NOTY APLIKACYJNE

SYSTEM SAFE ALERT SYSTEM (SAS) ZE SMARTWATCHEM H09

OPIS TECHNICZNO-FUNKCJONALNY, PRZYPADKI UŻYCIA, OGRANICZENIA STOSOWANIA, KLAUZULE ZABEZPIECZAJĄCE I OGRANICZENIE ODPOWIEDZIALNOŚCI

Wprowadzenie

System SAS ze smartwatchem H09 jest platformą technologiczną wspierającą bezpieczeństwo operacyjne personelu, przeznaczoną do stosowania w sytuacjach, w których pracownik może znajdować się w warunkach zagrożenia, izolacji, narażenia na określone niebezpieczeństwa, potrzeby zdalnego monitorowania, obowiązku przestrzegania procedur bezpieczeństwa lub konieczności szybkiego uruchomienia workflow awaryjnych.
Urządzenie H09 nie jest zwykłym konsumenckim urządzeniem ubieralnym. Jest to wyspecjalizowany terminal operacyjny, zaprojektowany do wykonywania w tle czynności monitorowania, zbierania sygnałów, klasyfikacji zdarzeń, weryfikacji zgodności z procedurami, lokalizacji operatora, lokalnej interakcji w przypadku zdarzeń krytycznych oraz włączania osoby w ustrukturyzowany przepływ alarmowania, eskalacji, komunikacji i audytu.
System nie ogranicza się do samego terminala noszonego na ciele, lecz obejmuje również moduły oprogramowania do lokalnego przetwarzania, mechanizmy scentralizowanej konfiguracji, kanały komunikacji, usługi backendowe, systemy rejestracji i identyfikowalności oraz, jeżeli przewidziano, Control Room lub inną jednostkę organizacyjną odpowiedzialną za nadzór nad zdarzeniami i ich obsługę.
System stanowi technologiczne wsparcie bezpieczeństwa operacyjnego. Nie stanowi wyrobu medycznego, nie stanowi środka ochrony zdrowia, nie stawia diagnoz, nie zastępuje nadzoru człowieka i nie zastępuje zakładowych procedur awaryjnych, nadzoru, prewencji i ratownictwa.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Spis treści

4 ..... Charakter systemu i przeznaczenie
4 ..... Ogólna architektura funkcjonalna
5 ..... Architektury zaawansowane
5 ..... Ogólna zasada działania
6 ..... Operacyjny heartbeat i telemetria stanu
6 ..... Klauzule zabezpieczające dotyczące operacyjnego heartbeat
6 ..... Wykrywanie bezruchu
7 ..... Klauzule zabezpieczające dotyczące wykrywania bezruchu
7 ..... Interfejs operatora
8 ..... Klauzule zabezpieczające dotyczące interfejsu operatora
9 ..... Zaawansowane strony operacyjne
9 ..... Klauzule zabezpieczające dotyczące zaawansowanych stron operacyjnych
9 ..... Wykrywanie upadku
11 ..... Klauzule zabezpieczające dotyczące wykrywania upadku
12 ..... Monitorowanie parametrów życiowych
13 ..... Klauzule zabezpieczające dotyczące monitorowania parametrów życiowych
13 ..... Weryfikacja obecności na nadgarstku
13 ..... Klauzule zabezpieczające dotyczące weryfikacji obecności na nadgarstku
13 ..... Workflow ostrzeżeń, alarmów, opóźnienia, eskalacji i anulowania
14 ..... Klauzule zabezpieczające dotyczące workflow alarmowego
15 ..... Funkcja dobrowolnego SOS
15 ..... SOS głosowe
15 ..... SOS ciche
16 ..... Opóźnienie umożliwiające anulowanie SOS
16 ..... Uruchamianie nagrywania audio i wideo
16 ..... Klauzule zabezpieczające dotyczące funkcji SOS
16 ..... Komunikacja wielokanałowa
17 ..... Bezpieczeństwo komunikacji
17 ..... Klauzule zabezpieczające dotyczące komunikacji adaptacyjnej
17 ..... Komunikacja adaptacyjna między Control Room a operatorem
18 ..... Klauzule zabezpieczające
18 ..... Wyłączna wielołużytkownikowa obsługa alarmów i organizacja przejmowania zdarzeń

19 .....Klauzule zabezpieczające dotyczące wyłącznej wieloużytkownikowej obsługi alarmów
20 .....Obsługa ŚOI bez Bluetooth za pomocą QR code lub wyboru z listy
Klauzule zabezpieczające dotyczące ŚOI bez Bluetooth rejestrowanych za pomocą QR lub
20 ..... wyboru z listy
21 .....Pozycjonowanie i lokalizacja operatora
22 .....Klauzule zabezpieczające dotyczące pozycjonowania
22 ..... Wspomagana lokalizacja dla zespołów ratowniczych i wsparcie w dotarciu do celu
22 ..... Klauzule zabezpieczające dotyczące wspomaganej lokalizacji celu
23 ..... Konfigurowalność systemu i zależność od przypadku użycia
23 .....Zdalne aktualizacje i rekonfiguracja platformy
23 .....Klauzule zabezpieczające dotyczące aktualizacji i rekonfiguracji
23 ..... Automatyczna i cicha aktualizacja aplikacji w trybie OTA
24 ..... Klauzule zabezpieczające dotyczące aktualizacji OTA
25 ..... Ogólne klauzule zabezpieczające dotyczące konfiguracji
25 ..... Stan ładowania i zawieszenie funkcji operacyjnych
25 ..... Klauzule zabezpieczające dotyczące stanu ładowania
25 .....Integracja smartwatcha z ekosystemem bezpieczeństwa
25 ..... Klauzule zabezpieczające dotyczące integracji z ekosystemem
25 .....Ogólne klauzule zabezpieczające dotyczące użytkowania
26 ..... Klauzule dotyczące niemedycznego charakteru systemu
26 .....Klauzule ograniczenia odpowiedzialności
26 ..... Oświadczenie końcowe

