***I.J. Engineering and Manufacturing*, 2020, 2, 1-14**
Published Online April 2020 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijem.2020.02.01

*Available online at* **http://www.mecs-press.net/ijem**

# Industry 4.0: The Oil and Gas Sector Security and Personal Data Protection

Tahmasib Fataliyev[a, *], Shakir Mehdiyev[b]

[a, b] *Institute of Information Technology of ANAS, B. Vahabzadeh street, 9A, Baku, AZ1143, Azerbaijan*

Received: 17 February 2020; Accepted: 17 March 2020; Published: 08 April 2020

## Abstract

Industry 4.0 is directly connected to the Internet of things, cyber-physical systems, artificial intelligence, robotics and other advanced technologies. It is these technologies that made fully automated digital production, controlled by intelligent systems in real-time with constant interaction via the Internet, a reality. They turned the production system into a “smart network factory”, where all activities are digitally controlled, and the use of financial and material resources becomes more efficient. Along with this, in Industry 4.0, a significant increase in data volumes brought to the forefront data protection issues, including in such a sensitive area as personal data. Illegitimate methods of using personal data to obtain additional preferences have become the goal of some communities of people. Video surveillance data are an integral part of personal data, therefore protection of personal data processed in video surveillance systems has been given increased attention. The video surveillance system includes video cameras, information and communication channels for data transmission, processing devices, analytics and personal data storage. The proposed model is a subsystem of smart video surveillance in the oil and gas sector, that consisting of such subsystems as a smart field, smart grid, smart maintenance, smart transportation, smart security, etc. Conceptual tasks are considered and recommendations for their solution are given.

**Index Terms:** Industry 4.0, Internet of things, cyber-physical systems, oil and gas sector security, personal data; protection of personal information.

* Corresponding author.
E-mail address:

## 1. Introduction

The concept of Industry 4.0, announced in 2011, symbolized the onset of a new era of the industrial revolution [1]. The purpose of this concept was more efficient, safe, environmentally friendly and less costly production, as well as the possibility of single production while maintaining the economic conditions of mass production. The key links in Industry 4.0 are the Internet of Things (IoT), cyber-physical systems (CPS), artificial intelligence (AI), robotics, and other advanced technologies. Comprehensive digitalization and intellectualization of production with a wide degree of integration of network and communication technologies did not pass by the oil and gas sector (OGS), which has not lost its significance for the economies of the countries against the background of technological and social processes taking place in the world. In various fields of OGS, tools such as smart sensors, controllers, intelligent video cameras and RFID systems used in operational processes were introduced [2]. These processes are very diverse: equipment monitoring, energy consumption in oil and gas production, further transportation, quick and accurate inspection of parts, equipment performance testing, environmental monitoring, personnel status data, geolocation, etc. Thus, in Industry 4.0 there is an exponential increase amount of different data. According to experts, a typical offshore oil platform may have more than 40,000 metadata [3]. Also in [4], numerical data are presented that are characteristic of some objects in OGS, for example, when monitoring the technical condition of a submersible electric pump, 5 GB of data is analyzed every day.

In this regard, along with the concept of safe production in the traditional sense, several problems have arisen regarding the security issues of information assets. That is, the risks of third-party (unauthorized) access to physical assets and exposure to them through the unlawful use of information assets have increased. It should be noted that one of the components of ensuring security in the Industry 4.0 sectors, including OGS, is video surveillance and image processing systems. These systems are used at all stages of production processes in OGS, from geological surveys, well drilling, production of raw materials, an inspection of its quality, monitoring of production, detection of defects, quality assurance and standards, etc., and help to achieve high economic efficiency. Technological innovations of modern video surveillance systems have several possibilities, among which are registration, recognition and diagnosis of the current state of equipment. Based on the results of such video analytics, intelligent solutions (instructions) are proposed that can be transmitted to personnel using augmented reality glasses (for example, Microsoft Hololens) [5]. Thus, the collection and processing of video information (video analytics) is also an urgent task to ensure safe production.

However, at the same time, video surveillance has significantly indicated the role of personal data (PD) belonging to a particular person. Therefore, for example, to achieve economic efficiency, financial benefits, and competitiveness many companies have made it necessary to carefully analyze relationships with customers to identify their preferences and to advance their interests. At the same time, PD are collected, processed, and distributed without restrictions. Besides, some enterprises exchange user data with a third party. Moreover, in most cases, the user does not even realize the moments when his PD are used regardless of his desire and without appropriate consent. Data is a valuable corporate resource of companies, and therefore, managers should do everything to protect their data and ensure the confidentiality of the data of employees and customers [6]. That is, automated systems of production processes along with the solution of common problems of management, security and reliability, created the problem of protection of PD, which are fundamental factors of universal human rights [7].

