Chapter 9

Security Systems in the Healthcare Sector

By Mathias Normann, George Suciu, Vasiliki Mantzana, Ilias Gkotsis, Mari-Anais Sachian, Gabriel Petrescu, Hussain Ijaz and Barry Norton

DOI: 10.1561/9781680836875.ch9

Published in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures* by John Soldatos, James Philpot and Gabriele Giunta (eds.). 2020. ISBN 978-1-68083-686-8. E-ISBN 978-1-68083-687-5.

Suggested citation: Mathias Normann *et al.* 2020. "Security Systems in the Healthcare Sector" in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Edited by John Soldatos, James Philpot and Gabriele Giunta. pp. 166–178. Now Publishers. DOI: 10.1561/9781680836875.ch9.

now
the essence of knowledge

To efficiently protect the healthcare sector is a major task. Healthcare is a highly specialized sector where the physical facilities are a mix of publicly-available, semi-private, private, and areas housing critical infrastructure. The healthcare sector spans many types of buildings, some open to the public with zones restricted only to staff and some completely restricted to the public. Some of the buildings will have patients all the time, some only during daytime, some will have important and expensive medical devices, and some will contain servers. The buildings can have physical medical records, computers used by the staff can have access to personal data, and the servers that store huge amounts of personal data, critical information, and critical software for the healthcare sector. Besides the normal software used for an office building, the healthcare sector's internal software is used to handle the medical data of patients and to run and control medical equipment and machines.

To protect all this, the healthcare sector keeps expanding the security systems within their facilities, so it is common to have several security systems to handle different security areas, as no system covers everything. This chapter will present

an overview of how a video management system, an access control system, a fire detection system, SCADA, ICS, and smart building sensors, as well as a Cybersecurity protection system works to make the healthcare sector a more secure environment.

9.1 Video Management Systems

With regard to physical security, camera surveillance is the most common way of getting an overview of what is happening. In years past, when analogue cameras were the only type available, large hardware set-ups were needed to record the video feeds from the cameras and store them on physical tapes. With such set-ups, one could not combine cameras from different manufacturers, as they only worked with their own management systems. In the 1990s the Internet Protocol camera (IP) was invented. IP-cameras can be connected to the internal network using ethernet cables, instead of being directly hooked up to specific hardware, as analog cameras must. It is easy to view video feeds, given further standardization in this sector, from an IP that is connected to the internal network, and this does not require a large hardware set-up. These days the video can even be viewed using a Web browser, or some of the commonly available media players, by accessing the IP using these networking protocols, which have now spread from the Internet to almost every corporate, and indeed home, computer network. The switch to IP-enabled digital cameras came to revolutionize the world of Video Management Systems (VMSs), as it is now a lot easier and cheaper to install new cameras, and VMSs can manage video from cameras across many manufacturers.

In the healthcare sector large installations of IPs are common, given the profusion of assets to protect—both people, medical devices and data—so to sufficiently protect everything, installations may require hundreds or thousands of cameras. For a human to keep track of all these cameras manually, using a browser or video players is completely impossible, and this is where a VMS comes into the picture, to help manage all cameras, to record and store their feeds when relevant, and to help retrieve or show live the most relevant segments of video streams to the operator.

In general, a modern VMS is constructed to have a central Video Management Server with the responsibility of handling all cameras, the data they create, enabling reactions to the data and enabling the user to interact with it. The general architecture of a VMS can be viewed in Figure 9.1, and the parts of the VMS is described in detail below:

- **Storing** the configurations and information of all registered cameras in the Device Management Database;