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Charakter systemu i przeznaczenie

System jest przeznaczony do wspierania bezpieczeństwa operacyjnego we wszystkich przypadkach, w których przydatne jest:

- wykrywanie z większym prawdopodobieństwem zdarzeń urazowych lub dynamiki odpowiadającej upadkowi;
- umożliwienie dobrowolnego wezwania pomocy;
- monitorowanie parametrów życiowych w celach prewencyjnych, lecz nie diagnostycznych;
- utrzymywanie ciągłego lub niemal ciągłego oszacowania pozycji operatora;
- weryfikacja zgodności w zakresie środków ochrony indywidualnej wymaganych w danym kontekście operacyjnym;
- powiązanie zdarzeń, pozycji, stanu urządzenia i reguł obszarowych w jednym obrazie nadzoru;
- uruchamianie przepływów komunikacji, powiadamiania, eskalacji i identyfikowalności w kierunku systemów zdalnych lub struktur kontrolnych.

Przeznaczenie systemu obejmuje zatem ograniczanie ryzyka, zwiększenie prawdopodobieństwa wykrycia nieprawidłowych warunków, wspieranie sprawności organizacyjnej interwencji oraz poprawę identyfikowalności zdarzeń.

System nie jest przeznaczony do zastępowania obowiązków pracodawcy w zakresie prewencji ani do stanowienia jedynego środka bezpieczeństwa pracownika.

Ogólna architektura funkcjonalna

Na terminalu noszonym na ciele odbywają się akwizycja danych z czujników, lokalne przetwarzanie, wstępna klasyfikacja zdarzeń, interakcja z operatorem, obsługa zdefiniowanych workflow oraz gromadzenie kontekstu operacyjnego. W backendzie znajdują się konfiguracje, profile, parametry progowe, logika komunikacji, reguły obszarowe, wykazy ŚOI, polityki lokalizacji, kryteria powiadamiania, systemy archiwizacji oraz kanały integracji z Control Room. Na poziomie organizacyjnym struktura nadzoru odbiera zdarzenia, ocenia je i uruchamia przewidziane procedury.

Control Room nie stanowi wyłącznie organizacyjnego poziomu odbioru, oceny i obsługi zdarzeń generowanych przez urządzenia noszone na ciele, lecz jest aktywną i strukturalną częścią architektury SAS jako centralny węzeł orkiestracji stanów bezpieczeństwa obiektu. W tym modelu Control Room jest zaprojektowana również jako natywne źródło alarmów, powiadomień operacyjnych i poleceń koordynacyjnych, które mogą być selektywnie kierowane do pojedynczych operatorów, zespołów, jednorodnych grup lub całego obiektu, w zależności od bieżącego scenariusza, profilu odbiorców, ich położenia logicznego lub geograficznego oraz dostępności indywidualnej łączności.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Takie podejście umożliwia platformie rozsyłanie w czasie zbliżonym do rzeczywistego instrukcji, stanów alarmowych i wskazówek dotyczących zachowania wynikających z ogólnej sytuacji na obiekcie. Obejmuje to na przykład wydawanie poleceń ewakuacji, wzywanie do punktów zbiórki, uruchamianie procedur odizolowania lub oddalenia się oraz rozpowszechnianie alarmów dotyczących zdarzeń na obiekcie. W tym samym modelu operacyjnym smartwatch może ponadto pełnić rolę terminala bezpośredniego doręczania poleceń, instrukcji i komunikatów operacyjnych wysyłanych z backendu (które mogą być również odczytywane na głos przez urządzenie), tak aby treści nakazowe lub dotyczące zachowania były natychmiast dostępne dla operatora bez konieczności aktywnego odczytywania wyświetlacza, co zwiększa skuteczność komunikacji w środowiskach dynamicznych, hałaśliwych lub o wysokim stopniu krytyczności.
Takie podejście sprawia, że platforma nadaje się do wspierania nie tylko zgłaszania zdarzeń, którym uległ pracownik, ale również skoordynowanego rozpowszechniania aktywnych środków ochronnych, w tym mających na celu dotarcie do określonych środków ochrony zbiorowej, bezpiecznych punktów, punktów zbiórki lub dróg oddalenia się, wyznaczonych w zależności od charakteru wykrytego zagrożenia. Control Room, jako logiczne centrum ekosystemu SAS, nie jest zatem jedynie końcowym odbiorcą alarmu, lecz strukturalnym elementem dynamicznego zarządzania bezpieczeństwem obiektu, zdolnym do generowania, korelowania i propagowania alarmów operacyjnych w zależności od ogólnego stanu systemu.

Architektury zaawansowane

Control Room ekosystemu SAS może być udostępniana według różnych modeli architektonicznych, tak aby dostosować się do uwarunkowań infrastrukturalnych, organizacyjnych i dotyczących łączności danego obiektu lub klienta. W pierwszej konfiguracji Control Room może być świadczona w formie scentralizowanej za pośrednictwem chmury Safe S.r.l., co umożliwia jednolite zarządzanie urządzeniami, zdarzeniami, workflow alarmowymi, konfiguracjami i interakcjami operacyjnymi, również w odniesieniu do wielu obiektów lub rozproszonych tenantów.
W środowiskach, w których nie jest dostępna ciągła i/lub stabilna łączność, ta sama architektura może być zarządzana on premises, tak aby system działał również w warunkach ograniczeń związanych z izolacją sieci, wymagań autonomii lokalnej lub polityk infrastrukturalnych nakazujących utrzymanie funkcji krytycznych w obrębie obiektu. W tej konfiguracji Safety control room oraz obsługujący ją backend działają lokalnie, zapewniając

