper AGV
Fork trucks	▶	Jungheinrich UK, AGV Forklift Trucks by Jungheinrich
Towing trucks	▶	DF Automation, AGV towing multiple trolleys
	▶	JD Universal, Unidirectional Towing AGV for Logistics Transportation
Unit load	▶	Dematic, Unit Load AGV - Warehouse Automation by Egemin Automation Inc.
	▶	IBG Automation, AGV - Automated Guided Vehicle
Light load	▶	SSI SCHAEFER Group, Automated Guided Vehicle Weasel®, E-Commerce, Supply Chain, Hermes Fulfilment GmbH

1.2 Use of autonomous vehicles in intralogistics

AMRs are used in intralogistics and warehouses for various purposes, such as:

- supply of production workstations,
- transport of goods in warehouses and distribution centers,
- support in the picking process, etc.

In industry, AMRs are mainly used to supply production workstations with the necessary materials. This supply is provided by dedicated autonomous vehicles, such as autonomous forklifts or universal autonomous vehicles, whose functionality is changed with a top module and thus adapted to specific tasks. In practice, the most common types of supply to production workstations are: (a) towing vehicles, (b) vehicles with a shelf rack, (c) with a transport system, and (d) with a lifting table.

In warehouses and distribution centers, autonomous vehicles are mainly used to support order picking. In parts-to-picker order picking, mobile racks and AMRs with a lifting mechanism are used. In the warehouse, the vehicle lifts the entire rack and transports it to the workstation where the order picker is located. When the order-picker picks the required products from the rack, the AMR transports the rack back to the warehouse. In picker-to-parts order picking, autonomous vehicles provide support to the order picker. Order pickers move along the aisles between the rack shelves and pick goods according to the order in the work order. Order pickers pick goods from the shelves and place them in boxes located on the autonomous vehicle, which transports the goods to the warehouse input/output area.

2 AMRs

AMRs contain numerous components (subsystems) that enable autonomous environmental sensing, localization, navigation, and transportation tasks. The most important ones include:

- Sensor system: This contains numerous sensors (inertial, optical, 3D cameras, ultrasonic sensors, etc.) with which the vehicle detects its surroundings. In addition to the basic sensors, some vehicles also have other sensors that are used for special tasks, such as barcode readers, radio frequency identification (RFID) readers, or environmental sensors.
- Location system: AMRs must know their exact location in the environment in which they are located. This is provided by the localization system, which, based on data obtained from various sensors, estimates the current position and orientation of the robot relative to its internal map.
- Navigation system: The navigation system is a key component for autonomous vehicle operation, as this system is responsible for route planning. Based on the initial and final locations and considering space restrictions (walls, prohibited

areas, etc.), the navigation system calculates the optimal path for the robot. In the event of a detected obstacle on the calculated path, it searches for an alternative.

- Safety system: Autonomous vehicles must not endanger the safety of people and/or equipment under any circumstances. As a result, vehicles include various safety components, such as safety laser scanners, collision detection sensors, and emergency stop buttons, which ensure safe operation of the vehicle even in the immediate vicinity of people.
- Battery management system: AMRs are usually battery-powered. The battery management system ensures optimal battery operation in order to achieve the longest possible battery life.
- Communication system: This enables communication with other systems. AMRs most often use wireless communication modules (e.g., Wi-Fi or Bluetooth).
- User interface: The user interface, which is usually accessible via a special touch screen or web interface, allows monitoring the status of the robot, manual control of the robot, display of notifications and warnings, display of an area map, programming of the robot, etc.
- Drive system: The drive system includes drive motors, gearbox, wheels, and drive motor controllers. By controlling the drive wheels appropriately, the vehicle follows a previously calculated path.
- Machine learning and artificial intelligence systems: Some advanced vehicles also include machine learning and artificial intelligence systems. These systems are used to recognize objects, optimize routes, tasks, etc.

2.1 Drive and Steering System Configurations

AMRs and AGVs contain a drive and steering system. The drive system enables the vehicle to move in the longitudinal direction, and the steering system enables the vehicle to turn. Generally speaking, there are four basic drive and steering configurations (Roboteq Inc., 2013)

1. Differential drive:
   - with four driving wheels.
   - with two driving wheels and one or more castor wheels.
2. Steer drive contains a wheel that is both drive and steer.

