SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2024
ORGANIZATION AND MANAGEMENT SERIES NO. 213

SECURITY OF CLOSED – CIRCUIT TELEVISION – CASE STUDY

Zygmunt MAZUR[1*], Janusz PEC[2]

[1] Wroclaw University of Science and Technology, Faculty of Information and Communication Technology, Department of Applied Informatics; zygmunt.mazur@pwr.edu.pl, ORCID: 0000-0003-1253-7895
[2] Polish Information Processing Society, Warsaw, Poland; janusz.pec@gmail.com, ORCID: 0009-00025450-5351
* Correspondence author

Purpose: The purpose of this paper is exemplification which illustrates the application of the simple analytic method to the analysis of the performance of a closed-circuit television system operated by a large nationwide organisation.
Design/methodology/approach: This straightforward approach conduce to readily adopted by businesses of varying sizes, enables the organisation and analysis of information pertaining to the entirety of an organisation's operations, structure and strategic orientation. The well known method SWOT is used.
Findings: The work shows the advisability of using the SWOT method to analyze the performance of CCTV. It is noted that the above method can serve as a preliminary stage for an in-depth analysis of the risk of CCTV operation and the selection of an appropriate organizational strategy in this matter.
Originality/value: The principal benefit of this approach is its versatility and simplicity. However, this also represents a potential drawback, namely the subjectivity that experts may introduce when performing it. The authors illustrated the efficacy of this approach in formulating a strategy for addressing a problem by constructing a dependency matrix between external and internal factors. This matrix enables the evaluation of the operational efficacy of a secure system, such as a closed-circuit television system, and the formulation of recommendations for its future development.
Keywords: Strengths, Weaknesses, Opportunities, Threats (Swot), Worst Case Analysis, CCTV (Closed-Circuit Television), FAT (Factory Acceptance Test).
Category of the paper: Case study.

1. Introduction

Security is a significant factor influencing the decision of business owners, irrespective of their size, to adopt closed-circuit television (CCTV). This early 20th-century invention has a variety of applications, both in a broader urban context and in a more limited domestic context. One of the fundamental components of an effective security system for safeguarding individuals

http://dx.doi.org/10.29119/1641-3466.2024.213.24

and assets on a given premises is the continuous monitoring of the premises through the use of video surveillance technology. In practice, the cameras are frequently utilised by companies across a range of industries, with an increasing prevalence in communal buildings and commercial premises.

The main objective of CCTV is to enhance the level of security, including the expeditious identification of potential threats and the implementation of suitable countermeasures.

The paper describes a certain exemplification of the use of the SWOT method to analyse the performance of a closed-circuit television system. The objective of this case study is to demonstrate the utilisation of the findings derived from the SWOT analysis. This easy-to-use method used in business can be successfully applied in small, medium and large organisations to organise and analyse information for every facet of the organisation's operations, structure and strategy. The principal benefit of this approach is its versatility and simplicity. However, this also represents a potential drawback, namely the subjectivity that experts may manifest when performing it. The paper will demonstrate the utility of this method in the selection of an optimal strategy for the resolution of a given problem. This is achieved through the creation of a dependency matrix between external and internal factors, which allows for the assessment of the operational quality of a secure system, such as a CCTV system. Furthermore, it enables the formulation of guidelines for the continued development of the system.

The selection of an appropriate system is not merely a matter of ensuring security or the prevention of unfavourable occurrences. The selection of the optimal solution is contingent upon a number of factors, including economic considerations, functionality, and the potential for installation and the associated limitations.

By undertaking a comprehensive risk and weakness **assessment** of the designed system, a proposal for a solution to the identified problem can be formulated. In order to conduct a comprehensive analysis of the functionality of the designed system, we will utilise an illustrative analogue closed-circuit television system of a prominent nationwide organisation, designated here as "ABC" (in the paper, the name of the organisation is altered). This system operates on a national scale in accordance with the Polish standard PN-EN 62676-4.

2. Closed-circuit television

Video surveillance, often referred to as closed-circuit television (CCTV) significantly increases the security level of the protected facility (Gaździcki, 2024). Closed-circuit television (CCTV) is a system whose basic elements are cameras. While the deployment of just cameras in strategic locations on a site allows for the tracking of various activities, this is insufficient for the effective implementation of closed-circuit television**.**

In the paper on principles for checking the effectiveness of closed-circuit television, ten principles for the responsible implementation of CCTV are cited, which were formulated by Nancy G. La Vigne of the Urban Institute in Washington, D.C. These principles apply to closed-circuit television in urban spaces, but a significant proportion of them also have relevance to private use.

Principles of closed-circuit television effectiveness (Kabzińska, Szafrańska, 2018):

1. identify the needs for which closed-circuit television is to be responsible and the budget for the investment,
2. planning (prior to investment) the principles of camera management, the necessary infrastructure and other costs that may arise from the operation of the monitoring over time,
3. selecting camera locations to ensure good visibility,
4. considering integrating closed-circuit television with other technologies (e.g. intelligent surveillance systems, crime maps),
5. balancing between the usefulness of the monitoring and the protection of privacy and other civil rights,
6. considering the benefits and costs of introducing cameras based on continuous active monitoring (uninterrupted observation of camera images by operators),
7. integrating the surveillance cameras into existing practices and procedures for ensuring public safety and order,
8. forming and maintaining realistic expectations of the quality of monitoring records,
9. using closed-circuit television as a tool to complement existing prevention (e.g. police patrols), identification and reconnaissance activities,
10. being aware of the evidentiary potential of closed-circuit television recordings, which can only (or as much as) complement other means of evidence (e.g. witness statements).