ciągłość funkcji nadzoru, obsługi alarmów, archiwizacji, lokalizacji i koordynacji operacyjnej również w przypadku braku stałego połączenia z zewnętrznymi usługami zdalnymi.
W przypadkach, gdy klient dysponuje już istniejącą, działającą Control Room, Safety control room ekosystemu SAS może zostać zintegrowana aplikacyjnie z istniejącą strukturą, co pozwala uniknąć tworzenia odrębnego środowiska i zamiast tego sprzyja rozszerzeniu możliwości używanej już Control Room. Integracja ta może być realizowana za pośrednictwem API udostępnianych przez system, które umożliwiają dwukierunkową obsługę alarmów, powiadomień, stanów operacyjnych i opisanych wcześniej interakcji, pozwalając tym samym zarówno na przekazywanie do istniejącej Control Room zdarzeń generowanych przez ekosystem SAS, jak i na uruchamianie z poziomu tej Control Room alarmów, workflow i poleceń przeznaczonych dla podłączonych urządzeń i podsystemów.
Platforma SAS może działać zarówno jako kompletna Control Room, jak i jako zintegrowany komponent istniejącej Control Room, zachowując w obu przypadkach tę samą logikę dwukierunkowej orkiestracji bezpieczeństwa operacyjnego.

Ogólna zasada działania

System działa w oparciu o logikę nieinwazyjnego monitorowania. Główne operacje przetwarzania odbywają się w tle; bezpośrednia interakcja z operatorem następuje, gdy zostanie wykryta sytuacja wymagająca uwagi, gdy zdarzenie musi zostać potwierdzone lub anulowane, gdy należy uruchomić komunikację lub gdy system wymaga wykonania określonej czynności proceduralnej.

Operacyjny heartbeat i telemetria stanu

System przewiduje okresowe generowanie przez urządzenie operacyjnych komunikatów heartbeat, rozumianych jako „komunikaty stanu" przesyłane do backendu lub do Control Room w celu nadzoru, weryfikacji osiągalności i aktualizacji obrazu operacyjnego pracownika. Heartbeat nie jest prostym sygnałem obecności w sieci, lecz konfigurowalnym kontenerem informacyjnym, który w zależności od profilu aplikacyjnego może obejmować stan naładowania urządzenia, główne parametry łączności, stan noszenia oraz dodatkowe metadane przydatne do nadzoru.
Z punktu widzenia zastosowania heartbeat pozwala platformie utrzymywać aktualny obraz stanu terminala i jego sprawności operacyjnej, również w przypadku braku jawnych alarmów. Dzięki temu Control Room może skuteczniej rozróżniać brak zdarzeń od braku osiągalności, normalną ciągłość działania od potencjalnej degradacji terminala, a także warunki pełnej

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

sprawności operacyjnej od warunków, w których niektóre funkcje są czasowo ograniczone lub niedostępne (na przykład brak połączenia Wi-Fi).
Częstotliwość, zawartość i poziom szczegółowości heartbeat mogą być konfigurowane w zależności od przypadku użycia, kontekstu ryzyka, ograniczeń łączności oraz polityk energetycznych systemu. W scenariuszach zwykłych transmisja może być utrzymywana na bardziej zachowawczym poziomie; w scenariuszach o wysokiej krytyczności lub w przypadku wystąpienia zdarzeń zawartość lub częstotliwość komunikatów stanu mogą być dostosowane w celu zwiększenia możliwości zdalnego nadzoru.

Klauzule zabezpieczające dotyczące operacyjnego heartbeat

Obecność regularnych komunikatów heartbeat nie stanowi bezwzględnej gwarancji pełnej sprawności wszystkich funkcji urządzenia, tak samo jak chwilowy brak heartbeat nie oznacza automatycznie pewnej awarii ani stanu zagrożenia operatora. Dostępność tych komunikatów zależy od łączności, stanu energetycznego, konfiguracji, integralności urządzenia oraz prawidłowego działania łańcucha transmisji.
Heartbeat stanowi narzędzie wspierające nadzór operacyjny i nie zastępuje procedur weryfikacji, kontroli organizacyjnej ani obsługi przez człowieka sytuacji potencjalnych nieprawidłowości.

Wykrywanie bezruchu

System przewiduje funkcję wykrywania bezruchu operatora. Urządzenie realizuje ją w sposób ciągły i w tle, zgodnie z logiką nieinwazyjnego monitorowania, która charakteryzuje całą architekturę. Funkcja opiera się na analizie ruchu wyłącznie terminala noszonego na ciele, co dodatkowo zapewnia anonimizację pracownika. Gdy urządzenie pozostaje w całkowitym bezruchu przez określony z góry przedział czasu, konfigurowalny na żądanie i wynoszący w konfiguracji fabrycznej 40 sekund, system interpretuje ten stan jako potencjalnie nieprawidłowy i uruchamia alarm.
Obsługa zdarzenia przebiega na dwóch kolejnych poziomach. W pierwszej fazie alarm jest obsługiwany lokalnie na urządzeniu, które daje operatorowi możliwość jego anulowania w ciągu pierwszych 10 sekund od uruchomienia. Ten przedział pozwala pracownikowi aktywnie zasygnalizować, że jego stan jest prawidłowy, i ogranicza w ten sposób przekazywanie nieistotnych zgłoszeń do Control Room. Jeżeli alarm nie zostanie anulowany w tym oknie czasowym, zdarzenie jest przesyłane do Control Room. Control Room przejmuje je do obsługi, weryfikuje je i w razie potrzeby uruchamia przewidziane procedury.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Z punktu widzenia zastosowania wykrywanie bezruchu pozwala platformie wychwytywać sytuacje, w których operator może nie być w stanie samodzielnie wezwać pomocy. Funkcja jest w pełni konfigurowalna. Kontrolę bezruchu można włączyć lub wyłączyć na etapie konfiguracji początkowej, bez wpływu na ogólne działanie urządzenia. Parametry czasowe określające uruchomienie alarmu oraz okno anulowania mogą być definiowane w zależności od przypadku użycia, wykonywanego zadania i kontekstu operacyjnego. Pozwala to dostosować czułość funkcji do rzeczywistego sposobu pracy, zapobiegając generowaniu niewłaściwych alarmów przez czynności, które z natury obejmują długie okresy pozostawania w bezruchu.