In this paper, some security issues and problems of PD protection in production structures of OGS, including when using video surveillance systems, are highlighted.

## 2. Background

Video surveillance is a technological system consisting of many cameras that are connected to closed-circuit television (CCTV). The history of video surveillance originates from the invention of an electronic transmitting television tube − an iconoscope [8]. Initially, the images from the cameras were sent to the monitoring centre, where the operator in front of the screen continuously monitored the events without the possibility of their analysis in the future. This was a significant drawback of such systems. Appearing in the middle of the XX century. Videotape recorders (VTRs) were able to solve this problem. Operators no longer needed to spend all the time in front of the monitor screen; all information was recorded on magnetic tape for further processing and analysis. However, due to the extremely high cost and cumbersomeness, the first VTRs were used professionally in telecentres. The situation changed significantly when the Video Home System format standard was proposed [9]. The popularity of video systems began to grow, and they were primarily equipped with stations, airports, banks, shops, gas stations and other facilities that are most exposed to external threats. Currently, video surveillance systems have become a reality in modern society, and their use is extremely wide, ranging from law enforcement and crime prevention, transport security and traffic monitoring. The growth trend of video surveillance systems and the number of cameras is typical for the USA, China, Japan and most countries. Further progress in video surveillance systems is associated with the transition of the IoT to the category of the Internet of everything, the improvement of digital cameras with high resolution, cloud, fog and edge computing, AI, 5G and 6G mobile technologies, etc. Note that existing video surveillance systems have several advantages. Among them are scaling; auto-tracking; the night vision; detection of details and signs invisible to the human eye; intelligent recognition of a person’s face and voice up to his emotional state; archiving images and the possibility of subsequent analysis; the availability of the video archive over the Internet from anywhere in the world. Based on the above analysis, we have identified four characteristic stages in the development of video surveillance systems, which are reflected in Fig. 1.

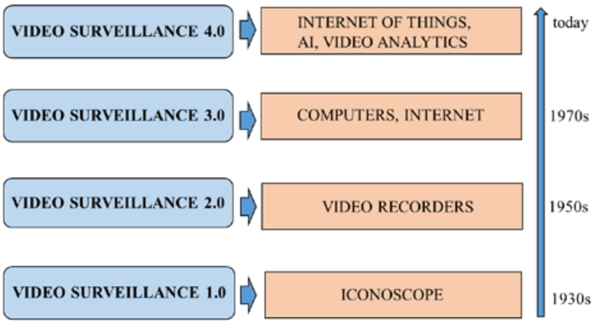

Fig. 1. Stages of development of video surveillance systems.

The technological platform of the fourth stage in this development largely coincides with the technological platform of Industry 4.0. This is the use of AI, CPSs, IoT, big data, blockchain, etc. Therefore, we offer the following names of the stages of the development of video surveillance systems: Video surveillance 1.0, Video surveillance 2.0, Video surveillance 3.0, and Video surveillance 4.0.

Video surveillance 4.0 provides the ability to quickly respond to unforeseen or dangerous situations and control processes without a personal presence at the scene. At the same time, it helps to effectively solve some production problems:

- organization of perimeter security of the territory belonging to the enterprise;
- access control at checkpoints and transport hubs;
- monitoring of work processes;
- visual observation of what is happening;
- accurate accounting of the working hours of each employee.

As the experience of operating video surveillance systems shows, there are many effective solutions for OGS. Consider the examples of implemented solutions.

*A. The video surveillance system at an offshore oil field.*

In [10], a video surveillance system for an offshore field with coverage of more than 300 drilling rigs for exploration and production at sea is presented. The system controls the drilling sites, helicopter-landing pad, and is equipped with specialized underwater cameras. The system is capable of identifying smokes, oil spills, unwanted movements at the rig site, and events are automatically recorded and stored. General monitoring of the process and additional remote (on land) access to the live broadcast are also possible.

