DOI: 10.38146/BSZ-AJIA.2025.v73.i1.pp205-217

Characteristics of security risks of large industrial investments and their management principles

Frigyes Gubics
Security Leader
Lenovo Hungary
fgubics@lenovo.com

Abstract

Aim: Major construction and investment security is important if order to be done successfully. The aim of this article is to describe and analyses security relations of these kind of projects. Analyzing several part of security they affect the result of construction activities, risk assessment and risk mitigation, and of course to protect stake holders interests are the main directions of security activity. Secured environment also a base of achieve the expected results and activity of loss protection. Transparency, finalized workflows and tactics also can guarantee of a stable background during planning, implementation and later on final operation.

Methodology: The author carried out qualitative research, using secondary data, and conducted a document analysis in order to provide a comprehensive picture of the security-related connections of major industrial investments. Empirical experience also helped the work, as the author himself participated in the management of a priority industrial investment project as a security manager.

Findings: The success of priority industrial investments is significantly influenced by its level of security. Effective security activities require the active cooperation of several organizations. Transparency, meticulous security processes and methods are a kind of guarantee for ensuring a stable framework in the phases of planning, implementation and then operation.

Value: Emphasizing the security risks arising during the preparation of industrial investments, involving interested organizations in the security activity, a kind

English-language republication. The Hungarian version of this article was published in Belügyi Szemle 2025, issue 1. DOI link: https://doi.org/10.38146/BSZ-AJIA.2024.v73.i1.pp113-126

of preventive security activity in order to prevent the loss of property and help the success of the project.

Keywords: Industrial investment, risk assessment, asset security, data protection

Introduction

Major industrial investment projects are key to economic growth, technological and infrastructure development. However, they face high number of security challenges that can jeopardize their success. This article addresses the security aspects of major industrial investments and provides a framework for each element.

Managing the various security risks, effective strategies and innovative technologies will contribute to project success, investor confidence and sustainable development. Cooperation between stakeholders, adherence to international security standards and continuous learning from past experience are key to managing security risks. These projects are interlinked and interdependent with many other sectors, such as energy suppliers, transport, raw material procurement and production, so the linking of these sectors can bring significant economic benefits to both local and global communities. At the same time, they present a number of challenges, one of the most important of which is security, as this can make or break the success of an investment. Proper management of the identified risks is critical, laying the foundations for appropriate security design of industrial investments.

Components of security

Several key factors come into play when planning major industrial investment projects. Understanding these is the basis for building an effective security system. Political stability and a predictable regulatory framework are essential considerations when a market company decides to invest in a country. This provides a favourable environment for investment, reducing the risks associated with governments and the legal background that can disrupt or prevent a project from going ahead. Assessing and managing financial risks, such as securing adequate financing, minimizing cost overruns and securing revenues. Cybersecurity and data protection are also important considerations in today's digitally connected world. As industrial projects increasingly rely on digital systems and data-driven processes, protection against cyber threats is becoming increasingly important. Protection against data leakage, unauthorized access and system vulnerabilities is essential to maintain operational integrity and protect sensitive information. According to Gergely Balázs Tiszolczi (2019), more and different types of technical knowledge are required to keep information secure, such as networking, basic IT skills and information security.

Physical security involves measures to protect project sites, equipment and infrastructure against theft, vandalism and unauthorized access. Thoughtfully designed security measures such as surveillance systems, access control and the implementation of physical/mechanical/electronic devices help to reduce potential risks.

These projects often involve complex supply chains with a high number of suppliers involved. This is particularly the case for multinational companies, where materials can come from all over the world. Ensuring the integrity and reliability of the supply chain (transport, logistics, procurement) helps to reduce risks such as fraud, product tampering, anomalies and delays in materials and services.

Ensuring sustainable development, complying with environmental regulations and working responsibly with local communities is important to mitigate negative impacts on ecosystems and communities. Failure to do so will not only damage the company's reputation, but may also lead to legal and regulatory proceedings, which could result in project delays.