Klauzule zabezpieczające dotyczące wykrywania bezruchu

Wykrywanie bezruchu opiera się na braku ruchu noszonego urządzenia, a nie na bezpośredniej ocenie stanu fizycznego operatora. W związku z tym uruchomienie alarmu bezruchu nie oznacza automatycznie stanu zagrożenia ani zasłabnięcia operatora. Analogicznie brak alarmu nie stanowi gwarancji jego bezpieczeństwa.
Skuteczność funkcji zależy od jej faktycznego włączenia w konfiguracji, ustawionych parametrów czasowych, prawidłowego noszenia urządzenia, jego stanu energetycznego oraz dostępności łączności niezbędnej do przesłania zdarzenia do Control Room.
Wykrywanie bezruchu nie zastępuje procedur weryfikacji, kontroli organizacyjnej ani obsługi przez człowieka sytuacji możliwego zagrożenia.

Interfejs operatora

Interfejs operatora urządzenia H09 został zaprojektowany jako interfejs prosty, niezawodny i ukierunkowany na szybkie użycie w kontekście operacyjnym, ze szczególnym uwzględnieniem zmniejszenia obciążenia poznawczego, minimalizacji przypadkowych aktywacji oraz możliwości użycia również w warunkach stresu, pośpiechu lub ograniczonej uwagi pracownika. Ogólna koncepcja interfejsu stawia bowiem na przejrzystość funkcjonalną, natychmiastową czytelność stanu urządzenia i szybki dostęp do funkcji krytycznych, unikając złożonych struktur nawigacji lub struktur niespójnych z charakterem noszonego terminala bezpieczeństwa.
Urządzenie jest wyposażone w ekran dotykowy, przednią kamerę, mikrofon i głośnik, co umożliwia nie tylko bezpośrednią interakcję wizualną, ale również funkcje komunikacji audio oraz, w przewidzianych przypadkach, wsparcie wideo. Uzupełniają je dwa przyciski fizyczne. Pierwszy służy do włączania i wyłączania terminala. Drugi, określany jako srebrny przycisk, jest

powiązany z funkcją SOS (cichą i jawną) oraz z uruchamianiem skanowania środków ochrony indywidualnej (ŚOI).
Oprócz przycisków fizycznych interfejs dotykowy udostępnia dodatkowe przyciski wirtualne, które pozwalają rozszerzyć dostępne funkcje bez wprowadzania dodatkowej złożoności mechanicznej urządzenia. Zestaw przycisków fizycznych i wirtualnych jest skonfigurowany tak, aby ograniczać ryzyko niezamierzonych aktywacji dzięki logice długiego naciśnięcia. Rozpoczęciu naciśnięcia towarzyszy krótka wibracja sygnalizująca start sekwencji aktywacji, a kolejna krótka wibracja potwierdza ważność naciśnięcia, a tym samym faktyczne przyjęcie polecenia. To rozwiązanie projektowe realizuje podwójny cel: z jednej strony ogranicza niezamierzone działania wynikające z uderzeń, otarć lub przypadkowych dotknięć, z drugiej zapewnia operatorowi natychmiastową informację zwrotną haptyczną, przydatną również wtedy, gdy uwaga wzrokowa skierowana na wyświetlacz jest ograniczona lub jej brak.
System jest przeznaczony dla osób noszących zegarek pod odzieżą roboczą, które muszą móc z niego korzystać, nie patrząc na niego. Jest domyślnie aktywny. Poza sytuacją alarmową ekran jest czarny i wyświetla jedynie, w lewym górnym rogu, zielone kółko, które pozwala stwierdzić, że zegarek działa prawidłowo.
Po lewej stronie ikony pojawiają się za każdym razem, gdy wystąpi sytuacja wymagająca uwagi:


Brak połączenia Wi-Fi, dostępna jest tylko sieć komórkowa. Ikona ta pojawia się na ekranie wyłącznie wtedy, gdy urządzenie zostało skonfigurowane i połączone z siecią Wi-Fi; w przeciwnym razie ikona ta nigdy nie zostanie wyświetlona.


Brak połączenia (zarówno Wi-Fi, jak i sieci komórkowej).


Słaby odbiór GPS. Szacowany błąd lokalizacji rzędu 50 metrów.


Brak odbioru GPS.


Niski poziom baterii, poniżej 30%.


Niski poziom baterii, poniżej 10%.


H09 nie jest prawidłowo założony.

Podczas alarmu na ekranie pojawią się dwa duże przyciski. U góry wyświetlany będzie zielony kciuk oznaczający „Wszystko OK”, a na dole ikona mikrofonu. Przycisk „Wszystko OK”, jeśli zostanie naciśnięty w ciągu 10 sekund od wysłania SOS, może anulować wezwanie, natomiast naciśnięty po uruchomieniu alarmu pozwala poinformować Control Room, że sytuacja jest

pod kontrolą. Mikrofon natomiast uruchamia nagrywanie dźwięku otoczenia i może być użyty wyłącznie po uruchomieniu alarmu. Nagrywanie to pozostaje aktywne do czasu, aż Control Room połączy się z urządzeniem. Po połączeniu Control Room nagrywanie zostaje automatycznie zatrzymane i jednocześnie przesłane do Control Room, która wyświetli je na ekranie.
Po uruchomieniu połączenia Teams interfejs automatycznie się dostosowuje, otwierając w dolnej części ekranu dedykowany render view do komunikacji audiowizualnej. Obszar ten jest automatycznie przewijany do widoku, aby umożliwić operatorowi zobaczenie osoby kontaktowej z Control Room lub w każdym razie obrazu wideo powiązanego z sesją komunikacji. Po zakończeniu połączenia Teams render view znika, a interfejs powraca do konfiguracji standardowej. Podsumowując, interfejs operatora został zaprojektowany tak, aby łączyć natychmiastowość użycia, odporność na niezamierzone aktywacje, szybki dostęp do funkcji krytycznych i dynamiczne dostosowanie do bieżących workflow, przy zachowaniu prostej struktury, spójnej z wykorzystaniem urządzenia jako noszonego terminala bezpieczeństwa.