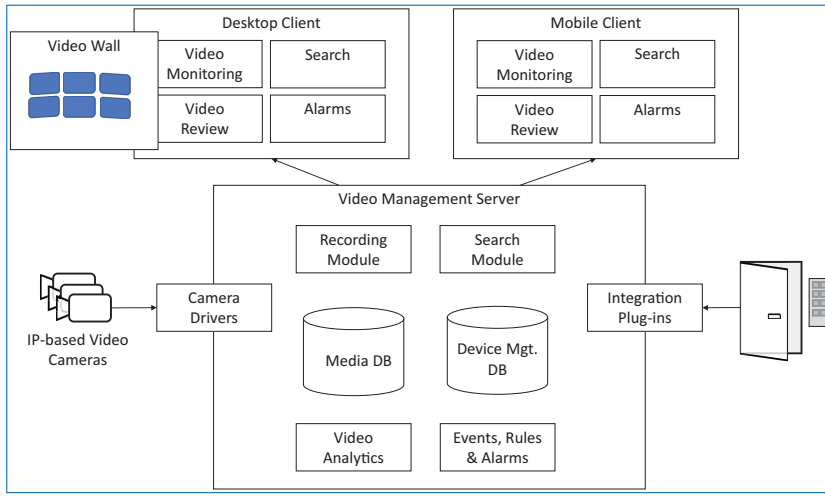

Figure 9.1. VMS architecture.

- **Recording** and **storing** the video streams from all cameras registered with the VMS into the Media Database;
- Enable **searching** for cameras and relevant video streams stored in the Media Database;
- Enable **Video Analytics** to be run on video streams, such as motion detection which can be used to only store video frames in the Media Database when there is motion in the view or to prioritize which video stream the human should watch;
- Handling of **events** happening within the system, upon which **rules** can be defined to react to conditions that can happen within the system and through which **alarms** can be raised by the system for the human operator to consider.

As mentioned above, cameras are manufactured by different companies, and even though the mission of the ONVIF standard (ONVIF, 2020) is to "provide and promote standardized interfaces for effective interoperability of IP-based physical security products," camera manufacturers are not obliged to use this standard, and even if they do, cameras can allow the configuration of features that the standard does not cover. Therefore, for a camera to work with a given VMS, in general a driver has to be developed for the camera, or for that series of cameras. Most VMSs today have drivers for at least the most common cameras in use.

In order for the operator to be able to view the live and recorded video streams, to review the alarms and to search, VMSs often provide both a desktop client and a mobile client. The desktop client can either be native to its host operating system or developed using Web interfaces to be used in the browser. Desktop clients can

also enable display in a video wall, wherein the application displays across several windows, with one or more video streams in each window, where each window is mapped to an entire monitor within a bank of such.

Alongside VMSs, there are a number of other software-based systems used in physical security, such as access control of doors within the buildings covered. In recent years, there has been a demand from users to integrate these systems together with the VMS. This integration enables a better understanding of what happens at the installation site and better alarm handling.

9.2 Integrations with Video-based Security Systems

Many security systems in an installation are managed by a single central system, which is used to set up the devices and configure the system to run without further human interaction. Take, for example, an access control system: after the system has been set up to allow the right people through the right doors, the system will run without human interaction to the management system, unless something goes wrong or some access rights have to be changed. This section describes the integration of some of such building security systems and sensors that can help improve the security in the healthcare sector.

9.2.1 Access Control Systems

An access control system restricts access to areas within a building, by having one or more door controllers connected to locking mechanisms on important doors, together with card/PIN readers and request-to-exit (REX) systems, as illustrated in Figure 9.2 and described below.

Door controller The central system that receives input from the lock, reader, and REX, stores or forwards the events, as well as applying defined rules, and thereby communicating: to the lock whether it should open and, to the reader what state to display.

Lock Inside the door, and potentially the door frame, is a mechanism by which the door can be held in a locked state. One important characteristic of this mechanism is that the locking can be "fail safe", i.e., unlocked if the power is removed, or "fail secure", i.e., locked if the power is removed.

Reader Any system that gives permission to pass through an access control point if the correct credentials are provided, such as card readers, PIN pads, and finger print readers.