It is important to mention the security management of the project, which is a significant position in terms of effectiveness. As emphasized by Christián, Major, & Szabó (2019), it is ideally channelled to the first decision-maker, which in the case of a new project is its manager or the company director. The importance of positioning lies in the effectiveness of advocacy, as several levels down, as middle managers, information goes through the filters of management before reaching decision-makers, which reduces effectiveness and influence, and can also lead to a reduction in the level of security. The security manager should be given showstopper[1] rights to stop certain processes in the event of serious security breaches, which can be restarted after corrective action has been taken, preventing loss of assets.

Political stability and legislative framework

The political background and legal framework vary from country to country and can have a significant impact on investment appetite and help determine whether a company should locate some or all of its industrial capacity in a given region.

[1] Showstopper: an obstacle to further development and progress.

It can now be said that multinational companies are seeking to diversify their production and to produce geographically where they sell their products. The political context and legal framework varies from country to country, which can have a significant impact on the incentives to invest and help determine whether a company should locate some or all of its industrial capacity in a given region. It can now be said that multinational companies are seeking to diversify their production and to produce geographically where they sell their products. Political stability provides an environment conducive to long-term project planning and implementation. The choice of location is key from a geopolitical perspective, as it can also increase investor confidence. A predictable political environment creates a favorable investment climate, attracting both domestic and foreign capital.

In addition, a stable, clear and transparent legal framework creates a clear playing field, as predictability and predictability are important for the return on investment. It protects the interests of all stakeholders[2] , increases trust and helps accountability. It sets the framework for environmental protection, health and safety, labor rights and financial activities.

Regular dialogue, consultation and coordination helps to ensure that policy is also adapted to the needs of industry, promotes economic growth and protects the interests of stakeholders, while successful project implementation is a cornerstone for promoting sustainable development in the region.

Economic stability and financial risks

The economic environment in which projects operate can significantly affect their viability and success. Fluctuations in macroeconomic indicators such as GDP[3] growth, inflation rates and interest rates can pose challenges and uncertainties for project planning and implementation and make financial planning difficult.

Financial risks, including funding constraints, cost overruns and revenue uncertainties, are inherent risks of large industrial projects. Attention must also be paid to securing adequate sources of finance and managing cash flow effectively.

Sound financial management, rigorous budgeting, accurate cost estimation and careful financial planning are essential to mitigate financial risks. Conducting thorough, comprehensive financial feasibility studies and thinking through

[2] Stakeholders: interested parties.

[3] GDP (Gross Domestic Product): in economics, the gross domestic product is a measure of the economic output of a certain area, usually a country, over a given period of time. It measures national income and output.

different scenarios can help identify potential risks and facilitate preparation and forward planning. It is also worth involving financial experts at the planning stage.

Cyber security and data protection

In our digital world, cybersecurity and data protection have become critical security factors for large industrial investments. These projects rely heavily on interconnected systems, digital technologies and data-driven processes, making them vulnerable to cyber threats and misuse of information, including personal data.

The implementation of well-designed cybersecurity measures is crucial to protect infrastructure, sensitive data and intellectual property.

Data protection is equally important as projects often involve large amounts of sensitive and proprietary information.

The use of secure data storage, access control and data encryption help prevent the unauthorised handling, disclosure or theft of sensitive data.

Strong firewalls, intrusion detection systems and encryption protocols can help protect against unauthorised access and data leakage. Vulnerability scans[4] and penetration tests[5] can help identify potential weaknesses and vulnerabilities, enabling timely response.

Compliance with data protection regulations, such as the GDPR[6] and the Info Act[7] in Hungary, ensures the protection of personal data.

Training for employees plays an important role in maintaining cybersecurity and data protection. Educating staff about potential risks, frequent password exchanges, and stressing the importance of reporting suspicious activities are essential elements of a comprehensive cybersecurity strategy.

The involvement of cybersecurity experts and specialist firms further reduces cybersecurity risks. Collaboration with industry partners, government agencies and cybersecurity organisations can facilitate the application of best practices and information sharing on emerging threats and vulnerabilities.