Klauzule zabezpieczające dotyczące interfejsu operatora

Interfejs urządzenia został zaprojektowany w celu ograniczenia ryzyka przypadkowych aktywacji i ułatwienia szybkiego korzystania z funkcji krytycznych, jednak **nie może w sposób bezwzględny wyeliminować możliwości niezamierzonych aktywacji, braku ważnych naciśnięć, błędów interakcji lub nieprawidłowego użycia w szczególnie trudnych warunkach operacyjnych.** Skuteczność interakcji zależy również od czynników zewnętrznych, takich jak używanie rękawic, położenie ramienia, warunki otoczenia, uderzenia, wibracje, stan uwagi operatora, integralność ekranu dotykowego, sprawność przycisków fizycznych oraz ogólny stan urządzenia.
Ikony i wskaźniki stanu wyświetlane na ekranie stanowią skrócone przedstawienie warunków operacyjnych wykrytych przez system i nie mogą być interpretowane jako bezwzględna gwarancja ciągłej dostępności odpowiedniej funkcji.
Dostępność przedniej kamery, mikrofonu, głośnika lub render view połączenia nie gwarantuje sama w sobie jakości, ciągłości ani faktycznej przydatności komunikacji audio-wideo w każdych okolicznościach. Funkcje te zależą od łączności, stanu urządzenia, warunków otoczenia, jakości sygnału, konfiguracji systemu oraz dostępności zaangażowanych usług zdalnych.
Interfejs operatora, choć zaprojektowany do szybkiego użycia w kontekście bezpieczeństwa, nie zastępuje szkoleń, ćwiczeń, procedur operacyjnych ani protokołów awaryjnych.
Prawidłowe korzystanie z funkcji SOS, anulowania (abort), potwierdzenia, komunikacji i

rejestracji ŚOI wymaga uprzedniego przeszkolenia personelu w sposób spójny z przyjętym przypadkiem użycia.

Zaawansowane strony operacyjne

Interfejs urządzenia może zostać rozszerzony, w zależności od zastosowanej konfiguracji, o strony operacyjne przeznaczone dla określonych potrzeb w zakresie bezpieczeństwa, nadzoru lub wsparcia działań. Strony te nie są prostymi, ogólnymi ekranami informacyjnymi, lecz funkcjonalnymi komponentami architektury aplikacyjnej, aktywowanymi w zależności od profilu operatora, kontekstu ryzyka, stanu systemu lub bieżącego workflow.
Możliwe konfiguracje obejmują, przykładowo, strony przeznaczone do skróconego podglądu parametrów życiowych, strony wspierające nawigację wspomaganą do punktów zbiórki lub bezpiecznych miejsc w scenariuszach ewakuacji, a także strony ukierunkowane na lokalizowanie lub dotarcie do określonych środków ochrony zbiorowej lub innych elementów wspierających zarządzanie sytuacją awaryjną dostępnych na obiekcie, takich jak apteczki pierwszej pomocy, defibrylatory, sprzęt przeciwpożarowy lub podobne punkty o znaczeniu operacyjnym.
W takich przypadkach urządzenie pełni nie tylko funkcję generatora lub odbiornika alarmów, ale również funkcję terminala kontekstowego wsparcia działań, zdolnego do udostępniania operatorowi skróconych i praktycznych wskazówek spójnych z bieżącą sytuacją.

Klauzule zabezpieczające dotyczące zaawansowanych stron operacyjnych

„Zaawansowane strony operacyjne” stanowią narzędzia wsparcia kontekstowego i nie zastępują szkoleń, znajomości obiektu, oznakowania bezpieczeństwa, procedur awaryjnych ani koordynacji przez ludzi. Faktyczna przydatność wyświetlanych informacji zależy od poprawności konfiguracji, jakości danych kontekstowych, dostępności lokalizacji oraz aktualności informacji w backendzie.

Wykrywanie upadku

Podsystem wykrywania upadku opiera się na analizie danych z akcelerometru i czujników inercyjnych w czasie rzeczywistym, z wykorzystaniem logiki wielofazowej, która nie sprowadza decyzji do wystąpienia pojedynczego szczytu przyspieszenia. System analizuje natomiast całą sekwencję dynamiczną odpowiadającą możliwemu rzeczywistemu upadkowi osoby, odróżniając ją od gwałtownych gestów, przypadkowych uderzeń nadgarstka, wibracji