*B. Video surveillance at the refinery.*

Here this system carries out general monitoring and is designed to detect and prevent suspicious events, malfunctions, accidents and thefts. In addition to this, specialized cameras can continuously monitor production processes in explosive, toxic and high-temperature environments where personnel are not allowed to stay. The capabilities of thermal imaging cameras allow you to control temperature changes, carry out intelligent analytics, and, thanks to integration with fire and gas alarm systems, you can take proactive security measures in advance. In general, the Industry 4.0 concept in such enterprises (for example, Honeywell's TDC 3000 control system) increased productivity by almost 10 times [11].

*C. Pipeline monitoring.*

Oil or gas leaks are often invisible or difficult to detect, and sometimes such an event can last several hours, which poses significant risks before they get noticed. For early counteraction to such events, solutions based on thermal imaging cameras and intelligent video analytics are proposed [12].

*D. Video surveillance from drones.*

Another approach to monitoring oil and gas pipelines and environmental inspection of the area is video surveillance from drones. Video images from his video cameras are used to identify the current state of pipelines and assess the environmental situation [13]. The drone-based leak detection system provides high-quality images in real-time and the Deep Learning methods allow you to quickly detect oil spills and identify unauthorized activities in protected areas.

*E. Video analytics in maintenance.*

The use of video surveillance systems in maintenance can have a significant effect. For these purposes, the capabilities of smart cameras can be used [14]. They use statistical methods and big data processing methods to obtain information from images and apply them throughout the enterprise. For example, you can determine when a piece of equipment fails before the maintenance team detects a problem. The system recognizes warning signs, uses the data to schedule proactive maintenance of equipment before a problem occurs. Images recorded in parts can be compared with thousands of others stored in the cloud to determine correlations and trends. At the same time, to achieve greater effect, video surveillance can be combined with another monitoring system – wireless sensor networks (WSN). WSN helps to obtain physical information from monitoring objects: thermal, chemical, magnetic, vibrational and other characteristics [15]. The integration of both technologies makes it possible to create an intelligent maintenance system.

*F. Video surveillance to control and comply with the requirements for safe work.*

This type of observation is necessary to comply with the rules and regulations for the performance of work, to prevent uncertified personnel or unauthorized persons from entering hazardous areas. The implementation of such activities became possible thanks to the use of artificial intelligence in video surveillance systems and pattern recognition algorithms. Modern algorithms in real-time allow you to instantly establish a person’s personality, gender and age, emotional state [16]. However, the use of these technologies has made the risks of serious breaches of confidentiality and misuse of PD extremely high.

*G. Augmented Reality (AR).*

AR shows help, instructions, and animations using real objects around a person performing their functions. The video camera of the device captures the image, and the technology recognizes it and displays the relevant information on the monitor [17]. Using AR, for example, can significantly improve the efficiency of maintenance and the quality of equipment repairs. The special code with which the serviced unit is marked is read by AR video cameras. All information about the equipment and its use are transferred to the service centre. Over feedback, the staff receives recommendations on further actions on the screen of the AR assistant. As a result, the time for diagnosing and eliminating the problem is reduced, and the human factor is minimized.

Thus, the examples examined show that video surveillance systems play a significant role in ensuring the security and reliable operation of enterprises and processes in OGS.

## 3. Risks and vulnerability of personal data

It should be noted that the most effective and reliable solutions for OGS can be obtained by presenting it as CPS within the framework of the current Industry 4.0 trend. CPS is a system in which the real world of physical objects through the global Internet of things is integrated into the virtual world of computing processes (embedded computers, network and cloud technologies). CPS components are potential targets for industrial espionage, DoS attacks (Denial of Service) and other hacker attacks. One possible scenario is to take control of the physical device level. For example, 2.5 million miles of oil, gas and chemical pipelines have been laid in the United States, and intrusions into control systems can do more than simply disrupt supplies [18]. Hypothetically, an attacker could force the control system to perform dangerous functions.

The increased attention to security problems in OGS is because violations or interruptions in its functioning can have significant negative consequences since it refers to critical infrastructures. In this case, critical infrastructure refers to physical and virtual objects and services that form the basis of a country's defence, a strong economy, and the health and security of its citizens [19]. Oil and gas are still the most important sources of energy, directly or indirectly; employ a large number of people. Disruptions in the supply of oil and gas negatively manifest themselves in the energy and transport sectors, creating inconvenience and difficulties for people in their daily activities, affect the supply of water and food, limit the activities of telecommunications and broadcasting, medical services, and the financial system.