[4] Vulnerability scan: is the testing of a product (website, application, software, network) under development or completed. During the test, ethical hackers look for bugs (flaws) that a malicious attacker can exploit (XSS, RCE, LFI, SQLi).

[5] Penetration test: a security exercise in which a cyber security expert tries to find and exploit vulnerabilities in a computer system.

[6] GDPR (General Data Protection Regulation): the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 96/45/EC (General Data Protection Regulation).

[7] Info Act: Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information.

Physical security and protection of property

Projects often involve valuable assets such as equipment, infrastructure and raw materials that need to be protected against theft, sabotage and unauthorised access.

The implementation of complex physical security measures is essential to protect the project sites and assets. This includes security staff, the deployment of surveillance systems and the establishment of entry and exit points. The use of devices such as CCTV[8], motion detectors and intrusion alarm systems will improve the effective detection of potential security threats and response.

Additionally, to providing a direct project site, the transport of materials and equipment needs to be considered. Furthermore, to providing an immediate project site, the transport of materials and equipment needs to be considered. Securing supply chains and proper tracking and monitoring can help prevent theft and tampering in transit.

According to Tamás Berek and Gyula Bodrácska (2010), cooperation with local law enforcement agencies and security professionals can provide valuable information on the local security situation and risks, thus helping to develop a tailored security strategy. However, I argue that the planned activity in the future completed facility, i.e. the corporate profile, should be taken into account, as this is a risk element to be managed in order to design security.

Supply chain security

A primary aspect of supply chain security is the availability of materials, parts and products of the right quality and in the right quantity. A rigorous quality control system, conducting supplier audits in advance and maintaining traceability throughout the supply chain will help minimize the risk of inappropriate quality and quantity of materials entering the project. Regular audits and inspections can verify compliance with quality standards and contractual requirements.

Supply chain disruptions pose a significant risk to the timing and cost of projects. Natural disasters, geopolitical events, strikes or transport disruptions can all affect the timely delivery of materials and services. Establishing contingency plans, diversifying suppliers and maintaining transparent communication channels with key supply chain partners can help mitigate these risks and ensure that alternative options are available.

[8] CCTV (Closed-Circuit Television): a closed-circuit camera system.

Sharing security information, such as information on potential threats or best practices,[9] will help you identify and address potential vulnerabilities. Clear expectations and requirements for suppliers and contractors on security protocols and standards ensure a consistent and uniform approach to supply chain security.

Technological advances such as blockchain[10] technology and IoT[11] help us to have transparent and up-to- date, accurate records of transactions and product movements.

Environmental and social risks

Environmental risks include pollution, habitat destruction, deforestation and depletion of natural resources. Large industrial projects must comply with environmental regulations, carry out a thorough environmental impact assessment and take preventive measures to avoid pollution. Using renewable energy sources and minimizing waste generation will help to mitigate environmental risks and reduce the project's ecological footprint.

Social risks arise from potential disruption to local communities, conflicts over land and negative impacts on cultural heritage. Understanding and addressing social concerns requires the involvement of stakeholders, including local communities. Local livelihood programs (job creation), respect for cultural heritage and support for local development initiatives will help to minimize social risks and can also help to ensure a positive social perception of the project.

Human rights considerations are also an integral part of managing environmental and social risks. Respecting labor rights, ensuring fair pay and safe working conditions are essential to maintaining ethical operations. Adherence to internationally recognized human rights standards and guidelines will help to achieve this.

In addition, regular monitoring and evaluation of environmental and social impacts allows for continuous improvement and adaptation. Independent

[9] Best practices: a good/best practice is a way of working, a model, a solution, the main details of which can be learned and applied elsewhere. Usually a widely recognised ideal process, streamlined model or solution that can be adapted to a given organisation under the same or at least similar environmental conditions and external circumstances.

[10] Block chain: a database that differs from a traditional database in that the information is not stored on a centralised network, i.e. a central server, but on a distributed network.

[11] IoT (Internet of Things): refers to a variety of uniquely identifiable electronic devices that are able to recognise some kind of meaningful information and communicate it to another device over an internet-based network.

audits can provide objective insight into whether a project meets environmental and social standards, ensuring accountability and transparency.

