PSIM und Management-Systeme

Eine umfassende Übersicht

Building.
Technology.
Solutions.

messe frankfurt

Inhaltsverzeichnis

1. Was ist PSIM? 1

2. Schlüsselfunktionen von PSIM 2

2.1 Integration: PSIM-Systeme kombinieren verschiedene Sicherheitssysteme zu einer Benutzeroberfläche 2

2.2 Situationsbewusstsein: Bediener erhalten ein Echtzeitbild der aktuellen Lage 2

2.3 Automatisierung: PSIM kann vordefinierte Aktionen basierend auf bestimmten Ereignissen auslösen 3

2.4 Vorfallmanagement: Hilfe bei der Dokumentation und Verwaltung von Sicherheitsereignissen 3

2.5 Skalierbarkeit: PSIM sind für einzelne Gebäude, Industriekomplexe, als auch für ganze Städte geeignet 4

3. Arten von Managementsystemen 5

4. Installation von Managementsystemen 6

5. Der Markt 8

6. Das Angebot an PSIM und Managementsoftware für Sicherheitsanwendungen 9

6.12 Fragen an die Hersteller 9

7. Anbieter von PSIM und Managementsoftware 10

7.1 AARMTech (Indien) 10

7.2 Advancis (Deutschland) 10

7.3 American Dynamics/Johnson Controls (USA) 12

7.4 ARES Security/Vidsys (USA) 14

7.5 Bold Group (USA) 16

7.6 Eagle Eye Networks (USA) 16

7.7 Fast Systems (Schweiz) 18

7.8 Funkwerk (Deutschland) 20

7.9 Genetec (Kanada) 22

7.10 Gretsch-Unitas (Deutschland) 23

7.11 Hexagon (Schweden) 25

7.12 Hikvision (China) 27

7.13 Honeywell (USA) 27

7.14 Integrated System ISS (USA) 28

7.15 Milestone Systems (Dänemark) 28

7.16 Nanoderms (USA) 29

7.17 Network Harbor (USA) 29

7.18 Persistent Sentinel (USA) 29

7.19 Primion (Deutschland) 30

7.20 Prysm Software (Frankreich) 32

7.21 SureView Systems (USA) 33

7.22 Veracity Solutions (Schottland) 34

8. Über den Autor **35**

1. Was ist PSIM

Mit zunehmender Vernetzung und Digitalisierung werden auch die Anforderungen an Sicherheitslösungen immer komplexer. Physical Security Information Management (PSIM) und andere Managementsysteme sind unverzichtbare Werkzeuge in der modernen Sicherheitslandschaft, um den wachsenden Anforderungen gerecht zu werden. Sie bieten eine zentrale Plattform zur Integration und Steuerung verschiedener Sicherheitstechnologien, wodurch die Effizienz und Reaktionsfähigkeit erheblich verbessert wird. Durch die Automatisierung und das Situationsbewusstsein helfen sie, Bedrohungen frühzeitig zu erkennen und angemessen zu reagieren.

Dieses Whitepaper gibt einen umfassenden Überblick über PSIM und weitere sicherheitsrelevante Managementsysteme, ihre Funktionen, Vorteile und stellt führende Anbieter auf dem Markt vor.

PSIM steht für Physical Security Information Management. Es handelt sich um eine Softwareplattform, die mehrere unverbundene Sicherheitssysteme integriert und diese über eine einheitliche Schnittstelle steuert. Kurz gesagt, fungiert PSIM als das Gehirn eines Sicherheitssystems. Es sammelt Daten von verschiedenen Sicherheitsgeräten wie:

- Videokameras
- Zutrittskontrollsysteme (z.B. Kartenleser)
- Brandmeldeanlagen
- Einbruchmeldesysteme
- Sensoren und IoT-Geräte (z.B. Bewegungs- oder Temperatursensoren)

Anschließend analysiert PSIM die Daten, alarmiert das Sicherheitspersonal bei potenziellen Bedrohungen und kann automatische Reaktionen entsprechend vorbestimmter Abläufe, sogenannter Standard Operation Procedures (SOP), auslösen (z.B. Türen verriegeln, Evakuierungen veranlassen und Alarmketten auslösen).

2. Schlüsselfunktionen von PSIM

2.1 Integration: PSIM-Systeme kombinieren verschiedene Sicherheitssysteme zu einer Benutzeroberfläche

Die Integration von Daten aus der Videoüberwachung, Zugangskontrolle, Einbruchmeldeanlagen, Brandmeldesystemen oder Gebäudemanagementsystemen in eine zentrale Plattform erfolgt in der Regel über offene Schnittstellen und APIs (Application Programming Interface). PSIM-Systeme nutzen dabei standardisierte Protokolle (z. B. ONVIF, OPC, BACnet) oder herstellerspezifische APIs, um mit den verschiedenen Sicherheitssystemen zu kommunizieren. Über diese Schnittstellen werden Daten empfangen, interpretiert und in einem gemeinsamen Format dargestellt. Oft setzen PSIM-Plattformen auch Middleware ein, die als Vermittler zwischen den heterogenen Systemen fungiert. Diese Middleware übersetzt proprietäre Protokolle in ein einheitliches Datenmodell, das vom PSIM verarbeitet werden kann. Man spricht dann häufig von einer tiefen Integration dieses Herstellers bzw. von Produkten eines Herstellers.

Die empfangenen Daten aus unterschiedlichen Quellen werden im PSIM-System normalisiert, also in ein einheitliches Format überführt. Dadurch können Alarme, Statusmeldungen oder Steuerbefehle systemübergreifend verarbeitet werden. Zur Verarbeitung kann auch eine Analyse gehören, wenn ein PSIM die integrierten Datenströme analysiert und hilft Zusammenhänge zu erkennen und automatisch Aktionen einzuleiten.

2.2 Situationsbewusstsein: Bediener erhalten ein Echtzeitbild der aktuellen Lage

Eingebunden in PSIM-Systeme bieten gerade Videomanagementsysteme (VMS) visuelle Echtzeitinformationen. Die Live-Kamera-Feeds liefern sofortige visuelle Einblicke in sicherheitskritische Bereiche, damit Sicherheitsmitarbeiter genau sehen was passiert und nicht nur, dass ein Alarm ausgelöst wurde. Funktionen wie Multiscreen-Anzeige, PTZ-Steuerung (Schwenken, Neigen, Zoomen) und Heatmaps verbessern das Lagebild. PSIM-Systeme kombinieren Kamerabilder mit anderen Datenquellen wie z. B. Informationen aus der Zutrittskontrolle, Alarmmeldungen und Sensorendaten und sorgen für ein kontextreiches Gesamtbild der Situation. So wird klar, wer hat wann wo versucht, Zugang zu erhalten, welche Sensoren wurden zeitgleich ausgelöst und gibt es ungewöhnliche Muster im Verhalten? Die gesammelten Informationen werden in einer einheitlichen grafischen Oberfläche dargestellt – oft mit Karten, Dashboards und Live-Feeds – sodass das Sicherheitspersonal schnell und gezielt reagieren kann.

2.3 Automatisierung: PSIM kann vordefinierte Aktionen basierend auf bestimmten Ereignissen auslösen

PSIM-Systeme können bei bestimmten Ereignissen automatisch vordefinierte Reaktionen auslösen wie z.B. bei Zutrittsversuchen mit gesperrter Karte ein Live-Video der entsprechenden Tür anzeigen und Alarm auslösen. Das kann automatisch erfolgen, oder dem Bediener werden Schritt-für-Schritt-Anweisungen zur Reaktion auf Vorfälle gegeben („Guided Response"). Dies sorgt für standardisierte, nachvollziehbare Abläufe bei kritischen Ereignissen.

Lernende Systeme und fortschrittliche PSIMs mit KI-Unterstützung können darüber hinaus ungewöhnliches Verhalten wie z. B. das Verweilen an sensiblen Orten automatisch erkennen, Muster in Daten identifizieren (z. B. wiederkehrende Vorfälle) und helfen so Abläufe zu optimieren.

Eine systemübergreifende Steuerung innerhalb des PSIM erlaubt auch die automatisierte Steuerung anderer Systeme und Subsysteme bei einem Vorfall. So kann beispielsweise bei einem erkannten Einbruch das Licht eingeschaltet und die Türen verriegelt werden. Die Polizei wird benachrichtigt und Kameras werden fokussiert.

2.4 Vorfallmanagement: Hilfe bei der Dokumentation und Verwaltung von Sicherheitsereignissen

Das Vorfallmanagement in einem PSIM-System ist ein zentraler Bestandteil seiner Funktion. Es ermöglicht Sicherheitsorganisationen, Sicherheitsereignisse effizient zu erkennen, bewerten, steuern und dokumentieren. Wenn ein Vorfall erkannt wird wie z. B. eine Türöffnung außerhalb der Dienstzeit, ein Feueralarm oder ein Eindringversuch, erzeugt das System ein „Event". Für jeden Vorfalltyp sind standardisierte Reaktionspläne (SOPs) interlegt. Das System leitet den Operator Schritt für Schritt durch die richtige Reaktion (z. B. Kameraansicht öffnen, Polizei verständigen, Evakuierung einleiten), wobei manche Reaktionen automatisiert werden können. Das System dokumentiert automatisch, wer was wann getan hat und ermöglicht die Kommunikation mit externen Stellen und internen Teams. Eskalationen werden ausgelöst, wenn keine Reaktion innerhalb einer definierten Zeit erfolgt.

Jeder Vorfall wird umfassend protokolliert (inkl. Videos, Systemdaten, Maßnahmen), Berichte können dabei automatisch erstellt und für Audits oder Auswertungen genutzt werden. In der Nachbearbeitung („Post-Incident Review") können nach Abschluss des Vorfalls wichtige Erkenntnisse („Lessons Learned") dokumentiert werden. Intelligente Systeme unterstützen so bei der Analyse von Schwachstellen oder der Optimierung von SOPs.

2.5 Skalierbarkeit: PSIM sind für einzelne Gebäude, Industriekomplexe, als auch für ganze Städte geeignet

Die Skalierbarkeit eines PSIM-Systems ist einer seiner größten Vorteile – besonders in komplexen, heterogenen oder stark wachsenden Sicherheitsinfrastrukturen. Gute Systeme sind horizontal skalierbar, das heißt, ein PSIM kann an mehreren Standorten (z. B. Filialen, Niederlassungen, Produktionsstätten) gleichzeitig eingesetzt werden und neue Standorte oder Systeme lassen sich einfach in die bestehende Architektur integrieren, ohne das System neu aufsetzen zu müssen. Die meisten Systeme sind auch modular aufgebaut, sodass man neue Funktionalitäten nach Bedarf hinzufügen kann.

3. Arten von Managementsystemen

Neben PSIM gibt es eine Vielzahl weiterer Managementsysteme, die spezifische Sicherheitsanforderungen erfüllen. Dazu gehören unter anderem:

- Video Management Systeme (VMS): Diese Systeme verwalten und steuern die Videoüberwachung.
- Zutrittskontrollsysteme: Sie regeln den Zugang zu verschiedenen Bereichen eines Gebäudes.
- Alarmmanagementsysteme: Diese Systeme überwachen und verwalten Alarme aus verschiedenen Quellen.

4. Installation von Managementsystemen

Ob im PSIM- und Managementsysteme am besten in der Cloud oder On-Premise installiert werden, hängt stark von den Anforderungen, der IT-Infrastruktur und dem Sicherheitsniveau der Organisation ab. Beide Modelle haben klare Vor- und Nachteile.

Vergleich: Cloud vs. On-Premise im PSIM-Umfeld

Kriterium	Cloud-Lösung	On-Premise-Lösung
Installationsaufwand	Gering (bereitgestellt durch Anbieter)	Hoch (eigene Server, Netzwerk, Konfiguration)
Skalierbarkeit	Hoch – neue Standorte/Systeme leicht integrierbar	Eingeschränkt – physische Hardware begrenzt
Kosten	OPEX (monatliche/jährliche Gebühren)	CAPEX (hohe Anfangsinvestitionen)
IT-Personalbedarf	Gering – Wartung durch Anbieter	Hoch – eigene IT-/Sicherheitsabteilung notwendig
Updates & Wartung	Automatisch durch Anbieter	Manuell, oft mit Ausfallzeiten verbunden
Datensicherheit & DSGVO	Abhängig vom Anbieter & Region	Volle Kontrolle über alle Daten
Verfügbarkeit	Hoch – redundante Cloud-Rechenzentren	Abhängig von lokaler IT-Infrastruktur
Konnektivität	Internetverbindung zwingend notwendig	Kann auch offline betrieben werden
Kritische Infrastruktur	Nicht immer erlaubt (z. B. Behörden, Militär)	Standard bei Hochsicherheitsbereichen

Wann ist On-Premise besser?

Für Betreiber kritischer Infrastruktur, Betreiber, die die volle Datenhoheit behalten wollen, deren Standorte keine stabile Internetanbindung haben oder die keine Abhängigkeit vom Anbieter oder der Cloud wünschen.

Wann ist die Cloud besser?

Eine Cloud-Installation erhöht die Flexibilität und lässt sich schnell skalieren. Sie bietet auch Vorteilen, wenn ein Unternehmen verteilte Standorte oder ein zentrales Lagezentrum hat. Die Einstiegskosten sind geringer und es wird weniger IT-Personal gebraucht. Manche KI-gestützten PSIM-Funktionen sind cloudbasiert.

Hybrides Modell – der Mittelweg

Viele Unternehmen und Organisationen gehen mittlerweile den hybriden Weg, d. h. lokale Datenverarbeitung und Datenspeicherung On-Premise (z. B. Videodaten, Zutritt) und eine zentrale Steuerung, Analyse, Reporting über die Cloud.

Fazit: Für kleinere bis mittelgroße, dynamische Organisationen ist die Cloud oft praktischer. Für große, sicherheitskritische Organisationen mit hohen Compliance-Anforderungen ist On-Premise häufig die bessere Wahl und ein hybrides Modell bietet bei guter Installation und Konfigurierung das Beste aus beiden Welten.