3. Ackerman drive. In this configuration, the rear wheels are driven and the front wheels are steered.
4. Mecanum configuration is similar to that of the differential drive with four drive wheels, but instead of regular wheels, so-called mecanum or Swedish wheels are used. By appropriately guiding these wheels, it is possible to achieve movement of the mobile robot in any direction.

In autonomous and automatically guided vehicles, the most commonly used differential drive with two drive wheels (Figure 6.3) is because this configuration is quite simple to implement and at the same time allows for sufficiently precise vehicle control. This differential drive configuration also includes one or more support wheels that prevent the vehicle from overturning. The drive wheels are mounted on the same axle, and the speed of rotation of each wheel is determined by the speed of rotation of the corresponding electric motor. If the drive wheels rotate at the same speed, the vehicle drives straight; otherwise, the vehicle turns in the direction of the wheel that rotates more slowly. A vehicle with a differential drive can also rotate in place (around the axis of rotation), namely when the wheels rotate at the same speed, with one rotating forward and the other rotating backward.

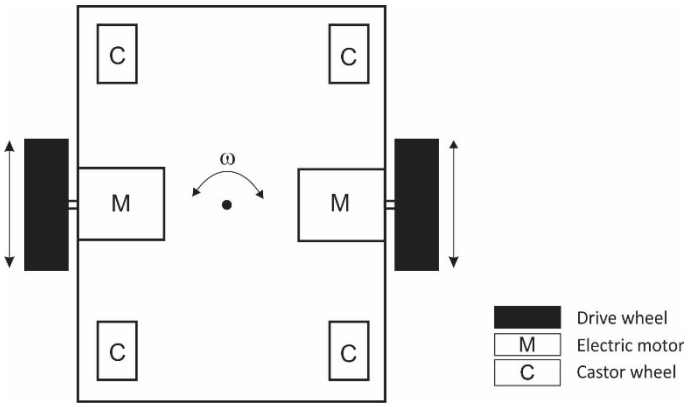


Figure 6.3: Differential drive with two drive wheels and four support (castor) wheels
Source: own.

Table 6.2 contains links to YouTube videos that demonstrate the operating principles of various propulsion and control system configurations.

Table 6.2: Examples of drive and control system configurations

Configuration	Video	Keywords
Differential drive		Kollmorgen - Autonomous Mobile Solutions, AGV Vehicle Types, Differential drive
Wheel drive		Kollmorgen - Autonomous Mobile Solutions, AGV Vehicle Types, Steer drive
		SICK AG, Monitoring automated guided vehicles (AGV) - with Safe Motion Control from SICK
Mecanum		ERobtic, ERobtic Mecanum Wheel
		Torwegge GmbH & Co. KG, TORsten Mecanum Rad | Animation | TORWEGGE
		KUKA - Robots & Automation, Clever Autonomy for Mobile Robots - KUKA Navigation Solution
		Neobotix GmbH , Neobotix mobile Roboterplattformen

2.2 External and internal sensors

Autonomous vehicles contain many external and internal sensors. External sensors are used to sense the environment, while internal sensors are used to detect internal process variables. Combinations of data obtained from various sensors are used for environment detection, localization, and navigation. The most used sensors are:

- Inertial Measurement Units (IMUs). These are used to maintain vehicle stability and in localization and navigation algorithms. IMUs include three basic sensors, namely: (1) a 3-axis accelerometer, which measures the vehicle's acceleration in all three directions (x, y, z), (2) a 3-axis gyroscope, which measures the angular velocity or rotation rate of the vehicle around each axis, (3) a 3-axis magnetometer, which measures the strength and direction of the magnetic field in all three axes. In combination with other sensors, the data from the inertial measurement unit improves the accuracy of the robot's location estimation.
- Light Detection and Ranging (LiDAR) sensors. These sensors are a key sensor component used in AMRs for navigation, obstacle detection, mapping, and localization. LiDAR sensors use laser beams to measure distances to objects in the robot's surroundings, enabling precise mapping and navigation.
- Drive wheel sensors; these are mounted on the drive motors and thus capture the speed and position of the drive wheels. These sensors enable a rough determination of the direction and speed of the vehicle's movement. Due to various errors (random slippage of the drive wheels, geometric errors, resolution

of incremental encoders, etc.), such a system for determining the vehicle's speed is not absolutely accurate, so additional sensors (accelerometers, gyroscopes, etc.) are required to supplement the estimate of the speed of movement with more precise measurements. Drive wheel sensors provide information that helps with vehicle localization, especially in algorithms based on odometry.

