SSR Journal of Engineering and Technology (SSRJET)

Homepage: https://ssrpublisher.com/ssrjet/

Volume 3, Issue 2, 2026 ISSN: 3049-0383

Design and Implementation of Digital Security System Layout to Curve the Menace of Theft and Burglary at Federal Polytechnic Kabo Environment

Ibrahim Abba

Department of Electrical Electronics Engineering Technology, School of Engineering, Federal Polytechnic Kabo, Kano Nigeria

Received: *20.01.2026* | ***Accepted:*** *14.02.2026* | ***Published:*** *19.02.2026*

***Corresponding author:** Ibrahim Abba

DOI: *10.5281/zenodo.18693752*

Abstract **Original Research Article**

This research addresses the security challenges affecting the School of Technology by implementing a video surveillance system capable of capturing real-time activities across the entire premises. It examines the underlying concepts of video surveillance, outlines the various system types, and describes the components involved. The study also details the selection of suitable equipment for the project, including POLYVISION/AHD/HD/32CH/DVR units, 2MP (1080P) day/night cameras, a 2TB hard disk drive, and a 12V DC/2A centralized power supply, among others. The system incorporates modern technological features that enable remote viewing on mobile devices from any location worldwide. This enhancement significantly strengthens the security infrastructure by improving monitoring efficiency and providing clear visual coverage that supports security personnel in their duties. The monitor presents the expected output based on a simulated implementation of the system. Additionally, potential upgrades and future improvements are discussed.

Keywords: Video surveillance system, security infrastructure, real-time monitoring, remote viewing technology, digital video recorder (DVR) system.

1.0 INTRODUCTION

There are various types of CCTV systems—analogue or digital, wired or wireless—each with different modes of operation. However, they all share several essential components: a camera, a lens, a monitor, and in the case of wired systems, cables for signal transmission. Many systems also include video recorders to store the captured footage. The camera captures visual information from the monitored area through its lens, which determines the camera's viewing distance and field of vision. Lenses are often purchased separately. Cameras may operate using either wired or wireless configurations. In wired systems, the camera transmits signals to the monitor through a physical cable, whereas in wireless systems, the camera sends signals directly to the monitor without cabling. The monitor may be a basic television set (without tuning capability), a personal computer, or a laptop. Most wired analogue CCTV systems rely on TV monitors, while digital and wireless systems generally use computers, which also enable remote viewing—often via the internet.

For recording, the monitor is used alongside a video recorder: a VCR in analogue systems, or a DVR (Digital Video Recorder) or NVR (Network Video Recorder) in digital systems. In many cases, a DVR can replace the monitor entirely because it can receive, record, and store footage as a stand-alone unit. CCTV (Closed-Circuit Television) refers to a surveillance setup in which camera signals are transmitted to a specific destination, such as a monitor or computer. CCTV systems are widely used to secure banks, shopping malls, government buildings, and increasingly, private homes and businesses as the technology becomes more affordable and user-friendly.

2.0 LITERATURE

Video surveillance plays a vital role in securing critical infrastructure. With the rapid growth of digital and networking technologies across the globe—and their integration into traditional industrial sectors—the video surveillance industry has quickly embraced these innovations. Using existing Internet infrastructure has made modern surveillance systems easier to deploy and far more cost-effective compared to conventional hardwired CCTV systems.

A typical digital video surveillance system consists of three main components: video capture units, network transmission, and a central control module.

The video capture units generally include a set of digital cameras or analogue cameras connected through a video encoding device (switcher), which converts analogue signals into digital form. This module captures video footage, compresses the raw data, and encodes it into widely used formats such as MPEG, Motion JPEG, H.261, H.263, or H.264.

The network transmission module sends the encoded video stream over an IP-based network, which may be a Local Area Network (LAN) or the Internet.

The central control module is responsible for displaying and recording each video feed. It also manages camera operations by issuing control commands. Two types of data flow between these modules, the most important being control data. The devices that send control commands can include PCs, control keyboards, or matrix switchers, which may pass the commands on to other switchers. These commands are received by devices such as IP-based PTZ (pan–tilt–zoom) dome cameras, matrix switchers, or DVR/NVR units.

