3D sensors in critical infrastructure

Marcanik Miroslav[1], *Sustek* Michal[1], and *Jasek* Roman[1]

[1]Tomas Bata University in Zlin, Faculty of Applied Informatics, Nad Stranemi 4511, 760 05, Zlin, Czech Republic

Abstract. The danger of terrorism is a result of the increased risk of critical infrastructure. We will focus on enumerating each area then listing of possible real uses in security and protection and finally we will focus in the list of used 3D sensors (in practice focused mainly on the use of laser scanning of space, camera sensing and subsequent transfer to cyberspace or scanning with infrared sensors).

1. INTRODUCTION

Nowadays, advances in technology makes life simplier. We rely on technology and manual work is replaced by machines. Every technological innovation hides the potential for hidden threats for its users. One of the main threats is the theft of private personal data and informations. Digital data getting more and more popular and users are trying to secure their information with highly encrypted passwords and passwords. Misuse and theft of security measures are on the rise. The disadvantage of security errors in passwords results in duplication or counterfeiting of cards and their misuse. [1]

The article is divided into sections. In section 2, authors define globally the critical infrastructure and the subsequent use of 3D sensors in section 3.

The fourth section focuses on the issue of sensors and their principles.

In the fifth and final sections, the authors tried to outline the camera systems and the principles of camera motion detection.

2. CRITICAL INFRASTRUCTURE

On the basis of the terminology dictionary of the Ministry of the Interior, we can define critical infrastructure as "production and non-production systems and services, the malfunctioning of which would have a serious impact on state security, economy, public administration and security of the basic living needs of the population". In the case of public infrastructure, the definition of the National Research Council (in the United States of America), which says that "public infrastructure covers both specific functions - motorways, streets, roads and bridges; public transport, airports and airline networks; water and water resources; wastewater treatment plants; processing of municipal waste; production and transmission of electricity; telecommunication and hazardous waste processing - and where multifunctional multifunctional systems ". [2]

It is accepted in the Czech Republic (decision of VCNP 24 September 2002) to focus the national critical infrastructure on the following nine areas:

- energy supply system, especially electricity;
- water supply system;
- waste management system;
- transport network;
- communication and information systems;
- banking and financial sectors;
- emergency services (police, fire brigade, health);
- public services (food supply, social services, funeral services);
- government and local government.

If we look at the critical infrastructure as a complex system, we can say that a critical infrastructure is connected to a network of elements that are interconnected by the connectors and because of a linked network that where the individual connectors and forced to create a node. If any node is infected, it may result in more or less downtime and thus endanger the functionality of other nodes. For this reason, critical infrastructure nodes should be protected.

Protection of individual nodes or units results in increased resilience against the impact of extraordinary situations. Critical infrastructure is interacting outside the state sector, but also to the private sector. That is why we can not expect the state to protect it continuously. This implies that the state can not invest state money in the protection of critical infrastructure that is in private hands, but can not even force a private entity to invest its money in the protection of critical infrastructure, for example in the form of preventive measures. Nevertheless, the state has to deal with issues of critical infrastructure protection, which is not only owned by the state but also owned by private entities because it needs it to provide the basic life needs of the state and the population. The importance of critical infrastructure in terms of population protection is illustrated in the Figure 1.

* Corresponding author: marcanik@utb.cz

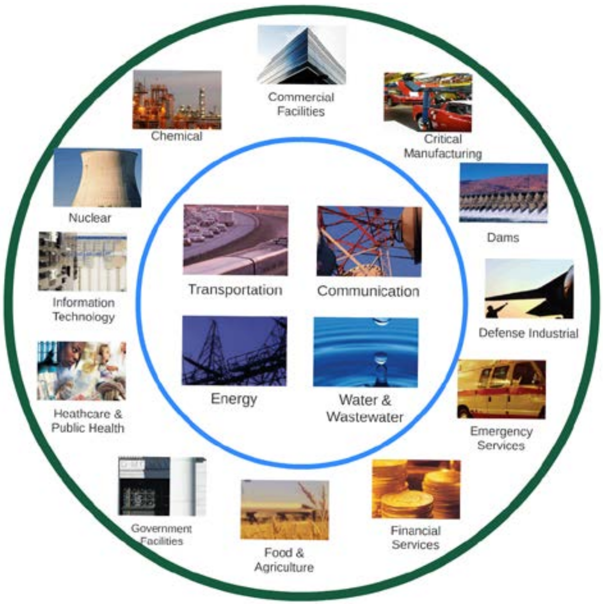

Fig. 1. Critical Infrastructure from a Population Protection Point of View [3]