5. Der Markt

Der globale Markt für die gesamte IoT in gewerblichen Gebäuden (Building IoT/BIoT) Gebäuden wird voraussichtlich von 64,1 Milliarden USD im Jahr 2024 auf 101,0 Milliarden USD im Jahr 2030 wachsen, was einer durchschnittlichen jährlichen Wachstumsrate von 7,87 % im Basisszenario entspricht.

Memooris neuer Bericht „IoT Platforms in Smart Commercial Buildings 2025 to 2030", liefert hier nützliche Informationen zu diesem sich schnell entwickelnden Ökosystem.

Der weltweite Umsatzmarkt für Sicherheitssoftware erreichte im Jahr 2023 einen Spitzenwert von über 82 Milliarden US-Dollar. Dies entspricht einem Anstieg von 13,4 Prozent im Vergleich zum Vorjahr. In dieser Zahl ist allerdings auch Software für IT-Sicherheit enthalten.

Nach einer Studie von Markets and Markets soll die Größe des globalen PSIM-Marktes von USD 3,5 Milliarden im Jahr 2024 auf USD 4,3 Milliarden bis 2029 mit einer jährlichen Wachstumsrate von 4,6 % steigen. Die Nachfrage nach PSIM-Lösungen wächst aufgrund der Notwendigkeit, Organisationen gegen zunehmend ausgeklügelte Bedrohungen zu schützen. Die Konvergenz von Cyber- und physischen Risiken treibt diese Entwicklung weiter voran.

Mordor Intelligence schätzt die Größe des globalen Marktes für physisches Sicherheitsinformationsmanagement im Jahr 2024 auf 1,66 Milliarden US-Dollar. Der Markt soll bis 2029 3,53 Milliarden US-Dollar erreichen, was einem durchschnittlichen jährlichen Wachstum von 16,24 % im Prognosezeitraum (2024–2029) entspricht.

6. Das Angebot an PSIM und Managementsoftware für Sicherheitsanwendungen

Will man das umfassende Angebot an Software für das Sicherheitsmanagement näher analysieren, muss man die Systeme der einzelnen Anbieter im Detail betrachten. Die folgende Übersicht erklärt das Angebot vieler führender Anbieter, ohne einen Anspruch auf Vollständigkeit zu erheben. Der Autor hat eine Auswahl führender Anbieter im Vorfeld kontaktiert und um Beantwortung der Fragen gebeten. Die Antworten der Hersteller, die gefragt wurden und geantwortet haben, sind in diesem Kapitel aufgeführt. Zunächst werden die Hersteller vorgestellt und das Angebotsspektrum der Anbieter erläutert, bevor die Antworten der Anbieter auf die folgenden Fragen zusammengefasst werden.

6.1 Fragen an die Hersteller

Um ein besseres Verständnis für die Fähigkeiten und Einsatzmöglichkeiten von PSIM- und anderen Managementsystemen im Sicherheitsbereich zu bekommen, wurden führende Anbieter gebeten, folgende Fragen zu beantworten:

- Sehen Sie Ihr(e) System(e) als übergreifendes PSIM oder eher als integraler Baustein von PSIM-Systemen?
- Was leisten Ihr(e) System(e) bezogen auf die Integration von Sicherheitskomponenten und wo liegen die Hauptvorteile?
- Welche Anwender benötigen ein PSIM-System und wer ist mit Managementsystemen besser bedient, die Teilbereiche abdecken?
- Für welche Zielgruppe (Unternehmensgröße, Branche, Komplexität der Installation) eignet sich ihr System am besten bzw. wo kann es seine Stärken am besten ausspielen?
- Welchen Rat würden Sie Anwendern geben, die über eine Neueinführung eines PSIM-Systems nachdenken?
- Welchen Rat würden Sie Anwendern geben, die ihr PSIM auswechseln möchten?

7. Anbieter von PSIM und Managementsoftware

7.1 AARMTech (Indien)

AARMTech mit Hauptsitz in Indien bietet eine Softwareplattform für physisches Sicherheitsinformationsmanagement (PSIM) an, die verschiedene Sicherheitssystemmodule integriert, darunter Zugangskontrolle, Überwachung, Brandmelder, Straßensperren und Perimetersicherheit. Die PSIM-Lösung von AARMTech bietet eine effektive Lösung für die Verwaltung von Sicherheitsabläufen in Kontrollräumen, die große Datenmengen verarbeiten. Die Plattform umfasst mehrere Module, die funktionale Erweiterungen für bestimmte Designbereiche ermöglichen, wie beispielsweise Schaltungssimulation, und verfügt über eine umfassende Schnittstelle zur Erfassung von Schaltplänen. Ihre Simulationsalgorithmen basieren auf Knotenanalyse und Trapezregelintegration. Darüber hinaus steigert die Software die Produktivität durch die Unterstützung von Modulen, die speziell für das Informationsmanagement in bestimmten Branchen entwickelt wurden. Die Integration mit Perimeter Intrusion Protection, GIS-Kartierung und anderen Netzwerken – wie Command and Control-Systemen, Telefonie und Funkkommunikation – ermöglicht die Erstellung robuster, maßgeschneiderter Sicherheits- und Kontrolllösungen, die alle über ein einheitliches Bedienfeld verwaltet werden.

7.2 Advancis (Deutschland)

Advancis bietet mit WinGuard eine umfassende Lösung für Physical Security Information Management (PSIM). Die offene Integrationsplattform ermöglicht die zentrale Verwaltung und Steuerung verschiedener Sicherheits-, Gebäude- und Kommunikationssysteme. WinGuard integriert zudem IT-Infrastruktur sowie Einsatzleit- und Ticketing-Systeme. Das System sammelt Ereignisse aus verbundenen Anlagen und visualisiert sie intelligent, um dem Anwender die Situationserkennung zu erleichtern. Dynamische Anweisungen und automatische Aktionen unterstützen den Anwender in der Leitstelle.

Sehen Sie Ihr System als übergreifendes PSIM-System oder eher als integralen Baustein von PSIM-Systemen?

Unser System WinGuard ist ganz klar als übergreifendes PSIM-System konzipiert. Das bedeutet: Wir bieten keine Einzellösung für beispielsweise Video oder Zutritt, sondern eine herstellerneutrale Plattform, die verschiedenste sicherheits- und gebäudetechnische Systeme in einer zentralen Oberfläche zusammenführt. WinGuard fungiert als übergeordnetes Managementsystem, das die einzelnen Subsysteme nicht ersetzt, sondern deren Funktionen intelligent verknüpft, visualisiert und prozessorientiert nutzbar macht. Dabei steht nicht nur die technische Integration im Vordergrund, sondern auch die operative Effizienz – also wie Informationen intelligent und nutzerfreundlich dargestellt und wie Abläufe im Ereignisfall geführt und dokumentiert werden. Damit positionieren wir WinGuard bewusst als zentrale Plattform im Sinne eines echten PSIM-Systems – also nicht als Baustein in einem PSIM, sondern als dessen Kern.

Welche Leistungen erbringen Ihr System in Bezug auf die Integration von Sicherheitskomponenten und wo liegen die Hauptvorteile?

WinGuard sammelt die Ereignisse aus den unterschiedlichen angebundenen Anlagen und Systemen. Eine intelligente Visualisierung dieser Ereignisse, dynamische Verfahrensanweisungen sowie automatisch im Hintergrund ablaufende Aktionen unterstützen und entlasten sodann den Anwender in der Leitstelle. Damit werden die komplexen Arbeitsabläufe erheblich vereinfacht und der Anwender wird in die Lage versetzt, auftretende Situationen vollständig zu erfassen und optimal zu lösen. Derzeit stehen über 550 Schnittstellentreiber zu verschiedensten Anlagen der Sicherheits-, Gebäude- und Kommunikationstechnik, darunter auch zu Anlagen aus den Bereichen IoT und Robotik und Drohnen (UAV) zur Verfügung. Darüber hinaus ist die Entwicklung neuer Schnittstellen ebenfalls möglich. Durch diese Herstellerneutralität und die offene Architektur kann die gesamte technische Infrastruktur eines Gebäudes mit WinGuard visualisiert und gesteuert werden.

Welche Anwender benötigen ein PSIM-System und welche sind mit Managementsystemen, die Teilbereiche abdecken, besser bedient?

Ein PSIM-System wie WinGuard kommt immer dann zum Einsatz, wenn eine Vielzahl unterschiedlicher sicherheitsrelevanter Systeme in einer zentralen Plattform integriert und übergreifend gesteuert werden soll. Das betrifft vor allem Anwender mit komplexen Infrastrukturen – zum Beispiel Betreiber von Flughäfen, kritischen Infrastrukturen, Industrieunternehmen mit Werkschutz, Rechenzentren oder öffentliche Einrichtungen. Diese Organisationen setzen meist eine Vielzahl heterogener Systeme ein – wie Videoüberwachung, Zutrittskontrolle, Einbruch- und Brandmeldeanlagen, Gebäudeautomation oder auch Kommunikationssysteme. Ein PSIM-System führt diese Welten zusammen, schafft Transparenz und ermöglicht es dem Bediener, in kritischen Situationen schnell und standardisiert zu reagieren.

Für Anwender, bei denen nur wenige Teilsysteme vorhanden sind oder deren Anforderungen rein operativ oder technisch weniger komplex sind, kann ein spezialisiertes Managementsystem – z. B. ein reines Videomanagement- oder Zutrittskontrollsystem – die wirtschaftlich sinnvollere Lösung sein. Diese Systeme sind oft auf eine spezifische Funktion optimiert und bieten genau dort sehr gute Leistungen. Der entscheidende Faktor ist nicht die Anzahl der Systeme allein, sondern auch die Frage, wie stark Prozesse automatisiert, standardisiert und zentralisiert werden sollen – und welche Rolle z. B. Compliance, Dokumentation und Interoperabilität spielen. Ein PSIM ist kein Ersatz für Fachsysteme, sondern die zentrale, übergeordnete Plattform, die deren Potenziale im Verbund nutzbar macht.

Für welche Zielgruppe (Unternehmensgröße, Branche, Komplexität der Installation) eignet sich Ihr System am besten bzw. wo kann es seine Stärken am besten ausspielen?

Abgesehen von der Industrie, dem Finanz- und Verwaltungsbereich, Rechenzentren, Justizvollzugs- und forensischen Einrichtungen, dem Transport- und Verkehrswesen, Gesundheitswesen oder militärischen Einrichtungen wird WinGuard in vielen weiteren Branchen genutzt, z. B. in Freizeitparks, Stadien oder in Museen. Neben speziellen Lösungen für unterschiedliche Branchen ermöglichen offene Schnittstellen und die Zusammenarbeit mit anderen Unternehmen die Erweiterung des Systems sowie die Abdeckung weiterer Anwendungsfälle. Dabei ist WinGuard vom Einplatzsystem bis zu international vernetzten Leitstellen skalierbar und kann jederzeit um zusätzliche Server und Bedienplätze, Funktionsmodule und Schnittstellen erweitert werden.

Welchen Rat würden Sie Anwendern geben, die über eine Neueinführung eines Managementsystems nachdenken?

Unser Rat lautet: Denken Sie prozessorientiert und langfristig. Analysieren Sie sorgfältig, welche einzelnen Gewerke und Systeme integriert werden sollen, welche Prozesse unterstützt werden müssen und wie skalierbar die Lösung zukünftig sein sollte. Achten Sie auf herstellerunabhängige Plattformen mit offener Architektur, um Flexibilität und Unabhängigkeit zu gewährleisten. Zudem sollten alle relevanten Stakeholder frühzeitig eingebunden werden – von der IT-Abteilung über das Gebäudemanagement bis hin zur Leitstelle.

Welchen Rat würden Sie Anwendern geben, die ihr Managementsystem ersetzen möchten?

Sie sollten genau prüfen, welche Schwachstellen das bestehende System hat und was im neuen System verbessert werden soll. Wichtig ist ein klarer Migrationsplan, um Ausfallzeiten zu vermeiden. Setzen Sie auf eine flexible, offene Plattform mit breiter Schnittstellenunterstützung – so können vorhandene Systeme weiter genutzt oder bei Bedarf schrittweise integriert werden.

7.3 American Dynamics / Johnson Controls (USA)

American Dynamics, eine Marke von Tyco Security Products (jetzt Teil von Johnson Controls), bietet eine umfassende Palette an physischen Sicherheitslösungen. Obwohl diese traditionell nicht unter PSIM (Physical Security Information Management) eingeordnet werden, bieten ihre Produkte Funktionen, die eng mit den Zielen von PSIM übereinstimmen. Der Victor Unified Client ist die Flaggschiff-Plattform von American Dynamics, die entwickelt wurde, um Videoüberwachung, Zugangskontrolle und andere Sicherheitssysteme in einer einzigen, einheitlichen Schnittstelle zu vereinen.

Sehen Sie Ihre Systeme als übergreifende PSIM oder eher als integralen Baustein von PSIM-Systemen?

Die Antwort auf diese Frage hängt von den Anwendungsanforderungen des Kunden ab. Ein PSIM kann für verschiedene Menschen unterschiedliche Bedeutungen haben. Der Victor-Client von American Dynamics kann in beiden Bereichen eingesetzt werden. Er kann sowohl ein PSIM als auch ein integraler Bestandteil eines PSIM sein. Wir sagen das, weil der Victor-Client flexibel in seiner Anwendung und Bereitstellung ist. Die Abgrenzung hängt von den anderen Systemen ab, mit denen er integriert wird. Der Sinn eines PSIM oder einer integrierten Sicherheitslösung besteht darin, eine Sammlung von Sicherheits-, Lebensrettungs- und Gebäudemanagementsystemen zusammenzuführen und mindestens eine einzige Schnittstelle für die Mitarbeiter des Sicherheitszentrums bereitzustellen, über die sie aus Sicht der Lageerkennung interagieren können, zusätzlich zur Erleichterung von Aktions-/Reaktionsszenarien über mehrere unterschiedliche Systeme hinweg. Beispielsweise löst ein Feueralarm ein Ereignis aus, um die Karte des Brandbereichs aufzurufen und die lokalen Kameras zu aktivieren, um zu sehen, was passiert. Außerdem können dieselben Informationen bei der nachträglichen Bewertung eines Ereignisses bereitgestellt werden.