Control data typically exhibit the following characteristics:

- ✓ Small packet size: Control commands usually consist of a few ASCII characters, resulting in very small network packets.
- ✓ Burst transmission: Control packets are sent only when the system is being used or when specific events occur, meaning the transmission is intermittent and triggered by user actions or alarm-based events.
- ✓ High correlation: Many commands depend on previous commands for context. For example, a PAN LEFT instruction is only meaningful after a CAMERA SELECTION command has been issued.
- ✓ Significant importance. The control packets may contain confidential data, such as user name and password, system administration configuration and key distribution information.

The disclosure of these data may result in severe breach of security. For example, recorded data may be tampered and deleted, or the system control may be totally lost. The second type of data is the video stream. IP cameras, IP video servers and DVRs are the source of digital video data.

The recipients of digital video can be a PC or a digital video decoder. In contrast with control data, the video data features the following properties:

The Huge volume of data; The digital video requires up to 4 Mbps network bandwidth. Video surveillance systems demand real-time display of the target site information, which results in a stringent requirement for network throughput and processing capability.

Secondly, time-sensitivity; The video data on the network is real-time and thus, grabbing the content afterwards is of limited importance for

ongoing attacks. There are potential security threats to the IP based video surveillance systems. Adversaries can capture the video frames by simply listening on the network transmission channel. Security is a must in order to make the IP based video surveillance systems practical and usable.

2.1 SURVEILLANCE SYSTEM:

The switcher accepts video signals from many different camera types and connects them to one or more monitors or recorders. Using manual or automatic activation or an alarming signal input, the switcher selects one or more of the cameras and diverts their video signal to a specified monitor, recorder, or some other device or location. There are 4 basic switcher types:

1. Manual switcher: connects one camera at a time to the monitor, recorder or printer.

2. Sequential switcher: automatically switches the cameras in sequence to the output device

3. Homing switcher: the operator can override the automatic sequence in the sequential switcher.

4. Alarming switcher: connects the alarmed camera to the output automatically, when the alarm is received. Although switchers are analogue video Surveillance components, they are also implemented in DVRs and NVRs therefore the feature is available in digital systems as well.

2.2 THE MONITORS

Video monitors can be divided into: - Monochrome, Color, CRT, LCD, Plasma or Computer display. Large video monitors do not necessarily have better picture resolutions or the ability to increase the amount of intelligence available in the picture. This is dependent on the TV standard.

2.3 VIDEO MOTION DETECTOR (VMD)

This is a component that produces an alarm signal based on a change in the video scene. The VMD can be built into the camera or be a separate component inserted between the camera and the monitor software in a computer.

The VMD electronics either analogue or digital, store the video frames, compare subsequent frames to the stored frames, then determine whether the scene has changed. In operation the VMD ‘decides’ whether a change is significant and whether to flag it as an alarm in order to alert the guard or some equipment or declare it a false alarm.

2.4 ASSESSMENT OF IP BASED VIDEO SURVEILLANCE SYSTEMS FOR SECURITY APPLICATIONS

The following was looked at with a view of assessing the effectiveness of an installed Video Surveillance system.

Camera sensitivity, digital compression and decompression, servers and workstations, the network and integration with sensor alarms.

2.4.1 IP VIDEO ARCHITECTURES

Three different options currently exist in the commercial market for IP-based Video Surveillance Architectures. For those systems using analogue cameras, network-based DVR's (Digital Video Recorders) and analogue encoders make it possible to digitally encode an analogue video feed and incorporate it into an IP network. These systems are typically limited to lower-resolution IP video feeds (a maximum of 4CIF, or 704x480). Higher resolution offerings are impractical due to the inherent resolution limitations of analogue video. Native IP cameras allow creation of an entirely IP-based video platform and offer more flexibility in terms of 4CIF and higher pixel resolution video streams. However, these native IP systems are significantly different in terms of infrastructure when compared to DVR's or encoders and may require additional network infrastructure in the field if upgrading an existing, analogue system. Systems with analogue encoders or native IP cameras both use.

3.0 METHODOLOGY

First step to undertake any installation of video surveillance system(s) an in-depth study of the site must be carried out with the following aims, To Identifying need of the system and to identification of the objective of the security concern, whether it is outside or inside, near or

far, also the identification of area needing surveillance for the location where the cameras will be installed. Finally, the analysis of capture information recorded by the CCTV.