- Ultrasonic Sensors emit sound waves and measure the time it takes for the emitted waves to bounce off the detected objects. They are used to detect transparent objects, such as glass doors, which are difficult or impossible for optical sensors (LiDAR, cameras) to detect.
- Camera systems are used to visually detect objects, especially those that cannot be detected by other sensors. LiDAR sensors detect objects in a plane that is a certain distance above ground (the height depends on the installation of the sensor on a mobile platform). Objects that are higher or lower than this plane are not detected by LiDAR sensors. 3D cameras are used to detect such objects, which are usually installed on the front of the vehicle.
- Radar Sensors transmit radio waves and measure the time of flight from transmission to reception. Radars use radio frequency (RF) signals, usually in the microwave band, and enable the detection of objects at relatively long distances. Compared to optical sensors such as LiDAR or cameras, radar is less affected by adverse weather conditions such as rain, fog, or snow, making it suitable for autonomous vehicles operating outdoors. However, radars generally have lower resolution than LiDAR sensors, making them less suitable for mapping areas or detecting smaller objects.
- Touch sensors; these sensors are used to detect collisions with objects. In general, contactless and contact systems are used to detect obstacles. The latter are used in automatically guided vehicles, while contactless systems are usually used in autonomous vehicles. Safety bumpers with touch sensors installed inside are used as a contact system. These sensors are activated when the vehicle comes into direct contact with an obstacle.
- Global Positioning System (GPS). Some AMRs use Global Positioning System technology to provide information about the global position of the vehicle, anywhere on the globe. This is especially useful for vehicles used outdoors, such as in agriculture or last-mile delivery. GPS signals cannot penetrate buildings, so they are not used in vehicles that operate indoors.
- Other sensors: Depending on the intended use, autonomous vehicles may also contain other sensors, such as sensors for measuring external quantities

(temperature, humidity, gas concentration), sensors for detecting barcodes, RFID tags, etc.

2.2.1 Safety laser scanners

Safety laser scanners (Figure 6.4) enable contactless detection of objects in the vicinity of a mobile robot. These sensors have a so-called safety zone and two or more warning zones, which are adjustable and intended for various support functions, such as a warning sound. If the vehicle detects an obstacle within the warning zone (yellow and orange zones) in the direction of movement, it must start normal braking. If the detected object is located within the safety zone (red zone), the vehicle must stop in an emergency using the built-in brake (Wikipedija, 2023). Modern safety laser scanners allow the configuration of multiple zones, using the associated software. AMRs usually contain two or more safety laser scanners. The most common are two, which are installed on the diagonal edges of the vehicle. Such an installation allows 360° detection of the vehicle's surroundings, which means that the AMR can also detect objects located to the side of the vehicle. This is especially important in the case of a robot turning in place.

Figure 6.4: Example of a safety laser scanner
Source: (SICK AG, 2018).

Safety laser scanners are used for non-contact detection of objects in many areas (Table 6.3) and are very often found in the field of protecting the working areas of industrial robots.

Table 6.3: Examples of the operation and use of safety laser scanners

Scope of application	Video	Keywords
Mobile robots		SICK AG, Monitoring automated guided vehicles (AGV) - with Safe Motion Control from SICK
Robotic cells		SICK Sensor Intelligence, Safe Robotics: safe sequence monitoring
		SICK AG, Safe Robotics: Palletizing application

2.3 Location and navigation systems

Autonomous and AGVs contain a location and navigation system. In the case of AGV, this is quite simple, as the vehicles only follow predetermined paths. Autonomous vehicles, on the other hand, contain a wide range of sensors and advanced navigation algorithms, which allow them to adapt to transport routes in a changing environment.

