SENSTAR | Sensor Fusion Engine

Sicherheit verbessern.
Falschalarme reduzieren.

Falschalarme: Ein anhaltendes Problem

Die frühzeitige Erkennung von Eindringlingen, während sie sich noch am Perimeter und außerhalb von Gebäuden oder sensiblen Bereichen befinden, ist ein wichtiger Bestandteil des Sicherheitskonzeptes jeder Liegenschaft. Moderne Konzepte mit Perimeterdetektionssystemen und Videoanalyse haben in Vergangenheit stets ein hohes Maß an Leistung bewiesen und schützen kritische Standorte und Infrastrukturen auf der ganzen Welt.

Herkömmliche Perimeterdetektionssysteme weisen jedoch typische Einschränkungen auf, insbesondere bei bestimmten Grenzfällen, die Falschalarme erzeugen.

Alle individuellen Technologien zur Erkennung von Eindringlingen haben jedoch inhärente Probleme beim Einsatz, insbesondere in bestimmten Situationen. Die Hauptschwierigkeit besteht darin, eine hohe Erkennungswahrscheinlichkeit beizubehalten, ohne die Falschalarmrate (NAR) zu erhöhen.

	Zaunsensoren	**Videoanalyse / Line-of-Sight-Sensoren**
Erkennungsmethode	Schwingungen im Zaun analysieren	Analyse von Veränderungen im Erfassungsbereich oder von Datensignalen
Stärken	Erkennt eine tatsächliche Bedrohung direkt an der Zaunlinie - dem wichtigstem Grenzpunkt	Erkennt Aktivitäten innerhalb des Erfassungsbereichs und arbeitet unabhängig von physischen Barrieren wie Zäunen
Herausforderungen	• Angriffe ohne Zaunberührung • Torbereiche • Schlechte Qualität des Zaunes • Extreme Bedingungen	• Einschränkungen bei der Sichtlinie • Schlechte Sichtverhältnisse • Aktivitäten in der Nähe, die keine Bedrohung darstellen • Rekalibrierungen aufgrund von Standortänderungen

Die meisten dieser Herausforderungen können durch verschiedene Methoden gemildert werden, z.B. durch die aufwendigere physische Sicherheitsmaßnahmen, die Aufrechterhaltung störungsfreien Umgebung und eine sorgfältige Standortplanung. Doch was wäre, wenn es einen anderen Weg gäbe, der sowohl äußerst kosteneffizient ist als auch mit diesen

Herausforderungen umgehen kann?

Eine Lösung für die reale Welt

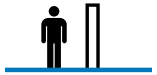
Sensor Fusion löst ein für alle Mal das Problem der unerwünschten Falschalarme. Durch den Einsatz ausgeklügelter KI-Technologien werden die Daten von verschiedenen Sensortypen ausgewertet und kombiniert, um Sicherheitsbedrohungen intelligent und zuverlässig zu erkennen. Sensor Fusion kann Falschalarme verhindern und gleichzeitig die Erkennungswahrscheinlichkeit erhöhen. Sie ist ideal für den Schutz bestimmter Bereiche, Zonen oder Situationen, in denen die vorhandenen Einzeltechnologien nicht ausreichen.

Hochrisikozonen

Zonen, in denen ein hohes Einbruchsrisiko besteht (z. B. abgelegene Abschnitte des Perimeters oder solche mit verdeckten Sichtlinien), erfordern möglicherweise ein höheres Maß an Sicherheit.

Tore

Je nach Konstruktion können einige Tore während des Betriebs und bei starkem Wind übermäßige Vibrationen an oder in der Nähe der beweglichen Sektion(en) erzeugen. Sensor Fusion kann die daraus resultierenden störenden Alarme eliminieren und gleichzeitig die Erkennungsfunktionen aufrechterhalten.



Unzureichende Zäune

Sensor Fusion kann dazu beitragen, das höhere Risiko an Standorten mit Zäunen zu kompensieren, die zukünftigen oder unvorhergesehenen Sicherheitsanforderungen nicht gerecht werden (z. B. Zäune mit unzureichender Höhe oder Ausladung sowie beschädigte oder lose Zaunmatten).