3.1 SITE STUDY AND ANALYSIS

It is important to work with the end user to understand what field of view is required to be seen on the monitor. The field of view is the width and height of the scene as viewed by the lens. It depends upon the focal length and distance of the object.

Any field of view has some critical area which is the target area. For example, when the camera is viewing a gate, the space the car is coming through is the critical viewing area or if one is watching the door, the space occupied by a person walking through the door is a critical a viewing area. In the same way every scene has a critical viewing area. Below is the proposed design for the installation.

3.2 THE INSTALLATION OF THE SYSTEM

Among us the students using a wheel measuring tool and all length per camera was measured and recorded as shown below.

Table 1: Measurements of the cameras in distance meters

Name of camera	Name of view	Distance measured (m)
Camera 01	showing the school gate entrance	90
Camera 02	showing movement out of the gate	100
Camera 03	showing Rector's car park	105
Camera 04	showing the school vehicle park	182
Camera 05	showing laboratory block view	182
Camera 06	showing front of auditorium	173
Camera 07	inside Auditorium left view	183
Camera 08	inside Auditorium right view	183
	Total cable length used	**1,016meters**

The digging took place among the students of the department done from the admin block to the ICT building where majority of the distant cameras are located. We run all RG59 with power coaxial cable to various individual camera points through a 1.5" pvc pipes to serve as additional protection to the laid down cables. Below is the image of site experience.

Figure 1: Shows the roll of RG 59 cable

RG59 cable with power connected as single cable was run from each camera point to the DVR as seeing image for figure :1

However, the BNC ploughs was connected to both end of the coaxial cable per each camera to establish connection between the camera and the DVR.

Figure 2: DC plough connectors

Figure 2 shows the DC plough was also connected to one end of the power cable and the other end to the 12v dc central power to power the camera. The positive and negative terminal of the power cable was connected accordingly to their corresponding terminals. A 32'' colored television was used as a monitor considering the number of cameras to be viewed. A VGA cable was connected to serve as a link between the monitor and the DVR. Figure 3 and figure 4 shows the VGA cable connector and the 12Vdc control system.

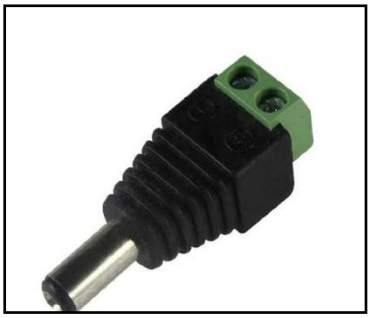

Figure 3: VGA connector

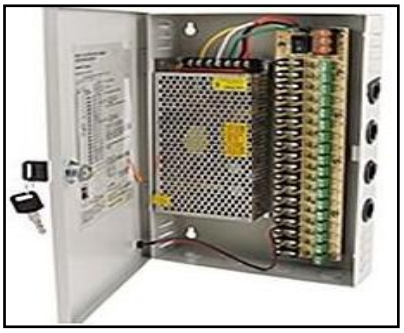

figure 4: The 12Vdc power supply

The remote view explains top link router was used with modem and a sim card with data from a service provider to send the DVR online for remote view on your mobile phone.

3.5.1 IDENTIFICATION OF THE AREA UNDER SURVEILLANCE.

Figure 5: wireless router

For the purpose of this research Federal Polytechnic Kabo was chosen and the camera views and the area they cover was indicated as stated: Camera 1: showing the school gate entrance as indicated in figure 6.

Figure 6: Camera shows the entrance to the school premises

Another image is the second Camera showing the School hall as shown in figure 7

Figure 7: institution hall viewed by the CCTV

Figure 8: CCTV showing the location of the school laboratories

This indicated that the cameras positioned in a strategic location so that they captured every movement and activities at that location.

4.0 RESULT

This chapter will present data collected, from the given questioner distributed among several people. The discussion of finding is also presented in this section.

4.1 RESEARCH FINDINGS

A collection and analysis of data the expected result was obtained. From the responses of the respondent, we would get to understand that the CCTV camera has a great function in preventing the crime occurrences, and as well its impact by such is very limited.