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

mechanicznych, intensywnych czynności roboczych, uderzeń nieurazowych, upadku samego urządzenia lub zwykłego bezruchu terminala.
Początkowa faza oceny dotyczy poszukiwania wiarygodnego stanu odciążenia grawitacyjnego, czyli znacznego zmniejszenia przyspieszenia pozornego, odpowiadającego utracie podparcia. Faza ta nie jest traktowana jako warunek wystarczający, lecz jako element wartowniczy uruchamiający pogłębioną analizę. Aby została uznana za istotną, musi wykazywać spójność czasową i nie może być lepiej wyjaśnialna jako szum, przypadkowe drganie lub ruch bez znaczenia urazowego.
Następnie system poszukuje spójnej fazy uderzenia, czyli zmiany przyspieszenia odpowiadającej zakończeniu dynamiki upadku. Również uderzenie nie jest traktowane jako kryterium samowystarczalne, ponieważ nie każde uderzenie odpowiada rzeczywistemu upadkowi i nie każdy upadek powoduje wyraźne uderzenie. Rolą uderzenia jest zwiększenie wiarygodności sekwencji, gdy jego amplituda i moment wystąpienia są spójne z fazą poprzedzającą.
Analizie tej towarzyszy faza obserwacji następczej, mająca na celu ocenę zmniejszenia aktywności ruchowej lub stanu względnego bezruchu. Bezruch nie jest uznawany za kryterium autonomiczne i wystarczające, ponieważ nieruchome urządzenie mogło zostać po prostu odłożone, zdjęte lub nie być noszone. Ograniczona aktywność następcza nabiera natomiast znaczenia, gdy występuje po dynamice uznanej już za istotną, i wzmacnia hipotezę, że obserwowane zdarzenie miało rzeczywiste skutki dla osoby.
System ocenia ponadto końcową pozycję ciała oraz zmianę orientacji terminala, traktując je jako dodatkowe czynniki spójności. Elementy te mogą pomóc odróżnić rzeczywisty upadek od zwykłego gwałtownego gestu, pojedynczego uderzenia lub wibracji niezgodnej ze zdarzeniem urazowym.
W logice klasyfikacji uczestniczą również mechanizmy histerezy, walidacji wielopróbkowej, okna czasowe obserwacji, penalizacja wzorców niezgodnych z rzeczywistym zdarzeniem oraz kryteria odporności mające na celu ograniczenie niewłaściwych aktywacji. W szczególności weryfikacja, czy urządzenie jest faktycznie noszone, pozwala ograniczyć ryzyko, że upadek samego terminala zostanie zinterpretowany jako upadek osoby, choć nie eliminuje go w sposób bezwzględny.
Z punktu widzenia zastosowania typowym przypadkiem użycia jest pracownik, który nagle traci równowagę lub doznaje zapaści o dynamice na tyle wyraźnej, że powstaje sekwencja odciążenia, uderzenia i następczego ograniczenia ruchu. W takim scenariuszu system może wygenerować lokalne ostrzeżenie (warning), zarejestrować zdarzenie, przekazać je do systemów centralnych i, w przypadku braku anulowania, uruchomić przewidzianą procedurę eskalacji.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Drugi przypadek użycia dotyczy zdarzenia niejednoznacznego lub granicznego, w którym wykryta dynamika wykazuje pewne elementy zgodne z upadkiem, ale nie pełną spójność. W takich okolicznościach system może przyjąć ostrożną klasyfikację, zażądać interakcji od operatora lub uruchomić mniej agresywne workflow, w zależności od zastosowanej konfiguracji.
Trzeci przypadek użycia dotyczy typowego dla nadgarstka fałszywie dodatniego wyniku, w którym intensywna aktywność fizyczna, powtarzające się uderzenia lub szybkie ruchy generują wzorce częściowo podobne do upadku. W takich przypadkach architektura wielofazowa, weryfikacja po zdarzeniu oraz możliwość anulowania ostrzeżenia stanowią główne narzędzia ograniczania szumu decyzyjnego.
Pomimo stopnia złożoności analizy wielofazowej, obecności mechanizmów stopniowej walidacji, penalizacji niespójnych wzorców i modulacji ryzyka końcowego, podsystem wykrywania nie może w sposób bezwzględny wyeliminować możliwości wyników fałszywie dodatnich lub fałszywie ujemnych. Złożoność rzeczywistego zjawiska biomechanicznego, umiejscowienie czujnika na nadgarstku, indywidualna zmienność ruchów, nie w pełni deterministyczny charakter rzeczywistych upadków oraz konieczność działania na energooszczędnym urządzeniu wbudowanym (embedded) sprawiają, że istnienie resztkowego marginesu błędu decyzyjnego jest naturalne. Analiza wielofazowa zwiększa odporność modelu i zmniejsza zależność od pojedynczych szczytów lub zbyt uproszczonych kryteriów, ale nie przekształca systemu w nieomylny klasyfikator zdarzenia urazowego. W ujęciu aplikacyjnym model jest zatem zaprojektowany w celu zwiększenia prawdopodobieństwa prawidłowego wychwycenia upadków zgodnych z obserwowalnymi sygnałami, a nie w celu zagwarantowania pewnego i uniwersalnego rozpoznania każdego możliwego zdarzenia.
Podsystem wykrywania upadku stosuje logikę wyraźnie zoptymalizowaną pod kątem energooszczędnych wbudowanych urządzeń ubieralnych, w której równowaga między dokładnością wykrywania, szybkością decyzji, zużyciem energii, zajętością pamięci i obciążeniem obliczeniowym stanowi strukturalny wybór projektowy, a nie przypadkowe ograniczenie implementacji. W tym kontekście częstotliwość próbkowania akcelerometru nie jest podnoszona do teoretycznie możliwych wartości maksymalnych, lecz utrzymywana na poziomie zgodnym z ciągłym monitorowaniem na urządzeniu noszonym na ciele, tak aby zachować autonomię operacyjną, stabilność systemu i akceptowalne obciążenie obliczeniowe w długim okresie.
Przyjęcie umiarkowanej częstotliwości próbkowania zapewnia istotne korzyści: zmniejsza zużycie energii przez czujniki i CPU, ogranicza obciążenie wywołań zwrotnych (callback) czujników, ogranicza wewnętrzny ruch danych, zmniejsza ryzyko zaległości w przetwarzaniu i