2.1. Areas of National Critical Infrastructure approved in 2007[2]

Energy

- Gas
- Electricity
- Petroleum and petroleum products

Water management

- water supply
- security and management of surface water from underground water sources
- sewage system

Food and Agriculture

- food production
- grooming
- agricultural production

Health care

- pre-hospital emergency care
- hospital care
- protection of public health
- manufacture, storage and distribution of pharmaceuticals and medical devices

Transport

- road
- railway
- airline
- inland waterway

Communication and telecommunication networks

- Fixed telecommunication network services
- mobile telecommunication networks
- radio communication and navigation
- satellite communications
- TV and radio broadcasting
- postal and courier services
- Internet access and data services

Banking and financial system

- public finance management
- banking
- insurance
- capital market

Emergency services

- The fire brigade
- Police of the Czech Republic
- Army of the Czech Republic
- Predictive alert and reporting service

Public administration

- State administration and local government
- Social protection
- The exercise of justice and the prison system.

3. PRACTICAL USE OF 3D SENSORS IN CRITICAL INFRASTRUCTURE

With the gradual development of miniaturization and increased general threats, 3D security sensors.

Biometric authentication **PalmSecure**:

- Verification of physical access / attendance for objects with high security requirements (data centers, research laboratories, critical infrastructure objects, airports, ...)
- Verify users to PC, applications, or server systems
- OEM terminals (POS, ATMs or information kiosks)
- Government / commercial systems for identifying people
- Other industry-specific applications
- By reducing the size of the sensor, reducing its cost, and simplifying development using the SDK, this technology can now be used in a variety of applications.

Modular system for positioning and orientation in space.

Utilization of a two-station long range system for perimeter protection

- Passive sensor system using camera units
- The system will allow accurate measurement of the coordinates of its target velocity vector and target path extrapolation, including data transfer to users
- Focused on the measurement of ground and air targets.

Laser scanning in hydrotechnical assessment of watercourses.

Control and manipulation of the remote robot in infected or life-threatening areas.

4. SENSORS

First of all, what are the sensors or sensors? Sensors are elements that create an input block of the measuring chain that is subsequently in direct contact with the measured environment. Other sensor concepts include sensor, detector, transducer, scanner. [4]

Depending on usability, individual sensors can be divided into individual categories:

- For measuring quantities
- For Physical Principles
- For the measured environment
- For signals according to their transformation
- For manufacturing technologies

Changes in the measured quantity are read across the sensitive element often referred to as a sensor and subsequent evaluation directly in the sensor circuits (A / D converter), where the measured value is usually converted to an electrical signal that can be further processed or is equal to the output variable.
The principle of the sensor is illustrated graphically in Figure 2.

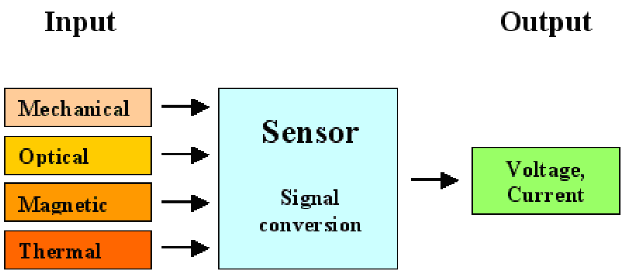

Figure 2. Principle shooting [5]

The Beckenbridge and Husson Intelligent Sensor defined the Beckenbridge and Husson Intelligent Sensor in 1978 as: The Intelligent Sensor includes functions for measuring measured data, automatic correction of measured data, it can automatically detect and eliminate abnormal and incorrect values. It also contains a set of algorithms that allow you to respond to changing external conditions. The block diagram can be seen in Figure 3.

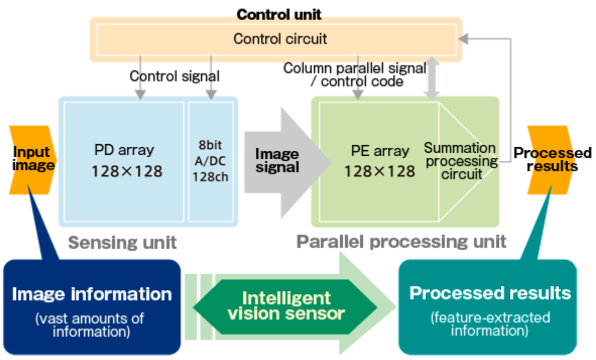

Figure 3. The principle of intelligent sensors [5]

Therefore, 3D sensors can be defined as a measuring unit that scans an object in 3D space or occupies angles X, Y and Z. 3D sensors work on the principle of two or more camcorders, or the majority of the laser scanner can be used to capture the third dimension. This makes it possible to transform the whole or just its particular parts into 3D and then analyze the 3D scene and then select the best method of processing. [4]

From the above description, 3D sensors can be divided into two basic categories according to the use of individual sensors. Active and passive scanning.