Wenn das vorherrschende Ökosystem für Brand, Einbruch, BMS und Zugangskontrolle aus dem JCI-Portfolio oder von einem der strategischen Partner von JCI stammt, bietet der Victor-Client PSIM-Funktionalität. Wenn die installierten Systeme sehr unterschiedlich sind und nicht von einem einzigen Hersteller oder wenigen Herstellern stammen, ist ein übergreifendes PSIM unerlässlich, um eine zentrale Überwachungsfunktion bereitzustellen.

Welche Leistungen erbringen Ihre Systeme in Bezug auf die Integration von Sicherheitskomponenten und wo liegen die Hauptvorteile?

Der Victor-Client von American Dynamics ist in erster Linie ein Videomanagementsystem, das mit unseren eigenen Produkten und strategischen Drittanbietern integriert werden kann. Die Integrationsliste findet man auf unserer Webseite.

Aufgrund der Flexibilität und Skalierbarkeit des Victor VMS kann die angebotene Lösung bei Einbeziehung der Integrationen vielfältig sein. Letztendlich kann die Lösung daher auf der Grundlage von Video allein Situationsbewusstsein bieten (die richtigen Informationen zur richtigen Zeit an die richtige Person liefern, damit diese ihre Aufgaben genau und effizient ausführen kann) oder mit Integrationen wie Zugangskontrolle, Brandschutz und Einbruchschutz wird die Lösung ganzheitlicher und erleichtert die „Single Pane of Glass"-Philosophie: ein

einziger Punkt, an dem die Informationen präsentiert werden, damit sich der Bediener auf einen einzigen Kunden konzentrieren kann.

Welche Anwender benötigen ein PSIM-System und welche sind mit Managementsystemen, die Teilbereiche abdecken, besser bedient?

Dies hängt von den betrieblichen Anforderungen des Endnutzers ab. Ein PSIM eignet sich insbesondere für Kunden, die über mehrere VMS-, Brandmelde- und Einbruchmeldesysteme usw. verfügen. Die Aufgabe des PSIM besteht dann darin, letztlich als Frontend für all diese unterschiedlichen Systeme verschiedener Hersteller zu fungieren. Wenn die Produktumfrage entweder vollständig intern durchgeführt wird oder die Produkte von strategischen Partnerherstellern stammen, kann der Victor-Client als Frontsystem fungieren und die Aktionen/Reaktionen über die Systeme hinweg verwalten.

Für welche Zielgruppe (Unternehmensgröße, Branche, Komplexität der Installation) eignet sich Ihr System am besten bzw. wo kann es seine Stärken am besten ausspielen?

Der Victor-Client wird in der Regel, wenn auch nicht ausschließlich, von Unternehmenskunden, kritischen Infrastrukturen, Finanzinstituten und ähnlichen Einrichtungen genutzt. Ebenso kann er in kleineren Installationen eingesetzt werden. Der Schlüssel liegt in der Skalierbarkeit der Plattform. Die größte Stärke ist der lösungsorientierte Ansatz bei der Produktentwicklung und die Fähigkeit, das bereits erwähnte hohe Maß an Situationsbewusstsein zu bieten. Darüber hinaus gibt es die intrinsischen Funktionen, die ein hohes Maß an Redundanz ermöglichen (unverzichtbar für kritische Infrastrukturen), den offenen Plattformansatz für Integrationen; ebenso wichtig ist, dass das Kundenfeedback die Produktentwicklung vorantreibt.

Welchen Rat würden Sie Anwendern geben, die über eine Neueinführung eines Managementsystems nachdenken?

Recherchieren, recherchieren, recherchieren! Machen Sie sich klar, was die Anforderungen und Erwartungen sind. Die Integration unterschiedlicher Systeme ist eine Herausforderung. Daher müssen Sie wissen, wie die Richtlinien des PSIM-Anbieters hinsichtlich der Aktualisierung seines Produkts im Verhältnis zur Aktualisierung der integrierten Produkte durch deren Hersteller aussehen. Ein PSIM ist nicht immer erforderlich. Eine Lösung eines einzigen Anbieters für Sicherheit, Lebensschutz und Gebäudemanagement kann oft die erforderliche Funktionalität bieten, ohne dass zusätzliche Kosten für ein PSIM anfallen. Ermitteln Sie die laufenden Kosten für SSAs und Software-Updates.

Welchen Rat würden Sie Anwendern geben, die ihr Managementsystem ersetzen möchten?

Im Grunde genommen gilt dasselbe wie in der obigen Frage. Seien Sie auch realistisch in Bezug auf die Anforderungen: Wenn das Managementsystem ersetzt wird, ältere Sicherheits-/Lebensschutzprodukte jedoch nicht, kann dies zu Integrationsproblemen führen. Stellen Sie fest, welche Systeme das neue Managementsystem in Bezug auf Produktintegrationen unterstützen kann. Gehen Sie nicht davon aus, dass ein Managementsystem mit einem bestimmten Protokoll, beispielsweise BACnet, mit einem anderen BACnet-System kompatibel ist. Testen und überprüfen Sie dies.

7.4 ARES Security/Vidsys (USA)

ARES Security ist ein führender Anbieter von Sicherheitssoftware und Entwickler der Enterprise Security Platform, die sich in zahlreichen Branchen als kostensenkend und effektivitätssteigernd bewährt hat. Die Avert-Software wurde 1999 in Zusammenarbeit mit der Defense and Threat Reduction Agency zum Schutz der nuklearen Anlagen der USA entwickelt. Seitdem schützt die Lösung die wichtigsten Anlagen des Landes. Im Jahr 2012 wurde ARES Security gegründet, um Avert zu kommerzialisieren und seine Funktionen zu erweitern.

ARES Security ist durch eine Reihe von Übernahmen und Weiterentwicklungen gewachsen und bietet nun eine umfassende Suite von Lösungen, die den Sicherheits- und Schutzmaßnahmen jedes Unternehmens zugutekommen. Das Unternehmen stärkte seine Position im PSIM-Bereich durch den Erwerb von Vermögenswerten und Verträgen von Vidsys mit Sitz in Wien. Vidsys, jetzt ein Unternehmen von ARES Security, bietet missionskritische PSIM-Software (Physical Security Information Management) für Regierungsbehörden, Unternehmen, Transportunternehmen und andere bedeutende Einrichtungen in Nordamerika, dem Nahen Osten und im asiatisch-pazifischen Raum.

Sehen Sie Ihre Systeme als übergreifende PSIM oder eher als integralen Baustein von PSIM-Systemen?

Die Enterprise Security Platform (ESP) von ARES Security ist eine übergreifende Lösung, die weit über die traditionellen Grenzen des physischen Sicherheitsinformationsmanagements hinausgeht. Sie ist als umfassendes anwendungsbasiertes Ökosystem konzipiert, das unterschiedliche Subsysteme für Sicherheit, Schutz, Reaktion und Gebäudemanagement vereint. Die ESP ist als zentrale Intelligenzschicht konzipiert und bietet fortschrittliche Funktionen wie digitale Zwillingmodellierung, KI-gestützte Analysen und autonome Roboteroperationen – all dies erweitert ihren Wert über den eines typischen PSIM-Systems hinaus.

Welche Leistungen erbringen Ihre Systeme in Bezug auf die Integration von Sicherheitskomponenten und wo liegen die Hauptvorteile?

Das ESP bietet eine nahtlose Integration mit über 450 Sicherheits-, Gebäudeinformations- und Erkennungssystemen – darunter Zugangskontrolle, Einbruchserkennung, Videoüberwachung, Brandmelder, Notfallkommunikation und Gebäudeautomation. Diese Integrationen werden durch eine vom Benutzer konfigurierbare Schnittstelle ergänzt, die Warnmeldungen, Arbeitsabläufe und automatisierte Reaktionen in einer einzigen Übersicht zusammenfasst.

Welche Anwender benötigen ein PSIM-System und welche sind mit Managementsystemen, die Teilbereiche abdecken, besser bedient?

Organisationen mit komplexen oder groß angelegten Abläufen – wie kritische Infrastrukturen, Behörden, Unternehmensstandorte, Flughäfen und Versorgungsunternehmen – profitieren am meisten von einem echten PSIM-System. Diese Nutzer verwalten in der Regel zahlreiche unterschiedliche Systeme an mehreren Standorten und benötigen eine einheitliche Übersicht, eine schnelle Bedrohungsanalyse und koordinierte Reaktionsmöglichkeiten. Umgekehrt können kleinere Einrichtungen mit begrenzten Integrationsanforderungen oder statischen Sicherheitsumgebungen mit Teilbereichsmanagementsystemen auskommen. Mit der Weiterentwicklung der Risiken und der Technologie benötigen viele Organisationen jedoch die Skalierbarkeit und Ausfallsicherheit, die eine PSIM-Plattform bietet.

Die Enterprise Security Platform (ESP) von verfügt über eine integrierte Datenföderation und umfassende Unterstützung für Standardarbeitsanweisungen, die vollständig auf bestehende Richtlinien zum Informationsaustausch und organisatorische Hierarchien abgestimmt sind. Dieses anpassungsfähige Framework

ermöglicht es der Plattform, sich effizient an die sich ändernden Anforderungen eines Unternehmens anzupassen – von lokalen Bereitstellungen bis hin zu unternehmensweiten Implementierungen in globalen Betrieben.

Für multinationale oder geografisch verteilte Kunden ermöglicht die Architektur von ESP einzelnen Standorten oder Einrichtungen einen unabhängigen Betrieb unter Verwendung maßgeschneiderter Integrationen und Funktionen, die speziell auf ihren Betriebskontext zugeschnitten sind. Diese dezentralen Implementierungen sind zentral miteinander verbunden und ermöglichen eine Überwachung auf Führungsebene über ein einheitliches Dashboard, das unternehmensweite Transparenz bietet und gleichzeitig die Autonomie auf Standortebene bewahrt. Diese Architektur unterstützt auch erweiterte Sicherheitsfunktionen für den Datenaustausch zwischen mehreren Behörden, sodass Kunden die Sicherheit an die (öffentlichen und privaten) Vereinbarungen zwischen den Behörden anpassen können, einschließlich ereignis- und regelbasiertem Datenaustausch.

Für welche Zielgruppe (Unternehmensgröße, Branche, Komplexität der Installation) eignet sich Ihr System am besten bzw. wo kann es seine Stärken am besten ausspielen?

Die Enterprise Security Platform eignet sich am besten für mittelständische bis große Unternehmen, die in risikoreichen, stark regulierten oder logistisch komplexen Umgebungen tätig sind. Dank der effektiven Skalierbarkeit der Plattform kann die Lösung jedoch auch von kleineren Behörden oder Organisationen genutzt werden. Die Stärke von ESP liegt in seiner Anpassungsfähigkeit. Es kann schrittweise oder als unternehmensweite Plattform eingesetzt werden und ist besonders wertvoll, wenn integrierte Kommandozentralen, fortschrittliche Analysen oder autonome Operationen (z. B. Drohnen- oder Roboterpatrouillen) gewünscht sind.

Welchen Rat würden Sie Anwendern geben, die über eine Neueinführung eines Managementsystems nachdenken?

Bei der Einführung eines neuen Managementsystems sollten Anwender zunächst ein klares Verständnis ihrer langfristigen operativen Ziele und Risikoprofile entwickeln. Es ist unerlässlich, eine Plattform zu wählen, die offen und skalierbar ist und bestehende sowie zukünftige Systeme integrieren kann. Dabei ist es entscheidend, benutzerfreundliche Oberflächen zu priorisieren, die eine schnelle Einarbeitung ermöglichen und eine intuitive Bedienung bieten. Suchen Sie außerdem nach Lösungen, die Automatisierung, Simulation und Notfallübungen unterstützen, um die Bereitschaft sicherzustellen. Es ist wichtig, nicht nur die aktuellen Anforderungen zu berücksichtigen, sondern auch die Zukunftsfähigkeit der Lösung – insbesondere angesichts des zu erwartenden Wachstums von KI, Robotik und Digital-Twin-Technologien.

Welchen Rat würden Sie Anwendern geben, die ihr Managementsystem ersetzen möchten?

Für diejenigen, die ältere Managementsysteme ersetzen, ist es von entscheidender Bedeutung, die Datenkontinuität und die Integration in die bestehende Infrastruktur sicherzustellen. Bei der Bewertung von Anbietern ist es wichtig, deren bewährte Interoperabilität und zukunftsorientierte Innovationskraft zu berücksichtigen. Es ist ratsam, Einheitslösungen zu vermeiden und sich stattdessen für modulare Architekturen zu entscheiden, die mit dem Wachstum des Unternehmens mitwachsen können. Eine sorgfältige Planung des Änderungsmanagements, einschließlich Anwenderschulungen und einer schrittweisen Implementierung, ist erforderlich. Die Gelegenheit zum Austausch des Systems kann dazu beitragen, die Abläufe zu vereinheitlichen und die allgemeine Ausfallsicherheit zu erhöhen. Die Enterprise Security Platform zeichnet sich durch den Übergang von isolierten Systemen zu integrierten Sicherheitsökosystemen aus und bietet robuste Migrationsunterstützung und umfassende Kompatibilität mit Drittanbietern.