The legal basis for using CCTV depends on the situation – it will be different at work, at home and when it's related to a city or county. It would seem reasonable to posit that the primary obligation is to notify the monitoring operation. The use of a hidden camera could result in legal ramifications.

The basic set of components of a closed-circuit television system consists of (Gaździcki, 2024):

- cameras – which read and transmit images in real time to the recorder,
- a video recorder – which, thanks to its software, enables the reading of images from cameras on the screens of the monitors connected to it, as well as the recording of images on a hard drive connected to it or, in the case of digital video recorders (DVRs), also on a server,
- monitoring software,
- a keyboard – to control the system,
- a monitor (or more) – with which it is possible to observe the image from the cameras.

It is a closed-circuit because all its components are tightly interconnected. Unlike conventional television, this system is designed for a limited audience. Cameras, as the most important component of a CCTV system, which allow dangerous situations to be detected completely remotely, without leaving the observation post and control keyboard panel. The CCTV system plays a vital role in ensuring the security of the site, providing invaluable assistance to the security personnel and enhancing their capabilities. A CCTV system can operate by connecting individual devices together either wired – using coaxial cables or network cables – or wirelessly**,** using an internet connection. The choice of the type of equipment will therefore determine its installation. It should be noted here that the most important components that make up a closed-circuit television system are the cameras and the video recorder.

The image transmitted from the cameras is only received at the receiving centre. In analogue systems, the images from the cameras are recorded by the video recorder on video tapes for later playback. Keyboards are also connected to the video recorder to control the system, including panning and focusing the image. However, these are analogue systems that are increasingly being displaced by modern digital systems.

The primary purpose of monitoring is to increase the level of security, including in particular the rapid identification of potential threats and the taking of appropriate countermeasures. Modern monitoring allows 24/7 observation of the protected objects and thus allows to:

- increase protection against burglary, theft and robbery,
- reduce the cost of employing physical security staff,
- increase productivity in industrial buildings,
- improve the company’s image.

CCTV systems have the following advantages:

- the ability to detect the presence of unwanted people and dangerous situations,
- 24-hour supervision supported by a member of staff or not,
- guaranteeing a sense of security in public places,
- providing evidence in the case of misdemeanours and crimes committed and caught on camera.

Depending on one’s subjective opinion, a CCTV system may or may not be considered necessary on a property. Furthermore, the surveillance system can be controlled remotely from the control room and the cameras can operate continuously, providing uninterrupted images from sensitive locations. Therefore, this system is used by many commercial establishments, services, workplaces and even private users.

The presence of IP cameras often makes potential perpetrators choose not to commit a crime for fear of being recognised. Closed-circuit television footage is often used to apprehend the offender and explain the resulting incidents. The use of CCTV very often facilitates the work of those supervising motorways and the traffic that is on them. This allows them to deploy units in a quick and organised manner in the event of an accident of some kind or to pass on information about traffic jams. CCTV systems also increase the sense of security on public transport, informing the services when a crime has occurred so that the police can respond more quickly and get to the scene. Additionally, cameras are utilised by proprietors of commercial and service establishments, including shopping centres, hotels and restaurants, to guarantee the security of their clientele and personnel.

The operation of closed-circuit television is straightforward. The cameras, deployed in various locations, transmit images to a video recorder, which allows them to be read on monitors and allows them to be recorded on an external hard drive or servers. In order for devices to communicate with each other, they are connected by cables, or in modern systems by transmitters, using Wi-Fi. Thanks to Internet access, they can in turn transmit images directly to users' mobile devices, who can thus remotely monitor the facility from anywhere.

The cameras must be connected to a video recorder or video server, as must the monitor(s) that allow the image to be read, the control keyboard and external storage media that allow the surveillance image to be recorded. Furthermore, a surveillance system installed on a server or video recorder is required to carry out surveillance. Only a system configured in this way enables video tracking.

Closed-circuit television is a system of cameras installed on the premises to track activity. Its operation is based on the installation of CCTV cameras and the tracking of all movements and processes on the premises through them**.** Due to the extensive functionality of CCTV cameras, they are used in various types of facilities.

Closed-circuit television consists of several different pieces of equipment because the installation of cameras alone does not allow for surveillance. Conducting surveillance with cameras definitely makes it easier to identify potential threats on the protected premises. Regardless of how the premises are being used. However, the specifics of a particular site may limit the effectiveness of particular cameras**,** so it is advisable to select the equipment that works best for it. Equipment in analogue monitoring is mainly used to track activity at close range.

Analogue cameras have many advantages:

- Simpler to install and cheaper than their digital counterparts – we connect each camera to a video recorder, meaning we have no devices between the camera and the video recorder.
- Stable transmission without delay – live viewing is real-time, without delay.
- Long signal transmission distance – using coaxial cable, the maximum distance between the camera and the video recorder is up to 0.5 km.
- Compatibility – the vast majority of the system's equipment supports all standards, making it possible to freely combine cameras and recorders from different manufacturers.