2.3.1 AGV

In AGV, inductive wires and magnetic strips are most often used to mark the route (Table 6.4). The inductive wire is the oldest system for guiding vehicles and is still used today, mainly due to its high accuracy and reliability. However, this system has one important limitation; namely, the wire must be installed in a special slot below the ground surface, approximately 1 cm deep. This means that physical intervention in the infrastructure in the area where the vehicle will perform transport tasks must be carried out. A similar intervention in the infrastructure must also be carried out whenever the route is changed. Unlike inductive wires, magnetic strips are installed on the ground surface. Their key advantage is that they can be easily attached, removed, or relocated. Magnetic strips are very robust and resistant to damage and dirt.

For path detection, so-called inertial navigation systems are also used, in which it is not necessary to mark the entire path of the vehicle, but only certain points. Inertial systems are based on measuring accelerations in all three directions (x, y, z) and angles of rotation around the longitudinal, transverse and vertical axes of the vehicle Wikipedia (2025). Based on the measured accelerations and angles of rotation, the current position of the vehicle in space is estimated using integration methods. Due to various errors (sensor errors, integration method errors, etc.), differences occur

between the actual and estimated position of the vehicle, which is why additional ground markings are usually used in this type of navigation. When the vehicle crosses such a marking, the sensor detects the exact position and corrects the estimated position of the vehicle. Generally, small permanent magnets are used as markings, but there are also solutions using RFID or QR tags.

2.3.2 Autonomous vehicles

In autonomous vehicles, two methods are often used for localization and navigation, namely 2D laser scanning and Simultaneous Localization and Mapping (SLAM).

2D laser scanning works on the principle of measuring the reflection of a laser beam from fixed reflectors in space. Based on the reflection of laser beams from different reflectors, the current position of the vehicle is determined using triangulation. Laser technology provides high resistance to false reflections and high accuracy of position determination. This technology is usually used on slightly higher platforms, for example, in forklifts, because in these cases the laser is mounted quite high and, as a result, the laser beams are not interrupted when people are present.

Table 6.4: Examples of how different location-based navigation systems work

Location and navigation system	Video	Keywords
Inductive wire	▶	Jungheinrich AG, Jungheinrich Inductive Guidance for Forklift Trucks
	▶	Götting KG, Götting FTF Spurführungstechnologien / AGV Track Guidance Technologies
Magnetic strips	▶	Götting KG, Götting FTF Spurführungstechnologien / AGV Track Guidance Technologies
	▶	Roboteq, Magnetic track following Mobile Robot demonstrator
Inertial system	▶	DS AUTOMOTION, Magnetic Navigation by DS AUTOMOTION GmbH - Automated Guided Vehicle (AGV)
2D laser	▶	Götting KG, Götting FTF Spurführungstechnologien / AGV Track Guidance Technologies
	▶	DS AUTOMOTION, Laser navigation by DS AUTOMOTION GmbH - Automated Guided Vehicle (AGV)
SLAM	▶	cygbot lab, 2D/3D Dual SLAM Robot using ROS and LiDAR with Raspberry Pi

When using SLAM algorithms, a vehicle builds a consistent map of the area it is in, and at the same time determines its current location on this map. SLAM often involves sensor fusion, in which data from multiple sensors is combined to improve the accuracy of mapping and localization. SLAM algorithms are classified based on the sensors they primarily use. LiDAR SLAM prioritizes LiDAR for sensing the environment, while Visual SLAM uses a machine vision system or camera as the primary sensor. SLAM is suitable for unknown or dynamic environments, where the layout of facilities can change over time. SLAM algorithms are computationally very expensive and consequently require a lot of processing power and memory. SLAM depends on the quality and accuracy of sensors, so sensor calibration is crucial.