- Active scanning uses the use of a laser / camera, additional information or other auxiliary equipment. The concept of active scanning is very closely related to the concept of "deep map creation".
- Passive capture uses only one camera / laser sensor than active scanning.

Since these are improved sensors, the categorization of 3D sensors may be similar. Figure 4 shows a general division. [4]

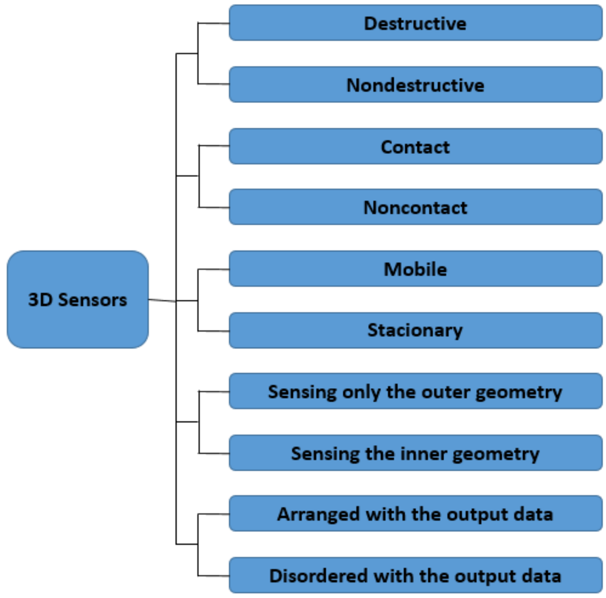

Figure 4. Distribution of 3D sensors [4]

5. CAMERA SYSTEMS

At the time of the Internet and the vastness of technology, motion tracking systems are a big topic with many pros and cons. Almost every street you will notice the installed camera system. Nowadays, this protection of privacy or property is affordable for almost everyone.

5.1. Types of surveillance cameras

We can divide them into three basic groups.

- **Analog cameras**
- **HD-SDI**
- **IP cameras**

5.2. Detectors and techniques for detonation

We divide the motion detectors into four areas according to the functional requirements they perform when protecting the object. These areas are:

- Perimeter protection
- Cloak protection
- Spatial protection
- Subject protection

Motion detectors fall into the area of perimeter and space protection.
For the purpose of protecting property or monitoring people's movement, a lot of mechanisms have been created to achieve this. These include static cameras that are installed in homes. One-sided Motion Detection can be achieved by using photo-frames that capture an ambient image in the event of movement. This method is used, for example, to prove the existence of some rare

animal species. Further, there are thermocouples whose output is an infrared sensor, capturing the heat of the image.[5]

- Motion Detector Pro - This mobile app is created for Android. In the case of motion detection, using the built-in camera on your mobile, the user is sent a picture with the move to an email address or a text message to another phone number
- AXIS Video Motion Detection - Axis Communication (Axis) is one of the largest cameras security companies. It offers a large number of cameras that are specific to a particular activity.
- Synology Společnost - Synology provides operator and management of CCTV systems.
- Background reading - This technique is used for motion detection to distinguish the foreground of a frame that contains motion and a background that is invariant.
- Two-frame difference method - The method detects motion by comparing the image that is taken as the background and the image that varies over time. This principle only works when all pixels in the foreground move and all background pixels are static.

$$|I(x,y,t) - B(x,y,t-1)| > Th \quad (1)$$

- Mean filter - In this case, N pictures stored in the buffer are selected from which the background is assembled using an average value. The pixel values from the same frame (x, y) are selected from each frame in the buffer, and the mean value representing the pixel of the background is the same (x, y).

$$B(x,y,t) = \frac{1}{N}\sum_{i=0}^{N-1} I(x,y,t-i) \quad (2)$$

$$\left| I(x,y,t) - \frac{1}{N}\sum_{i=0}^{N-1} I(x,y,t-i) \right| > Th \quad (3)$$

- Median filter - The principle of this procedure, described in equations (4) and (5), is to use the median values of the last N frames for the background model. In a later improvement of the method, according to Piccardi [9] it is proposed to calculate the median from a set of values consisting of the last of the images and the last calculated median.