It is known [20] that technological processes in the structure of OGS are carried out sequentially in three sectors, which are usually called Upstream, Midstream and Downstream (Fig. 2):

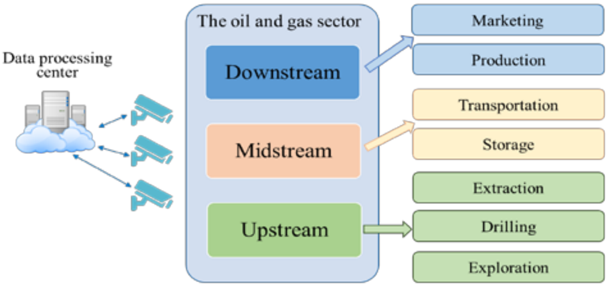

Fig. 2. The video surveillance system in OGS

These three sectors cover oil and gas production ranging from offshore exploration and drilling platforms to offshore oil wells; transportation of raw materials through pipelines to oil refineries; the processing of raw materials into the final product and its delivery to consumers. Such a multifaceted activity creates many problems of general security. As a rule, oil and gas fields cover vast territories that can be located in remote places on land or the high seas and are often exposed to adverse environmental conditions. These objects have some key nodes, which can become targets for the penetration of unauthorized persons.

Such actions may result in acts of sabotage, intentional damage to technical equipment, theft or, in the worst case, sabotage or terrorist act. Thus, the operation of most facilities and production facilities with a maximum level of security requires constant monitoring and remote monitoring, since any small disruption in the operation of each facility can lead to a malfunction of the whole system and, as a result, to economic and even human losses and environmental disasters. At the same time, security has to be ensured at technically complex and large (for example, oil refineries) and long (oil pipelines) facilities. Such a distributed architecture makes it possible to create a unified information infrastructure from complexes of various security systems that combines video surveillance, security and fire alarms, perimeter security systems, access control and management systems, audio control, etc. In this infrastructure, you can implement information processing and data mining functions that can respond flexibly to various events. However, in this case, the volumes of intranet interaction between people and production and logistics systems increase sharply. This also increases the likelihood that PD will be received, processed, and, under certain circumstances, transmitted along with other data.

The risks of data loss in the CPS can also be associated with personnel assistance systems, such as tablets, smartphones, virtual and augmented reality glasses, and portable data terminals. They provide technical assistance to staff by providing them with relevant background information, i.e. used exclusively in production processes. In this case, the data can be intercepted and analyzed to identify commercial secrets, for example, geological exploration data, prospect characteristics of explored deposits.

The result of deliberate or unintentional leaks of PD of certain criminal groups can be theft of money from bank accounts, blackmail with extortion of money, and discredit of company employees. Through PD, it is possible to cyberattacks on the physical assets of companies. For example, using sensitive PD of key employees, data on financial problems or threats of incriminating disclosures, using blackmail to force them to bypass security systems and cause problems with equipment, jeopardizing production and technological processes. In cases of such cyber-attack scenarios, possible accidents and environmental pollution can cause millions of losses and damage to the reputation of the company and their products and cause an increasing public outcry. Also, because of leaks and theft of PD, you can get confidential information of a commercial nature, about tender activity, data of contracts with partners and contractors, working conditions, etc. Possible damage from such leaks can be expressed in lost profit because of a damaged image; in compensation for legal claims; in reducing stock quotes; in the value of lost tenders and other financial losses. Based on the above assumptions, the following generalized data structure in OGS systems is proposed (Fig. 3).

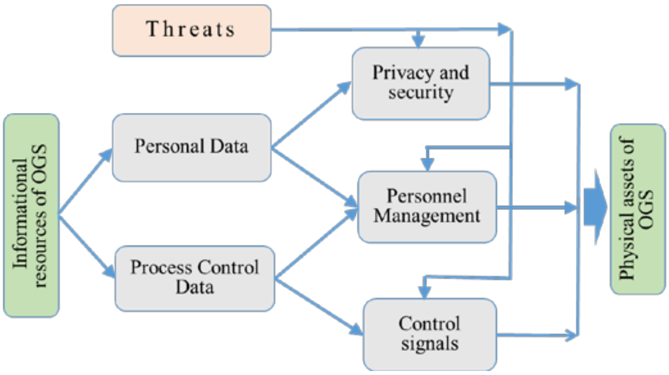

Fig. 3. The data structure in the OGS

As follows from Fig. 3, the data included in the information resources of the OGS are classified as follows: data for management and PD. Data for control after appropriate processing by the control signals or specific instructions for the personnel are transmitted to actuators (actuators) of physical assets.