3 Autonomous vehicle MiR100

The MiR100 (Mobile Industrial Robots., 2023) is an autonomous vehicle with a payload of up to 100 kg, manufactured by Mobile Industrial Robots. It can be used exclusively in closed production areas, warehouses, or other industrial facilities. The MiR100 (Figure 6.5) has two built-in safety laser scanners (Figure 6.6), which are mounted on the diagonal edges of the robot, enabling scanning of the entire area around it. The vehicle also contains ultrasonic sensors and a 3D camera. As a result, the MiR100 can operate near people and other dynamic obstacles and is able to drive through narrow corridors or doors. The MiR100 operates on a differential drive, namely, it has two drive wheels and four support wheels (Castor wheels). The vehicle can be manually operated via a built-in web interface, but it is primarily intended for autonomously performing various transport tasks. The robot performs localization and navigation via a map that can be imported or created at the first start.

Figure 6.5: MiR100
Source: own.

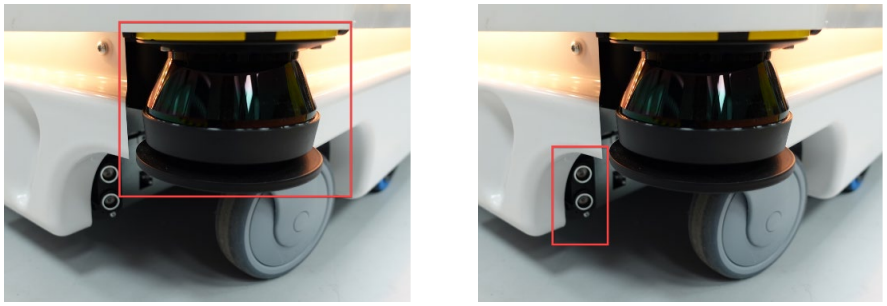


Figure 6.6: Safety laser scanner (left) and ultrasonic sensor (right)
Source: own.

The MiR100 is a basic mobile platform on which various Top Modules can be fitted to modify the functionality of the vehicle (Figure 6.7). For example, the MiR Hook 100 top module turns the MiR100 into a towing vehicle, allowing the towing of loads on attached trolleys. Examples of some of the modules added above to the MiR100 are given in Table 6.5 below.

Table 6.5: Examples of the top modules for the MiR100

Top module	Video	Keywords
Roller, belt	▶	Omni Automation, MiR 100 Robot - Top Module Roller Conveyor
	▶	Mobile Industrial Robots, Mir100 hos SAXE på Elmia Automation 2016
CLAMP	▶	Robotcenter, Clamp top module for MiR100/MiR200
Towing	▶	Mobile Industrial Robots, MiR 100 Hooking a Trailer Automatically
With a collaborative robotic arm	▶	Mobile Industrial Robots, MiR100 with UR cobot arm at SGIMRI

Figure 6.7: Example of a top locking module
Source: own.

3.1 User interface

MiR robots have a built-in Wi-Fi access point, through which it is possible to access the robot's user interface. The user interface, designed in the form of a web page, allows: (1) creating dashboards, (2) mapping the space, (3) creating missions, (4) monitoring the current state of the robot, (5) managing users, (6) manually controlling the robot, (7) updating the software, etc.

Dashboards allow direct access to individual key functions of the robot and are primarily intended for different groups of users. Each dashboard consists of visual widgets that represent system features, such as a specific mission, a map, the current queue of missions, etc. Dashboards can be created and edited using the built-in dashboard designer. An example of a dashboard is shown in the figure below (Figure 6.8).

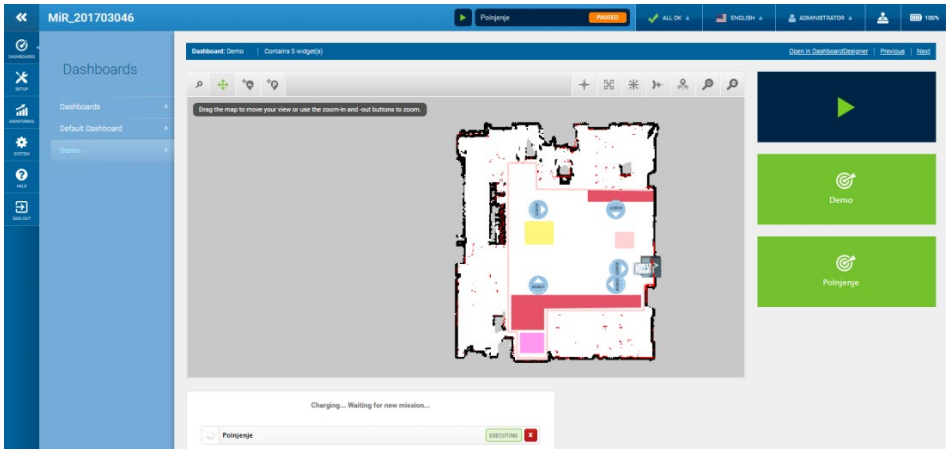


Figure 6.8: Example of a built-in dashboard
Source: own.