sprawia, że ciągłe monitorowanie przez cały czas trwania zmiany jest bardziej wykonalne. Wybór ten sprzyja ponadto lepszej zgodności z architekturą wbudowaną, w której urządzenie musi jednocześnie realizować inne funkcje, takie jak komunikacja, lokalizacja, obsługa workflow alarmowych, interakcja z użytkownikiem i kontrola ogólnego stanu operacyjnego. Wobec tych korzyści niewysoka częstotliwość próbkowania wiąże się również z określonymi kompromisami technicznymi. W szczególności zmniejsza rozdzielczość czasową, z jaką obserwowane są najszybsze stany przejściowe, może sprawić, że szczegółowa rekonstrukcja bardzo krótkich zdarzeń impulsowych będzie mniej dokładna, i może obniżyć czułość na niezwykle szybkie lub mało trwałe mikrowzorce. Aby skompensować to ograniczenie, system nie opiera decyzji na pojedynczej próbce, lecz stosuje logikę okien czasowych i walidacji wielopróbkowej, w której zdarzenie jest interpretowane jako całościowa struktura dynamiczna, a nie jako ciąg elementarnych szczytów (spike).
Podsumowując, podsystem wykrywania upadku został zaprojektowany zgodnie z logiką kontrolowanego kompromisu: częstotliwość akcelerometru dobiera się tak, aby ciągłe monitorowanie na urządzeniu ubieralnym było wykonalne, natomiast przetwarzanie wsadowe (batching) i analiza okienkowa służą odzyskaniu odporności semantycznej, ograniczeniu szumu i ograniczeniu kosztu obliczeniowego. Rezultatem nie jest model ukierunkowany na maksymalną surową reaktywność, lecz model ukierunkowany na najlepszą niezawodność operacyjną możliwą do osiągnięcia przy rzeczywistych ograniczeniach wbudowanego urządzenia noszonego na nadgarstku.

Klauzule zabezpieczające dotyczące wykrywania upadku

Podsystem wykrywania upadku stanowi narzędzie wspierające bezpieczeństwo osobiste i nie gwarantuje pewnego rozpoznania każdego zdarzenia urazowego. Mogą nie zostać wychwycone powolne upadki, stopniowe zapaści, poślizgnięcia z częściowym podparciem, zdarzenia o nietypowej dynamice, zdarzenia ze znaczącym ruchem resztkowym nadgarstka lub zdarzenia, które wystąpiły przy nieprawidłowo noszonym urządzeniu.
System nie gwarantuje braku wyników fałszywie dodatnich ani braku wyników fałszywie ujemnych. Wykrywanie zależy od dynamiki zdarzenia, położenia urządzenia, stanu noszenia, warunków operacyjnych oraz zastosowanej konfiguracji.
Niewykrycie upadku lub wygenerowanie niewłaściwego alarmu nie stanowi samo w sobie automatycznego dowodu pewnej wadliwości działania ani podstawy odpowiedzialności na zasadzie ryzyka producenta lub dostawcy.
Podsystem wykrywania upadku nie zastępuje nadzoru człowieka, zakładowych procedur awaryjnych, oceny ryzyka, szkolenia personelu, środków zapobiegawczych, specjalistycznych ŚOI ani innych zabezpieczeń przewidzianych w danym kontekście operacyjnym.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Monitorowanie parametrów życiowych

System obejmuje podsystem monitorowania parametrów życiowych, służący do wykrywania potencjalnie nieprawidłowych stanów fizjologicznych podczas pracy. Monitorowanie zostało zaprojektowane jako **funkcja prewencyjna, niediagnostyczna** i opiera się na zbieraniu parametrów życiowych możliwych do pozyskania przez noszone urządzenie, przekształcanych w aplikacyjne wskaźniki uwagi lub ryzyka.

Przetwarzanie parametrów życiowych nie ogranicza się do oceny chwilowej wartości pojedynczego pomiaru. Każdy parametr jest natomiast analizowany w czasie jako szereg czasowy, na podstawie którego system może wyznaczać średnie, statystyki narastające, wskaźniki zmienności, odchylenia od zwykłego zachowania, warunki utrzymywania się oraz kryteria stabilności sygnału. Takie podejście pozwala skuteczniej odróżniać przejściowe wahania o niewielkim znaczeniu od powtarzających się lub utrzymujących się anomalii.

System może zatem identyfikować różne sytuacje aplikacyjne.

- U pracownika występuje parametr, który w sposób stabilny przekracza próg uwagi lub jest znacząco nieprawidłowy w stosunku do jego własnego profilu historycznego. System może wygenerować „ostrzeżenie" (warning), które należy obsłużyć zgodnie ze skonfigurowanym workflow.
- Anomalia wynika nie tyle z wartości bezwzględnej, ile ze znaczącego odchylenia od średniej indywidualnej. W tym scenariuszu funkcja monitorowania jest szczególnie przydatna w przypadku urządzeń przypisanych na stałe temu samemu operatorowi, ponieważ historia osobista zwiększa czułość na zmiany niekoniecznie skrajne w wartościach bezwzględnych, lecz istotne w stosunku do zwykłego zachowania fizjologicznego danej osoby.
- Kilka równoczesnych parametrów wykazuje umiarkowane, lecz spójne odchylenia. System może wówczas połączyć wkład poszczególnych modułów w globalną ocenę ryzyka, traktując obraz w sposób bardziej systemowy i mniej zależny od pojedynczego, odosobnionego pomiaru.

Monitorowanie parametrów życiowych współdziała ponadto z weryfikacją obecności na nadgarstku. Pozyskiwanie tych wartości ma bowiem znaczenie techniczne tylko wtedy, gdy urządzenie jest z dużym prawdopodobieństwem noszone, a kontakt z ciałem jest wystarczająco niezawodny. W przypadku braku tych warunków wartość informacyjna danych może znacznie się zmniejszyć.

Klauzule zabezpieczające dotyczące monitorowania parametrów życiowych

Monitorowanie parametrów życiowych służy wspieraniu bezpieczeństwa operacyjnego i nie ma celów diagnostycznych, terapeutycznych ani klinicznych. System nie jest wyrobem medycznym, nie wydaje dokumentacji medycznej, nie zastępuje oceny lekarskiej i nie

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

może być używany jako jedyne narzędzie do potwierdzania, wykluczania lub leczenia stanu chorobowego.