After a total of 25 questioner was distributed among the student, CCTV installers and other individuals that are related to it. A total of 20 questioner was returned and below table are their responses.

Table 2: The perception, effect and prevention of CCTV Camera

Questions	Sub-questions	No of Respondents
What is the perception of CCTV Cameras	CCTV system is a system that deter crimes.	2
	CCTV camera records and captures incidents	3
	CCTV camera stores pictures of crimes	4
	CCTV camera is not useful in crime deterrence	2
The effect of CCTV Camera on Crime	CCTV camera criminals the opportunity of crime	2
	CCTV camera block criminals the opportunity of crime	1
	CCTV camera can identify criminals	2
	CCTV camera is not effective in preventing crime	2

Questions	Sub-questions	No of Respondents
The expectation of CCTV Camera on Detecting and recording of crimes.	CCTV camera can detect crime in the INSTITUTION.	2
	CCTV is expected to combat crime in INSTITUTION.	1
	CCTV has the ability of removing criminals from the area covered by the system	5
	CCTV does encourage crimes under its coverage	0
The Impact of CCTV Camera on fundamental human right.	CCTV can transmit the undesired signal which can violate the privacy of the citizens.	0
	CCTV monitored people in their private places and put them in doughs condition.	2
	CCTV reduce the freedom of association as part of their basic right and freedom.	2
	CCTV encourage the violation of human right.	0
The level of impact of CCTV on Crime	High	3
	Low	2
	Medium	1
	CCTV camera monitors real-time criminal Too low	2
How CCTV Camera helps in preventing Crimes	CCTV camera relay real-time visual information about event status at a given time	2

The table 2 states the perception, effect and prevention of CCTV Camera: on the perception of CCTV cameras, the survey shows that, 11.0% of the respondents agreed that CCTV camera is a system perceived to deter crime, 7.0% of the respondents believe that CCTV camera is perceived .to records and captures incidents, 2.0% respondents indicated that CCTV camera stores pictures of crime. Based on the results presented in table 1, it could be deduced that CCTV camera is a system that deter crime, block criminals the opportunity of committing crime and monitors real-time criminal incidents in an area covered by the system. This agrees with the works of which maintain that CCTV cameras are

effective in crime prevention and reduces the rate of crime in the area covered by the system.

The table 2 above shows the expectation, impact, and the detection of CCTV camera. Out of the 20 respondents, 8.0% of the respondent response on the high expectation of the CCTV camera in detecting the crimes. However, 4.0% of the respondent agreed that the CCTV camera has high impact on the fundamental human right, while 8.0% of them respond accordingly on the impact level of the CCTV camera on crime.

4.3 Test of hypothesis

4.3.1 Hypothesis 1

From table 2 above we understand that the CCTV camera is the best tool use in preventing and reducing the criminology aspects. However, we would also understand the effectiveness of the CCTV and how it acts perfectly in detecting the crime.

4.3.2 Hypothesis 2

From table 2 above, it was concluded that the privacy and human right violation of CCTV is limited than how it acts in detecting and monitoring of the criminals.

4.4 DISCUSSION OF FINDING

From the above hypothesis, we can all agree that the CCTV camera is the best tools, and its concept is the best concept in detecting and maintaining security. At the same time the CCTV camera has some impacts on the fundamental human right, but reference to the stated points of reconciliation in 3, 4 and 5 and the responses by the students, CCTV installers and those has well knowledge on human right and privacy. Our research finding could be concluded by what stated in [19] journal.

“The privacy issue lies at the heart of an ongoing debate in nearly all Western democracies between liberalists and communitarians over the question of how to balance individual rights with collective goods, individual rights and community interests. In the case of the issue of privacy, this debate opposes those who argue that it is necessary to protect the privacy of individuals by limiting the access to personal information, and those who believe that it is necessary to open this access because it will benefit the community. Some have argued that this is a contrived opposition, but it remains a real tension which emerges in all sorts of cases involving the infringement of privacy, such as, for instance, undercover actions led by the police on the internet, the disclosure of medical files for health insurance purposes or epidemiological research, the linking and matching of databases to detect fraud in social security, soliciting information about on-line behavior of internet users from access providers in criminal justice cases and the use of Closed Circuit Television (CCTV) in public places for crime prevention. As a society we value privacy, but at the same time we value security and the availability of information about citizens. This tension is exemplified in the debates about CCTV cameras in public places. We either accept to trade our privacy for security by installing cameras everywhere, or we refuse to do so in the name of the respect of privacy, and thus settle for less security. Smart CCTV systems allow us to have our cake and eat it, because their smart architecture integrates the surveillance function with systems that limit the flow and availability of recorded information.