For PD, there are risks of threats, for example, blackmailing a specific person, through which the impact on the object is carried out. The impact on the object can also be carried out using control data, which in the form of a set of false technical instructions are transmitted to the monitor of a particular person using his biometric parameters. And finally, a spoofing attack can be implemented.

Thus, it follows that in the security structure of OGS enterprises in the context of Industry 4.0, a significant role should be given to the protection of information resources, among which a special role is given to the protection of PD.

## 4. Conceptual issues of protection of PD at OGS

The principles of protection of PD, guaranteeing the right of citizens to privacy, have continuously evolved. A modern interpretation of these principles in the most concentrated form is presented in the EU General Data Protection Regulation (GDPR) [21]. The GDPR aims to give citizens primarily European countries control over their PD and to simplify the regulatory framework for international economic relations by unifying the regulation within the EU.

In the United States, some laws at both the state and federal levels regulate data privacy. Thus, the California Consumer Privacy Act (CCPA) is a law designed to protect the privacy of citizens of California. [22] This law requires companies to provide consumers with additional information on how their PD can be passed on to third parties. It also ensures that consumers have the opportunity to refuse to use their information in a way that they do not approve of.

The law on cybersecurity in force in China defines the rights and obligations regarding the legality and necessity of collecting and using PD [23]. Other countries also have restrictions and various penalties and fines for the improper use of PD. For example, the Labor Code of Azerbaijan provides for organizational, physical and technical (hardware) measures to protect personal information from unauthorized and accidental access, destruction, alteration and copying.

According to the GDPR, any information related to an identified or identifiable individual can be attributed to the PD. Statistical data, including data related to individuals, are not considered PD provided that they are truly anonymous, that is, individuals cannot be identified.

Any operations performed with PD or with sets of PD, regardless of whether they are performed by automatic means, such as collection, recording, organization, structuring, storage, adaptation or modification, search, consultation, use, disclosure by transfer, distribution or otherwise the provision, alignment or combination, restriction, deletion or destruction qualifies as processing PD. Thus, it is obvious that problems with PD can occur in all areas of activity and all aspects of life in general since information with which individuals can be identified can be found almost everywhere [24].

Based on the analysis, the following PD categories were identified:

*1. Private data – these include:*

- Contact information – initials, company name, position, work and mobile phones, work and personal email address and postal address.
- Professional data – information about the history of work and career, education and professional membership, published articles, as well as information on insurance and retirement benefits.
- Financial information – this subgroup of personal data includes taxes, payroll, investment interests, pensions, assets, bank details, bankruptcy records.

*2. Sensitive PD:*

- Identification documents that can reveal race, religion or ethnic origin, political views.
- Any information disclosing data on health or data relating to the personal life of an individual, information on being under investigation, a conviction for a crime.

*3. Biometric data – unique biological and physiological characteristics that allow you to identify a person.*

*4. Data that is protected by the intellectual property law (copyright, trademark law, database law, patent law) and obtained because of processing geographical locations.*

The indicated categories of PD can be used by cybercriminals for unlawful purposes, both as a result of deliberate and random actions of persons responsible for the security of information. These actions may be as follows:

- Intentional leaks: their main reason is the actions of employees who have access to secrets legally, due to their official duties.
- Theft of information (from the outside): hacking a computer using malware and stealing information for purposes of personal gain (hacker attacks).
- Theft of storage media: the intentional theft of laptops, smartphones, tablets and removable storage media in the form of flash memory, hard drives.

- Accidental leaks: occur due to the loss of storage media (flash memory, laptops, smartphones, etc.) or erroneous actions of employees of the organization. This type of loss occurs because of the erroneous placement of confidential information on the Internet.
- Social engineering: based on social and psychological techniques that allow so-called social hackers to access private data. They use people's trust to find out account numbers, credit cards, passwords and other personal information without causing any suspicion.
- Localization and tracking: accurate data on the location of personnel can be obtained through geolocation or mobile devices connected to the Internet.

The serious risks of PD leaks can be judged by one example when a violation of the security of Montana state medical records data jeopardized the social security of approximately 1.3 million people [25].