- Unified system – the heart of the entire system is the video recorder and it manages all the cameras, is responsible for intelligent event detection and alerts and generates notifications.
- Independence from the Internet network – Analogue cameras can record events regardless of Internet access due to the camera's direct connection to the video recorder via a signal cable.

Disadvantages of analogue cameras:

- They require a cable to be run to each unit, which is not always possible due to building installation constraints.
- Difficult to configure cameras – the OSD menu in analogue cameras requires technical expertise to properly configure the entire system.
- Fewer image adjustments – analogue cameras have fewer image configuration features than digital IP cameras.
- Integration limitations – analogue systems have limited integration possibilities with other security systems, such as access control or alarm systems.
- No standalone operation – analogue cameras do not have standalone operation, they require connection to a video recorder.
- Low video resolution – traditional analogue systems operating in the PAL standard allow video recording at a maximum resolution of WD1 – 960H (960x576).
- High failure rate – analogue cable video transmission carries the risk of signal interference and numerous associated failures.
- Low security – high vulnerability to video interception as the image is not encrypted in any way, you just plug in the cable from the camera and you get the image. With a little knowledge, the image seen on the monitor side can be easily manipulated.

Traditional analogue systems are recommended to customers who do not need high quality, but only an overview image from the cameras. It is also an excellent solution for those who are looking for, an inexpensive – economical solution. In many companies, standard analogue systems are still in place. They are regularly extended and upgraded, and their users often report to us the need to adapt their existing monitoring installation to the needs of the new standard

3. SWOT analysis and company strategies

SWOT – is a popular heuristic technique for organising and analyzing information. The name is an acronym from the words for the four components of the analysis (*Strengths*, *Weaknesses*, *Opportunities* and *Threats*). While not a substitute for risk analysis, it can be seen as a preliminary element of it, particularly in cases where there is a lack of an appropriately tailored methodology and basic parameters to perform a level III risk analysis. This may be for a specific information system or more generally for a digital processing system.

The purpose of the SWOT analysis is not only to prepare a suitable matrix table of the relationships between the above-mentioned four components of the SWOT analysis), but on the basis of this matrix, the relationships between opportunities-threats and strengths-weaknesses can be established and, consequently, a strategy can be set for the further development of the company. The SWOT analysis should be developed in a quantitative way, assigning an appropriate scale to each of the factors analysed, and it is recommended that appropriate weights are set to them.

SWOT analysis is a tool used in the process management approach to strategic planning that helps identify strengths, weaknesses, opportunities and threats. Most commonly, SWOT analysis, is used to plan a company's business strategy, but it can also be used in new marketing strategies or personal development. We very often turn to the SWOT tool when reviewing management and defining the context of the organisation, more specifically the internal and external factors relevant to the purpose and strategic direction of the organisation, as well as those that affect the organisation's ability to achieve its intended results. SWOT analysis, is also a reliable tool for risk assessment. Guidance on this aspect is provided in VDA4 – Quality Assurance in the Process Landscape, Section 2: Risk Analyses (VDA, 2020)**.**

SWOT analysis consists of dividing the information gathered about the activities and planned development strategy of a given enterprise into four groups (four categories of strategic factors):

- **S** (Strengths) – anything that represents an asset, a superiority, an advantage,
- **W** (Weaknesses) – anything that represents a weakness, a barrier, a disadvantage,
- **O** Opportunities) – anything that represents an opportunity for beneficial change,
- **T** Threats) – anything that poses a danger of adverse change.

Information that cannot be correctly categorised into any of these groups is not considered further in the analysis.

The SWOT analysis distinguishes four action strategies that a company can take: aggressive, defensive, competitive and conservative (SWOT, 2024). It all depends on which boxes on the SWOT matrix dominate the others, i.e. get the most points.

1. **Aggressive strategy** (**strengths** and **opportunities** dominate) – this is the best possible situation. This **strategy** relies on the company's strong expansion and seizing opportunities.
2. **Conservative strategy** (**strengths** and **threats** dominate) – should be considered when a company has internal potential but an unfavourable environment prevents it from growing strongly. This strategy assumes that strengths must be used to deal with external threats.

3. **Competitive strategy** (dominated by **weaknesses** and **opportunities**) – involves exploiting opportunities while eliminating the company's weaknesses. The advantage of this situation is a friendly environment that allows the company to maintain its position in the market.
4. **Defensive strategy** (**weaknesses** and **threats** dominate) – if the negative factors outweigh the positives, there is a risk of the business failing. The focus should therefore be on the survival of the organisation (e.g. merging with another company).