7.5 Bold Group (USA)

Seit über 40 Jahren bedient die Bold Group die Sicherheits- und Alarmbranche mit einem umfassenden Angebot an Alarmüberwachungs- und integrierten Finanz- und Unternehmensmanagementlösungen. Diese Lösungen sind speziell darauf ausgelegt, eine optimale Geschäftsleistung für zentrale Überwachungsstationen, Händler und Integratoren zu erzielen. Die Bold Group wurde im März 2019 durch die operative Fusion von Perennial Software, Bold Technologies, SIMS und Secure Global Solutions (SGS) gegründet und ist als zuverlässiger Anbieter von unternehmenskritischer Alarmüberwachungs- und Finanzmanagementtechnologie in der Branche anerkannt. Das Unternehmen bietet flexible, automatisierte Lösungen, die Kundenworkflows optimieren, die Effizienz steigern und konsistente Prozesse gewährleisten. Diese Funktionen ermöglichen kritische Reaktionsdienste, die Leben und Eigentum schützen.

Das Produktportfolio der Bold Group umfasst renommierte Alarmüberwachungssysteme wie Manitou, stages und SIMS. Diese fortschrittlichen Systeme werden durch erstklassige Buchhaltungs- und Unternehmensmanagementsysteme wie SedonaOffice und AlarmBiller ergänzt. Die umfassende Lösungssuite wird durch ein Netzwerk aus strategischen Partnerschaften, technischem Support und umfangreichen Weiterbildungsprogrammen unterstützt.

7.6 Eagle Eye Networks (USA)

Eagle Eye Networks ist ein weltweit führender Anbieter von Cloud-Videoüberwachung und stellt eine offene Cloud-Plattform zur Verfügung, die künstliche Intelligenz integriert und dadurch die Funktionalität von Videoüberwachungssystemen erweitert. Durch den Einsatz von Video-KI unterstützt das System Kommunen und Unternehmen bei der Optimierung ihrer Geschäftsabläufe und ihres Kundenservice. Herstellern wird zudem ermöglicht, Produkte unter verbesserten Sicherheitsbedingungen und in höherer Qualität zu fertigen.

Die zu 100 Prozent cloudbasierten Lösungen von Eagle Eye sind intelligent, einfach und sicher. Das Eagle Eye Cloud VMS (Video Management System) ist robust und flexibel genug ist, um die Zukunft der Videoüberwachung und -intelligenz voranzutreiben. Es wurde speziell für die Cloud und KI entwickelt und erfüllt die Sicherheitsanforderungen der Kunden mit unbegrenzter Skalierbarkeit, flexiblen Preisplänen, einer Vielzahl fortschrittlicher Analysen und einer offenen RESTful-API-Plattform für unbegrenzte Anpassungsmöglichkeiten. Eagle Eye wurde 2012 gegründet und hat seinen Hauptsitz in Austin, Texas, sowie Niederlassungen in Amsterdam, Bangalore und Tokio.

Sehen Sie Ihre Systeme als übergreifende PSIM oder eher als integralen Baustein von PSIM-Systemen?

Eagle Eye Networks bietet ein cloudbasiertes Videomanagementsystem (VMS) an, das als Schlüsselkomponente innerhalb eines PSIM-Frameworks fungiert. Es fungiert nicht als vollständiges PSIM, lässt sich jedoch über offene APIs und branchenübliche Protokolle problemlos mit PSIM-Plattformen und anderen Sicherheitstechnologien verbinden.

Welche Leistungen erbringen Ihre Systeme in Bezug auf die Integration von Sicherheitskomponenten und wo liegen die Hauptvorteile?

Eagle Eye Networks bietet Cloud-Videoüberwachung mit integrierten Funktionen zur Verbesserung von Sicherheitssystemen. Die Plattform lässt sich nahtlos mit Zugangskontrollsystemen, Alarmsystemen und Analyseplattformen verbinden und bietet so umfassende Sicherheitslösungen. Zu den wichtigsten Vorteilen dieses

Systems gehören eine cloudbasierte Architektur, die lokale Server überflüssig macht, sicherer Zugriff auf Live- und aufgezeichnete Videos von jedem Standort aus, KI-gestützte Such- und Objekterkennungsfunktionen, zentralisierte Verwaltung für den Betrieb mehrerer Standorte und offene APIs, die die Verbindung mit Systemen von Drittanbietern erleichtern.

Welche Anwender benötigen ein PSIM-System und welche sind mit Managementsystemen, die Teilbereiche abdecken, besser bedient?

Organisationen mit komplexen Infrastrukturen und mehreren Sicherheitssystemen – wie Verkehrsknotenpunkte, stadtweite Anlagen und kritische Infrastrukturen – benötigen ein PSIM. Unternehmen, die sich hauptsächlich auf Videoüberwachung konzentrieren, wie Einzelhandelsketten, Schulen oder kleine Büros, können ihre Ziele mit einem dedizierten VMS erreichen.

Für welche Zielgruppe (Unternehmensgröße, Branche, Komplexität der Installation) eignet sich Ihr System am besten bzw. wo kann es seine Stärken am besten ausspielen?

Eagle Eye Networks eignet sich am besten für Unternehmen mit mehreren Standorten, beispielsweise im Einzelhandel, Gesundheitswesen, Logistik und Gastgewerbe. Es ist auch ideal für kleine und mittlere Unternehmen, die eine schnelle Bereitstellung und Skalierbarkeit benötigen. Das System ist besonders vorteilhaft für Organisationen mit begrenztem IT-Personal, die wartungsarme Lösungen bevorzugen. Darüber hinaus eignet es sich für Unternehmen, die einen effektiven zentralen Videozugriff über mehrere Standorte hinweg benötigen.

Welchen Rat würden Sie Anwendern geben, die über eine Neueinführung eines Managementsystems nachdenken?

Definieren Sie Ihre Ziele, listen Sie Ihre bestehenden Systeme auf und wählen Sie eine Plattform, die Integration, Fernzugriff und zukünftiges Wachstum unterstützt. Konzentrieren Sie sich auf Systeme, die die Komplexität reduzieren, die Transparenz verbessern und sich an Veränderungen in Ihrem Unternehmen anpassen.

Welchen Rat würden Sie Anwendern geben, die ihr Managementsystem ersetzen möchten?

Beginnen Sie mit einem klaren Verständnis dessen, was nicht funktioniert – Leistungslücken, Hardware-Einschränkungen oder hohe Supportkosten. Suchen Sie nach Systemen, die die Infrastruktur vereinfachen, Ihre Investitionen in vorhandene Geräte schützen und den Betrieb vom ersten Tag an optimieren.

7.7 Fast Systems (Schweiz)

Fast Systems ist ein Pionier auf dem Gebiet der digitalen Sicherheits- und Überwachungstechnologien und revolutioniert die Art und Weise, wie Unternehmen und Behörden Menschen, Eigentum und Vermögenswerte schützen.

Das TERRA 4D PSIM-System organisiert Sensor- und Systemdaten in strukturierten Formaten und präsentiert sie in einem geografischen Kontext, wodurch das Situationsbewusstsein in Echtzeit verbessert wird. Durch die Analyse ausreichender Daten und Muster liefert das System wertvolle Erkenntnisse, die schnellere Korrelationen ermöglichen und Sicherheitsbeamte bei der Entscheidungsfindung, der Identifizierung von Protokollen, der Zuweisung von Ressourcen und der Festlegung von Einsatzstrategien unterstützen. Die Bediener können eine virtuelle Schnittstelle nutzen, um Ereignisse über Zeit und Raum hinweg zu überprüfen und so ein besseres Verständnis der Abläufe zu erlangen.

TERRA 4D basiert auf einem 3D-Geografischen Informationssystem, in dem ein Digitales Geländemodell (DGM) eine dreidimensionale Höhenlage des Bodens darstellt. Ergänzt wird dies durch Satellitenbilder sowie aktuelle und historische Luftbilder.

Sehen Sie Ihr System als übergreifendes PSIM-System oder eher als integralen Baustein von PSIM-Systemen?

Unsere TERRA 4D Plattform bietet Tools, die die Reaktionsfähigkeit in Leitzentralen und durch mobile Einsatzkräfte deutlich beschleunigen, die Effizienz steigern und die Betriebskosten in jeder Phase des Situationsmanagements senken. TERRA 4D ist herstellerunabhängig und unterstützt plattformübergreifende Interoperabilität. Die einheitliche Benutzeroberfläche ermöglicht die Fernsteuerung anderer Plattformen, angeschlossenen Sensoren und Subsystemen, einschließlich luft-, land-, see- und weltraumgestützter Plattformen.

Welche Leistungen erbringen Ihr System in Bezug auf die Integration von Sicherheitskomponenten und wo liegen die Hauptvorteile?

In der heutigen, zunehmend vernetzten Welt sind Systemplattformen mit mehreren geografischen Standorten, zahlreichen Informationsquellen und unterschiedlichen Verantwortungsbereichen immer häufiger anzutreffen. Daher sind nahtlose Integrationen für effiziente Abläufe wie Krisenmanagement, Kriminalitätsbekämpfung oder alltägliche Routineaufgaben unerlässlich.

Die Hauptvorteile unserer TERRA 4D Plattform umfassen die Vorhersage von Ereignissen, die mehrere Standorte und Verantwortungsbereiche betreffen und schnellstmöglich darauf zu reagieren. Gleichzeitig bewahrt TERRA 4D die individuellen Verantwortlichkeiten aller Beteiligten, als auch die Kontrolle über die Informationseigentümerschaft und stellt sicher, dass nur relevante Informationen ausgewählt werden und dem richtigen Bediener zugänglich gemacht werden.

Integrierte Lösungen basierend auf der TERRA 4D Plattform ermöglichen ein umfassendes Lagebild, das auf einem 3D-GIS-Modell basiert und bestehende sowie zukünftige Datenquellen georeferenziert. Die Plattform sorgt für eine selektive Verteilung von Daten nach Bedarf und bietet Zugriff auf verschiedene Datendienste wie Umweltinformationen, Wetterdaten, Nachrichtendienste und aktuelle Nachrichten. Darüber hinaus verbessert sie die Meldung, Reaktion, Bearbeitung und Lösung von Vorfällen, steigert die Effizienz und senkt die Betriebskosten. Mit ihrer Fähigkeit, die Reaktionszeiten zu verkürzen und Risiken zu minimieren, stellt die TERRA 4D Plattform eine zukunftsweisende Lösung für komplexe Sicherheitsanforderungen dar.

Welche Anwender benötigen ein PSIM-System und welche sind mit Managementsystemen, die Teilbereiche abdecken, besser bedient?

Ein umfassendes PSIM-System wie TERRA 4D eignet sich besonders für Anwender, die einen zentralen Überblick über ihre Sicherheitsinfrastruktur benötigen, insbesondere in komplexen Umgebungen wie kritischen Infrastrukturen, Industrieanlagen oder Flughäfen. Es ist ideal für diejenigen, die schnelle und koordinierte Reaktionen auf Ereignisse erfordern, da das System ein umfassendes Lagebild und automatisierte Workflows bereitstellt. Zudem profitieren Anwender, die umfassende Datenanalysen nutzen möchten, um Trends zu erkennen und fundierte Entscheidungen zu treffen. TERRA 4D hilft, die Komplexität von Systemen zu reduzieren und die Effizienz zu steigern, indem Prozesse zentralisiert und redundante Aufgaben vermieden werden. Darüber hinaus ist das System flexibel und skalierbar, was es besonders geeignet für Organisationen macht, die zukünftige Erweiterungen und Technologien planen.

Managementsysteme, die Teilbereiche abdecken, sind insbesondere für kleinere Unternehmen geeignet, die nur spezifische und isolierte Sicherheitsanforderungen haben, wie beispielsweise eine einfache Videoüberwachung. Sie sind sinnvoll, wenn die Sicherheitsinfrastruktur übersichtlich ist und keine Vernetzung erfordert oder wenn das Budget eine umfassende Integration nicht erlaubt. Die Wahl zwischen einem PSIM-System und einer spezialisierteren Lösung hängt letztlich von den individuellen Bedürfnissen, der Komplexität der Sicherheitsanforderungen und den langfristigen Zielen des Anwenders ab. Unsere Erfahrung zeigt, dass integrierte Plattformen wie TERRA 4D besonders in anspruchsvollen Umgebungen durch ihre zentrale Steuerung, verbesserte Effizienz und Skalierbarkeit überzeugen.

Für welche Zielgruppe (Unternehmensgröße, Branche, Komplexität der Installation) eignet sich Ihr System am besten bzw. wo kann es seine Stärken am besten ausspielen?

TERRA 4D eignet sich optimal für mittelständische bis große Unternehmen und Konzerne in Branchen mit hohen Sicherheitsanforderungen und komplexen Infrastrukturen. Dazu zählen insbesondere kritische Infrastrukturen (KRITIS), Industrie, Logistik, öffentliche Einrichtungen und Behörden. Die Stärken von TERRA 4D kommen am besten bei anspruchsvollen Integrationsprojekten mit heterogenen Systemlandschaften zur Geltung, die eine zentrale Lagebilderstellung, Automatisierung zur Effizienzsteigerung und verbesserte Sicherheit benötigen. TERRA 4D bietet Skalierbarkeit, Flexibilität und die Möglichkeit zur individuellen Anpassung für Organisationen, die ihre Sicherheit zukunftssicher gestalten wollen.

Welchen Rat würden Sie Anwendern geben, die über eine Neueinführung eines Managementsystems nachdenken?

Die Einführung eines neuen Managementsystems ist ein strategischer Schritt, der gut durchdacht sein sollte. FAST Systems empfiehlt Anwendern, die Expertise des Anbieters durch Referenzen und Kundenfeedback zu prüfen und auf eine zukunftssichere, skalierbare Plattform zu achten. Eine schrittweise Implementierung mit einem Pilotprojekt erleichtert die Einführung und mindert Risiken. Klare Zielsetzungen, Benutzerfreundlichkeit sowie höchste Standards bei Datensicherheit und Compliance sind entscheidend für den langfristigen Erfolg.

Welchen Rat würden Sie Anwendern geben, die ihr Managementsystem ersetzen möchten?

