WHITE PAPER

Ending the Era of False Alarms

False alarms plague the security industry. According to the Urban Institute, 90-99% of all security alarm calls received by police are false. The ASU Center for Problem-Oriented Policing says the chances of alarm notifications indicating a real threat are only 2-6%.

Not only are false alarms a nuisance that can cause customers to lose faith in their security systems, most are also subjected to false alarm fees from their local municipalities. Cities that adopt false alarm reduction plans, which include fees and verification procedures, experience a 60% reduction in false alarms.

False alarms also waste police resources. When law enforcement responds to a false alarm, it takes time away from actual threats and investigations. Some cities have considered or adopted a verified response policy, in which they only respond to alarm events that have been verified as real threats. In previous decades, this required a video monitoring service—someone who is watching the video feeds to confirm an intruder is visible on the scene. This can be costly, requiring additional operators and equipment. Reducing false alarms is a high priority for law enforcement and security providers, but determining the most effective ways to do so were challenging, until recently.

> ***90-99% of all calls received by police as a result of alarms from security systems or panic alarms are false.***

The Evolution of Video Verification

Video monitoring is a service that monitoring centers can offer to ensure customers that their premises are always being observed. However, to provide these services, monitoring centers need to have operators viewing the video 24/7. Setting this up can be complicated and operators must juggle several different kinds of software. While video cameras record evidence of what happened, it comes at a cost—generating days and days of video to comb through when a security event occurs.

Video monitoring allows for visual evidence to be considered, but does little to reduce false notifications. Cameras with basic motion detection start recording when motion happens in their field of view. At this point, a video verification operator can view the recording and verify whether there's a security concern. However, motion detection could be set off by wind blowing leaves or shadows, or even a stray balloon—requiring the operator to analyze whether the recording necessitates a dispatch. The development of video analytics is bringing more precision to this process.

New video technology uses analytics to detect events and help cameras identify what is showing up in their field of view. Current capabilities include detecting people, vehicles, animals, and consider factors like time spent loitering and the direction of travel. This eliminates nuisance notifications by differentiating between important and non-important motion activity. The incorporation of AI and machine learning has led to better accuracy and more detailed differentiation, such as facial recognition. As video analytics evolve, they are increasingly seen as a way to reduce false alarms.

AlarmVision®
Taking this evolution to the next level is AlarmVision, a patent-pending detection technology from DMP that enables video analytics integration with the control panel. This truly integrated system allows cameras to talk to the panel natively. When a security event occurs, all information from the system and the cameras is sent to the monitoring center and to the end user.

AlarmVision turns existing cameras into smart motion detectors with the addition of one, easy-to-use XV Gateway. XV Gateways with AlarmVision bring analytics to any IP camera system, turning those simple cameras into powerful alarm detection devices. For example, cameras can differentiate between person, vehicle and animal, then trigger the alarm panel based on the object type and system settings.

AlarmVision gives security companies the ability to offer their customers the convenience of video verification without the additional labor costs of manual video monitoring. AlarmVision provides real-time video monitoring 24 hours a day, which multiplies the capability of monitoring center operators.

Areas vs. Partitions
AlarmVision capitalizes on DMP's integrated systems that leverage the power of access control, intrusion and role-based actions in a single panel. This enables users to create multiple, intelligent "areas" controllable with any keypad on the system.

Although some use the terms "area" and "partition" interchangeably, the difference is profound. Today's legacy single-function systems like CHeKT Bridge require a separate connection for each area, with information limited to whether a "partition" is armed or not, and no simple way for panels to share information with each other.

AlarmVision allows panels to know not just whether a person is trying to access the area, but who that person is and what level of access they have.

AlarmVision turns existing cameras into smart motion detectors with the addition of one, easy-to-use XV Gateway.

Reduce False Alarms
In traditional intrusion systems, motion sensors monitor open areas, but they are highly prone to false alarms and can be easily defeated. With video analysis of the event, the cause of the motion is determined before sending the alarm to the monitoring center. Using video analytics in this way virtually eliminates false alarms. Cameras become intelligent motion detectors able to trigger actions and alarms, the same way an intrusion sensor would, but with the ability to differentiate types and sources of motion to identify real threats in real time.

In addition to reducing false alarms, AlarmVision reduces false alerts to the customer. Fewer notifications mean the customer is more likely to use their system the way it's intended, rather than disabling it after feeling like it's an inconvenience.

Instead of alerts about moving leaves, shadows and light, customers receive notifications about people, vehicles or animals. This technology detects the motion events that matter, thus drastically reducing false alarms and the penalty fees associated with them. AlarmVision uses analytics to determine a real alarm condition in real time, leading the way into a new era where false alarms could be a thing of the past.

Top 10 Major Cities with Highest False Alarm Fees

City	Alarm Fine Schedule	Total for 10 False Alarms/Year
San Jose	1st: No fine 2nd: $250 3rd: $350 4th: $500 5th or more: $750	$6,350.00
Los Angeles	1st: $267 2nd: $317 ($267 plus a penalty that increases by $50 with each subsequent alarm) 3rd: $367 4th: $417 5th: $467 ... 10th: $717	$4,920.00
Atlanta	1st: No fine 2nd: $50 3rd: $100 4th-6th: $200 7th or more: $500	$2,750.00
Mesa	1st: $50 2nd: $100 3rd: $150 4th: $200 5th: $250 6th: $300 7th or more: $400	$2,650.00
Columbus	1st: No fine 2nd: $50 3rd-4th: $100 5th-6th: $200 7th-8th: $300 9th-10th $500 11th or more: $800	$2,250.00
San Francisco	1st: No fine 2nd: $100 3rd: $150 4th: $200 5th or more: $250	$1,950.00
Sacramento	1st-2nd: No fine 3rd: $75 4th: $100 5th: $200 6th or more: $250	$1,625.00
Jacksonville	1st-2nd: No fine 3rd: $50 4th: $100 5th: $150 6th or more: $250	$1,550.00
Baltimore	1st-2nd: No fine 3rd-4th: $70 5th: $105 6th: $140 7th: $175 8th: $210 9th: $280 10th: $350 ... 14th or more: $700	$1,400.00
Fresno	1st: No fine Each subsequent alarm: $155	$1,395.00

Source: https://www.deepsentinel.com/blogs/home-security/false-alarms-fines/

COMPETITIVE ANALYSIS

XV Gateway vs. CHeKT Bridge

What are the differences?	XV Gateway	CHeKT Bridge
Camera regions as alarm zones	✓	✓
Includes analytics	✓	
Delivers video footage to monitoring center	✓	✓
Video footage initiates alarm	✓	
Determines if alarm should be presented to Dispatch	✓	
Reduces false alarms	✓	
Auto detects cameras for easy setup	✓	
Wireless connections to cameras for fast installation	✓	
Cameras are supervised	✓	
Transmission	Encrypted Data	Dry Contact Input/Output
Integrates with Access Control Areas	✓	
Arming inputs	16-32 Areas	1 (Key Switch)

⚠ **The CHeKT Bridge does not include analytics.** It only supports the pairing of alarm zones to cameras and delivers video footage of the alarm trigger to the monitoring center. A system with a CHeKT Bridge but without a Camect Hub require analytics in each camera. Simple motion detection causes hours and hours of unneeded video clips.

DMP.com | 800-641-4282
2500 N. Partnership Blvd
Springfield, MO 65803

LT-3011 | 3/13/2025