In order to carry out a good SWOT analysis of a company you need to:

1. The first step is to assemble a team. Define the purpose and object of the company's SWOT analysis and explain to all involved the meaning of the analysis activities – i.e. *what* we want to achieve and *why*.
2. Introduce the adopted SWOT analysis procedures to the participants. Explain *exactly* what is meant by each term and provide examples to illustrate them. Encourage people to ask questions in order to dispel any doubts at this stage.
3. Have the team members prepare a thorough description of the business and its growth prospects and develop an individual analysis of the advantages, disadvantages and opportunities and threats that they see as strategic for the company.
4. Develop a common SWOT analysis matrix and enter the factors listed by all team members there. Eliminate those that are strategically irrelevant. Prepare a glossary of basic terms – so that no one is in any doubt as to the meaning of particular terms.
5. Hold a discussion with the team on the conclusions of the analysis. To try to look at the results from different points of view. Points can be awarded to individual factors according to their importance: from -2 to 0 for *weaknesses* and *threats* and from 0 to +2 for *strengths* and *opportunities*.
6. Based on the results, develop an initial action strategy to be further refined and implemented by the company's management.

Such an analysis can also be presented graphically as a SWOT analysis diagram. The related diagram is presented at Figure 1.

SWOT	**Opportunities (O)**	**Threats (T)**
Strengths (S)	Aggressive strategy	Conservative strategy
Weaknesses (W)	Competitive strategy	Defensive strategy

Figure 1. SWOT analysis diagram.

4. Sources of information about the proposed system

During the preparatory work for the analysis of the analogue closed-circuit television system on the example of a certain nationwide organisation ABC (name of organisation changed in the paper) using the Polish standard PN-EN 62676-4 (Polska Norma, 2024). The primary sources of information about the proposed system were:

1. Interviews with system supervisors and operators.
2. Local inspections.
3. System documentation provided.

Re 1. personal sources of information:

- Information obtained from an interview with the CCTV system server administrator.
- Information obtained during a telephone conversation with an employee from the LAN management team.
- Information from an employee in the organisational unit responsible for protection of classified information.
- Information obtained as a result of an interview with the head of the unit referred to in the previous bullet point.
- Information obtained from security company personnel regarding the history of events and incidents.

Re 2. local inspections:

- Viewing at the reception of an operator station consisting of an event recorder, a keyboard together with a joystick.
- Overview of the analogue video system server administrator workstation with dedicated system management and monitoring software.

Re 3. the system documentation provided included the following documents:

- Polish standard PN_EN 62676-4 „Systemy dozoru wizyjnego stosowane w zabezpieczeniach" (en: Video surveillance systems for security applications) – Part 4: Application guidelines (Polska Norma, 2018).
- Contract between the organisation and the contractor for the maintenance of the analogue closed-circuit television system.
- As-built documentation of the modernisation of CCTV in the organisation (Dokumentacja podwykonawcza, 2013).
- DVS control keyboard user manual (DVS, 2007).
- Documentation of PSS (Professional Surveillance System) software for surveillance of small CCTV networks (Przewodnik użytkownika).
- Video recorder description and user manual – the video recorder is responsible for recording and processing the video supplied directly from the cameras via the coaxial cable (Quick start guide).

5. Detailed SWOT analysis for the closed-circuit television system

This paper assumes that the SWOT analysis will be supported at some points by a Worst Case Analysis – especially where there is insufficient information about a problem or something has not been done or has been done badly. It is a method used, for example, in issues of computational complexity of algorithms, in electronics when testing electronic circuits, and in economic issues such as portfolio management.

As written in the introductory chapter of this paper, we will now discuss the four basic categories of factors that define the SWOT analysis. We will start by identifying the components influencing the so-called strengths of the surveillance system under analysis.

Strenghts

Components shaping the strengths of the system:

S1. Experienced staff – trained security company personnel.

S2. Consulting the system operating guidelines with the head of the unit responsible for the protection of classified information.

S3. Possibility of seconding IT staff from other organisational units to operate and maintain the CCTV system.

S4. Server with practically no downtime.

S5. Maintenance contract – up to date, maintenance reports every 3 months.

S6. Dedicated CCTV surveillance server located in a guarded room.

S7. Certified malware protection standard.

S8. Zoning – III zones – use of tripods, magnetic cards, register of people entering and leaving.

S9. Due diligence in establishing monitoring modes including priorities and tracking paths.

S10. Partial compliance in some points with the Polish standard referred to in Re 3 of the previous section, e.g. for compression, export and playback of video recordings in commonly available file formats.

We now turn to an analysis of the system's weaknesses. Unfortunately, there are many more weaknesses in comparison to the strengths.

Weaknesses

Weaknesses in the system, anything that constitutes a weakness, a vulnerability in the system:

W1. No assumptions for the system – preliminary design + specifications + OR (operational requirements) – in accordance with PN-EN 62676-4[1].

W2. No information on the performance of the following tests:

- Regression – should be done after the cameras have been replaced (retrofit). Regression tests are important, as the replacement/addition of new cameras usually results in a change in the electrical operating parameters of the system – including the operating parameters of individual cameras. In order to assess the performance of individual cameras (see tests in annexes B, C, D, E of the Polish standard) after their replacement and possibly propose changes in camera settings, it is necessary to have and compare the camera specifications described in the system assumptions (OR) with the results of regression tests. It is an essential thing.
- Acceptance – in accordance with the aforementioned standard. These are *user acceptance tests (OR), and technical acceptance tests*[2].
- Technical acceptance tests according to the aforementioned standard include[3]:
  - Imaging quality.
  - Verification of image quality in terms of:
    - Contrast,
    - Colour reproduction resolutions,
  - Coherence of the imaging chain.
  - Tests of the cameras' ability to fulfil their function:
    - Inspections,
    - Recognitions,
    - Observations,
    - Detection,
    - Surveillance – event response levels and false alarm test (Annex E of the standard),
    - Identification of vehicle number plates.
    - As an option, in the event of system modifications – e.g. hardware and software localisation – factory acceptance testing (FAT) by the manufacturer is available on request.

