NVI SOLUTIONS

ООО «НВИАЙ СОЛЮШЕНС»

Платформа видеоаналитики owl.Guard+

Описание функциональных характеристик

2024

Оглавление

Сокращения

API - Application Programming Interface (программный интерфейс системы);
CI/CD - Continuous Integration/Continuous Delivery (Непрерывная интеграция/Непрерывная доставка);
SSO — Single sign-on (технология единого входа);
АСУ ТП — Автоматизированная система управления технологическими процессами;
БД - база данных;
ВСП - верхний силовой привод;
ОС - операционная система;
ПБ - правила безопасности;
ПО - программное обеспечение;
ПРР - погрузо-разгрузочные работы;
СВП — силовой верхний привод;
СИЗ - средства индивидуальной защиты (перчатки, очки, каска, респиратор и т.д.)

Термины и определения

Адресное оповещение – оповещение конкретного участка или помещения о выявленном на нем событии.

Дашборд - набор графиков, диаграмм, табличной и графической информации отражающий основные показатели в легко воспринимаемом виде;

Зона - ограниченная часть сцены, внутри которой осуществляется выявление закрепленных за ней событий.

Контролируемый объект — сооружение или территория с производственной инфраструктурой, в рамках которой, платформа видеоаналитики owl.Guard+ осуществляет распознавание событий.

Событие - совокупность данных, отражающих факт нарушения сотрудниками определенного правила производственной безопасности или неисправности в работе технологического оборудования, например: "Нахождение сотрудника в опасной зоне", "Сотрудник открыл люк и ушел далее, чем на 2 метра от него", "Обнаружена течь технологической жидкости".

Сцена - ограниченная территория, комната, помещение или его часть, предназначенная для детектирования людей и определение их точного местоположения, а также расположения одной или нескольких зон, внутри которых осуществляется детектирование событий.

Трекер людей – алгоритм цифрового зрения, отслеживающий траекторию движения обнаруженных людей на наблюдаемой сцене;

Кадр - отдельно взятый стоп-кадр из видеопотока конкретной видеокамеры, который сделан в момент детектирования системой события.

Разметка - набор условных обозначений в виде, точек, иконок, линий, полигонов и текстовых надписей, помещаемых системой сверху кадра, для иллюстрации события.

1. Краткие сведения о системе

1.1. Общие сведения

Платформа видеоаналитики owl.Guard+ – программно-аппаратный комплекс, разработанный специалистами компании ООО «НВИАЙ СОЛЮШЕНС» с применением современных технологий

цифрового зрения. В основе комплекса лежат низкоуровневые разработки наших инженеров в области запуска и обработки нейронных сетей, подсистемы и модули с открытым исходным кодом, разработанные сообществом.
Система owl.Guard+ постоянно развивается, расширяется функционал, количество, качество распознаваемых событий, а также скорость анализа видеоряда.
Техническая поддержка комплекса осуществляется специалистами нашей компании, сведения о технической поддержке можно найти в разделе 2 настоящего документа.
По вопросам приобретения, функциональности или консультаций по системе в целом можно обратиться по телефону: **+7 (499) 397-87-58** или адресу электронной почты: support@nvi-solutions.com, дополнительную информацию о продукте и компании можно получить на сайте https://www.nvi-solutions.ru

1.2. Назначение

Платформа видеоаналитики owl.Guard+ - платформа видеоаналитики, предназначенная для автоматического выявления событий, связанных с соблюдением сотрудниками правил безопасности на производстве и эксплуатацией технологического оборудования, обеспечивающая в автоматическом режиме круглосуточный мониторинг производственной инфраструктуры, местоположения, состояния и действий персонала, автоматического оповещения заинтересованных специалистов и внешних информационных систем посредством API-интерфейса, о выявленных событиях на основе анализа потоков видеоинформации и, опционально, данных АСУ ТП для выявления сложных производственных событий.

2. Функциональные характеристики

2.1. Обработка видеопотоков:

- использование протокола rtsp, кодеки h.264, h.265;
- перенаправление потоков во внешние видеосистемы без конвертации и задействования ресурсов процессора;
- сохранение видеопотоков в файловый архив;
- автоматическая очистка старых видеоархивов (ротация видеоархива).

2.2. Совместимость со следующими распознающими модулями программных продуктов семейства owl.Guard:

- Модуль обнаружения автомобилей;
- Модуль определения корректности парковки автомобиля относительно выезда;
- Модуль определения наличия автомобиля в запретной зоне;
- Модуль определения наличия автомобиля в огнеопасной зоне;
- Модуль определения движения автомобиля задним ходом на человека;
- Модуль определения ведения погрузо-разгрузочных работ;
- Модуль обнаружения строительной техники;
- Модуль обнаружения не смонтированной линии долива;
- Модуль обнаружения вставка №2;
- Модуль определения отсутствия запорного оборудования;
- Модуль определения отсутствия штанги ПВО;
- Модуль определения отсутствия шпильки на фонтанной арматуре;
- Модуль определения движения штанг ПВО;
- Модуль обнаружения шарового крана;

