CPNI
Centre for the Protection of National Infrastructure

Anomaly Detection Guidance

PUBLISH DATE: May 2020

CLASSIFICATION: Official

Video Analytics – Guide to Anomaly Detection

Version 1.0

Table of Contents

Physical Security

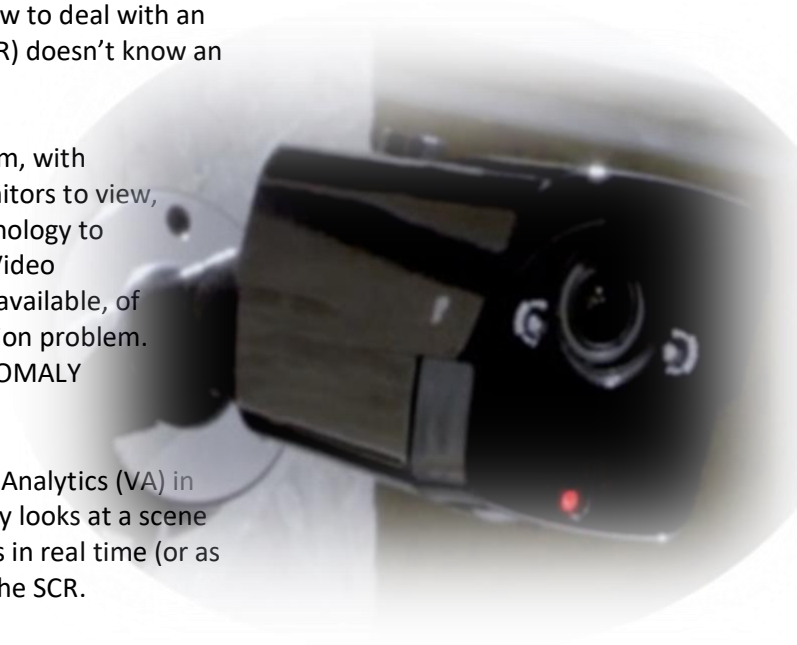
Executive Summary

The Security Control Room, SCR, can be a busy place. It is the central hub for all things security related. The operators in the SCR will be trained professionals within their field. But all professionals require the correct tools to do their job correctly. The SCR operator is no exception.

This information sheet will outline the CPNI view on ANOMALY DETECTION video analytic software available at the moment. This will not reference any particular system or capability.

Introduction

The *detection* of an incident remains the greatest challenge facing a control room when dealing with a situation. All the training in the world on how to deal with an incident is invalid if the Security Control Room (SCR) doesn't know an incident is taking place in the first place.



It is unlikely that an operator in a busy control room, with potentially hundreds of cameras and multiple monitors to view, will see an attack happen. Many sites turn to technology to assist with the detection. One such technology is Video Analytics. There are a number of analytic systems available, of which many claim to offer a solution to the detection problem. One technology which is becoming available is ANOMALY DETECTION.

Anomaly detection differs from 'traditional' Video Analytics (VA) in that rather than being rules based[1], this technology looks at a scene and is able to spot unusual activity then report this in real time (or as close to real time as possible) to the operators in the SCR.

[1] Rules Based analytic systems are those which require a specific set of events/circumstances to occur in order that a report or alert will be generated. This limits the use to situations whereby events can be predicted.

Operation

Anomaly detection software uses Machine Learning Algorithms[2] in order to understand the 'normal' world that cameras are viewing and reports when something which is not 'normal' happens. Generally, the software will be event agnostic insomuch as it does not know what it is looking at, simply that it sees something it does not recognise. Given the huge array of possible situations that could occur in life, this is restrictive and potentially not suitable for monitoring a complex and changing scene.

Deployment

There are a number of things to be aware of when considering this kind of software which we will discuss as the document goes on. The main thing to mention at this point is that software should sit behind the currently installed cameras in the site. Therefore, Data Protection Impact Assessments and Operational Requirements should be available for all cameras already, but the site must satisfy themselves that they are still compliant. More to follow. Remember, these systems only tell the operator that something (the system doesn't know what) is happening on camera XX and they may want to have a look. We will refer to this as a "tap on the shoulder" for the operator. The decision on whether to act and the action taken will rest with the operator. These systems will not need to record any footage that is not already being recorded onsite. Retention periods will depend on the in-force policy of the site. *See the CPNI note on video retention available on the CPNI Website*.