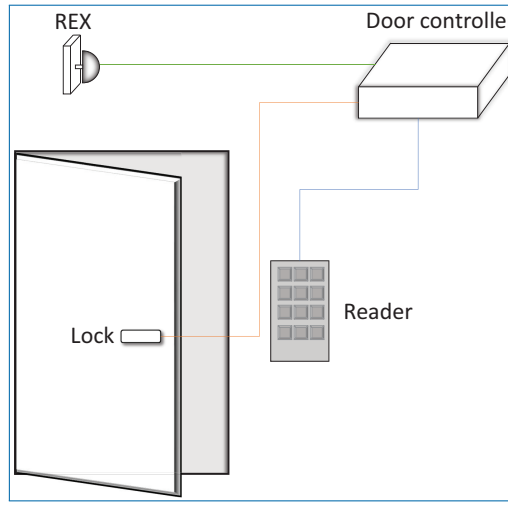

Figure 9.2. Access control system.

REX Any system that gives permission to pass through an access control point without providing credentials, such as a push button, an asymmetric door handle mechanism, or a motion sensor.

In an office building, restricting door access, and sometimes lift access, to employees and invited guests only is often a simple and easily-defined problem. This access regime can be effected by installing an access control point at every entrance of the outer perimeter of the building and only allowing the public into the reception area, until invited further in.

In the healthcare sector, however, defining those areas where the public may enter can be a much more complicated problem. There might be a lot of areas that are restricted to staff only, but that are still physically accessible to the public, as it would disrupt the hospital workflow too much to have too many access control points. To ensure adequate surveillance of such restricted areas, more intelligent solutions are required in addition to basic access control, such as integration with the video-based security systems.

When an access control point is used, if the access control system is integrated with a VMS, then the VMS can be informed of authentication and door open/close events, in order to capture the relevant video feed covering the access control point and associate this video with the access control events produced. It is a feature of such integration that the video preserved and associated with the access control event precedes the triggering event by several seconds, requiring buffering. By knowing the video feeds covering the access control point, the VMS may further apply analytics to determine and classify malicious uses. One example is to

automatically detect "tailgating," by determining if more than one person passes through the access control point, while access through the access controller only grants one authorization.

9.2.2 Fire Detection System

The fire detection system in a hospital is vital for the safety of the personnel and patients. Fire is not uncommon in a hospital environment, either malicious or accidental, and false alarms are even more common.

The main components in such a system are the sensors and the control panel which supervises the whole building. In providing physical security to the healthcare sector, there is often a larger monitoring system, which allows operators to inspect and detect various attacks which could affect equipment and put the personnel of the hospital in harm's way. In installing a fire detection system, it is necessary that each room should have specialist sensors to detect both heat and smoke. Each fire incident detected will directly be forwarded as an alert to the control panel, and so on to the people which are in charge of the monitoring, can act fast, and call the firefighters.

In case of fires, integrated physical security systems can be used to diagnose causal or contributory factors such as:

1. The bad wiring of a power socket;
2. Inflammable substances left unattended in certain operations rooms;
3. An arson started by a malicious intended person;
4. A bombing attack;
5. Mishandling of electrical equipment.

As regards the use of video in fire detection, lately various convolutional neural networks (CNN)-based methods have been applied in specific environments with reasonable accuracy and execution time. However, those approaches failed to detect fire in uncertain environments, for instance, those having excessive smoke, fog, fire, and snow. Furthermore, achieving efficiency with reduced running time and model size is quite challenging for resource-constrained devices, such as edge-based analytics, i.e., within cameras, motivating the centralized approach of VMS-based video analytics.

A CNN-based method, illustrated in Figure 9.3, can thereby be used for fire detection in videos of health facility. The approach can be extended for the extraction of detailed contextual information from fire scenes such as an object on fire, burning degree, and fire growth rate, etc. Furthermore, a hybrid system can be developed by integrating smoke detection methods with the current work for

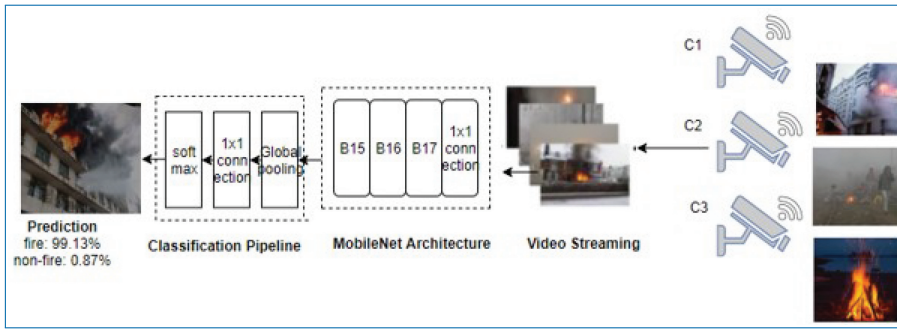

Figure 9.3. Efficient deep CNN for fire detection in video captured in uncertain environment C1, C2, and C3.