Extreme Bedingungen

Die meisten Falschalarme, die durch starke Winde verursacht werden, können durch eine ordnungsgemäße Wartung der Zäune und Sensorkalibrierung vermieden werden. An Standorten mit starken Stürmen, unregelmäßigen Windböen oder in Umgebungen mit starken Vibrationen kann Sensor Fusion an bestimmten Abschnitten der Umzäunung installiert werden, die für Falschalarme anfällig sind.

Sensor Fusion Engine: Perimetersicherheit weiterentwickelt

Die Senstar Sensor Fusion Engine ist eine bahnbrechende Technologie, die Daten aus verschiedenen Systemen zusammenführt, um verwertbare Informationen zu generieren. Die Sensor Fusion Engine ist mehr als nur eine einfache boolesche Logikintegration und greift auf Metadaten der Sensoren zu, um potenzielle Risiken intelligent zu charakterisieren. Durch die Datensynthese kann das System ein Leistungsniveau erreichen, das das der einzelnen Sensoren übertrifft.

Wie funktioniert es?

Die Senstar-Sensoren zur Erkennung von Eindringlingen und die Videoanalyselösungen (intern trainierte Deep-Learning-Modelle) bieten eine branchenführende Leistung und haben sich als geeignet für die anspruchsvollsten Sicherheitsanwendungen erwiesen. Durch die Synthese der Rohdaten von einzelnen Sensoren und Videoanalysen - ein Prozess, der die Analyse mehrerer Datentypen und -quellen beinhaltet - wird die Leistung der Gesamtlösung jedoch erheblich verbessert, wobei der Schwerpunkt auf der Verringerung, wenn nicht sogar der Beseitigung von Falschalarmen liegt.

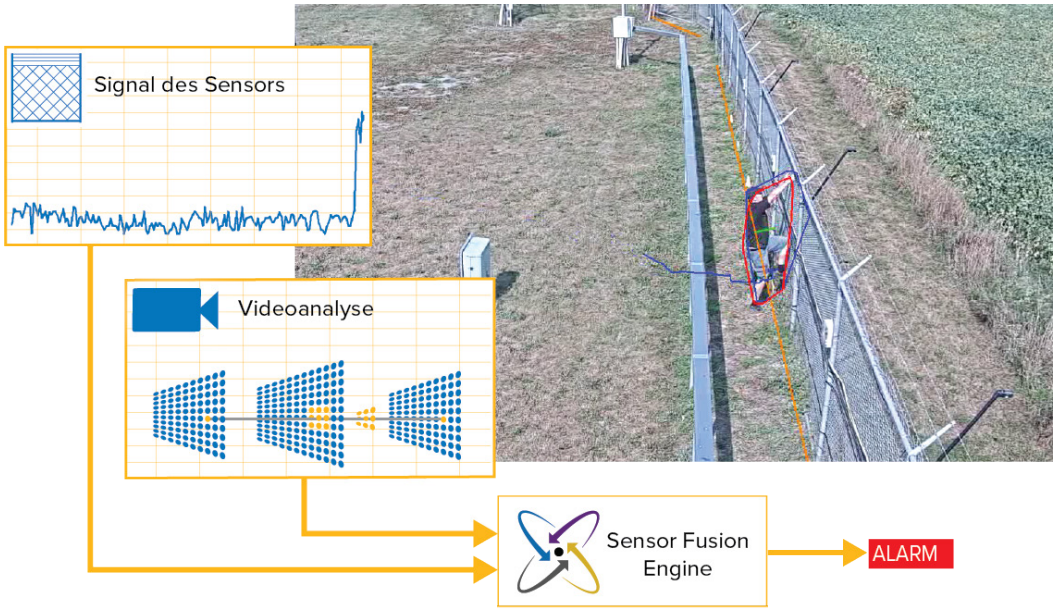
Gleichzeitig erhöht Sensor Fusion die Erkennungswahrscheinlichkeit (Probability of Detection, PD), indem das System Multi-Input-Wahrscheinlichkeitsberechnungen auf kleinere Einflüsse reagieren kann. Eine integrierte Zuverlässigkeitsberechnung vereinfacht die Systemkonfiguration und stellt gleichzeitig sicher, dass die optimale Leistung erreicht wird.