[1] Admittedly, it is not currently mandatory for entities carrying out public tasks to use Polish standards, but this is a strong indication of the substantive correctness of the solution presented.

[2] According to §5.2 PN-EN 62676-4 of the standard – absence (OR) means the impossibility of determining whether the system meets the stated objective. In practice, this means that the standard states that it is impossible to assess the system. In this case, we cannot use the Worst Case Analysis to support the SWOT analysis, as this would mean that this study could not be carried out.

[3] Here we apply the Worst Case Analysis principle as much as possible.

- Random.
- Electrical and commissioning (Vedemecum I, 1999; Vademecum II, 2002) – in addition to taking system resistance measurements:
  - Attenuation – for both RG 6 and UTP cable.
  - Higher overtones produced by equipment such as switching power supplies, smartphone chargers and affecting the performance of the electrical network by causing non-linear distortion and power loss in three-phase receivers – transformers, capacitor banks (e.g. in UPS). Higher overtones generate interference (noise) in electrical networks especially in inductive and capacitive components – the need for appropriate filters. They are generated by IT equipment and are introduced into the installation causing overheating of the transformer windings. They are particularly dangerous for capacitor batteries (Siemek, 2002).
  - Interrogation (remote and proximity) in the section on twisted pair (Derfrer, and Freed, 2000).
  - Wave impedance for both types of cable – twisted-pair UTP and coaxial cable – is not the same as measuring resistance.
  - Grounding – surge and lightning resistance[4].
  - Signal-to-noise measurement.
- The distances to the cameras are not stated in the documentation.

W3. Some analogue cameras presented an older model – older standard – insufficient resolution – no audio recording.

W4. Lack of logical and physical separation of the CCTV system server software, especially in terms of security, from the organisation's LAN network.

W5. Scarcity of technical documentation on the system – e.g. commissioning documentation and formal acceptance document, declaration of conformity with national regulations – concerning national or international law – compliance with standards if necessary, recommendations for operation and maintenance of the system.

W6. No information on the number of system failure events – statistics – e.g. abrasion of PVC pipe cables during façade works – if any, drive failures etc.

W7. No information on further training received by security company staff beyond purchase training.

W8. No power balance for the system's cameras.

W9. No re-testing of system resistance according to maintenance rules.

W10. Lack of information on the statistics of events recorded by the system in the sense of the standard – use of the following functions:

[4] The signal grounds from all cameras should connect at the recorder, but should not connect at the camera side. Also, there should be no connection between the signal ground and the camera power ground – this is particularly important in cameras powered by 24 VAC, and not even allowed in cameras powered by 230 VAC. Active video separators are used to eliminate interference and various power supply problems.

- Inspection.
- Identification.
- Recognition.
- Detection – the archiving practically covered 28 days – it is then overwritten.

W11. The DVS keyboard software has not been updated for several years.

W12. No expansion possibility of the recorder.

W13. No formal written procedures for analogue system operators.

W14. Poor quality reporting of maintenance inspections – curtly limited to a statement of positive acceptance – see standard § 17.3 PN-EN 62676-4.

W15. Non-compliance with the Polish standard in some points of the standard's recommendations.

Threats

Hazards, anything that poses a risk, a danger of adverse change.

Threats arising:

T1. in the absence of tests carried out – the actual technical condition of the system determines the resistance of the system, especially in bad weather conditions – fog, heavy rain, snow, etc.,

T2. from the lack of formulated requirements – assumptions for the system – the lack of a path to the target point and its definition, which should be described in the chapter on the "system life and development cycle",

T3. due to the lack of formalised procedures,

T4. from the scarcity of technical documentation,

T5. from the lack of maintenance of incident statistics – inability to assess the probabilities of incidents,

T6. from the lack of logical and physical separation of the CCTV system server – the possibility of a hacking attack,

T7. resulting from the lack of periodic training, which affects routine handling of situations that require deeper analysis of incidents,

T8. lack of software updates, which reduces the efficiency of system use (server software, DVS keyboard software),

T9. from the requirements of GDPR (General Data Protection Regulation).

Opportunities

Opportunities, anything that creates a chance for positive change[5]

O1. Opportunity to upgrade the system when the organisation receives external orders – additional income from the organisation's regulations and charters (opportunity to subsidise the closed-circuit television system).

O2. Potential for additional full-time positions.

O3. Possibility of additional training related to system upgrades.

O4. Possibility of evolution of the analogue system to IP digital surveillance supervised from the technical side by a company contracted to technically maintain the closed-circuit television system.

O5. Possibility to refine and complete the documentation (formalisation of procedures) in order to manage and operate the system more efficiently.

O6. Ability to perform missing tests in order to obtain reliable information on the state of the system and make necessary changes resulting in improved system performance – especially user acceptance tests.

