Alarm Verification for Alarm Management

en Application note

Table of contents

1 Introduction

Alarm Verification is a feature for the Alarm Management service that reduces the occurrence of unwanted alarms generated by intelligent video cameras.
This feature helps alarm operators that manage a high number of centralized alarms to focus on the moments that matter. The reduction of presented alarms to the operator decreases fatigue from repetitive work. This helps to make better decisions, to start interventions quicker and to react more appropriately.
The main platform for the Alarm Verification feature is Alarm Management. To use this feature for a specific camera a connection of this camera to Remote Portal, an existing Alarm Management license and the activation of Alarm Verification in Remote Portal is required.

2 Functionality

2.1 General

Alarm Verification is a functionality of the Alarm Management service. Alarm Verification behaves similarly to existing and known functions like Live Intervention. To verify alarms, Alarm Verification requires that a camera generates an initial event that is received by Alarm Management.
If the Alarm Verification feature is activated for a camera, Alarm Management sends alarm events generated by this camera to a centralized cloud service for verification. This service verifies by using metadata and deep neural network fusion, whether a moving person or vehicle is visible in the alarm area of the scene.
For connected Bosch cameras, Alarm Verification ignores stationary objects and objects outside the alarm bounding box area generated by the intelligent camera. After verification, Alarm Verification returns a confidence value to Alarm Management. Depending on this value, Alarm Management can suppress the event from the Event List.
Alarm Verification uses artificial intelligence detectors developed and maintained by Bosch. These detectors are continuously improved and automatically updated to detect more vehicle classes, persons and to support domain-specific applications.
Before putting Alarm Verification into operation, Bosch recommends ensuring the functionality for the specific application and project first. This can happen by using walk tests that guarantee proper coverage of the intended scenario.
Alarm operators can provide feedback to the service inside Alarm Management about whether or not the right decision was taken by the service. This feedback is used to improve the service over time to achieve better performance.

2.2 Requirements

To use the Alarm Verification feature, following requirements must be fulfilled:
- The cameras must be visible in Remote Portal.
  - Bosch cameras are connected to Remote Portal via the Video Relay.
  - 3rd party cameras are connected via the Video Extension Relay (commissioning done via Alarm Management).
- The cameras must have an activate Alarm Management license.
- Alarm Verification must be activated in Remote Portal.
- The camera must be commissioned to an Alarm Management instance.
- An Alarm Verification scenario must be configured in Alarm Management.
- The cameras must have sufficient uplink bandwidth to transfer alarm clips.

Required camera configuration settings
- The cameras must have configured alarms (EVA, IVA, Motion+ or generic VCA).
- The cameras must have active continuous local recording (SD card, VRM or DIVAR IP).
- Alarm Verification is compatible with all cameras that are supported by Alarm Management.
  Consider that for 3rd party cameras contrary to Bosch cameras, the full frame of the alarm video is evaluated and metadata information is not included in the evaluation. For proper function it is therefore recommended to mask areas that are not required.

2.3 Configuration options

Alarm Verification can be set-up and configured in Alarm Management similar to other functions (for example Live Intervention) with features such as scheduling, automatic actions, alarm transmission and more. Main differences are the in following aspects:

- **AI Sensitivity Threshold:** This option allows to increase or decrease the sensitivity threshold for verifying alarms. Bosch recommends using the default value for evaluation periods to achieve a balanced result.
  A lower value will continue to show more events to the operator, while a higher value will suppress more events. The right value depends on each individual project and scenario.
- **Show/Hide from Event List:** This option allows to select whether to continue to show rejected alarms in the event list or not. This is helpful for evaluation periods that leave it to the operator to open rejected events or not.
  If the evaluation is complete, users may choose to send rejected alarms directly to the event history (thereby not showing them in the event list). This will reduce the amount of displayed alarms.

2.4 Usage

Alarm Verification returns three states to the Alarm Management Event List for each alarm:

- **Verified**: Alarm Verification was able to confirm that this alarm raised by the camera is true (by the assessment of the AI service).
  This means that the returned confidence score of a person or vehicle in the alarm event is higher than the threshold for suppression.
- **Rejected**: Alarm Verification was unable to confirm person or vehicle presence in the alarm.
  This means that the returned confidence score is below the threshold.
- **Unverified**: This covers the case that Alarm Verification was unable to process the alarm event and returned it without a classification.
  The reason for this classification can be unavailability of service, a long delay in the clip upload or an unusable input format.

All alarms analyzed by Alarm Verification are stored for 30 days in the Event History for review, independent of whether they are rejected, verified or unverified.
It is possible to check the performance of Alarm Verification by using the Diagnosis Module that is available to customers of a dedicated Alarm Management service solution.

2.5 Infrastructure

The Alarm Verification feature is based on a cloud-hosted service operated, maintained and supported by Bosch out of the European Union, hosted on infrastructure by AWS.
The service is currently not available as an on-premises solution or as a dedicated service.
Any video input or metadata used to process alarm verification is used during the processing phase and permanently deleted thereafter.
The cloud service is automatically scaling if load or number of alarms increase, no user action is required.
The cloud service is not limited on the maximum number of alarms it can process. However, Bosch retains the right to monitor and enforce fair use principles. This means that connected cameras that create unwanted alarms in high and continuous frequency due to

lack of proper alarm configuration for the scene may violate fair use. Bosch monitors the individual load and will inform customers accordingly on any violation and the subsequent measures.

3 Configuration notes

Before setting up Alarm Verification, note the following information:

- Alarm Verification is designed for but not limited to verification of events exposed to severe environmental effects. This exposure is typically common in use cases as perimeter security of remote outdoor locations, construction sites, industrial premises or commercial buildings.
- The verification results depend on the evaluation of the cloud service. This means that the service can differentiate persons and vehicles against other alarm causes but not persons with good intentions (for example visitors) against those with bad intentions (for example intruder). This decision is still to be taken by the operator.
- The service requires a standard camera orientation. Bosch recommends a minimum of 20 pixels on target in Full HD resolution to ensure performance in all main conditions. While the service also performs in low light conditions, better illumination of the target increases accuracy.
  Ensure appropriate function and performance using a walk test.
- The activation of Alarm Verification adds additional latency of maximum 10 seconds from receiving the alarm in Alarm Management to showing it to the operator in the Event List.
  If the service does not provide the required information within 10 seconds, a timeout will result. The timeout causes the alarm event to be displayed as **Unverified** to the operator.
- Alarm Verification currently supports both, alarm events with metadata and alarm events without metadata. Bosch recommends using metadata for improved performance.
- Default values are optimized to reduce false-negative decision to below 0.5% of alarms.
- The service detects and verifies moving persons and vehicles. These objects must be uncovered and in clear contrast to the background.
- The service is optimized to work with the 10-second alarm clips used by default in Alarm Management by Bosch. Longer clip times or different settings can increase response times.
- Bosch recommends the following settings and conditions:
  - High-speed internet connection
  - Full HD resolution
  - At least 1 frame per second
  - 1 keyframe per second
  - No frame drops

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Building solutions for a better life

202411141235