intelligent management of fire disasters. Finally, such an approach can be combined with industrial systems, 5G IoT, traffic, and robotics for more safe automation, traveling, more vibrant, and trustworthy experience (Muhammad *et al.*, 2018).

9.2.3 SCADA, ICS, and Smart Building Sensors

SCADA is a control systems architecture, based in both software and hardware, that has many benefits for the industry. SCADA's features include to process real-time data, record specification into a log document, control mechanical procedures, and connect further devices. The architecture consists of several interconnected elements, each with a different purpose and design, varying from a Remote Telemetry Unit (RTU) that interacts with the physical environment to an Human Machine Interface (HMI) that connects with the users (Rodofile *et al.*, 2017). An Industrial Control System (ICS) is one of the various kinds of control systems used to monitor industrial processes. Depending on the size, it can be made up of several controllers or a complex network of interactive control systems. These systems obtain data from remote sensors that monitor and measure process variables that will be compared with set-points. Hence, SCADA and ICS infrastructure capture data relevant to security issues which can affect the well-being of the personal and patients in a hospital environment.

A SCADA system can be used to connect to sensors and actuators which are in charge of collecting various parameters from devices on the field. The signal sent by SCADA devices is stored in an analogue format, and it is converted by a RTU, a Programmable Logic Controller (PLC), or a Intelligent Electronic Device (IED). After this process is done, the converted data is sent via a communication channel to the respective SCADA presentation and the control unit, whereas the sent data is analyzed, and each operation is sent back to each sensor (Mobolarinwa, 2017). The communication between devices and the SCADA host can be classified as dial-up,

satellite, telephone, radio, and Wireless Local Area Network (WLAN). Within a SCADA system exists four layers, such as a collection, conversion, communication, and control layer. Each of these layers can be used as an attack entry point into the system, because protocols such as WLAN do not have authenticity and encryption from the manufacturing phase. Subsequently, the data sent to end-devices can be intercepted by an attacker and also operational errors can lead to a vulnerability in a HMI, and this can be exploited by the malicious intended attacker.

A recent approach called "Tactile Internet" involves gathering multiple technologies by permitting intelligence through mobile edge computing and data transmission over a 5G network, though time will tell whether this approach gains traction in the healthcare space.

Major classes of security vulnerabilities (Mobolarinwa, 2017) in the Industrial SCADA IoT Infrastructure are:

- Human Machine Interface (HMI) vulnerabilities: Hard-coded Credentials, Poor Input Field Validation, Poor Authentication and Authorization, Zero-day Exploits
- PLC vulnerabilities
- Social Engineering
- Inadequate Physical Security
- SCADA Protocol Vulnerabilities
- Connection with the Corporate Network

9.3 Cyber-security in Healthcare Contexts

As introduced previously, the healthcare sector faces unprecedented risks and compounding regulatory compliance requirements. It is usual that healthcare organizations have many assets that are essential for their operation and should be protected. Assets that can be attacked include the facilities and buildings themselves, data, interconnected clinical information systems, mobile devices, networking equipment, identification systems, networked medical devices, and remote care systems, with the two most critical hospital's assets being the interconnected clinical information systems and networked medical devices (Independent Security Evaluators, 2016). Patient records contain valuable information, such as Personal Identifiable Information (PII) and Protected Health Information (PHI), that can be the most attractive information for attackers. Healthcare organizations and their assets suffer from vulnerabilities that can be technical (application & OS, control gaps and design flaws, unpatched devices, unprotected networks, weak credentials, lack of cyber threat prevention and

detection, lack of smart sensors, remote access policies, lack of employee training and awareness, etc.) or organizational and social (behavior of users, human errors, etc.).