O7. Ability to conduct a risk analysis of the video system as recommended by the standard after receiving basic guidelines from the Information Security Management Committee/Commission of the organisation's top management for establishing the components of the risk analysis for the organisation-approved by this body, and the results of an independent audit of the system regarding e.g. good practices and probability estimates of information security management events in the ministry, and the security policies of the other 2 levels (level 1 was approved by the previous management of the organisation).

O8. Possibility of external audit of CCTV system for compliance testing.

O9. The possibility of applying for a quality certificate after improvements and expansion of the system.

O10. Ability to mobilise the system maintenance company to fulfil the scope of the contract in terms of producing more accurate reports on the maintenance work carried out.

O11. Ability to set up an event log to enable relevant statistics to be kept.

Based on the above established facts, we can now construct a matrix of relationships between the aforementioned categories of strategic factors, assuming the following conditions:

CON1. We treat the strengths and weaknesses of the system as a set of internal factors.

CON2. We treat opportunities and threats as a set of external factors.

CON3. We take the degree of dependency in the form of an impact level on the following scale:

[5] Otherwise, these are potential opportunities that may or may not be exploited, but all possible ones are considered in this case.

0 – no significant impact,
1 – weak interaction – indirect relationship,
2 – strong impact.

The 25 x 20 global dependency matrix M (Figure 2) below consists of four sub-matrices M1, M2, M3, M4 of the following dimensions:

- M1: matrix 10x11.
- M2: matrix 10x9.
- M3: matrix 15x11.
- M4: matrix 15x9.

$$M = \begin{array}{|c|c|}\hline \text{M1 (S)} & \text{M2 (T)} \\ \hline \text{M3 (W)} & \text{M4 (O)} \\ \hline \end{array}$$

Figure 2. Global dependency matrix M and four sub-matrices M1, M2, M3, M4.

Thus, the dependency matrix M has 500 elements, which map the existing reality, i.e. the current state of analogue monitoring. Designations have been adopted here in accordance with the previously adopted notation. In particular:

- S1, S2, ..., S10 – denotes the strengths of the system – there are 10 of them – the letter S is an abbreviation for Strengths. These form part of the set of internal factors of the SWOT analysis, as per condition CON1.
- W1, W2, ..., W15 – indicates the weaknesses of the system – there are 15 of them. The letter W is an abbreviation for Weaknesses. They form part of the set of internal factors of the SWOT analysis, according to condition CON1.
- O1, O2, ..., O11 – denotes opportunities that can be exploited to improve the performance of the system – there are 11 of them. The letter O is an abbreviation for Opportunities. These form part of the SWOT analysis's set of external factors, according to the condition CON2.
- T1, T2, ..., T9 – denotes threats to the system – there are 9 of them. The letter T is an abbreviation for Threats. They form part of the SWOT analysis's set of external factors, according to condition CON2.

The scale adopted and the components of the 4 strategic category groups listed above map the current state of the system in the matrix given below. The individual values of the matrix demonstrate the extent to which the individual components of the strategic factors are related to the knowledge of the expert performing the analysis, as derived from the information sources provided, as previously outlined in chapter 2. It is inherently subjective – it can be objectified by repeating the assessment of the creation of matrix values by several other experts, calculating average values and entering them into the resulting dependency matrix in place of the previous values.

A twin method called TOWS should also be mentioned here. A SWOT analysis commences with an evaluation of the organisation’s internal strengths and weaknesses. This is followed by the identification of opportunities for optimising the organisation’s performance, with due consideration of the external environment. In contrast, a TOWS analysis begins with the identification of external opportunities and threats, and the subsequent analysis of the organisation’s capabilities in light of these. This approach is therefore reversed to that of the SWOT method. These opportunities and threats are then contrasted with the existing conditions (strengths and weaknesses) to exploit opportunities to remove or offset threats (Bubacz, 2010).

The matrix M of relationships between sets of internal and external factors is presented in Table 1.

Table 1.
The global dependency matrix M

	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10	O11	T1	T2	T3	T4	T5	T6	T7	T8	T9
S1	0	0	1	1	2	0	1	1	1	1	2	0	0	2	1	2	0	2	2	1
S2	0	2	1	2	2	2	2	2	1	2	2	1	2	2	2	2	1	2	1	1
S3	2	0	2	2	1	2	1	0	0	0	0	0	2	1	1	0	2	1	1	0
S4	0	0	0	1	1	0	0	0	1	0	0	0	0	0	1	0	0	0	2	1
S5	1	1	1	2	2	2	1	2	2	2	1	1	1	1	2	2	1	1	1	1
S6	1	0	0	2	2	0	0	0	1	1	0	1	0	0	1	0	2	1	0	1
S7	1	0	1	1	1	1	1	1	1	0	0	1	1	2	0	2	2	1	1	1
S8	0	0	1	1	1	1	1	0	1	0	0	0	1	1	0	1	0	0	0	1
S9	1	1	1	1	1	1	1	2	2	2	1	1	2	2	1	1	1	2	1	1
S10	1	0	1	1	1	2	1	1	0	1	0	2	2	1	2	1	1	1	1	1
W1	2	1	2	2	2	2	2	2	2	1	2	2	2	2	2	1	1	2	1	2
W2	1	1	1	2	1	2	2	1	1	1	0	2	1	1	2	1	2	0	2	2
W3	2	0	0	2	1	2	0	2	1	2	0	2	1	0	1	0	0	1	1	1
W4	1	0	1	1	1	2	1	0	2	0	0	0	1	1	1	1	2	1	0	0
W5	1	1	1	1	2	2	1	1	1	1	0	1	2	0	1	0	1	1	1	2
W6	1	0	0	0	1	1	1	1	1	1	1	1	1	2	1	2	2	1	1	0
W7	1	0	2	0	2	1	0	0	1	1	0	1	1	1	0	1	1	2	1	1
W8	0	0	0	1	2	2	1	1	1	0	0	2	2	1	1	0	0	1	0	0
W9	1	0	0	0	1	2	1	1	1	2	0	2	0	1	1	0	0	0	0	0
W10	2	0	1	1	2	2	2	2	2	1	1	2	2	2	1	1	0	1	0	2
W11	1	0	2	1	2	2	1	1	2	2	0	1	2	1	1	0	1	2	2	0
W12	2	0	2	2	0	1	2	0	2	0	1	1	2	0	0	1	0	1	0	1
W13	1	1	1	1	2	1	1	2	1	2	2	2	2	2	2	2	2	2	2	2
W14	2	1	1	1	2	2	2	2	2	2	0	2	2	1	2	0	2	0	0	1
W15	1	1	1	1	2	2	2	2	2	1	1	1	2	1	2	1	1	2	2	2