Es ist entscheidend, die Schwachstellen des aktuellen Systems klar zu definieren und die Ziele des neuen Systems präzise zu formulieren. Ebenso sollte die Integrationsfähigkeit des neuen Systems mit der bestehenden Infrastruktur gründlich überprüft werden, um mögliche Probleme zu vermeiden. Eine schrittweise Einführung hilft dabei, Risiken zu verringern und die Nutzerakzeptanz zu erhöhen. Ein benutzerfreundliches Design spielt eine zentrale Rolle, da es den Schulungsaufwand reduziert und die Effizienz der Anwender steigert. Für langfristige Zukunftssicherheit ist es sinnvoll, einen Anbieter mit einer klaren Entwicklungsstrategie und einem Fokus auf neue Technologien zu wählen. Schließlich sollte der Partner über umfangreiche Erfahrung und fundiertes Know-how in der Branche verfügen, um einen reibungslosen Übergang sicherzustellen.

7.8 Funkwerk (Deutschland)

Funkwerk Security versteht sich als Lösungsentwickler und Systemintegrator für innovative Sicherheitstechnik. Mit über 50 Jahren Erfahrung und einem Expertenteam bietet das Unternehmen branchenübergreifende Komplettlösungen, wobei das Leistungsangebot alle Projektschritte umfasst von der Beratung und Planung über die Systemtechnikauswahl bis hin zur Errichtung sowie dem Service, der Wartung und der kontinuierlichen Weiterentwicklung der Installation.

Sehen Sie Ihr System als übergreifendes PSIM-System oder eher als integralen Baustein von PSIM-Systemen?

ViPRO.gms 5 KRITIS ist ein eigenständiges, übergreifendes PSIM-System, das sämtliche sicherheitsrelevanten Systeme auf einer zentralen Plattform zusammenführt. Es erfüllt dabei höchste Anforderungen an Verfügbarkeit, IT-Sicherheit und die präzise Abbildung von Prozessen. Die Lösung adressiert sowohl betriebliche Effizienz als auch regulatorische Anforderungen in sicherheitskritischen Umgebungen.

Welche Leistungen erbringt das System in Bezug auf die Integration von Sicherheitskomponenten und wo liegen die Hauptvorteile?

Das PSIM-System ViPRO.gms 5 KRITIS übernimmt die zentrale Integration und Steuerung verschiedenster Sicherheits- und Gebäudetechnik-Komponenten innerhalb einer einheitlichen Plattform. Dazu gehören unter anderem Videoüberwachungssysteme, Brandmeldeanlagen, Zutrittskontrollanlagen, Einbruchmeldetechnik sowie Kommunikationssysteme. Alle Informationen aus diesen Systemen werden in vordefinierten Prozesslogiken zusammengeführt, visualisiert und in automatisierte oder manuelle Handlungsszenarien überführt.

Der entscheidende Vorteil liegt in der Standardisierung und Zentralisierung der Bedienoberfläche: Bediener, insbesondere bei wechselndem Personal wie z. B. Wachdiensten, müssen nicht mehr auf verschiedene unterschiedliche Systeme geschult werden. Stattdessen stehen alle sicherheitsrelevanten Informationen und Steuerungsmöglichkeiten einheitlich und übersichtlich zur Verfügung. Das steigert die Reaktionsgeschwindigkeit, minimiert Fehlerquellen und reduziert erheblich die Personalkosten für Schulungen und Betrieb.

Ein besonderes Alleinstellungsmerkmal von ViPRO.gms 5 KRITIS ist, dass wir als Hersteller drei zentrale Softwarelösungen – PSIM, Videomanagement und Kommunikationssysteme – aus einer Hand anbieten und diese vollständig integriert sind. Im Gegensatz zu Lösungen, bei denen externe Systeme über Schnittstellen angebunden werden, sind unsere Software-Plattformen direkt miteinander verbunden. Das ermöglicht eine besonders stabile, performante und zukunftssichere Systemarchitektur, bei der alle Module optimal aufeinander abgestimmt sind.

Welche Anwender benötigen ein PSIM-System und welche sind mit Managementsystemen, die Teilbereiche abdecken, besser bedient?

Wir sind mit unseren Lösungen vor allem im Umfeld der Kritischen Infrastrukturen (KRITIS) aktiv. In diesen Bereichen ist der Bedarf nach einer übergreifenden, zentralen Steuerungs- und Überwachungsplattform klar definiert und gesetzlich sowie regulatorisch oft vorgeschrieben. Der Einsatz eines PSIM-Systems ist hier unverzichtbar, da es darum geht, verschiedenste sicherheitsrelevante Systeme aus unterschiedlichen Gewerken zentral zusammenzuführen, auszuwerten und schnell steuerbar zu machen.

Managementsysteme, die nur Teilbereiche abdecken, können hingegen in weniger sicherheitskritischen Umgebungen sinnvoll und ausreichend sein wie zum Beispiel in einem Bürogebäude, in dem vorwiegend eine Zutrittskontrolle mit Videoüberwachung kombiniert werden soll. Das gilt auch in kleineren Industrieanlagen ohne hohe Sicherheitsvorgaben, wo einzelne Subsysteme wie Videomanagementsysteme (VMS) oder Gebäudeleittechnik ausreichen.

Für welche Zielgruppe (Unternehmensgröße, Branche, Komplexität der Installation) eignet sich Ihr System am besten bzw. wo kann es seine Stärken am besten ausspielen?

Unser PSIM-System entfaltet seine Stärken insbesondere bei Objekten, die der kritischen Infrastruktur und NIS2 zugeordnet sind - Infrastrukturen mit hoher Komplexität, sicherheitskritischen Anforderungen und dezentralen Strukturen. Dazu zählen vor allem Objekte und Unternehmen, die den Vorgaben der KRITIS-Verordnung und der NIS2-Richtlinie unterliegen. Typische Anwender sind Betreiber aus den Bereichen Energieversorgung, Wasserwirtschaft, Gesundheitswesen, Transport und Verkehr sowie staatliche Einrichtungen.

Welchen Rat würden Sie Anwendern geben, die über eine Neueinführung eines Managementsystems nachdenken?

Unser wichtigster Rat an Anwender ist: Setzen Sie auf einen Hersteller, der nicht nur die Software liefert, sondern auch die Planung, Errichtung und Inbetriebnahme des Systems direkt aus einer Hand verantwortet. Gerade PSIM-Systeme sind hochkomplex und erfordern neben fundiertem Wissen über klassische Sicherheitstechnik auch umfassende Kenntnisse über IT-Security, Netzwerktechnik, Prozesssteuerung und anlagenspezifische Besonderheiten. Diese Kompetenz liegt in der Regel beim Hersteller selbst und lässt sich über reine Partner- oder Distributorenmodelle nur schwer sicherstellen.

Ebenso entscheidend für einen reibungslosen und zukunftsfähigen Betrieb ist die IT-Kompetenz des Anbieters. Die meisten praktischen Herausforderungen entstehen an der Schnittstelle zwischen Sicherheits- und IT-Systemen. Unsere langjährige Erfahrung hat gezeigt, dass genau an dieser Schnittstelle häufig Integrations- und Betriebsprobleme entstehen. Bei der Einführung eines PSIM-Systems sollte der Fokus nicht nur auf der reinen Softwarelösung liegen, sondern auf einem kompetenten, erfahrenen und IT-affinen Hersteller, der das System plant, liefert, integriert und langfristig betreut – am besten alles aus einer Hand. Das Managementsystem sollte die individuellen Betriebsprozesse abbilden – nicht umgekehrt

Welchen Rat würden Sie Anwendern geben, die ihr Managementsystem ersetzen möchten?

Ein Managementsystem-Wechsel ist ein sensibler und komplexer Prozess, der nicht nur technisch, sondern auch organisatorisch gut vorbereitet sein sollte. Der Kunde sollte sich ausreichend Zeit für eine fundierte Beratung und intensive Vorbereitung nehmen. Ein PSIM- oder Managementsystem soll nicht nur Technik integrieren, sondern vor allem die individuellen Prozesse des Betreibers abbilden und effizient unterstützen. Deshalb empfehlen wir, sich frühzeitig und direkt vom Hersteller beraten zu lassen und dabei die eigenen Abläufe und Anforderungen detailliert zu erklären.

7.9 Genetec (Kanada)

Genetec ist ein führender Anbieter intelligenter, innovativer und vernetzter Sicherheitsprodukte, -dienstleistungen und -lösungen. Das Unternehmen verfolgt seit jeher das Ziel, durch den Einsatz verschiedener Sicherheitssysteme entstehende Redundanzen zu minimieren. Kundenrückmeldungen zeigten, dass die Integration einzelner Sicherheitsprodukte mit erheblichem Zeit-, Kosten- und Wartungsaufwand für Instandhaltung und Upgrades verbunden war. Daraus entwickelte sich eine Plattform für physische Sicherheit, die mehrere Produkte integriert und so konzipiert ist, dass sie als einheitliches System funktionieren.

Genetec Mission Control ist ein Entscheidungsmanagement-System, das hilft, sich entwickelnde Ereignisse zu verstehen und schnell die beste Vorgehensweise zu bestimmen. Es vereinfacht die Reaktionskoordination zwischen den Beteiligten und beschleunigt die Lösung von Vorfällen.

Security Center SaaS ist eine einheitliche physische Sicherheitslösung, die man wahlweise in der Cloud oder als Hybridlösung einsetzen kann. Sie vereint Zugangskontrolle, Videomanagement, forensische Suche, Einbruchsüberwachung, Automatisierung und viele andere fortschrittliche Sicherheitsfunktionen. Genetec Security Center liefert als vereinheitlichte Sicherheitsplattform Funktionalitäten, die über die eines reinen PSIM hinausgehen.

Sehen Sie Ihr System als übergreifendes PSIM-System oder eher als integralen Baustein von PSIM-Systemen?

Genetec Security Center ist ein vollständiges, vereinheitlichtes Sicherheitssystem, das die klassischen Grenzen eines PSIM überwindet. Es integriert Videoüberwachung, Zutrittskontrolle, automatische Nummernschilderkennung, Kommunikation, Einbruchmeldetechnik und mehr nativ innerhalb einer Plattform. Das System wurde von Grund auf als vereinheitlichte Lösung konzipiert, die sich mit den Anforderungen von Unternehmen entwickelt.

Welche Leistungen erbringt das System in Bezug auf die Integration von Sicherheitskomponenten und wo liegen die Hauptvorteile?

Security Center integriert zahlreiche Sicherheitskomponenten auf einer gemeinsamen Plattform und geht dabei über eine reine Ereignisüberwachung hinaus: Security Center ist darauf ausgelegt, Daten zentral zu bündeln – für ein effektives Management von Sicherheitsrichtlinien, die Überwachung laufender Vorgänge und die Durchführung fundierter Analysen. Unternehmen profitieren auf diese Weise von einer verbesserten Situationswahrnehmung, vereinheitlichten Befehls- und Steuerungsfunktionen sowie der erleichterten Systemverwaltung und Skalierbarkeit.

Welche Anwender benötigen ein PSIM-System und welche sind mit Managementsystemen, die Teilbereiche abdecken, besser bedient?

Genetec Security Center ist skalierbar und modular erweiterbar. Es kann zu Beginn als Stand-Alone Video-Management oder als Zutrittskontroll-System eingesetzt werden. Der Kunde kann es nach seinen Wünschen, Budgets und in seinem Tempo auf die Funktionalität der vollständigen Sicherheitsplattform erweitern. Somit eignet es sich, anders als ein herkömmliches PSIM, nicht nur für Unternehmen mit komplexen Abläufen, sondern auch für Anwender, die zunächst nur kleinere Strukturen schaffen wollen, aber zukünftiges Wachstum durchaus einplanen.

Für welche Zielgruppe (Unternehmensgröße, Branche, Komplexität der Installation) eignet sich Ihr System am besten bzw. wo kann es seine Stärken am besten ausspielen?

Genetec Security Center eignet sich für Organisationen jeder Größe, insbesondere für Branchen mit erhöhtem Sicherheitsbedarf wie Banken, Energie- und Versorgungsunternehmen, Städte und Kommunen, Flughäfen, Rechenzentren, Bildungseinrichtungen, Gesundheitswesen, öffentliche Sicherheit, Einzelhandel, Glücksspiel,

Verkehr und Veranstaltungsorte. Das System entfaltet seine Stärken vor allem in Unternehmen mit mehreren Standorten, in komplexen Installationen sowie bei Bedarf nach zentralem Management. Dank der vereinheitlichten Architektur profitieren auch kleinere Setups – etwa mit 40 Kameras und 30 Zutrittslesern – von den umfassenden Funktionen.

Welchen Rat würden Sie Anwendern geben, die über eine Neueinführung eines Managementsystems nachdenken?

Nicht zu lange nachzudenken – gerade treiben neue Gesetzgebungen wie das KRITIS-Dachgesetz oder die NIS2 -Richtlinie die Modernisierung in Sicherheit und Cybersicherheit massiv an. Vor der Einführung eines neuen Systems sollten Sicherheitsverantwortliche die eigenen Anforderungen ganzheitlich bewerten: Welche Funktionen werden jetzt und in Zukunft benötigt? Welche Integration bestehender Systeme ist erforderlich? Genetec empfiehlt, auf offene, skalierbare Plattformen zu setzen. Ein wichtiger Parameter ist außerdem die Bereitstellung: Die Cloud ist längst in den meisten Unternehmensbereichen angekommen – hingegen zeigen Security-Abteilungen im Vergleich zu anderen Einheiten noch Aufholbedarf. Dabei sind hier, ob als komplette Cloud- oder Hybrid-Lösung – große Potenziale zu heben: Mehr Sicherheit, hohe Skalierbarkeit und permanente Verfügbarkeit sowie die Möglichkeit, Datenpotenzial noch gezielter zu nutzen.

Welchen Rat würden Sie Anwendern geben, die ihr Managementsystem ersetzen möchten?