$$B(x,y,t) = median\{I(x,y,t-i)\} \quad (4)$$

$$|I(x,y,t) - median\{I(x,y,t-i)\}| > Th \quad (5)$$

- Moving Gaussian Diameter - The Gaussian moving average belongs among recursive techniques, so unlike previous background calculations, the buffer does not use, but recursively updates the background model. It is based on the correct location of one Gaussian probability density function on each pixel of the last N frames. Gpdf is characterized for each pixel scattering σ2 and mean value μ which are updated over time by means of a rolling average:

$$\mu_{t+1} = \alpha I_t + (1-\alpha)\mu_1 \quad (6)$$

- Gaussian Curves - The principle of this procedure is to determine whether an image pixel is part of a foreground or background using a mixture of N Gaussian curves that model each pixel. Most often, the value between 3 and 5 is chosen. At any time t, the specific pixel $(x0, y0)$ has its own history.

$$\{X_1, \ldots, X_t\} = \{I(x_0, y_0, i) : 1 \leq i \leq t\} \quad (7)$$

- Threshold - This is one of the image segmentation methods. The result of the threshold is a binary image that contains only 0 or 1 pixels. Depending on which value the pixel will take, the threshold is determined by T.

$$f(x) = \begin{cases} 1 \; pro \; x \geq T \\ 0 \; pro \; x < T \end{cases} \quad (8)$$

- Canny Edge Detector - One of the main ways to distinguish the size of an object in an image is through edge detection. John Canny described the most used procedure in this category in 1986.
- Morphological operators - Algorithms that detect movement often show noise or slight movement that may not always be desirable. For image smoothing, I've decided to use morphological operations to remove noise and highlight areas of interest. The basic elements of this algorithm are binary image and structural element. The procedure consists in applying the element to each pixel of the image, creating a new image. The element can have different size and shape, such as a square, circle, ellipse, etc. Another element that affects the result is the number of iterations of the operation. With greater number of operations, better results are achieved, but overall application runs slow down. If the image is opened or opened. closure, other opening applications, closing the picture will no longer affect. A more detailed description of these operations is described in Haralick, Sternberg, Zhuang.

CONCLUSION

Iit is good to think about Maslow's pyramid of needs, where security is second only, and when choosing specific security elements / systems, we choose especially those that are proven by the market or specialized people.

The aim was to outline the possible threats and the effort to bring the individual types of sensors closer together with a simple description and specific features. The attempt was not to specify individual types of sensors but rather to focus on the global perspective.

As existing and constantly evolving other intelligent electronic devices that require contactless measurement of position, speed and motion detection or acceleration, the range of integrated accelerometers and gyroscopes is growing. These sensors are crucial for robots, navigation, gaming consoles, cameras and cameras, some mobile phones, and mainly aircraft, cars and boats. We can also find them in better washing machines, dryers and other white machines and devices where something is rotating, moving or vibrating.

ACKNOWLEDGMENT

With support by grant No. IGA/FAI/2018/09 from IGA (Internal Grant Agency) of Thomas Bata University in Zlín.

REFERENCES

1. Raj Jain. *A Survey of Biometrics Security Systems*. In: WUSTL (2011)
2. M. Senovsky, V. Adamec, P. Senovsky, *Critical infrastructure protection*, ostrava, **141** (2007)
3. Emergency management division, *Infrastructure Resilience Sub-Committee (IRSC),* (2017)
4. Sensors & Transducers, **206** (2016)
5. MEMS *Sensors and Actuators*: Sensors General, (2006)
6. P. Skoupy, *3D optical measuring and scanning systems for engineering*. Brno: (2007)
7. H. Foell, *MEMS Sensors and Actuators*, (2011)
8. Fujitsu: *PalmSecure,* (2008)
9. M. Vrbova at al. *Lasers and modern optics*,**474** (1994)
10. Emerging Nanotechnology Power: Nanotechnology R & D And Business Trends In The Asia Pacific Rim. World Scientific, (2009)
11. Mechatronics | *Introduction: Sensors* (2005)
12. M. Jankova, J. Dvorak, . *The ICT possibilities in the virtual universities cyberspace*. (post-conference proceedings of selected papers extended versions). Brno: MITAV, **59-65** (2014)
13. K. Schroeder, B. Lorensen, *Visualization Toolkit: An Object-Oriented Approach to 3D Graphics*, 4th Edition. Kitware, (2006)
14. Cordeiro, Frederick Joaquim Barbosa. *Gyroscope*. Place of publication not identified: Nabu Press, (2010)