- Модуль определения отсутствия штурвала задвижки;
- Модуль определения уровня загазованности;
- Модуль обнаружения механического или гидравлического ротора;
- Модуль обнаружения возгораний;
- Модуль обнаружения задымления;
- Модуль обнаружения огневых работ;
- Модуль обнаружения конусов, огораживающий место проведения огневых работ;
- Модуль обнаружения утечек внутрискважинной жидкости;
- Модуль обнаружения утечек горячей жидкости;
- Модуль обнаружения человека;
- Модуль определения наличия человека за ограждением люльки верхового;
- Модуль обнаружения человека между движущимся ключом и колонной;
- Модуль обнаружения человека в запретной зоне;
- Модуль определения человека, не держащегося за перила;
- Модуль определения натяжения на тяговом тросе УМК ключа;
- Модуль обнаружения открытого люка, с которым не работает человек;
- Модуль определения наличия человека у открытого работающего шнекового конвейера;
- Модуль определения отсутствия перчаток;
- Модуль определения отсутствия СИЗ органов зрения;
- Модуль определения отсутствия каски на персонале;
- Модуль определения отсутствия ремешка у каски;
- Модуль определения отсутствия сигнального жилета;
- Модуль определения отсутствия СИЗ органов дыхания;
- Модуль обнаружения постороннего человека;
- Модуль определения отсутствия страховочной привязи при работе на балконе;
- Модуль определения отсутствия страховочной привязи у края роторной площадки;
- Модуль обнаружения человека в несоответствующей форме одежды;
- Модуль обнаружения человека в опасной зоне при спуске-подъеме труб;
- Модуль определения операций с трубой до остановки талевого блока;
- Модуль обнаружения человека под грузом при ПРР;
- Модуль обнаружения человека опасной зоне при движении СВП или талевого блока;
- Модуль обнаружения человека без верхней спецодежды;
- Модуль обнаружения излива из затрубного пространства;
- Модуль обнаружения излива из трубного пространства;
- Модуль определения корректной герметизации скважины;
- Модуль определения работы неполной вахтой при проведении спуско-подъемных операций;
- Модуль определения соответствия объема доливаемой жидкости;
- Модуль обнаружения сбития или загрязнения камеры.

2.3. Расширяемость состава модулей распознавания:

- Встраивание новых алгоритмов распознавания;
- Возможность получения данных телеметрии с систем АСУ ТП и использования их для выявления сложных производственных событий в совокупности с методами цифрового зрения;
- Встраивание новых типов событий без необходимости изменения основного кода платформы, с использованием новых и существующих алгоритмов распознавания;
- Автоматическое дополнение web-приложения, при появлении новых типов событий.

2.4. Ретроспективный анализ видеоархивов:

- Запуск процедуры выявления событий на основе видеоархивов;
- Запись событий, выявленных методом ретроспективного анализа в БД с включением этих событий в отчёты и статистику.

2.5. Формирование подтверждающих материалов:

- Формирование одного или нескольких фотоизображений, подтверждающих выявленное событие;
- Формирование одного или нескольких видеороликов, подтверждающих выявленное событие;
- Запись информации о событии в БД, в составе следующей информации: дата\время начала события, дата\время окончания события, тип события, наименование сцены, наименование наблюдаемой зоны, подтверждающие фото и видеоматериалы.

2.6. Оповещение пользователей (опционально):

- Оповещение через систему громкоговорителей методом синтеза речи;
- Светозвуковое оповещение пользователей с использованием web-приложения путём вывода информационного всплывающего окна с возможностью перехода к соответствующему событию;
- Оповещение внешних информационных систем с использованием технологии web-hook;
- Оповещение путем отправки электронного письма по спискам рассылки после выявления события;
- Оповещение через интеграцию с существующими системами оповещения производственного объекта;
- Автоматическое формирование и отправка по электронной почте отчётов о событиях по расписанию.

2.7. Отображение списков событий:

- Вывод списка событий в составе следующих данных: дата, время, наименование типа события;
- Настройка списка событий: сортировка по новизне, тип события, место события;
- Отображение карточки события, при выборе события из списка;
- Перемещение по страницам списка.

2.8. Работа с карточками событий:

- Отображение карточки события, содержащей следующие сведения: дата, время, место события, тип, внутренний идентификатор, подтверждающие фотографии;
- Масштабирование на всю область отображения карточки при щелчке по выбранной фотографии.;
- Загрузка подтверждающих видеороликов в виде видеофайлов с разметкой системы.

2.9. Работа с архивом событий:

- Установка фильтра интересующих событий в составе следующих параметров: интервал дат, тип события, сцена события;
- Вывод списка событий, удовлетворяющих выбранным параметрам фильтрации;
- Вывод карточки отображения архивного события.

2.10. Формирование и отображение отчётов о событиях:

- Установка следующих параметров формирования отчёта: интервал дат, часовой пояс, выбор мест (сцен) событий, выбор типов событий, название отчёта;
- Отображение перечня событий на экране;
- Сохранение списка событий в виде отчетов в форматах CSV, ODS, XLSX, PDF, PDF с фото подтверждениями.