Ein Wechsel sollte gezielt geplant werden. Wichtig sind dabei die Migrationsfähigkeit vorhandener Geräte und Daten, die Einhaltung betrieblicher Abläufe während der Umstellung und Offenheit für zukünftige Erweiterungen. Im Gegensatz zu geschlossenen, proprietären Systemen mit eingeschränkter Kompatibilität ohne Update-Garantie, können Unternehmen bei Lösungen mit offenen Architekturen eine Vielzahl von Kameras, Analysetools und anderen Geräten integrieren. Bei der Auswahl der neuen Lösung sollten Systeme bevorzugt, werden, bei denen Cybersicherheit und Datenschutz von Vornherein berücksichtigt ist. Eine sorgfältige Planung und Zusammenarbeit mit erfahrenen Partnern erleichtert den Übergang und stellt Betriebskontinuität sicher.

7.10 Gretsch-Unitas (Deutschland)

Seit 1990 entwickelt ela-soft – ein Unternehmen der Gretsch-Unitas-Gruppe – das herstellerneutrale Gebäudemanagementsystem GEMOS PSIM. Seit 2019 wird GEMOS von BKS vertrieben. Mit dem System ist es möglich eine Vielzahl an Medien, Kommunikation und Sicherheit herstellerneutral zu managen wie zum Beispiel: Brandmeldeanlagen, Überfall- und Einbruchmeldeanlagen, Videoüberwachungsanlagen, Zutrittskontrollanlagen, Lösch- und RWA-Anlagen und vieles mehr. Mit GEMOS werden alle technischen Einrichtungen unter einer zentralen, einfach bedienbaren Oberfläche integriert.

GEMOS ist ein herstellerunabhängiges PSIM-System, das zahlreiche Sicherheits-, Medien- und Kommunikationssysteme integriert. Es bietet eine zentrale Plattform zur Überwachung und Steuerung sicherheitsrelevanter Subsysteme wie Brandmelde-, Video- und Zutrittskontrollsysteme. Die offene Architektur und Standardprotokolle ermöglichen eine nahtlose Integration in übergeordnete Systeme. Es unterstützt sowohl Gefahrenabwehr als auch die Umsetzung erhöhter Anforderungen aus Gesetzen wie NIS-2 und dem KRITIS-Dachgesetz, die IT-Sicherheit und Resilienz stärken.

Welche Leistungen erbringen Ihr(e) System(e) in Bezug auf die Integration von Sicherheitskomponenten und wo liegen die Hauptvorteile?

Mit einem GEMOS werden alle Sicherheitsinformationen und -ereignisse wie (Störungen, Alarme und andere Zustände) aller integrierten physischen Sicherheits- und Informationssysteme (GEMOS-Schnittstellen) überwacht, erkannt und dabei transparent und übersichtlich dargestellt. Ein GEMOS (Gebäudemanagementsystem), das wir Gebäudemanagement- und Organisationssystem nennen, ist mehr als nur eine technische Maßnahme zum Bündeln von Informationen. Es organisiert die zentrale Überwachung, Verarbeitung und Visualisierung der umfangreichen Sicherheitsinformationen aus verschiedenen Branchen in ein unabhängiges Risikomanagementsystem. Das System bietet eine ganzheitliche Sicht (Was-Wann-Wo) auf alle Sicherheitsereignisse. Dies erhöht die Effizienz bei der Überwachung, Erkennung und Reaktion auf Sicherheitsvorfälle erheblich.

GEMOS bietet Module, die Sicherheitsanforderungen individuell erfüllen können. Zu den Hauptvorteilen zählen die herstellerunabhängige Integration von Subsystemen, die Plattformunabhängigkeit mit Unterstützung von Windows und Linux, sowie die anpassbare grafische Oberfläche. Die webbasierte Bedienung ermöglicht eine Nutzung ohne zusätzliche Softwareinstallation, während die zentrale Datenhaltung sicherstellt, dass alle Informationen auf dem GEMOS-Server gespeichert werden.

Das GEMOS „Enterprise One Server“ gewährleistet sicherheitstechnische Ausfallsicherheit. Der Austausch von Echtzeitdaten erfolgt verschlüsselt gemäß BSI-Standards mit TLS 1.3 und AES-256. Der automatische Datenabgleich zwischen den GEMOS-Servern bietet zusätzliche Sicherheit durch eine überwachte und verschlüsselte Replikation.

Welche Anwender benötigen ein PSIM-System und welche sind mit Managementsystemen, die Teilbereiche abdecken, besser bedient?

Die Wahl eines PSIM-Systems (Physical Security Information Management) oder spezialisierter Teilbereichs-Managementsysteme hängt von den individuellen Anforderungen ab. Typische Anwender für PSIM-Systeme kommen aus folgenden Bereichen: Industrie, Finanzwesen, Smart Building, Gesundheitswesen, Rechenzentren, Energieversorger, Handel, öffentliche Einrichtungen, Bildungs- und Forschungswesen, Justiz, Logistik, Transport und Verkehr sowie Veranstaltungskomplexe.

Das kommende NIS-2-Umsetzungs- und Cybersicherheitsgesetz (NIS2UmsuCG) wird etwa 30.000 Unternehmen in Deutschland zu einer erhöhten Resilienz verpflichten, insbesondere bei der physischen Sicherheit kritischer Infrastrukturen. Die Betreiber kritischer Infrastrukturen (KRITIS) in acht Sektoren müssen sich auf strengere Vorgaben und regulierte Anforderungen einstellen. Derzeit gibt es 1.132 registrierte Betreiber mit 2.095 Anlagen, doch die Zahl der betroffenen Unternehmen wird durch gesetzliche Anpassungen und erweiterte Sektoren deutlich steigen.

Für welche Zielgruppe (Unternehmensgröße, Branche, Komplexität der Installation) eignet sich Ihr System am besten bzw. wo kann es seine Stärken am besten ausspielen?

GEMOS eignet sich für Unternehmen jeder Größe. Kleine Betriebe können einfache Lösungen nutzen, während Großkonzerne komplexe Systeme zentral steuern. Es ist modular und skalierbar, mit Funktionen, die sich an die Anforderungen anpassen lassen.

Das System ist speziell für sicherheitskritische Branchen wie kritische Infrastrukturen, Strafanstalten oder Rechenzentren geeignet. Es bietet gewerkübergreifende Interaktionen, intuitive Bedienung und flexible Anpassungsmöglichkeiten.

Mit über 750 Schnittstellen ist GEMOS ein führendes herstellerneutrales Gebäudemanagementsystem in Deutschland. Die webbasierte Oberfläche erlaubt individuelle Bedienkonzepte, grafische Anpassungen und die

direkte Einbindung von Gebäudegrundrissen. Alarmbearbeitung, Workflow-Management und umfassende Protokollierungen sind Kernfunktionen. GEMOS gewährleistet höchste Verfügbarkeit durch Redundanzkonzepte wie Netzwerk- und Serverausfallssicherungen.

Welchen Rat würden Sie Anwendern geben, die über eine Neueinführung eines Managementsystems nachdenken?

Ein herstellerneutrales Gebäudemanagementsystem wie GEMOS bietet hohe Sicherheit, Effizienz und Zukunftsfähigkeit. Klare Ziele sollten definiert werden: zentrale Steuerung, Prozessautomatisierung, Resilienz der Infrastruktur oder regulatorische Vorgaben. Eine Analyse der aktuellen Systemlandschaft ist notwendig, um bestehende Subsysteme und Schwachstellen zu identifizieren. Zukunftssicherheit und Skalierbarkeit sollten berücksichtigt werden, ebenso wie Schulungen für Mitarbeitende, um das System effektiv zu nutzen.

Welchen Rat würden Sie Anwendern geben, die ihr Managementsystem ersetzen möchten?

Ein Systemwechsel sollte gut durchdacht sein. Risikoanalysen müssen kontinuierlich durchgeführt und an aktuelle Bedrohungen angepasst werden. Oft kann ein gezieltes Upgrade oder eine funktionale Erweiterung das gewünschte Ergebnis erzielen, ohne einen kompletten Systemwechsel vorzunehmen. GEMOS bietet eine zukunftssichere Plattform, die mit den Anforderungen des Unternehmens wächst. Es empfiehlt sich, einen GEMOS-Partner oder die BKS GmbH direkt zu kontaktieren, um fundierte Entscheidungen zu treffen und Investitionen zu schützen.

7.11 Hexagon (Schweden)

Die Safety, Infrastructure & Geospatial Division von Hexagon hat erst kürzlich die Erweiterung ihres Lösungsportfolios für physische Sicherheit sowie dessen Umbenennung in HxGN dC3 bekannt gegeben. Der neue Name spiegelt die zentralen Schritte bei der Reaktion auf sicherheitsrelevante Ereignisse wider – Detektion, Koordination, Steuerung und Zusammenarbeit (Detect, Command, Control and Collaborate) – und beschreibt den Ansatz von Hexagon, Menschen, Liegenschaften und Werte durch das ganzheitliche Management eines Vorfalls zu schützen, um so negative Auswirkungen zu minimieren

Seit der Übernahme von Qognify, einem führenden Anbieter von Lösungen für physische Sicherheit, im April 2023 hat Hexagon sein Angebot in diesem Bereich vertieft und in sein breites Technologie-Ökosystem integriert. Für Hexagon ist das erst kürzlich erweiterte Portfolio der Ausgangspunkt für einen weiteren Ausbau seiner Präsenz im wichtigen Marktsegment physischen Sicherheit.

Neu im Portfolio ist das KI-gestützte HxGN dC3 LidarVision (vormals Accur8vision), ein 3D-Überwachungssystem auf Basis volumetrischer LiDAR-Detektionstechnologie. Es geht über den herkömmlichen Perimeterschutz hinaus und sichert ganze Areale statt nur den Zaunverlauf, mit der Fähigkeit, Eindringlinge auch bei schwacher Beleuchtung zu verfolgen und Objekte mithilfe des firmeneigenen KI-Neuronalen Netzes DeepTection von Hexagon zu klassifizieren.

Zum Portfolio gehört außerdem HxGN dC3 Video (vormals Qognify VMS), eine offene Video-Management-Software (VMS), sowie HxGN dC3 Orchestrator (vormals Situator), eine physische Sicherheitsinformationsmanagement-Software (PSIM) der Enterprise-Klasse. Lösungen für fortschrittliche Videoanalysen, forensische Suche sowie die zentrale Verwaltung und Überwachung physischer Sicherheitssysteme an mehreren Standorten runden das Kernportfolio von HxGN dC3 ab.

Sehen Sie Ihre Systeme als übergreifende PSIM oder eher als integralen Baustein von PSIM-Systemen?

Der HxGN dC3 Orchestrator fungiert als umfassendes PSIM, während HxGN dC3 Video ein wesentlicher Bestandteil von PSIM-Systemen ist.

Welche Leistungen erbringen Ihre Systeme in Bezug auf die Integration von Sicherheitskomponenten und wo liegen die Hauptvorteile?

Hexagon bietet einen „Single Pane of Glass", das heißt die Visualisierung der Informationen vielfältiger Subsysteme in einer Oberfläche mit einheitlicher Bedienbarkeit. Durch die Zusammenführung und Kombination von Informationen erlangt der Nutzer eine verbessertes Situationsverständnis. Die Anreicherung vorfallsbezogener Daten erfolgt durch standardisierte, dynamische Eingabeformulare, die eine strukturierte und einheitliche Erfassung relevanter Informationen ermöglichen. Das System führt die Nutzer anhand digitalisierter Standard Operating Procedures (SOPs) durch den optimalen Reaktionsprozess und unterstützt so eine effiziente und standardisierte Bearbeitung von Vorfällen.

Welche Anwender benötigen ein PSIM-System und welche sind mit Managementsystemen, die Teilbereiche abdecken, besser bedient?

Ein PSIM-System ist insbesondere für Organisationen mit einer zentralen Sicherheitsleitstelle von Bedeutung. Ebenso eignet es sich für Unternehmen, die eine Vielzahl von Subsystemen betreiben – insbesondere, wenn es sich um Systeme gleicher Art von unterschiedlichen Herstellern handelt, wie etwa verschiedene Video-Management-Systeme (VMS).

Für welche Zielgruppe (Unternehmensgröße, Branche, Komplexität der Installation) eignet sich Ihr System am besten bzw. wo kann es seine Stärken am besten ausspielen?

Das System entfaltet seine Stärken besonders im Enterprise-Umfeld, also bei größeren Organisationen mit einem komplexen technologischen Ökosystem. Dies betrifft unter anderem Branchen wie den Transportsektor (Schiene und Luft), Unternehmenscampus großer Firmen sowie städtische Infrastrukturen.

Welchen Rat würden Sie Anwendern geben, die über eine Neueinführung eines Managementsystems nachdenken?

Bei der Einführung eines Managementsystems sollten die Sicherheitsziele und die daraus abgeleiteten Anwendungsfälle (Use Cases) stets im Mittelpunkt stehen – die Auswahl der Technologie sollte sich daraus ergeben. Zudem ist es wichtig, in Prozessen zu denken: Aggregierte Informationen sind zwar hilfreich, sollten aber immer im Kontext der Ereignis- und Vorfallsreaktion betrachtet werden. Ein weiterer wichtiger Schritt ist das Mapping der bestehenden Technologien und Subsysteme sowie der Abgleich mit den verfügbaren oder noch zu entwickelnden Schnittstellen. Schließlich sollte die Einbindung der Nutzer in das System- und Informationsdesign frühzeitig erfolgen, um Akzeptanz zu schaffen und eine tatsächliche Wertschöpfung sicherzustellen.

Welchen Rat würden Sie Anwendern geben, die ihr Managementsystem ersetzen möchten?

Vor dem Austausch eines bestehenden Managementsystems sollten Anwender sorgfältig abwägen, welche zusätzlichen Funktionen und Anwendungsfälle (Use Cases) sie sich von einem neuen System erwarten. Ebenso sollte ermittelt werden, welche Defizite die Nutzer im aktuellen System sehen und welche konkreten Verbesserungen sie sich von einer neuen Lösung versprechen. Ein weiterer zentraler Aspekt ist die sorgfältige Prüfung, ob und in welchem Umfang die vorhandenen Subsysteme vom neuen System unterstützt werden. Nicht zuletzt ist es entscheidend, die Nutzer frühzeitig in das System- und Informationsdesign einzubinden, um die Akzeptanz des neuen Systems zu fördern und eine nachhaltige Wertschöpfung sicherzustellen.