Reducing security risks

Reducing the security risks of large industrial investment projects requires a comprehensive and proactive approach.

By using certain tools, we can increase the overall security of industrial investment projects and minimize risks. Proactive measures, cooperation and continuous assessment and monitoring contribute to the resilience and long-term success of these projects in an ever-changing security environment. According to Lawrence J. Fennelly (2013), creating a secure environment through careful design requires consideration at the project preparation stage, and simple solutions such as adequate lighting, unobstructed views of objects, or connections to surrounding buildings and road infrastructure can be an advantage when designing a complex security system.

Risk assessment and management

According to Tamás Horváth (2018), the results of the risk analysis can be used to determine whether the security systems to be installed provide an appropriate response to the potential risks. In my view, it is also important to place vigilant guarding on the "chessboard" alongside technical solutions, together with well thought-out regime measures. Effective risk assessment and management is a key element of security in industrial investment projects. Comprehensive risk assessments are used to identify potential threats, vulnerabilities and problem areas that could impact on project security. The first step in a risk assessment is to identify and analyse potential risks from various perspectives, including political, economic, cyber security, physical and environmental factors. This includes a thorough assessment of the project environment, stakeholder interests and potential impacts. The involvement of experts, such as risk consultants or security specialists, can be a valuable asset.

Once risks have been identified, they should be ranked according to their likelihood and potential impact. This will allow appropriate resources to be allocated and targeted strategies to be developed. Risk management plans should include specific measures to mitigate the identified risks.

After analyzing the risks, Charles Sennewald (2011) recommends reviewing existing risk mitigation measures and making any necessary changes in the light of this. This requires a periodic review of the entire security system, including by an external expert or company. This underlines that risk analysis is carried out continuously in parallel with necessary changes in processes in order to be able to react in time to changing circumstances, thus reducing potential losses and keeping the risk low.

Regular monitoring and evaluation is essential to ensure that risk management strategies remain effective and up-to-date. This includes continuously monitoring potential threats, tracking changes in the project environment and reassessing risks as the project progresses. Risk management plans should be amended as necessary to keep up to date by tracking new risks as they arise or changing circumstances.

Anticipating security incidents allows you to develop a plan, establish communication protocols and ensure business continuity. These plans should be tested with simulations and exercises to assess their effectiveness and make the necessary improvements.

Depth of protection

Deploying defense in depth will help to effectively manage incidents as they occur. This includes regime measures, technical solutions, which can be mechanical or electronic, and the use of live force as an important part of the system. According to Garcia Mary Lynn (2007), a well-designed security system provides both depth and balance of protection, minimizing the consequences of failure of system components. In my view, we need to move away from the classical so-called perimeter protection and, in addition to a well-designed outer shell protection, we need to implement security processes in the workflows of each department and the operational activities of the security organization should be carried out at multiple levels of depth. For example, the establishment of security checkpoints or enhanced protection of sensitive, high-risk areas.

Cooperation and information sharing

By fostering cooperation between stakeholders, project owners, government agencies, security professionals and local communities, we can make a concerted effort to effectively identify and manage security risks.

Collaboration facilitates the sharing of information and good practice, allowing us to learn from each other's experiences and benefit from collective wisdom. By using different perspectives and insights, a more comprehensive and robust security strategy can be developed. This collaborative approach helps to identify potential blind spots, create innovative solutions and address security challenges holistically. Cooperation and information sharing can take various forms, such as regular meetings, workshops, conferences and joint simulation exercises. These facilitate open dialogue, strengthen relationships and build trust between stakeholders. In addition, partnerships with external organizations such as security organizations, research institutes or industry associations can provide access to specialized knowledge and resources. Government agencies also play an important role in facilitating cooperation and information sharing.

Stakeholder involvement and community relations

Stakeholder involvement involves actively listening to the concerns, needs and aspirations of different groups. It provides an opportunity to address potential security risks, gain insight into local dynamics and help develop strategies that are in line with the vision of all stakeholders. This collaborative approach increases the acceptance of projects and reduces the likelihood of conflicts or local resistance that could threaten security.