In the dependency matrix M presented in Table 1, we can distinguish four sub-matrices M1, M2, M3, M4 representing four different behavioural strategies:

- M1 (SxO) – proposes an aggressive strategy to solve the problem,
- M2 (SxT)– suggests a cautious behavioural strategy (conservative strategy),
- M3 (WxO) – proposes a strategy for addressing vulnerabilities in a stable external environment,
- M4 (WxT) – represents a defensive behaviour strategy called survival technique in SWOT analysis.

6. The concluding remarks of the SWOT analysis

The four fundamental sub-matrices of the primary dependency matrix, as previously outlined, can be employed to ascertain definitive conclusions regarding the optimal trajectory for the evolution of analogue video within an organisational context.

By taking into account the threats and weaknesses of the system (as defined in risk analysis terminology), the SWOT analysis enables the selection of an appropriate strategy to address the identified issues. It should be noted that the proposed approach does not replace the necessity for risk analysis, as previously mentioned at the outset of this paper. Rather, it can be viewed as a preliminary element of the risk analysis process.

Analysing the four sub-matrices M1, M2, M3, M4, we can see that the weight of a sub-matrix as the sum of all the values of its elements (counting by rows or columns) is for:

- sub-matrix M1 – 102.
- sub-matrix M2 – 92.
- sub-matrix M3 – 189.
- sub-matrix M4 – 151.

The above results can easily be checked using a simple sum function in MS Excel. Note that max {102, 92, 189, 151} = 189 , which suggests that :

1. In the system in question, efforts should first be concentrated on the task of eliminating the weaknesses of this system, which requires little investment, and is in line with the interpretation of the sub-matrix M3 with a weight of 165. These weaknesses have already been pointed out previously. The nature of this organisation is such that it operates in a fairly stable external environment and does not have to compete on it.
2. Next in line (according to the decreasing value of the weights) is sub-matrix M4 with a weight of 151 indicating a defensive strategy, i.e. a survival strategy (not making any changes to the system), which in my opinion should be firmly rejected if we want to develop the system or improve its performance.
3. The next most desirable option is the sub-matrix M1 with a weight of 102, which suggests the possibility of making a larger investment in the system – this is an aggressive strategy, i.e. the possibility of making larger modifications to the system, e.g. moving to a digital surveillance system with IP cameras, provided sufficient funding is available.
4. Finally, the least interesting option from the point of view of this case study is option 2 – the sub-matrix M2 (weighting 92), as it suggests as a solution a conservative strategy – little investment in technological innovations, in modern means of advertising, cautious development of the system based mainly on own savings – little use of credit lines.

7. Conclusion

The SWOT analysis is an essential tool in the process approach of business management for assessing the current situation of a company and determining key operating strategies (SWOT, 2024). SWOT helps to better understand the events surrounding a company and its effective use of results, allows for the construction of sound business strategies, adaptation to market changes and long-term success. It is not only a diagnostic tool, but also the foundation for making wise strategic decisions that lead to the sustainable development of the organisation.

It should be borne in mind that if the method of action presented in the paper is chosen, we should consider the main strategic objectives in the chosen company at all times**.** Sometimes the choice of a particular strategy is more complicated and depends on a particular combination of factors. Of course, SWOT analysis also has disadvantages. Above all, it is prone to subjectivity and its results are often obvious or lead to misinterpretations. Besides, not all relevant factors for a company can be encapsulated in terms of advantages, disadvantages, opportunities and threats.

All this means that this method, although popular, in practice can often be **questioned**. Thus, if we are interested in meaningful results, the SWOT analysis can be taken as a starting point for further assessment of the strategic situation of the company. This will be facilitated by a number of factors, including:

- ASTRA analysis.
- PEST analysis.
- Porter’s five forces concept.
- Scenarios of ambient conditions.
- Scenarios of possible events.
- Simulation scenarios.