7.12 Hikvision (China)

Hikvision bietet fortschrittliche PSIM-Lösungen, die Videoüberwachung, Zugangskontrolle und Alarmsysteme in einer zentralen Plattform integrieren. Die KI-gestützte Analyse verbessert die Sicherheitsüberwachung und die Reaktion auf Vorfälle für Unternehmen und kritische Infrastrukturen.

Die HikCentral Professional Series von Hikvision bietet modulare Plattformen für gängige Geschäftsanwendungen, darunter Video, Zugangskontrolle, Anwesenheitserfassung und mehr. Diese Anwendungen verfügen nicht nur über eigene Funktionen, sondern lassen sich auch flexibel kombinieren, um den Anforderungen einer Vielzahl von individuellen Szenarien wie dem Ihren gerecht zu werden. Darüber hinaus verfügen alle Anwendungsmodule über das gleiche Schnittstellendesign für die Plattformen der Serie, was den Lernaufwand für die verschiedenen Systeme erheblich reduziert.

7.13 Honeywell (USA)

Honeywell bietet im Rahmen seines Honeywell Building Automation-Angebots fortschrittliche PSIM-Lösungen (Physical Security Information Management) an, die Überwachung, Zugangskontrolle und Alarmmanagement in einer einheitlichen Plattform integrieren. Diese Systeme verbessern die Situationserkennung und optimieren die Sicherheitsabläufe für kritische Infrastrukturen und Unternehmen.

Honeywells WINMAG plus (V06) bietet eine neue gemeinsame Benutzeroberfläche mit verbesserter Menü- und Benutzerführung, ein neues, flexibleres Pay-as-you-go-Lizenzmodell und eine neue Softwarearchitektur, was es zu einer leistungsstarken, skalierbaren Lösung mit einfacher Integration und einfacher Integration macht Einhaltung von Compliance-Standards.

Darüber hinaus bietet WINMAG plus V06 erweiterte Unterstützung für Treiber für Brand- und Einbruchmeldeanlagen, Video- und Zutrittskontrollsysteme sowie Fluchtwegtechnik/Fluchttürsteuerung und Sprachalarmierung von Honeywell und die Integration von Systemen verschiedener Dritthersteller.

Die neue Softwarearchitektur der WINMAG plus V06 eignet sich sowohl für hochwertige Privatimmobilien als auch für globale Unternehmenslösungen mit verteilten Standorten. Eine wichtige Funktionserweiterung für den Installer ist die vereinfachte Erstellung von Arbeitsabläufen und eine anpassbare Benutzeroberfläche.

WINMAG plus V06 verwaltet und visualisiert Einbruchmeldetechnik, Brandmeldetechnik, Zutrittskontrolltechnik, Videotechnik, Rettungswegtechnik / Fluchttürsteuerung unter einer gemeinsamen Benutzeroberfläche. Meldungen werden grafisch oder in Textform angezeigt.

7.14 Integrated Systems (ISS) (USA)

Ein PSIM-System wie das von ISS ermöglicht es Organisationen, verschiedene Sicherheitsanwendungen und -geräte über eine zentrale Benutzeroberfläche zu integrieren und zu steuern. Dies unterstützt das Personal dabei, technische Herausforderungen effizient zu erkennen und zu bewältigen. Systeme wie Videoüberwachung, Zugangskontrolle, Sensoren, Netzwerke und Gebäudetechnik können in ein solches System integriert werden, wodurch Kontrolle, Übersichtlichkeit und Berichterstattung verbessert werden. Darüber hinaus können PSIM-Lösungen dazu beitragen, die Effizienz zu steigern, Kosten zu senken und die Sicherheit durch optimierte Informationsverarbeitung zu erhöhen.

7.15 Milestone Systems (Dänemark)

Milestone Systems ist ein weltweit führender Anbieter von Video-Management-Software (VMS) mit Hauptsitz in Brøndby, Dänemark. Das Unternehmen ist seit 2014 Teil der Canon-Gruppe. Das Produktportfolio umfasst die Videomanagementsoftware (VMS) XProtect, die fortschrittliche Analyseplattform BriefCam und die Videoüberwachung als Dienstleistung (VSaaS) Arcules. Milestone erleichtert die Zentralisierung von Kameras, Sensoren und Standorten und erschließt das volle Potenzial von Videodaten. Der Hersteller entwickelt offene Plattformlösungen für IP-basierte Videoüberwachung, die vor allem durch ihre Skalierbarkeit, Interoperabilität und Benutzerfreundlichkeit geschätzt werden. Die Lösungen von Milestone kommen in zahlreichen Branchen zum Einsatz, darunter kritische Infrastrukturen, Transport, Einzelhandel, Bildung, Gesundheitswesen und Stadtüberwachung.

Im Bereich Video Management Software (VMS) bietet Milestone mit seiner Hauptlösung XProtect eine modulare Plattform an, die sowohl kleine Installationen als auch großflächige, komplexe Systeme unterstützt. XProtect ermöglicht die Integration verschiedenster Kameras und Sensoren unterschiedlicher Hersteller und bietet Funktionen wie Live-Ansicht, Aufzeichnung, Ereignismanagement, KI-gestützte Analysefunktionen und skalierbares Systemdesign.

Im engeren Sinne bietet Milestone kein vollständiges Physical Security Information Management- System an. Jedoch lässt sich XProtect durch seine offene Architektur sehr gut mit anderen Sicherheitssystemen (z. B. Zutrittskontrolle, Brandmeldesysteme, Gebäudeautomation) integrieren und dient damit als zentrale Visualisierungs- und Steuerungsplattform. In Kombination mit Partnerlösungen aus dem Milestone-Ökosystem kann XProtect daher auch in erweiterten PSIM-Szenarien eingesetzt werden, insbesondere wenn es um die Zusammenführung und Darstellung sicherheitsrelevanter Informationen in einem zentralen Interface geht.

7.16 Nanodems (USA)

Nanodems bietet eine branchenführende, intelligente Plattform, die alle Komponenten der physischen Sicherheit nahtlos in einer konvergenten Plattform integriert. Die zentralisierte Steuerung und Kontrolle in Verbindung mit automatisierter Überwachung erhöht die betriebliche Effizienz und Sicherheit und reduziert gleichzeitig Risiken und Kosten. Die leicht erweiterbare Plattform mit offener Architektur hilft Anwendern, ihre bestehende Infrastruktur zu nutzen und Ihr Unternehmen zukunftssicher zu machen.

Die NDIS-Plattform von Nanodems bietet diesen kritischen Infrastruktureinrichtungen eine intelligente PSIM-Lösung, die alle unterschiedlichen physischen Sicherheitssysteme zusammenführt und vereint, um eine zentral verwaltete Kommando- und Kontrollstation bereitzustellen. Die Plattform verfolgt und überwacht nahtlos alle Systeme, einschließlich Perimeter, Gegensprechanlage, ACS, CCTV, UVIS, ANPR, Zugangskontrolle und Einbruchalarm- und Radarsysteme.

7.17 Network Harbor (USA)

Network Harbor liefert PSIM-Systeme für den Einsatz in Behörden, Unternehmen, Militär und Bildungseinrichtungen. Zu den Produkten gehören Tools für Videoüberwachung, Audiovernetzung und -aufzeichnung, Netzwerküberwachung, Personalmanagement, physische Zugangskontrolle und Integrationsplattformen wie LightHouse.

LightHouse ist so strukturiert, dass es diese Elemente zusammen mit kompatiblen Systemen von Drittanbietern in einem einzigen Rahmen vereint. Die Entwicklung des LightHouse PSIM-Systems umfasste mehr als vierzehn Jahre Forschung und Tests mit Schwerpunkt auf Qualitätssicherung. Das PSIM zielt darauf ab, Sicherheitskomponenten in einer Schnittstelle zu integrieren und bietet operative Kontrolle über eine einheitliche Plattform. Es ist mit einer Vielzahl von internen und externen Sicherheitsgeräten kompatibel. Das PSIM wurde in verschiedenen Bereichen eingesetzt, darunter in Regierungs-, Militär-, Energie-, Kommunal- und kommerziellen Einrichtungen.

7.18 Persistent Sentinel (USA)

Persistent Sentinel verfügt über mehr als 19 Jahre Erfahrung in der Entwicklung von PSIM-Software (Physical Security Information Management) für zivile und staatliche Sicherheitslösungen. Das vielseitige Design der HiRSA-Software eignet sich für Sicherheitsanwendungen in verschiedenen Bereichen: Installation, See- und Hafensicherheit sowie Terrorismusbekämpfung. Es kombiniert intelligente Agentensoftwaretechnologie mit bestehenden Kommunikationsinfrastrukturen, um ein robustes Netzwerk zur Erkennung und Bekämpfung verdächtiger und krimineller/feindlicher Aktivitäten zu schaffen.

Die HiRSA PSIM-Lösung bietet wesentliche Funktionen wie Ereigniserfassung, Analyse, Verifizierung, Lösung, Berichterstellung und Prüfpfade. HiRSA liefert ein detailliertes Common Operating Picture (COP) mit Sensorstandorten, die über Satellitenbildern visualisiert werden, und bietet den Bedienern einen umfassenden Sicherheitsüberblick.

7.19 Primion (Deutschland)

Primion Technology ist ein deutsches Unternehmen, das als anerkannter Anbieter insbesondere in den Feldern Zutrittskontrolle, Zeiterfassung und Gefahrenmanagementsysteme im Bereich Sicherheitstechnik gilt. Das Unternehmen entwickelt und realisiert integrierte Lösungen, die in sicherheitsrelevanten Umgebungen wie der Industrie, dem öffentlichen Sektor, Gesundheitswesen, Flughäfen und Rechenzentren Anwendung finden.

Primions SecurityManagement (pSM) ist ein Sicherheitsleitstandsystem, das von VdS anerkannt ist und verschiedene Sicherheitsgewerke auf einer Plattform kombiniert. Mit der Szenarien-Planung können Abläufe im Voraus automatisiert werden und manuelle Eingriffe werden durch Workflow-Szenarien unterstützt. Die mobile App ermöglicht die ortsunabhängige Steuerung. Die Lösung bietet ein einheitliches Sicherheitsmanagement für umfassende Sicherheit und kombiniert Zutrittskontrolle, Feueralarm, Videoüberwachung und viele weitere Sicherheitsfunktionen in einem einzigen System. Sie ermöglicht eine zentrale Kontrolle, die eine schnellere und effektivere Reaktion in Notfällen gewährleistet.

Sehen Sie Ihre Systeme als übergreifende PSIM oder eher als integralen Baustein von PSIM-Systemen?

Bei Primion verstehen wir uns als Lösungsanbieter, der beides bietet: wesentliche Bausteine wie Zutrittskontrollsysteme und eine vollständige PSIM-Anwendung zur Überwachung und Interaktion mit einer Vielzahl integrierter Systeme. Diese doppelte Kompetenz ermöglicht es uns, wichtige Aspekte der konvergenten Sicherheit abzudecken und maßgeschneiderte Lösungen für die individuellen Anforderungen jedes Kunden zu liefern – unabhängig davon, ob dieser einzelne Komponenten oder eine umfassende PSIM-Plattform benötigt.

Welche Leistungen erbringen Ihre Systeme in Bezug auf die Integration von Sicherheitskomponenten und wo liegen die Hauptvorteile?

Unsere Zugangskontrolllösungen gewährleisten die physische Sicherheit von Gebäuden, Räumen und sensiblen Bereichen – bis hin zu einzelnen Schließfächern oder Serverracks –, indem sie zu jedem Zeitpunkt nur autorisiertem Personal Zugang gewähren. In Kombination mit pSM, unserer PSIM-Anwendung, können Systemzustände in Echtzeit überwacht, Warnmeldungen an das zuständige Personal weitergeleitet und bei Bedarf sofort manuelle Eingriffe vorgenommen werden. pSM schafft eine zentralisierte Schnittstelle, die durch die Integration und Visualisierung einer Vielzahl von Systemen ein umfassendes Situationsbewusstsein ermöglicht. Ob es darum geht, eine Tür aus der Ferne zu entriegeln oder einen Rauchmelder während der Wartung zu deaktivieren – Benutzer profitieren von einer konsistenten, intuitiven Benutzererfahrung. Durch die Aggregation von Daten aus Brand- und Einbruchmeldesystemen, Videoüberwachung und sogar IoT-Geräten wie Temperatur- oder Hochwassersensoren zeichnet das System ein klares, konsolidiertes Bild potenzieller Bedrohungen – anstatt Benutzer mit isolierten Warnmeldungen und fragmentierten Informationen zu überfordern.

Die automatische Anzeige von Live-Videofeeds aus Bereichen, in denen Alarme ausgelöst werden, ermöglicht eine schnelle Einschätzung der Situation. In einigen Fällen können Kameras selbst Alarme auslösen, beispielsweise durch die Erkennung von unbefugtem Betreten oder ungewöhnlichem Verhalten in vordefinierten Zonen.

Welche Anwender benötigen ein PSIM-System und welche sind mit Managementsystemen, die Teilbereiche abdecken, besser bedient?

Subsysteme wie Zugangskontrolle oder Einbruchserkennung funktionieren oft gut als eigenständige Lösungen, und viele bieten bereits grundlegende Funktionen wie Alarmbenachrichtigungen. Bei kleineren Installationen oder Umgebungen mit minimaler Interaktion kann der isolierte Betrieb dieser Systeme ausreichend sein. Wir beobachten jedoch zunehmend, dass Kunden PSIM-Systeme auch dann einsetzen, wenn sie nur ein einziges Subsystem verwalten. Beispielsweise verbessert die Anzeige aller Rauchmelder auf einem digitalen Grundriss die

Benutzerfreundlichkeit und das Situationsbewusstsein erheblich im Vergleich zur direkten Interaktion mit dem Gerät selbst.