Support für Systemausfälle

Um mögliche Fehlbedienungen aufgrund von gestörten Videostreams, Geräteausfällen oder einem Verlust der Netzwerkverbindung zu vermeiden, überwacht die Sensor Fusion Engine alle Videostreams, den Datenfluss und die Kommunikation, um den Zustand der Sensoren zu ermitteln. Die Engine verschiebt die Gewichtung der Sensoren und verwendet bei Bedarf nur die Daten eines Systems, falls das andere ausgefallen ist. Der reguläre Betrieb wird automatisch wieder aufgenommen, sobald die normale Sensorfunktionalität und die Kommunikation wiederhergestellt sind. Beachten Sie, dass bei Geräte- und Netzwerkproblemen auch Alarme (Störung) ausgelöst werden, um sicherzustellen, dass die Bediener über den Status des Systems informiert sind.

Sensor Fusion vs. Boolesche Logik

Bei Sensor Fusion handelt es sich nicht um eine boolesche Verknüpfung von Sensoren, d.h. es werden keine logischen ODER/AND/XOR/NOR-Verknüpfungen mit einzelnen Sensoralarmausgängen durchgeführt. Vielmehr werden Metadaten aus der Videoanalyse und Rohdaten von Sensoren verwendet, einschließlich Zeit, Ort und historische Werte und mittels einer ausgeklügelten KI-Technologie kombiniert. Der Fusion-Prozess bietet bessere Erkennungsmöglichkeiten und geringere Falschalarmquoten als eine boolesche Logikintegration.



Sensor Fusion Engine bei der Erkennung eines Zaunüberwindung bei Tag. In diesem Beispiel verwendet die Engine Videoaufnahmen von einer beliebigen ONVIF-kompatiblen Überwachungskamera (einschließlich Low-Light- und Thermalkameras). Die Daten einer mit Deep Learning trainierten Videoanalyse werden mit Live- und historischen Sensorreaktionsdaten von einem FlexZone-Prozessor zusammengeführt, um das Risiko (gültiger Einbruchsversuch) intelligent zu charakterisieren.

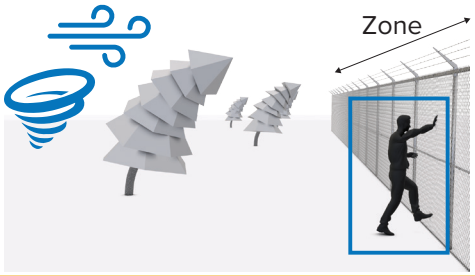
Sensor Fusion vs. Boolesche Logik

Die folgenden Szenarien zeigen Situationen, in denen das Potenzial für reelle Einbrüche als auch für Falschalarme besteht. Der Perimeter wird durch einen Zaun mit Zaunsensor und eine Kamera mit Videoanalysefunktion zur Personenverfolgung geschützt. Die Ergebnisse der Booleschen Logik und der Sensor Fusion Engine werden miteinander verglichen.

SZENARIO

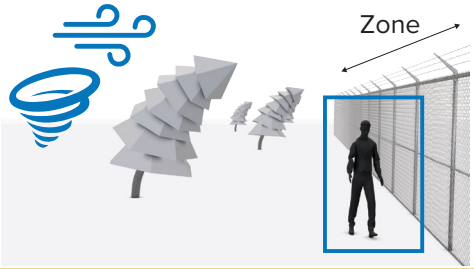
Eindringling

Ein Eindringling versucht, den Zaun in Zone 1 in der Position 30 m zu überklettern. Gleichzeitig verursacht eine Windböe mehrere Störungen am Zaun an den Positionen 10 m, 20 m und 40 m. Dies führt dazu, dass potenziell 4 Ereignisse erzeugt werden.



Fußgänger

Eine Person (kein Eindringling) geht entlang der des Zaunes bei Zone 1. Gleichzeitig verursacht eine Windböe mehrere Störungen am Zaun an den Positionen 10 m, 20 m und 40 m. Dadurch werden potenziell 4 Ereignisse ausgelöst.