5.0 CONCLUSIONS

5.1 SUMMARY

We all need security. That essence, is the exact reason which brought about the technology of the CCTV camera, so that the criminology would be reduce in our school and in the nationwide. With the insecurity we get our self, the privacy and the fundamental human right has to be maintain. In this research we have stated the concept of the CCTV camera in crime prevention and the reconciliation between safety, security, and fundamental human right that provided by the National constitution.

5.2 CONCLUSION

Our school and nearby environment will grow both in numbers and size. This growth poses a challenge to the police and other security agencies in effecting the policing. However, adoption of modern technology i.e. CCTV cameras in policing will ensure that insecurity within the nation is managed effectively with increased detection and prosecution of criminals. Planners should therefore endeavor to ensure that Street designs and building design help to

improve visibility and improve circulation within the school and all over the nation where human right should not be violated.

The CCTV cameras help in monitoring and controlling movement of vehicular traffic through pedestrian ways and streets, tracking and recording the movement of undesirable persons and their vehicles, increasing confidence of foreign investors and tourist in the country thereby increasing revenue propensity and improving the performance of the security agencies in crime detection and prevention.

5.3 RECOMMENDATIONS

The following recommendation were observed and stated out after the research:

The CCTV camera should not be installed in public and private places. This is due to violation of the right and freedom of individuals. Also Planning should endeavor to improve visibility to reduce the opportunity for occurrence of crime, improve guardianship by use of CCTV Cameras and improve circulation a swell as human right should be regularly maintained. Finally an institutional framework with an effective organizational structure clearly identifying the roles of key players can enhance stakeholder involvement.

ACKNOWLEDGMENT

The authors also would like to thank the management of Federal Polytechnic Kabo and Tertiary Education Trust Fund (TETFUND) who has sponsored the research work under institutional base research(IBR) funding.

REFERENCES

Cerezo, A. (2013). CCTV and crime displacement: A quasi-experimental evaluation. European Journal of Criminology, 10(2), 222–236.https://doi.org/10.1177/ 1477370812468379

Citizen Safety Promotion Division. (2024). “Number of surveillance cameras installed with subsidies from metropolitan, ward, city, and town governments”. Available at: Https://bouh antokyo.maps.arcgis.com/apps/MapSeries/index .html?appid=6967a8b9076a454 8b31f20fb17956c20 (accessed 29 July 2024).

Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. Crime and Justice, 4, 225–256. https://doi.org/10.1086/449090

Clarke, R. V. (1997). Situational crime prevention: Successful case studies (2nd edition). New York: Harrow and Heston.

Cornish, D., & Clarke, R. V. (1986). The reasoning criminal: Rational choice perspectives on offending. Hague: Springer- Verlag.

Cozens, P., & Van der Linde, T. (2015). Perceptions of crime prevention through environmental design (CPTED) at Australian railway stations. Journal of Public Transportation, 18(4), 73–92.

Farrington, D. P., Gill, M., Waples, S. J., & Argomaniz, J. (2007). The effects of closed-circuit television on crime: Meta-analysis of an English national quasi-experimental multi-site evaluation. Journal of Experimental Criminology, 3, 2138.

Fujisawa SST. (n.d.) Town service – Security. Available at: Https://fujisawasst.com/EN/ project/service/security/ (accessed 11 September 2024).

Sihan Y., Hiroki N., Yerim Y., Yuta S. and Hideki K. (2024)” The impact of surveillance cameras and community safety activities on crime prevention: Evidence from Kakogawa City, Japan” Journal of Sustainable Cities and Society, Vol.115, 15 November 2024, Elsevier.