These vulnerabilities can be exploited in different ways by attackers that use different types of malicious actions (e.g., virus, ransomware, hijack). The probability of these attacks can increase as healthcare organizations suffer also from system failures (e.g., software, hardware and network failure, inadequate firmware); human errors (users systems' misuse, unauthorized access, absence of audits and logs, etc.); and natural phenomena. Attackers have different goals, as they might wish to cause damage, obtain a ransom, cause the interruption of service, or collect data to prepare future attacks.

As such, health infrastructure is identified as a significant potential target of cyberattacks, which highlights the need to enhance protection from them. In order for healthcare organizations to prevent, or at least reduce, unauthorized access, use, disruption, deletion, and corruption, to respond effectively, quickly, and efficiently, and to minimize the impact of attacks to their networks and systems, it is important to take organizational and technical measures, such as those nominated below.

With regard to organizational measures that will enhance cybersecurity in healthcare organizations, it has been widely claimed that it is important for healthcare organizations to assess cyber risks. Cyber risk assessments are used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and national concerns, resulting from the operation and use of information systems (NIST, 2019b).

In addition, healthcare organizations should develop and incorporate both generic and case-specific laws, standards, plans, and policies that outline cybersecurity measures and crisis management procedures, such as the NIS directive (EU, 2016) and ISO 27001 (ISO, 2019), security procedures application in order to protect the venue and other sensitive, critical, or valuable assets and areas (e.g., computer room, central servers, clinical information systems, and electronic healthcare records) from attacks.

Since the human factor is one of the major security threats in the health domain, it is important that personnel are aware of the basic cybersecurity-related issues and their skills—both technical and behavioral—are improved (ECSO, 2018). Moreover, healthcare staff (including researchers, administrators, front desk workers, medics, transcriptionists, handlers of medical claims to IT, and technical staffs) should be properly trained on cybersecurity protection and crisis management issues, standards, plans, and protocols (Martin *et al.*, 2017). In doing this, stakeholders that find themselves affected by, or actively seek involvement in crisis management processes, can manage and cooperate effectively and in timely fashion on security planning, preparedness, response, recovery, and impact

mitigation. With regard to technical measures, it has been reported that healthcare organizations should adopt and implement different practices that will enhance data, systems, devices, and networks security, such as the following, according to ISO (2018) and NIST (2019a):

Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, sensors, service or application) and provides assurance that an entity is not attempting an unauthorized replay of a previous communication.

Access control (authorization)—much like physical access control, described above—guarantees that only individuals, as well as software and IT infrastructure, can only gain access to, and perform operations on, stored information and flows that they are authorized for. Unlike physical access control, different access levels can be granted to systems, devices, and networks.

Availability describes a security dimension that ensures there is no denial of authorized access to network elements, stored information, information flows, services, and applications due to events impacting the network.

Reliability has been defined as the ability of the system to perform its functions for a period of time. This is a high-level security requirement and to be achieved different mechanisms should be implemented (e.g., availability, communication security), as described in the respective sections above.

Non-reputation refers to the ability to prevent an individual or entity from denying having performed a particular action related to data, by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin; proof of ownership; proof of resource use).

Data confidentiality ensures that the data content cannot be understood by unauthorized entities.

Data integrity is a security dimension that ensures the correctness or accuracy of data. Data should be protected against unauthorized modification, deletion, creation, and replication and provide an indication of these unauthorized activities.

Backup is the process of backing up the operational state, architecture and stored data of database software.

Tracing systems should log access and errors to the collected and stored data (e.g. time, date, users' accessing the system, fails, wrong password).

Log files are automatically produced files, recording events, messages from certain software and operating systems.

Communication security is the security dimension that ensures that information flows only between the authorized end points; i.e., the information is not diverted or intercepted as it flows between these end points. To obtain communication security, mechanisms such as encryption through Secure Sockets Layer (SSL), Virtual Private Networks (VPNs), timestamps, auditing and restricting access per-user-group should be implemented.