Surveillance systems are highly valued in many companies, institutions, shops. Their main aim is to increase the level of security. Nowadays, the concept of CCTV has been replaced by closed-circuit television. Initially, CCTV cameras with all their equipment were mainly installed in industrial facilities for the surveillance of a particular building and the area around it. At the time, their aim was to prevent theft and minor offences by company employees.

Basically, we can divide closed-circuit television systems into: IP digital (network) monitoring, analogue monitoring – traditional, hybrid monitoring – is a combination of both technologies in one system. As the consumer society develops, closed-circuit television systems are mainly installed in public places such as parks, banks, restaurants, hypermarkets, residential buildings, guarded car parks, railway stations and main city streets.

Nowadays, it is possible to observe an increasing interest and demand for closed-circuit television systems due to the miniaturisation of cameras and all instrumentation. The solution presented in the example company "ABC" can be used as a starting point for further assessment of the companies' strategic situation.

Due to the ever-widening applications and growing demand for closed-circuit television, security system manufacturers continue to constantly improve the intelligent capabilities of cameras. Modern cameras can, among other things (Gaździcki, 2024):

- identify the object in the recording as a person or a vehicle,
- count persons or length of stay,
- detect left luggage,
- recognise suspicious behaviour and gatherings,
- recognise persons entering, leaving and passing through a marked line,
- detect the number of people in a queue,
- capture images of faces,
- determine a person's approximate age, gender, colour of clothing, facial expressions or additional items of clothing e.g. backpack, helmet or mask,
- identify features e.g. facial hair, glasses or headgear,
- detect burglary,
- detect scene changes,
- identify video sabotage,
- detect loss of focus,
- carry out vehicle detection,
- detect vehicle parking,
- recognise license plates (LPR),
- recognise the colour and model of the vehicle,
- track vehicles or people (PTZ cameras),
- thermal imaging fire warning,
- measure the temperature of the human body or objects.

Analogue monitoring works on the basis of the well-known analogue technology. In a nutshell, it is a set of devices that produce or mediate an analogue signal that allows analogue recording by rendering frequency and intensity in the form of an image, sound or text. Today, modern analogue monitoring is not really analogue – it is just a word for describing the system. Often, the only all-analogue component included is a coaxial cable with a combined power cable.

As in almost every industry, analogue technology is being displaced by digital technology so in the closed-circuit television industry, analogue monitoring is increasingly being displaced by digital (network) IP monitoring.

Modern systems use wireless connections and digital cameras, which can have much more functionality. What is more, a CCTV system designed with digital technology does not require cameras to be connected to a video recorder, as the image can be received remotely on mobile devices and computers using an internet connection. However, modern digital recorders allow camera images to be saved as a video on a hard drive or server.

Finally, it should be noted that there are cases of companies that, despite their previous assumptions, do not commit to such a development strategy at all.

References

1. Bubacz, K. (Ed.) (2010). *Zarządzanie strategiczne. Metody analizy strategicznej z przykładami.* Poznań: Wydawnictwo Politechniki Poznańskiej.
2. Derfler, F., Freed, L. (2000). *Okablowanie sieciowe w praktyce.* Gliwice: Helion.
3. *Dokumentacja Powykonawcza Modernizacji Monitoringu TV Przemysłowej w organizacji* (2013). Warszawa: BRABORK Laboratorium Sp. z o.o.
4. *DVS control keyboard, user manual* (from the hardware manufacturer), 5.10.2007.
5. Gaździcki, M. (2024). *CCTV – Co to? Czym jest monitoring CCTV?* Retrieved from: https://solidsecurity.pl/blog/cctv-co-to-czym-jest-monitoring-cctv, 10.10.2024.
6. Kabzińska, J., Szafrańska, M. (2018). Zasady ewaluacji skuteczności monitoringu wizyjnego. *Przegląd Policyjny, vol. 4, no. 132.*
7. Polska Norma [Polish standard] PN-EN 62676-4. *Systemy dozoru wizyjnego stosowane w zabezpieczeniach, Część 4, Wytyczne stosowania* (2018). Warszawa: PKN (Polski Komitet Normalizacyjny).
8. *Quick start guide for the video recorder* – pdf file on CD (from the hardware manufacturer).
9. Siemek, S. (2002). *Instalacje elektryczne dla zasilania urządzeń elektronicznych.* Warszawa: Centralny Ośrodek Szkolenia i Wydawnictw SEP.
10. *SWOT – Narzędzie planowania strategii biznesowej i analizy ryzyka* (2024). Retrieved from: https://akademiajakosci.com/swot-narzedzie-planowania-strategii-biznesowej-i-analizy-ryzyka/, 10.10.2024.
11. User guide. *Professional Surveillance System, ver. 4.06, pdf file* (from the hardware manufacturer).
12. *Vademecum Teleinformatyka I.* Praca zbiorowa (1999). Warszawa: IDG Poland S.A.
13. *Vademecum Teleinformatyka II.* Praca zbiorowa (2002). Warszawa: IDG Poland S.A.
14. VDA 4 – *Quality Assurance in the Process Landscape*. Sections 1–4. (EN). VDA4 – Quality Assurance in the Process Landscape, Sections 1-4: General, Risk Analysis, Methods, Process Models. 3rd edition, fully revised and updated, August 2020.