The simple idea with this kind of software is that it will operate in support of the currently installed camera system. As suggested earlier, software sits behind the currently installed CCTV system and is likely server based. In a nutshell, the site chooses which cameras to connect to the analytic software. An Internet Protocol (IP) connected system will be required. Its sole purpose is to give the control room operator that tap on the shoulder that something is happening on a particular camera.

[2] **Machine learning** (**ML**) is the study of computer algorithms that improve automatically through experience. Machine learning algorithms build a mathematical model based on sample data, known as training data, in order to make predictions or decisions without being explicitly programmed to do so.

The systems will require a period of 'bedding in'. That is to say time to 'learn' what the normal pattern of life is for that particular scene. This may take many days or even weeks depending on the frequency of action. It is useable right out of the box but will alert every time it sees a new action… which will be everything! The required 'bedding in' time will vary depending on the site and scene being monitored.

Example 1
For example, in a shopping centre a 7-day period will give a reasonable representation of life in the mall. 7 days will take into account the quiet Wednesday morning, or the busy Thursday evening and the packed Saturday afternoon. Most predictable and repeated events will happen over this period. Therefore, a software package may be deployable after these 7 days and give reasonably good returns. The longer it 'beds in' and sees events, the better it will appear at spotting anomalies.

Example 2
A West End theatre has a very predictable day… it opens its doors… people enter… they buy drinks…etc. This happens the same way every day with very little variation. In this case, the cycle might be a single day. So, the bedding in period could, in theory, be a single day.

There are potential pitfalls with a system that uses machine learning like this. The most obvious being that once it has decided that an event is 'normal' then it will stop reporting that event.

For example: there is a lot of knife crime in a particular location. Eventually, an anomaly detection system will stop seeing a knife attack as out of the ordinary and stop reporting it. Unfortunately, with machine learning we, as operators, will be unaware of what it has learned so will be unaware that a knife attack is now considered normal. Control Room operators will require training in order that they are able to interperate the information presented to them and make the correct decision.

The good news is that some systems will "forget" events after a certain length of time. So, if a reportable event happens today and tomorrow, but then not for XX days (or weeks) time, then the system will not count this as normal on the third event. What XX is, will depend upon the system being considered.

It is also important to understand that the systems will pick up on things which are not security related. For example, if a person were to fall down an escalator, clearly that is something that the site would want to be alerted to but may not be a security issue. Or perhaps there are a number of people running in an unexpected area… this may be security, it may be crime, it maybe youngsters causing trouble… but again it will be for the Security Officer to interpret. Training would need to be such that it is understood that all the system is giving is that 'tap on the shoulder' there is an event that may need attention. It may appear that the system is "false alarming" but this may not be the case. It therefore MUST NOT be used as a trigger for a response force. **IT IS THE OPERATOR WHO MAKES THE DECISION.**

A desirable feature of a system would be the addition of rules such that if an event is regular (and may be ignored by software) but still of interest it is flagged as an event. The knife crime example used earlier would be a case in point.

Data Protection

Since the software does not recognise a particular class of event, never mind individuals, there will not be any personal data being stored over and above that already being processed by existing CCTV installation. Data Protection Impact Assessments for the deployed cameras may need to be amended to include the use of anomaly detection software. The OR and the DPIA should reflect the purpose of the VA system. This is something a site must satisfy themselves of **prior** to installation. A reputable manufacturer/supplier would be happy to assist with any technical questions the site would have.

Summary

It is fair to say that IF this kind of software was infallible and ONLY alerted to attacks it would be perfect. This is not the case and not possible. Anomaly detection is just that… it detects anomalies…all anomalies, security related or not. Therefore, it provides a "tap on the shoulder" for busy security officers who may be doing other tasks. It learns what happens regularly and routinely – if bad things happen often it may ignore them. A hybrid solution of anomaly and rules may counter this to some degree. Remember that a 'bedding in' period will be required – the longer the bedding in period the better the results.

Anomaly detection offers real time detection of an attack or any other incident. It is not just a security product. Anomaly Detection has the potential to add value in many operational situations be they security, crime detection, safety, or any situation where an action may be required.