2.11. Просмотр изображений с камер видеонаблюдения:

- Вывод перечня доступных видеокамер в виде статичных миниатюр изображений с камер видеонаблюдения, сгруппированных по месту установки;
- Просмотр видеопотока выбранной видеокамеры с нанесённой разметкой зон и выделением людей и распознанных признаков.

2.12. Отображение статистики событий:

- Графическое отображение статистики в виде:
  - Круговой диаграммы событий по типу;
  - Круговой диаграммы событий по месту выявления;
  - Ленточной диаграммы по датам и типам событий;
  - Столбчатой диаграммы событий по месту выявления;
  - Линейного графика изменения во времени количества выявленных нарушений по типам;
- Фильтрация графического отображения статистики по: интервалу дат, типам событий, местам выявления.

2.13. Пользовательский интерфейс конфигурации подсистемы распознавания нарушений:

- Настройка предустановок поворотных камер;
- Настройка алгоритмов автоматического патрулирования поворотных камер;
- Управление поворотными камерами, переключение предустановок;
- Разметка опасных и запретных зон на ракурсах со стационарных камер и на предустановках поворотных камер;
- Настройка включенных модулей распознавания нарушений, настройка их параметров.

2.14. Сбор и отображение данных о состоянии системы:

- Сбор метрик, отражающих состояние системы;
- Ведение базы данных метрик состояний системы;
- Отображение данных о состоянии системы в режиме реального времени через пользовательский web-интерфейс;

• Анализ логов работы системы с использованием функционального web-приложения за указанные интервалы времени.

3. Функционал в области информационной безопасности

3.1. Идентификация и аутентификация:

• Анонимный доступ запрещён как к GUI, так и к API;
• Для идентификации пользователей при доступе каждому пользователю назначается уникальный персональный идентификатор;
• Доступ пользователей осуществляется посредством парольной аутентификации;
• При вводе идентификационной информации пароль маскирован специальными символами;
• Поддержка механизмов многофакторной аутентификации (MFA);
• Обеспечивается ограничение не успешных попыток входа;
• Парольная политика удовлетворяет следующим требованиям:
- политика сложности пароля;
- хранение истории паролей;
- установка срока действия пароля;
- возможность смены пароля при первом входе;
- возможность самостоятельной смены пароля.
• Централизованное управление учётными записями пользователей осуществляется путём применения службы каталогов (LDAP);
• Использование стойких хэш-алгоритмов PBKDF2;
• Авторизация пользователей на доступ производится после прохождения процедур идентификации и аутентификации.

3.2. Управление доступом:

• Используется система ролевого управления доступом для управления правами доступа пользователей;
• Подсистема разграничения доступа позволяет предоставлять права доступа в минимально необходимом объёме;
• Доступ к интерфейсу администрирования, а также конфигурационным файлам ограничены;
• Обеспечивается разграничение доступа между компонентами;
• Все учетные записи имеют возможность замены при их компрометации;
• Автоматическая блокировка сессии после установленного периода не активности (бездействия), восстановление сессии осуществляется после повторной аутентификации пользователя;
• При доступе по API устанавливается срок действия токена доступа.

3.3. Регистрация и учёт событий ИБ:

• Наличие механизмов регистрации и учёта событий ИБ;
• Предусмотрен централизованный интерфейс для работы с журналами событий безопасности;
• Подсистема регистрации и учёта событий ИБ обеспечивает:
- регистрацию даты и времени входа/выхода, попытки входа пользователя;

- регистрацию даты и времени запуска/остановки компонент;
- регистрацию изменения полномочий пользователей;
- регистрацию изменения настроек;
- регистрацию действий администраторов;
- регистрацию действий пользователей.

• Журналы регистрации и учёта событий ИБ хранятся в течение заданного периода времени;

• При заполнении установленного процента объёма памяти, выделенного для хранения журналов регистрации событий ИБ, выдаётся соответствующее предупреждение;

• Перезапись событий при заполнении установленного процента объёма памяти, выделенного для хранения журналов регистрации событий ИБ;

• Журналы событий ИБ защищены от несанкционированного просмотра и внесения изменений;

• Передача всеми компонентами системы событий безопасности и ошибок в syslog-сервер.

3.4. Защита программного обеспечения:

• Возможна совместная работа с антивирусным программным обеспечением при достаточных вычислительных мощностях;

• Контроль параметров конфигурации сканерами защищенности не оказывают существенного влияния на работоспособность запущенного экземпляра;

• Сборки распространяются после успешного тестирования сканерами информационной безопасности;

• Все используемые порты и протоколы описаны в документации;

• Возможность запуска от непривилегированной учетной записи;

• Реализован контроль целостности.

3.5. Сетевая безопасность:

• Работа в автономном режиме (без подключения к интернет);

• Шифрование канала связи на уровне доступа пользователей (поддержка https).