Leiterüberstieg

Ein geschickter Eindringling klettert über eine Leiter. Bei dieser Art des Eindringens werden möglicherweise nicht genügend Daten gesammelt, damit ein Zaunsensor einen Alarm auslösen kann (in der Regel wird hier durch den Einsatz von Zaunauslegern mit Stacheldraht und/oder einer Kabelkonfiguration mit mehreren Sensorkabelstrecken entgegengewirkt).

VERGLEICH DER ERGEBNISSE

Boolesche Logik-Integration

Bei einer UND-Verknüpfung werden 2 Falschalarme und 1 gültiger Alarm erzeugt.

Sensor Fusion Engine

Es wird nur 1 (gültiger) Alarm erzeugt (0 Falschalarme)

Boolesche Logik-Integration

Bei einer UND-Verknüpfung werden 3 unerwünschte Alarme erzeugt. Bei einer ODER Verknüpfung werden 4 unerwünschte Alarme erzeugt.

Sensor Fusion Engine

0 unerwünschte Alarme werden erzeugt

Boolesche Logik-Integration

Bei einer UND-Verknüpfung werden 0 Alarme erzeugt (das schlechtestmögliche Ergebnis!). Bei einer ODER-Verknüpfung würde 1 (gültiger) Alarm erzeugt.

Sensor Fusion Engine

1 (gültiger) Alarm wird erzeugt

SCHLUSSFOLGERUNGEN

Diese Szenarien zeigen, dass:

- UND-Verknüpfungen sind mit einem hohen Risiko verbunden: Wenn ein Sensor aufgrund einer fehlenden Detektion oder eines Geräte-/Netzausfalls keinen Alarm auslöst, wird auch kein Alarm auf Systemebene ausgelöst
- ODER-Integrationen erhöhen die Falsch- und Störungsalarmrate, was dazu führt, dass gültige Alarme ignoriert werden können
- Sensor Fusion alarmiert nur bei relevanten Ereignissen, so dass sich der Bediener auf wichtige Aufgaben konzentrieren kann

Überlegungen zum Einsatz

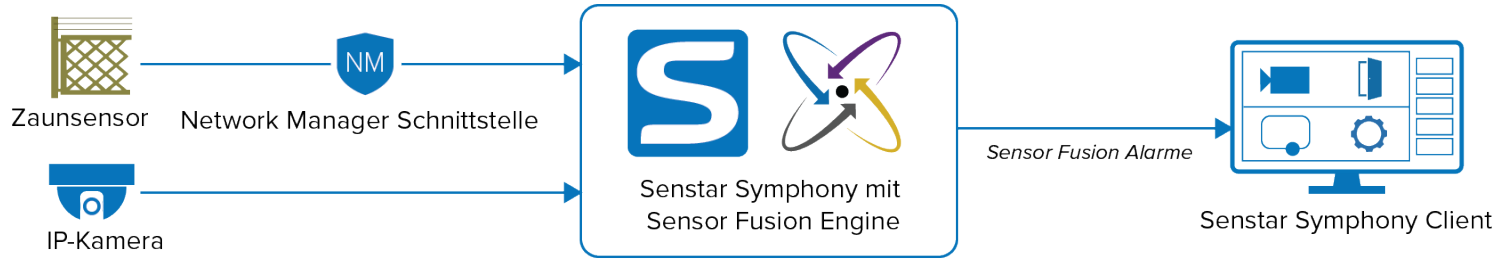
Die Sensor Fusion Engine wurde entwickelt, um spezifische Probleme im Zusammenhang mit risikoreichen oder problematischen Segmenten des Perimeters zu lösen. Sie kann auf spezifische Bereiche, einzelne Zonen oder entlang des gesamten Perimeters angewendet werden.
Je nach vorhandener Infrastruktur des Standorts kann die Sensor Fusion Engine als Teil einer vollständigen Senstar Symphony Common Operating Plattform-Lösung oder als Drop-in-Lösung eingesetzt werden, die das vorhandene Sicherheits- oder Videomanagementsystem eines anderen Anbieters (SMS/SMS) ergänzt.