Je komplexer die Infrastruktur und je mehr Subsysteme beteiligt sind, desto größer ist der Wert einer PSIM-Lösung. Mit pSM erhalten Benutzer eine zentralisierte Übersicht über alle Alarme und Ereignisse, können Aufgaben innerhalb ihres Teams zuweisen oder eskalieren und vermeiden die Notwendigkeit umfangreicher Schulungen für verschiedene Systeme. Durch die Abstraktion und visuelle Darstellung von Daten – unabhängig von ihrer Quelle – vereinfacht PSIM die Diagnose und Entscheidungsfindung, sodass sich Teams auf den Vorfall konzentrieren können und nicht auf das dahinterstehende System.

Für welche Zielgruppe (Unternehmensgröße, Branche, Komplexität der Installation) eignet sich Ihr System am besten bzw. wo kann es seine Stärken am besten ausspielen?

Wie bereits erwähnt, liegt die wahre Stärke von pSM in seiner Fähigkeit, mehrere Systeme zu integrieren und Abläufe in unterschiedlichen Umgebungen zu optimieren. Je mehr Subsysteme miteinander verbunden sind, desto größer sind die Vorteile – von der unterstützten Entscheidungsfindung bis hin zu automatisierten Arbeitsabläufen. Selbst kleine Unternehmen können davon profitieren: pSM kann beispielsweise einen schnellen Überblick über alle offenen Türen und Fenster bieten, bevor am Ende des Tages abgeschlossen wird. Mittlere Unternehmen, die möglicherweise kein Vollzeit-Überwachungspersonal haben, schätzen automatisierte Warnmeldungen und Prozesskontrollen.

Für große Unternehmen und Betreiber kritischer Infrastrukturen bietet pSM eine zentralisierte Kontrolle über komplexe Sicherheitsarchitekturen. Es ermöglicht die Überwachung und Verwaltung aller Infrastrukturkomponenten über eine einzige Schnittstelle – eine Aufgabe, für die sonst mehrere Spezialisten erforderlich wären.

Dank seiner intuitiven Visualisierungen und der Möglichkeit, flexibel durch Kameramaterial zu navigieren und in Echtzeit auf Warnmeldungen zu reagieren, können Mitarbeiter proaktiv eingreifen, bevor Vorfälle eskalieren. Ob es um die Verwaltung von Hunderten von Sensoren in einer großen Einrichtung wie einem Flughafen oder um die Verbindung mehrerer Remote-Standorte geht, pSM lässt sich mühelos skalieren.

Welchen Rat würden Sie Anwendern geben, die über eine Neueinführung eines Managementsystems nachdenken?

„Fangen Sie klein an – und wachsen Sie mit." Auch wenn das ultimative Ziel darin besteht, alle relevanten Systeme in eine PSIM-Plattform zu integrieren, können bereits kleine Schritte einen unmittelbaren Mehrwert bieten. Durch die frühzeitige Anbindung von nur einem oder zwei wichtigen Systemen können sich die Benutzer mit der Benutzeroberfläche vertraut machen und schnell die Vorteile erkennen: beispielsweise zentralisierte Warnmeldungen, optimierte Arbeitsabläufe oder ein verbessertes Situationsbewusstsein.

Dank des modularen Aufbaus von pSM können zusätzliche Systeme jederzeit integriert werden und profitieren sofort von bestehenden Prozessen wie automatisierten Benachrichtigungen oder Alarmweiterleitung. So kann beispielsweise die Integration von Notfallknöpfen in Aufzügen später zur Integration von CO_2-Sensoren oder Temperaturwarnungen führen – alles innerhalb desselben Ökosystems und unter Nutzung derselben etablierten Reaktionsabläufe.

Welchen Rat würden Sie Anwendern geben, die ihr Managementsystem ersetzen möchten?

„Denken Sie groß – und denken Sie voraus." Wenn Sie bereits mit den Vorteilen zentralisierter Managementsysteme vertraut sind, ist ein Systemwechsel die perfekte Gelegenheit, um zu erkunden, was noch möglich ist. Oft sind es die weniger offensichtlichen Integrationen, wie die Verknüpfung von CO_2- oder Luftqualitätssensoren, die wichtige Erkenntnisse liefern. Im Falle eines Schwelbrandes beispielsweise könnte eine frühzeitige CO_2-Erkennung entscheidend sein, noch bevor ein Rauchmelder reagiert.

Eine moderne und flexible Plattform wie pSM ermöglicht es Anwendern nicht nur, Vorfälle effektiver zu erkennen und zu bewältigen, sondern in vielen Fällen sogar zu verhindern, indem Daten aus verschiedenen Quellen intelligent kombiniert werden, um ein vollständigeres Bild zu erhalten.

Der Austausch eines Systems bedeutet auch, dass Sie Ihre Risikolandschaft neu bewerten müssen. Dies ist der ideale Zeitpunkt, um aktuelle und aufkommende Bedrohungen neu zu bewerten – einschließlich Cyberrisiken, die sich zunehmend mit physischen Sicherheitsproblemen überschneiden. Wenn Sie sich im Voraus auf diese Herausforderungen vorbereiten, können Sie sicherstellen, dass Ihre Mitarbeiter auch unter Druck souverän reagieren können.

7.20 Prysm Software (Frankreich)

Prysm Software ist seit 2022 Teil der Vitaprotech-Gruppe und auf Softwarelösungen für Sicherheitsanwendungen spezialisiert. Mit AppVision stellt das Unternehmen eine PSIM-Plattform für Sicherheits-, Schutz- und technische Managementsysteme bereit. Diese Plattform ist offen, skalierbar und neutral ausgerichtet und ermöglicht die Integration sowie Steuerung von Geräten und Anwendungen über eine zentrale Schnittstelle. Unabhängig von Projektgröße oder Komplexität kann AppVision eingesetzt werden. Durch gezielte Schulungen erhalten Partner das notwendige Wissen, um die Lösung eigenständig zu implementieren und weiterzuentwickeln. Dadurch wird sichergestellt, dass die Lösung den aktuellen und zukünftigen Anforderungen der Endnutzer entspricht.

Sehen Sie Ihre Systeme als übergreifende PSIM oder eher als integralen Baustein von PSIM-Systemen?

AppVision ist eine Softwareplattform, die auf Interoperabilität ausgelegt ist. Sie ist vollständig anpassbar und kann als Physical Security Information Management (PSIM)-System verwendet werden, aber ihre Anwendungsmöglichkeiten gehen weit darüber hinaus. Sie kann als Hypervisor, Überwachungssystem, Gebäudemanagementsystem (BMS oder BOS), Befehls- und Kontrollsystem, Krisenmanagementsystem oder sogar als Security Information and Event Management (SIEM)-System fungieren. AppVision vereint die Verwaltung verschiedener Systeme für Sicherheit, IoT und Energie. Es aggregiert Daten, um umfassende Lösungen zu erstellen, und entwickelt Tools wie Szenarien, Workflows, Berichte und Dashboards, die auf spezifische Anforderungen zugeschnitten sind. Seine Schnittstellen sind für verschiedene Rollen angepasst und ermöglichen einen effektiven Betrieb. Alarme werden mit Workflows, Schweregradkontrollen und Historien zur Überprüfung verwaltet. Echtzeit-Visualisierung und Unterstützung für 2D-, 3D- oder GIS-Karten verbessern die Betriebsüberwachung und Navigation.

Welche Anwender benötigen ein PSIM-System und welche sind mit Managementsystemen, die Teilbereiche abdecken, besser bedient?

Anwender, die ein PSIM-System benötigen, sind Sicherheitsbeauftragte, die Echtzeit-Betriebsfunktionen benötigen, Sicherheitsmanager, die nach effektiven Berichterstellungstools suchen, und Facility Manager, die den Energieverbrauch verwalten und Wartungsarbeiten vorhersagen möchten. Solche Systeme verbessern die Entscheidungsfindung, indem sie eine einheitliche Sicht und globale Überwachung über verschiedene betriebliche Anforderungen hinweg bieten.

Für welche Zielgruppe (Unternehmensgröße, Branche, Komplexität der Installation) eignet sich Ihr System am besten bzw. wo kann es seine Stärken am besten ausspielen?

Dank seiner Anpassungsfähigkeit und seinen Individualisierungsmöglichkeiten kann AppVision die Anforderungen aller vertikalen Märkte und aller Arten von Kunden erfüllen. Wir verfügen über bewährte Erfahrung. Je heterogener jedoch die zu verbindenden Systeme sind, desto mehr kommt unser System zum Einsatz. Ich würde sagen, dass

AppVision am besten für intelligente und sichere Städte, Gefängnisse, Rechenzentren, intelligente Gebäude und Unternehmen mit mehreren Standorten geeignet ist.

Welchen Rat würden Sie Anwendern geben, die über eine Neueinführung eines Managementsystems nachdenken?

Entscheiden Sie sich für ein Standardprodukt (keine spezifische Entwicklung für jedes Projekt), das offen, herstellerneutral und anpassbar ist. Offen bedeutet, dass Sie Konnektoren zu Systemen von Drittanbietern entwickeln können, wenn Sie über die technischen Fähigkeiten in Ihrem Team verfügen. Auf diese Weise vermeiden Sie, dass Sie bei der geringsten Entwicklungsanforderung an einen Lieferanten gebunden sind. Das System sollte herstellerneutral sein, damit Sie die Freiheit haben, die Produkte und Technologien auszuwählen, die Sie einsetzen möchten, und auch bestehende Infrastrukturen zu verbessern. Anpassbar, um den individuellen Anforderungen jedes vertikalen Marktes gerecht zu werden. Es ist auch wichtig, eine Softwarewartung zu erwerben, um regelmäßige Updates für Funktionen und Sicherheit zu erhalten.

Welchen Rat würden Sie Anwendern geben, die ihr Managementsystem ersetzen möchten?

Die Software muss sich an die Nutzung der Website anpassen und nicht umgekehrt. In Bezug auf das Projektmanagement empfehlen wir, eine Testumgebung zu planen und die Funktionsanalyse nicht zu vernachlässigen.

7.21 SureView Systems (USA)

Die SureView Suite von SureView Systems ist eine Physical Security Information Management (PSIM)-Plattform, die als Software as a Service (SaaS) bereitgestellt wird und drei Software-Ebenen umfasst, die die Verwaltung von physischen Sicherheitsprogrammen unterstützen sollen. Sie bietet eine einzige Schnittstelle zur Koordinierung von Alarmen und Ereignissen, die von einem Security Operations Center (SOC) von jedem System, Gerät oder jeder Quelle in Echtzeit empfangen werden. Die Reaktionsfunktionen ermöglichen es SOC-Teams und Außendienstmitarbeitern, sich zu verbinden, Situationsbewusstsein zu schaffen und Echtzeit-Standort- und Statusaktualisierungen für Personal und Vermögenswerte bereitzustellen.

Für Einsätze vor Ort sind Tools vorgesehen, die die Verfolgung und Untersuchung von Vorfällen sowie die Dokumentation, Einhaltung von Vorschriften und die Kommunikation zwischen Einsatz- und Untersuchungsteams ermöglichen.

7.22 Veracity Solutions (Schottland)

Mit einem umfassenden, innovationsreichen Produktangebot bietet Veracity im Bereich Sicherheitsmanagement wichtige Komponenten, Subsysteme und vollständig integrierte Lösungen. Diese werden für bestimmte Marktsegmente in verschiedenen Branchen entwickelt, darunter kritische nationale Infrastruktureinrichtungen und andere High-End-Sicherheitsanwendungen.

Die integrierten Sicherheitsmanagementsysteme von Veracity ermöglichen die Verwaltung und Steuerung mehrerer physischer Sicherheits- und verwandter Systeme. Diese manchmal auch als PSIM-Systeme (Physical Security Integration Management) bezeichneten Systeme bieten einen zentralen und umfassenden Überblick über die Sicherheitsinfrastruktur eines Unternehmens und ermöglichen so eine bessere Lageerkennung und ein effizientes Incident Management.

Die Veracity-Unternehmensgruppe hat VMS Ltd nach langjähriger enger Zusammenarbeit im Jahr 2019 übernommen und kann nun dank zusätzlicher Ressourcen und Mitarbeiter ein breiteres Spektrum an Sicherheitssystemlösungen anbieten. Anfang April 2022 wurde der Name des Unternehmens in Veracity Solutions Ltd geändert, um die engere Integration innerhalb der Veracity-Unternehmensgruppe und die noch engere Integration der wachsenden Produktpalette von Veracity in ihre PSIM-Lösungen widerzuspiegeln.

8. Über den Autor

Dr. Heiko Baumgartner

Freier Journalist mit Schwerpunkt auf den Bereichen Life Science, Sicherheit und Chemie

Dank seiner umfangreichen Erfahrung als Publishing Director bei einem führenden internationalen Wissenschaftsverlag und seinem Expertenwissen als Chefredakteur in verschiedenen Fachredaktionen baut Dr. Baumgartner eine Brücke zwischen Innovationen und Technologien sowie deren praktischen Anwendungen.

www.heikobaumgartner.com
https://www.linkedin.com/in/dr-heiko-baumgartner-b85853a/

Rechtliche Hinweise[1]

[1] Rechtliche Hinweise

Für Experten.
Von Experten.
Mit Experten.

Unsere Inhalte leben von den verschiedenen Blickwinkeln. Neugierig?

Zur Plattform

Wie sieht Ihre Perspektive aus?

Haben Sie Fragen, Ideen oder möchten etwas beitragen? Kontaktieren Sie uns – wir freuen uns auf Ihre Impulse!

Johanna Krumbiegel
Media Relations Manager Building. Technology. Solutions.
Telefon +49 69 75 75 - 52 20
johanna.krumbiegel@messefrankfurt.com

Rebekka Wolz
Koordinatorin Building. Technology. Solutions.
Telefon +49 69 75 75 - 62 72
rebekka.wolz@messefrankfurt.com