The vehicle can be manually controlled using a virtual joystick, which is an integral part of the user interface. The user interface allows the creation of multiple user accounts with different permissions, which allows controlled access to individual robot functions. The user interface also allows monitoring of the status of the robot (its location on the map, battery status, error and warning messages, etc.).

3.2 Mapping and editing maps

Mapping or creating area maps is the most important process that allows the vehicle to operate independently in a selected space. Creating a map is done in two steps. In the first step, a CAD file of an existing map of the space is loaded onto the robot, or the map is created by manually guiding the robot. In the second step, the map is edited using the built-in editor. The built-in mapping functionality allows you to create a map by manually moving the robot around the space using the built-in virtual joystick. During movement, data is captured from safety laser scanners, and based on this, the robot creates a map of the space. After capturing the map, editing follows. In addition to fixed objects (e.g. walls), the creation process also captures so-called dynamic objects (people, forklifts, carts, chairs, pallets, etc.), which are located in the vehicle's surroundings at the time of capture. These objects must be removed, otherwise they may extend the length of the vehicle's path. Scanning can also cause errors in detecting stationary objects (e.g. walls) and, as a result, objects appear as broken lines on the map. In this case, such objects must be corrected or drawn additionally using the built-in tools on the map.

On the edited map, using additional tools, it is possible to determine: (1) Preferred zones, (2) Unpreferred zones, (3) Forbidden zones, (4) Critical zones, (5) Speed zones, (6) Blink zones, Beep zones, etc.

The individual zones have the following meaning:

- Preferred zones: The robot always tries to drive in this zone.
- Unpreferred zones: The robot tries to avoid this area, but if there is no other option, it can also drive through this area.
- Forbidden zones: the robot must never enter this area.
- Critical zones: obstacles detected by installed cameras or scanners are ignored in these areas. This allows the robot to approach obstacles without triggering the safety stop system. When the robot leaves this area, the protective functions are reactivated. This area is useful, for example, in narrow passages, doors, etc.
- Directional zones: determine the direction of the robot's movement. The robot can only move in the selected direction in this area.
- Speed zones: In these areas, the vehicle's speed can be increased or decreased. For example, speed reduction is used if the vehicle is in an area with a lot of

people. The default robot speed is 1 m/s, the minimum is 0.1 m/s, and the maximum is 1.5 m/s.

- Blink zones, Beep zones: while driving in this area, the robot can play a selected sound and/or signal appropriately with the built-in LED light strip. Signaling is primarily used to alert people to the presence of the robot.
- I/O module area: When entering this area, the robot activates the Input/Output module.

Figure 6.9 shows an example of an edited map with special areas added.

Before creating transport tasks (missions), position points (markers) must be defined on the created map; these are points in space to which the robot can drive. Each point contains a name, X and Y coordinates of the point in meters, and the orientation of the vehicle in degrees.