It should be noted that in the PD category, like biometric data, video surveillance has created many problems. Among them, one can single out the interests of the individual in such a sensitive sphere as restrictions on movement, the right to privacy, issues of identification of the individual and, in general, PD. Besides, in July 2019, the European Data Protection Board (EDPB) adopted the draft Guidelines on processing personal data through video devices GPPDVD [26]. It states that the video recording of an individual cannot be regarded as biometric data per se unless it has been specially and technically processed to facilitate personal identification (i.e. for facial recognition). Processing biometric data is a problem if individuals do not agree to receive their biometric data and are presented in the footage. AI technologies and face recognition algorithms allow you to identify a specific person from the facial database. Along with face recognition algorithms directly by images or voice features, personal identification is possible by its other biometric features, for example, the nature of the behaviour, body shape, clothes, things that are with you, etc. The fact of the employee’s video recording at the workplace is already processing of PD. However, a priori such employee PD are confidential information, since this is information about an individual, and their processing without the consent of the relevant person is not allowed, except in cases clearly defined by law.

From a practical point of view, it is obvious that to avoid unnecessary misunderstandings between the employer who owns the PD, that is, the person who determines the content, purpose and procedure for processing the PD, and the employee who is the subject of the PD, that is, the individual whose PD is processed, the preference will be give consent in writing. One way to get consent is to inform people about video surveillance using signage, that is, display clear and visible characters in the area where video surveillance is carried out (then we can talk about tacit consent). By appointment, the video surveillance system should control the behaviour of people. However, it should also strive to maintain the anonymity of people by hiding their identity, using certain privacy protection mechanisms. To hide the identity of the observed people, the following methods are used [27]. The first method is to completely remove sensitive areas. In this case, along with the identification of the person, it is impossible to determine the nature of his behaviour. Another method is to reduce the level of detail of privacy-sensitive areas by blurring or pixelation while avoiding personal identification. However, the command remains recognizable.

A third method, called abstraction, is to remove sensitive areas and replace them with dummy objects, such as silhouettes or skeletons.

Similar PD threats arise when using drones to monitor the infrastructure of OGS, topographic surveys and environmental inspection of the area. In this case, the ongoing operations pose the risks of unintentional processing of PD. Therefore, for example, the capture of images of people in the background may occur. Here, the background refers to nearby places of residence, recreation areas, vehicles, etc.

Another danger of information leakage can occur since drones collect information in one of two ways: records are stored onboard (for example, on a memory card or hard disk) or transferred back to the central device, where they are then stored. Both methods have vulnerabilities. If a drone with an onboard data warehouse is lost or captured by an unauthorized third party, the same will be with the information that it carries. If the drone transmits information via a wireless connection, this connection can be intercepted and used to access or change information during transmission. Adequate security measures, such as password protection and encryption, should be used to address these vulnerabilities. Security of video surveillance systems, threats, vulnerabilities, attacks and measures to reduce them are considered in many works, references to which are given in [28].

Thus, it can be noted that video surveillance systems pose a threat to PD. At the same time, despite modern security systems such as digital signatures, cryptography, biometric security, firewalls, intrusion prevention systems and access control systems, security breaches also occur due to non-technical vulnerabilities related to the human factor. It is believed that a similar vulnerability was used in case of infection with the Stuxnet worm [29]. Stuxnet was launched on a system that had no access to an external network. However, the infection occurred through the USB drive of one of the employees. Given the foregoing in Fig. 4 presents an abstract model of video surveillance in OGS, functioning as CPS in Industry 4.0.

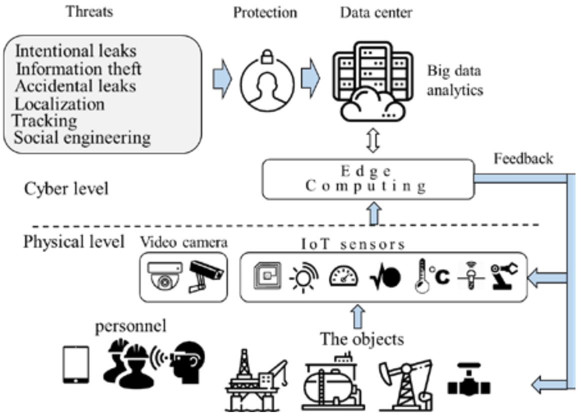

Fig. 4. Video surveillance model.

As it follows from Fig. 4, at the physical level OGS objects are equipped with sensors, with the help of which physical quantities, such as acceleration, displacement, temperature, pressure, etc., are converted, as a rule, into an electrical signal. Information represented by an electric signal can be easily converted to digital binary code, automatically recorded and transmitted at a distance, processed by mathematical methods and algorithms, and stored for a long time in computer systems (personal computers, data processing centers).