To secure networked devices and assets in the healthcare, it has been reported that: (a) inventories should be created and maintained, as they can ensure a sound understanding of the systems and their components, support configuration, and automated remediation management processes (Independent Security Evaluators, 2016); and (b) software should be regularly patched and updated.

In addition, the network can be protected through the implementation of a firewall and thereby segmentation and segregation techniques. Moreover, monitoring mechanisms should be employed, so as to support: (a) network protection from attacks, e.g., Intrusion Prevention Systems that detect threats over the network by examining communications and scanning ports for anomalies and can execute a real-time response to stop an immediate threat, detection of attacks, i.e., Intrusion Detection Systems that monitor systems, network traffic, data, and files access, etc. and detect attacks; and (c) response to attacks (Intrusion Response systems that choose the necessary action to take to respond to attacks and ensure the security of networks and computational system.

Finally, a security-by-design approach would complete the above countermeasures, focusing on the cybersecurity concerns with respect to new devices or systems that need to be planned and implemented from the start of the procurement, design, development, and maintenance phases.

9.4 Conclusion

This chapter has presented how security systems can be applied within the healthcare sector. The SAFECARE[1] project[2] is working to provide an integrated solution for both physical and cybersecurity in the healthcare domain. In terms of physical security, video surveillance, access control, fire detection, and building management

1. The SAFECARE project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no. 787002.

2. https://www.safecare-project.eu/

sensors are combined with video analytics and novel rule support across the various modalities of input data from all of these systems. In this way, integrated systems are made capable of signaling security incidents via intrusion detection; fire detection; detection of attacks on building management systems, such as power and heating, ventilation and air conditioning (HVAC); and suspicious behavior detection. Further, this approach to security sits alongside state-of-the-art cybersecurity provisions and, for both, SAFECARE provides sophisticated analyses of impact propagation, as described in a later chapter.

Acknowledgments

The SAFECARE project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no. 787002.

References

ECSO. 2018. *Healthcare Sector Report – Cyber security for the healthcare sector*. European Cyber Security Organisation (ECSO), Rue Montoyer, 10, 1000 Brussels Belgium.

EU. 2016. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed on 12/10/2019).

Independent Security Evaluators. 2016. *Securing Hospitals: A research study and blueprint*. URL: https://www.securityevaluators.com/wp-content/uploads/2017/07/securing_hospitals.pdf.

ISO. 2018. *ISO 22300:2018-Security and resilience—Vocabulary*. URL: https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-2:v1:en (accessed on 12/10/2019).

ISO. 2019. *ISO/IEC 27001:2013 [ISO/IEC 27001:2013] Information technology—Security techniques—Information security management systems—Requirements*. URL: https://www.iso.org/standard/54534.html (accessed on 12/10/2019).

Martin G., Martin P., Hankin C., Darzi A., and Kinross J. 2017. "Cybersecurity and healthcare: how safe are we?" *BMJ* 358(j3179).

Mobolarinwa T. Balogun. 2017. *A Comparative analysis of heathcare system IoT and Industrial SCADA IoT for Cyberterrorism*. URL: https://pdfs.semanticscholar.org/75db/5aae5318ee60d43db4b2fcc46aadbdbfe1be.pdf (accessed on 01/27/2020).

Muhammad, K., R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. Baik. 2018. *Secure Surveillance Framework for IoT systems using Probabilistic Image Encryption*. URL: https://www.researchgate.net/publication/322408159_Secure_Surveillance_Framework_for_IoT_systems_using_Probabilistic_Image_Encryption.

NIST. 2019a. *NIST – Digital Identity Guidelines*. URL: https://pages.nist.gov/800-63-3/sp800-63-3.html#def-and-acr (accessed on 12/10/2019).

NIST. 2019b. *NIST glossary*. URL: https://csrc.nist.gov/glossary/term/RA (accessed on 12/10/2019).

ONVIF (2020). *Open Network Video Interface Forum*. URL: https://www.onvif.org/ (accessed on 01/14/2020).

Rodofile, Nicholas R. and Radke, Kenneth and Foo, Ernest. 2017. *Framework for SCADA Cyber-Attack Dataset Creation*. URL: https://doi.org/10.1145/3014812.3014883.