Building strong community links is essential to creating a positive project environment. By building trust and maintaining open communication, we can address local community concerns, mitigate potential social risks and ensure that the project delivers tangible benefits to the local population. Participation in dialogue, regular community meetings and information about the project's security measures will help to build relationships and partnerships.

Training and skills development

By investing in the knowledge and skills of those involved in the project, we can strengthen our organization's ability to identify and respond effectively to security risks.

Developing security alertness,[12] training and implementing procedures for reporting suspicious activities contribute to a safe project environment. Regular

[12] Alertness: vigilance, readiness.

security audits help identify gaps or weaknesses in physical security measures, allowing for timely changes and improvements. Comprehensive training programs should be developed to educate employees on security protocols, procedures and best practices. Knowledge of potential threats, such as cyber-attacks, physical incidents or environmental hazards, and guidance on how to prevent and manage these risks should also be provided. Training should cover a wide range of security issues, such as risk awareness, emergency response, crisis management and incident reporting.

Training programs should emphasize the importance of a culture of security awareness. Developing a sense of vigilance, accountability and responsibility creates a collective mindset focused on security. Encouraging employees to report any suspicious activity or potential security risk will help to promote a proactive approach to maintaining project security. Provide regular refresher training to ensure that employees stay up-to-date despite the changing security environment.

Summary

The security of major industrial investments is complex and multifaceted. Managing the various security factors through effective strategies and innovative technologies is essential for project success, investor confidence and sustainable development. Collaboration between stakeholders, adherence to international security standards and continuous learning from past experience are key to managing security risks and creating a safe investment environment. In our globalizing world, multinational companies are present in our country, and it is in their vital interest to establish and maintain relationships that can lead to long-term cooperation with local communities based on common interests, taking into account all aspects of security. Safe project implementation requires support, which goes beyond good relations with public authorities and requires constant communication. Security needs to be seen in a local context, as global security processes have little direct impact on miro-communities, and therefore security systems need to be designed primarily with local specificities in mind. Its design and structure must closely follow the different phases of the project and respond to them in a timely and appropriate manner, following the evolution of the project. Tracking changes in risks is also an important part of building and operating an effective security system.

References

Berek, T. & Bodrácska, G. (2010). Az élőerős őrzés az objektumvédelem építőipari ágazatában. *[Live guarding in the construction sector of site protection.] Hadmérnök,* V. évfolyam 4. szám.

Christián, L., Major, L., & Szabó, C. (2019). *Biztonsági vezetői kézikönyv. [Security Manager's Handbook.]* Dialóg Campus.

Garcia, M. L. (2007). *Design and Evaluation of Physical Protection Systems.* Elsevier Science. https://doi.org/10.1016/B978-0-08-055428-0.50005-1

Horváth, T. (2018). Elektronikus megfigyelő-, és ellenőrző rendszerek objektumorientált kialakítása különös tekintettel a biztonsági kockázatok rendszere. *[Object-oriented design of electronic monitoring and control systems, with particular attention to security risks.]* Budapest: Óbudai Egyetem Biztonságtudományi Doktori Iskola.

Lawrence, J. F. (2013). *Effective Physical Security.* Butterworth-Heinemann.

Sennewald, C. A. (2011). *Effective Security Management.* Elsevier: Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-382012-9.00021-6

Tiszolczi, B. G. (2019). Fizikai biztonsági kontrollok tervezésének és alkalmazásának gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében. *[The practice of designing and applying physical security controls in light of the requirements of ISO/IEC 27001.] Magyar Rendészet,* 2–3, 233–249. https://doi.org/10.32577/mr.2019.2-3.12

Laws and Regulations

Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Reference of the article according to APA regulation

Gubics, F. (2025). Characteristics of security risks of large industrial investments and their management principles. *Belügyi Szemle*, *73*(1), 205–217 https://doi.org/10.38146/BSZ-AJIA.2024.v73.i1.pp205-217

Statements

Conflict of interest

The author has declared no conflict of interest.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.