The video surveillance subsystem includes video cameras, information and communication channels for data transmission, processing devices, analytics and PD storage. PD storage is responsible for the secure storage of data and restricts access to stored data. This model is a subsystem of smart video surveillance in the concept of OGS as a smart production system, consisting of such subsystems as a smart field, smart grid, smart maintenance, smart transportation, smart security, etc.

The technological infrastructure of smart manufacturing is a CFS platform that can solve the following problems both globally and locally [30]:

- Materials and equipment management.
- Monitoring equipment.
- Maintenance.
- Security.

- CCTV.
- Hazard detection and warning.
- User identification.
- Uninterruptible power supply.
- Tracking and identification of hazardous materials.
- Environmental monitoring.
- Creating a comfortable working environment.
- Waste management, etc.

Summarizing the above, we can draw the following results:

1. A significant increase in data volumes in Industry 4.0 brought to the forefront data protection issues, including in such a sensitive area as PD.
2. Video surveillance data is an important component of PD.
3. PD can be used exclusively for optimized planning and management, labour protection and health of staff.
4. The security policy for the protection of PD should be developed taking into account the requirements of international norms and standards and comply with domestic legal acts, regulatory documents and laws.
5. Existing legislation may not reflect all aspects in the field of protection of PD.
6. The dynamic nature of the development of modern ICT and their increased influence in all areas of activity may require the correction of both existing laws and methods of protecting PD.

## 5. Conclusion

In the framework of this work, we studied the conceptual issues and problems associated with the protection of PD, and their impact on production processes in OGS. An analysis in this area showed that the problem under study is critical and responsible. The advanced technologies increased the risks for privacy and data protection, but they also can propose technological solutions for better transparency and control for those whose data is processed. Video surveillance systems integrated with other security systems and developed using high quality and reliable tools can reduce risks in potentially critical areas, including OGS. However, video surveillance systems create contradictions between the main personnel control activities and processes and the scope of PD protection. Protection of PD in structures implemented based on the Industry 4.0 concept plays an important role in the production sphere and ensuring the security of physical assets. Each case of network interaction between people and production and logistics systems can lead to the fact that PD data will be received, processed, and, under certain circumstances, transmitted along with other data. At the same time, the risks of accidental or deliberate leaks of PD and their use for personal gain sharply increase. The paper presents the data structure in the OGS, the classification of PD and the types of threats that lead to their loss, and analyzes the stages of development of video surveillance systems. The proposed model of a video surveillance system in OGS is considered as a subsystem of smart production. Despite the significant progress achieved in the field of PD protection, the actual directions of future research are the improvement of existing and the development of new solutions.

## Acknowledgements

This work was supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) – Contract No.: 03LR – AMEA.

## References

[1] Kagermann H., et al. Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry; Final report of the Industrie 4.0 Working Group, p. 79, 2013. Available at: https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry4-0-data.pdf

[2] Fataliyev T. Kh., Mehdiyev Sh. A., Analysis and new approaches to the solution of problems of operation of oil and gas complex as a cyber-physical system, International Journal of Information Technology and Computer Science (IJITCS), vol. 10, no. 11, pp. 67-76, 2018.

[3] Martinotti S., Nolten J., and Steinsbo J. A., Digitizing oil and gas production, 08/2014. Available at: https://www.mckinsey.com/industries/oil-and-gas/our-insights/digitizing-oil-and-gas-production

[4] Lua H., Guo L., Azimi M., Huang K., Oil and Gas 4.0 era: A systematic review and outlook, Computers in Industry, vol. 111, pp. 68-90, 2019.

[5] White paper: Enterprise maintenance with augmented reality. Available at: https://www.re-flekt.com/white-paper-maintenance

[6] Compliance in the Era of Globetrotting Data. Available at: https://www.intel.com/content/www/us/en/business/enterprise-computers/gdpr-compliance.html

[7] Universal Declaration of Human Rights 217(3) International bill of human rights. 10 December 1948.

[8] Weimer P. K., A historical review of the development of television pickup devices (1930-1976), IEEE Transactions on electron devices, vol. Ed-23, no. 7, pp. 739-752, July 1976.

[9] Shiraishi Y., History of Home Videotape Recorder Development, SMPTE Journal, vol. 94, no. 12, pp. 1257-1263, dec. 1985.