Um die Sensor Fusion Engine zu implementieren, benötigt ein Standort:

- Netzwerkkameras mit Ausrichtung auf den Perimeter (bis zu 40 m pro Erfassungszone (für längere Strecken können mehrere Erfassungszonen verwendet werden)
- Einen FlexZone-60 Zaunsensor mit aktiviertem Ranging und Ethernet-Anbindung (Sterntopologie)
- Sensor Fusion Engine für jedes Kamera/Sensor-Segment aktiviert (entweder über die Senstar Symphony Common Operating Plattform Software oder über die Sensor Fusion Engine Drop-in-Lösung)

SENSTAR SYMPHONY COMMON OPERATING PLATTFORM LÖSUNG

In dieser Konfiguration wird die Sensor Fusion Engine in Senstar Symphony mit vollem Funktionsumfang eingesetzt, so dass die Bediener Sensor Fusion-Alarme zusammen mit Videos und Ereignissen von anderen Einbruchmeldesensoren, Zutrittskontrollgeräten und Videoanalysegeräten erhalten.



SENSOR FUSION ENGINE ALS DROP-IN-LÖSUNG

Bei dieser Konfiguration ist die Sensor Fusion Engine auf einer Physical Security Appliance (PSA) vorinstalliert und wird in ein vorhandenes SMS/VMS integriert. Alarme von der Sensor Fusion Engine werden über die Alarm Logic Engine (ALE) des Senstar Network Managers, die alle wichtigen SMS/VMS-Plattformen unterstützt und eine Reihe von Integrationsoptionen bietet, an das SMS/VMS weitergeleitet.

Technische Daten

	Senstar Symphony Common Operating Plattform		Drop-in-Lösung
	Serverfarm	E5000 Physical Security Appliance	(zur Verwendung mit beliebigen SMS/VMS)
DESCRIPTION			
Hardware-Plattform	R-Serie oder andere unterstützte Hardware	E5000 Physical Security Appliance	E5000 Physical Security Appliance
Senstar Symphony-Version	Standard oder Enterprise (die R-Serie umfasst Symphony-Gerätelizenzen, für andere Server Hardware sind separat zu erwerbende Lizenzen erforderlich), v8.5 oder neuer	Standard-Lizenz enthalten, v8.5 oder neuer	Keine
Artikelnummer	S8SW2091-XXY (nur Sensor Fusion Engine)	S8SW2091-XXY (nur Sensor Fusion Engine)	S8SP0303-001 (enthält PSA-Hardware und -Software)
Sensor Fusion Lizenz	1 pro Kanal (separate Lizenzen für NMS und Ranging Sensor erforderlich)	1 pro Kanal (separate Lizenzen für NMS und Ranging Sensor erforderlich)	1 pro Kanal (beinhaltet 1 Videostream und 1 Verbindung zum Ranging Sensor)
Anzahl der Sensor-Fusion-Kanäle	Abhängig von der Serverleistung	max. 4 pro Gerät	max. 4 pro Gerät
Network Manager-Lizenz	Nicht enthalten	Enthalten (v2.55 oder neuer)	Enthalten (v2.55 oder neuer)
Ranging Sensor Lizenz	Nicht enthalten	Nicht enthalten	Enthalten (1x Ranging Sensor)
Max. Zonenlänge	40 m	40 m	40 m
Unterstützter Kameratyp	Fixkamera	Fixkamera	Fixkamera
Kameraauflösung	min. 720p	min. 720p	min. 720p
Videomanagement	Ja	Ja	Nein
Zutrittskontrolle	Ja	Ja	Nein
Sicherheitsmanagement	Ja	Ja	Nein
Unterstützung zusätzliche Videoanalysen (mit Lizenz)	Ja (Anzahl abhängig Serverleistung)	Ja, bis zu 4 Videoanalysekanäle (inkl. Sensor Fusion Analyse)	Nein
ONVIF-Server	Ja	Ja	Nein
Network Manager Integrationsoptionen	Ja	Ja	Ja

Urheberrecht © 2023. Alle Rechte vorbehalten. Senstar und FlexZone sind eingetragene Marken der Senstar Corporation. Windows ist ein eingetragenes Warenzeichen der Microsoft Corporation. Senstar Symphony ist ein Warenzeichen der Senstar Corporation. R4-04/23

SENSTAR®