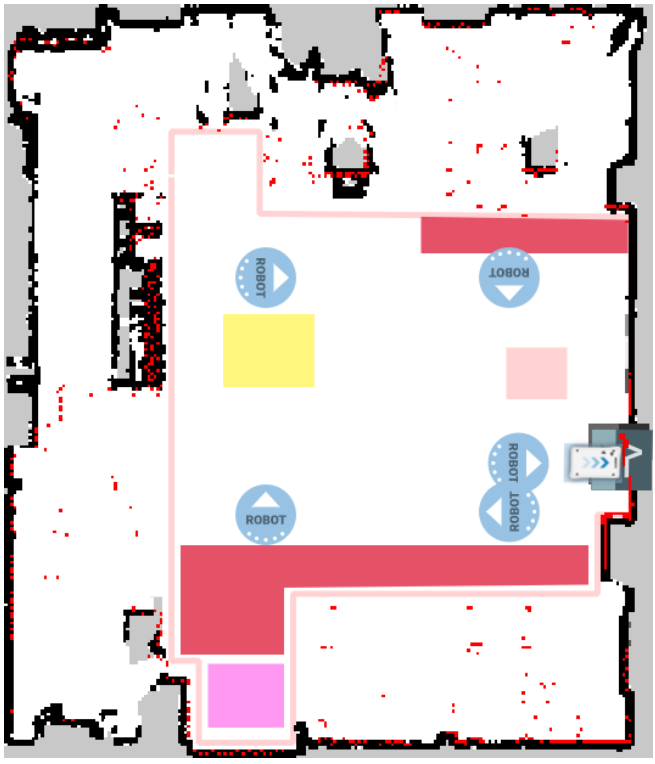


Figure 6.9: Example of an edited map with special areas added

Source: own.

3.3 Creating missions

After creating the map, the vehicle is programmed, or the so-called missions are created. A mission consists of various actions, such as: (1) moving the vehicle, (2) turning the digital signal on/off, (3) connecting/disconnecting the cart, etc. Individual actions represent the basic building blocks for creating missions, and they can also be used within other missions. Most actions have adjustable parameters.

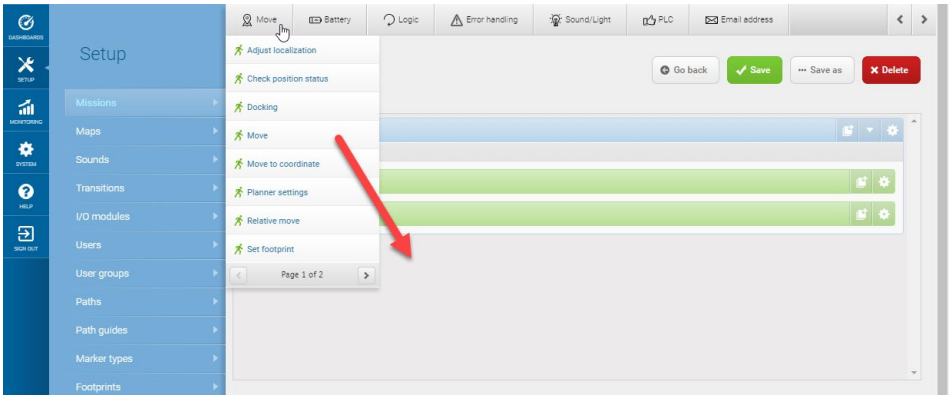


Figure 6.10: Mission Editor
Source: own.

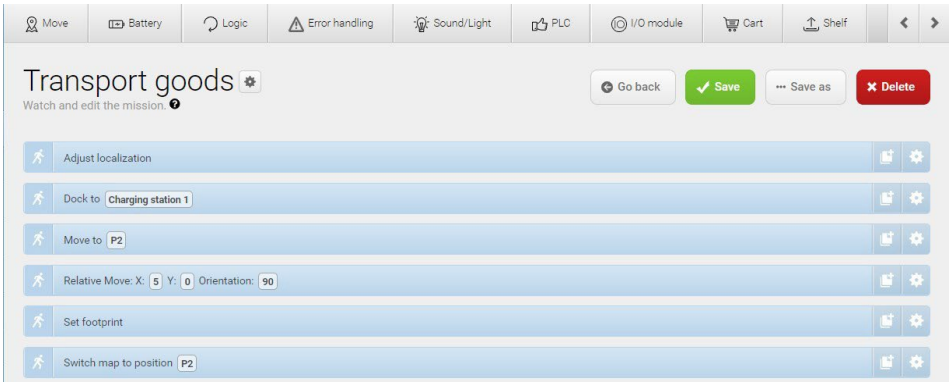


Figure 6.11: Example of a created mission
Source: own.