[10] IP CCTV solutions. Available at https://www.rolloos.com/media/2224/201702-rolloos-campro-ip-cctv-solutions.pdf

[11] Sharma G., How Industry 4.0 is Reshaping Oil and Gas Recruitment. Available at: https://www.rigzone.com/news/how_industry_40_is_reshaping_oil_and_gas_recruitment-19-feb-2019-158187-article/

[12] Thermal Imaging Provides Early Leak Detection in Oil and Gas Pipelines. Available at: https://www.petro-online.com/article/security/15/flir-systems/thermal-imaging-provides-early-leak-detection-in-oil-and-gas-pipelines/2427

[13] Gómez C., Green D.R., Small unmanned airborne systems to support oil and gas pipeline monitoring and mapping, Arab J-l Geosci, vol. 10, no. 9, pp. 202-219, 2017.

[14] Applications. Available at: https://www.tattile.com/applications/

[15] Alguliev R. M., Fataliev T. Kh., Agaev B. S., Aliev T. S., Sensor Networks: the State, Decisions and Prospects, Telecommunications and Radio Engineering, vol. 68, is. 15, pp. 1317-1327, 2009.

[16] Li H., The research of intelligent image recognition technology based on the neural network, International Conference on Intelligent Systems Research and Mechatronics Engineering. Atlantis Press, 2015.

[17] Tsakanikas V., Dagiuklas T., Video surveillance systems– current status and future trends, Computers and Electrical Engineering, vol. 70, pp. 736-753, August 2018.

[18] Krauss C., Cyberattack shows the vulnerability of gas pipeline network, 2018. Available at: https://www.nytimes.com/2018/04/04/business/energy-environment/pipeline-cyberattack.html

[19] Simon T., Critical Infrastructure and the Internet of Things, Global commission on internet governance, no. 46, p. 20., January 2017.

[20] Alguliyev R. M., Fataliyev T. Kh., Mehdiyev Sh. A., The industrial internet of things: the evolution of automation in the oil and gas complex, SOCAR Proceedings, no. 2, pp. 66-71, 2019.

[21] General Data Protection Regulation (GDPR). Official Journal of the European Union, 2016, pp. 1-88.

[22] Rothstein M. A., Tovino S. A., California Takes the Lead on Data Privacy Law, Hastings Center Report, Vol. 49, No. 5, pp. 4–5. doi:10.1002/hast.1042.

[23] Yang F., Xu J., Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law Asia Pac Policy Stud. vol. 5, no. 3, pp. 533-543, 2018. doi10.1002/app5.246.

[24] Henschke A., Ethics in an Age of Surveillance. Personal information and virtual identities, Cambridge University Press, Cambridge, p. 334, 2017.

[25] Zuckerman L., Montana health record hackers compromise 1.3 million people. 2014. Available at: https://www.reuters.com/article/us-usa-hacker-montana-idUSKBN0F006I20140625

[26] Dentons Boekel. GDPR Update — EDPB video surveillance guidelines. Available at: https://dentons.boekel.com/en/insights/alerts/2019/september/3/gdpr-update-edpb-video-surveillance-guidelines

[27] Rajpoot Q. M., Jensen C. D., Video Surveillance: Privacy Issues and Legal Compliance, Promoting Social Change and Democracy through Information Technology. IGI Global, pp.69-93, 2015.

[28] Costin A., Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations, TrustED '16: Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, Austria, pp. 45-54, October 2016.

[29] Kushner D., The Real Story of Stuxnet, IEEE Spectrum, February 2013.

[30] Fataliyev T. Kh., Mehdiyev Sh. A., Integration of cyber-physical systems in e-science environment: state-of-the-art, problems and effective solutions, International Journal of Modern Education and Computer Science (IJMECS), Vol.11, No. 9, pp. 35-43, 2019.

## Authors' Profiles

**Tahmasib Khanahmad Fataliyev** graduated from the Automation and Computer Engineering faculty of Azerbaijan Polytechnic University. His primary research interests include various areas in e-science, data processing and computer networks. He is head of the department at the Institute of Information Technology of ANAS, Azerbaijan. He is the author of above 100 scientific papers.

**Shakir Agajan Mehdiyev** graduated from the Automation and Computer Engineering faculty of Azerbaijan Polytechnic University. His primary research interests include various areas in e-science, computer networks and maintenance. He is head of the department at the Institute of Information Technology of ANAS, Azerbaijan. He is the author of about 25 scientific papers.

**How to cite this paper:** Tahmasib Fataliyev, Shakir Mehdiyev. "Industry 4.0: The Oil and Gas Sector Security and Personal Data Protection", International Journal of Engineering and Manufacturing(IJEM), Vol.10, No.2, pp.1-14, 2020. DOI: 10.5815/ijem.2020.02.01