A mission consists of individual actions or commands that can be selected in the Mission Editor menus (Figure 6.10). The commands are grouped into submenus: Move, Battery, Logic, etc. A command is added to a mission by dragging it to the

bottom of the editor (Figure 6.10). The commands are executed in sequence, from top to bottom. The parameters of the selected command can be changed by selecting the icon (gear) located on the far-right side of each command (Figure 6.11).

4 Conclusion

The chapter provides the reader with basic information on the operation of automated guided and autonomous vehicles and describes practical application examples. In a brief overview of the field of automated guided and autonomous vehicles, it can be observed that one and the other use different sensor systems to detect the surroundings and obstacles. Different actuators are used to achieve different modes of motion and, consequently, different vehicle kinematic and dynamic properties. The main difference between automated and autonomous vehicles lies in the decision-making systems directly linked to the sensing systems. A practical example of an autonomous mobile robot, MiR 100, illustrates the user interface and the basic functions for operation in intralogistics applications. It can be concluded that the MiR 100 is a basic autonomous platform but needs additional modules for more advanced applications. We foresee that the use of autonomous mobile robots will increase in the future, mainly due to the upgrading of existing automated guided vehicles and the automation of manual processes.

References

Mobile Industrial Robots. (2023). MiR100 User guide. Retrieved from https://www.mobile-industrial-robots.com/

Roboteq Inc. (2013). Building a Magnetic Track Guided AGV, Application Note AN1326. Retrieved from https://www.roboteq.com/index.php/applications/100-how-to/278-building-a-magnetic-track-guided-agv

SICK AG. (2018). SICK Web Site. Retrieved from https://www.sick.com

Siegwart, R., Nourbakhsh, I. R., & Scaramuzza, D. (2011). *Introduction to autonomous mobile robots*: MIT press.

Statista. (2023). Global autonomous mobile robot market size 2016-2028. Retrieved from https://www.statista.com/statistics/1285835/worldwide-autonomous-robots-market-size

Wikipedia. (2025). Inertial navigation system. Retrieved from https://en.wikipedia.org/wiki/Inertial_navigation_system

Wikipedija. (2023). Automated Guided Vehicle. Retrieved from https://en.wikipedia.org/wiki/Automated_guided_vehicle

Digital Transformation in Logistics and Supply Chain Management

Matevž Obrecht (ed.)
University of Maribor, Faculty of Logistics, Celje, Slovenia
matevz.obrecht@um.si

DOI
https://doi.org/10.18690/um.fl.2.2026

ISBN
978-961-299-074-9

The higher education textbook *"Digital Transformation in Logistics and Supply Chain Management"* is a comprehensive guide aimed at supporting digitization and digital approaches in logistics. It focuses on process digitalization, the use of tools far digital data processing and simulations, autonomous vehicles, machine learning in logistics processes, and cybersecurity. This interdisciplinary approach combines knowledge from various fields-computer science, information technology, mechatronics, machine learning, simulation methods, and business decision-making, providing a thorough understanding of digital logistics challenges and the application of practical knowledge to areas beyond logistics and supply chains. Readers are equipped with practical knowledge and skills to improve the efficiency and transparency of individual processes. The textbook covers topics such as: 1) Process Digitization - Planning; 2) Process Digitization - Execution; 3) Business lnformation Systems; 4) Simulations and Digital Twins; 5) Autonomous Vehicles in Logistics; and 6) lnformation Security. The entire content is focused on strengthening digital competencies essential for effectively managing modem logistics companies and building resilient supply chains.

Keywords:
autonomous vehicle, digitalization, interdisciplinary knowledge, digital logistics, green and digital transition, cyber security

University of Maribor Press

University of Maribor

Faculty of Logistics

Green LOGISTICS SKILLS

Digitalization – Planning
Borut Jereb

Digitalization – Implementation
Borut Jereb

Information and Computer Security
Nena Orel Šanko

Business Information Systems
Bojan Rupnik

Simulations in Decision Making
Bojan Rupnik

Autonomous Vehicles in Intralogistics
Darko Hercog, Primož Bencak

NOO | THE RECOVERY AND RESILIENCE PLAN

50 years University of Maribor

REPUBLIC OF SLOVENIA
MINISTRY OF HIGHER EDUCATION, SCIENCE AND INNOVATION

Funded by the European Union
NextGenerationEU