Pomiary na nadgarstku mogą być zakłócane przez wiele czynników, w tym nieoptymalny kontakt ze skórą, ruch kończyny, niewłaściwe zapięcie urządzenia, perfuzję obwodową, pocenie się, temperaturę otoczenia, warunki oświetlenia lub sygnału, stan czujnika, zdjęcie urządzenia lub jego nieprawidłowe użycie.

Wystąpienie alarmu nie jest równoznaczne z potwierdzeniem zasłabnięcia lub choroby; brak alarmu nie jest równoznaczny z wykluczeniem istotnych stanów klinicznych.

Odpowiedzialność za ocenę kliniczną spoczywa na właściwych podmiotach medycznych.

Weryfikacja obecności na nadgarstku

Weryfikacja obecności na nadgarstku jest funkcją przekrojową architektury SAS, ponieważ wpływa na jakość interpretacji w wielu podsystemach, w tym parametrów życiowych, upadku oraz obsługi niektórych workflow alarmowych. Jej celem jest odróżnienie sytuacji, w których urządzenie jest z dużym prawdopodobieństwem noszone, od tych, w których mogło zostać odłożone, zdjęte lub jest używane w sposób niezgodny z przeznaczeniem.

Z punktu widzenia zastosowania funkcja ta jest szczególnie ważna w trzech scenariuszach.

1. Zapobiega interpretowaniu jako informatywnych parametrów życiowych zebranych bez rzeczywistego noszenia urządzenia.
2. Zmniejsza ryzyko, że upadek samego terminala zostanie pomylony z upadkiem pracownika.
3. Przyczynia się do bardziej wiarygodnej kwalifikacji niektórych zdarzeń dotyczących stanu lub braku aktywności.

Weryfikacja nie jest równoznaczna z bezwzględnym fizycznym stwierdzeniem, że urządzenie faktycznie znajduje się na nadgarstku. Jest wynikiem klasyfikacji programowej opartej na dostępnych sygnałach, a zatem zwiększa ogólną odporność systemu, nie mogąc jednak mieć wartości pełnej pewności.

Klauzule zabezpieczające dotyczące weryfikacji obecności na nadgarstku

Klasyfikacja urządzenia jako noszonego lub nienoszonego stanowi szacunek aplikacyjny, a nie bezwzględny dowód rzeczywistego stanu terminala. Mogą zatem wystąpić klasyfikacje nie w pełni odpowiadające rzeczywistej sytuacji.

Przydatność tej funkcji polega na **ograniczaniu** błędów interpretacyjnych i niewłaściwych aktywacji, **a nie na ich bezwzględnym wyeliminowaniu.**

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Workflow ostrzeżeń, alarmów, opóźnienia, eskalacji i anulowania

System SAS stosuje ustrukturyzowany, stopniowy i zróżnicowany według klasy zdarzenia workflow obsługi zdarzeń. Potok przetwarzania nie ogranicza się do wyświetlenia powiadomienia, lecz obejmuje akwizycję zdarzenia, klasyfikację, weryfikację dopuszczalności, ewentualne opóźnienie, sygnalizację lokalną, rejestrację, powiadomienie zdalne, możliwe anulowanie przez operatora oraz ewentualną eskalację do jednostki nadzorującej.
Gdy funkcja systemu generuje istotne zdarzenie, urządzenie może przede wszystkim wygenerować lokalne ostrzeżenie (warning) w postaci powiadomienia na wyświetlaczu, sygnału dźwiękowego, komunikatu głosowego lub wibracji, w celu bezpośredniego poinformowania operatora i umożliwienia mu pierwszej reakcji. Jednocześnie zdarzenie może zostać już zarejestrowane i przesłane do systemów zdalnych na potrzeby audytu, logów i identyfikowalności.
W zależności od konfiguracji zdarzenie może podlegać opóźnieniu aplikacyjnemu. Opóźnienie pełni określoną funkcję techniczną i organizacyjną: pozostawia przedział czasu na ewentualne anulowanie wyniku fałszywie dodatniego, umożliwia pierwszą weryfikację lokalną i ogranicza bezkrytyczne przekazywanie zdarzeń jeszcze niepotwierdzonych.
Opóźnienie nie oznacza utraty zdarzenia, lecz jego tymczasowe, kontrolowane wstrzymanie w ramach workflow.
Jeżeli zdarzenie nie zostanie anulowane w przewidzianym czasie (10 sekund), system może przystąpić do eskalacji do skonfigurowanych odbiorców zdalnych. Eskalacja może przebiegać według zróżnicowanych polityk w zależności od rodzaju alarmu, stopnia priorytetu, profilu operatora, kontekstu obszaru lub innych kryteriów aplikacyjnych.
System obejmuje ponadto mechanizmy deduplikacji i okresu karencji (cooldown), które zapobiegają nadmiernemu powtarzaniu jednorodnych zdarzeń w krótkich odstępach czasu. Funkcja ta jest niezbędna w przypadkach, gdy ta sama anomalia generuje wiele kolejnych wyzwalaczy, ponieważ zapobiega przeciążeniu informacyjnemu backendu, operatora i Control Room.
Typowym przypadkiem użycia jest alarm upadku z lokalnym ostrzeżeniem i oknem anulowania. Jeżeli operator jest przytomny, a zdarzenie jest fałszywe, może przerwać workflow. Jeżeli nie zareaguje, system kontynuuje eskalację. Drugi przypadek użycia dotyczy zdarzeń, które choć nie mają dynamiki urazowej, wymagają powiadomienia i możliwej zdalnej weryfikacji. Trzeci przypadek użycia dotyczy alarmów proceduralnych lub dotyczących zgodności, które mogą przebiegać według innych ścieżek, w mniejszym stopniu

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

ukierunkowanych na natychmiastową sytuację awaryjną, a w większym na przejęcie sprawy przez organizację.
Anulowanie przez operatora wstrzymuje dalszą eskalację, ale niekoniecznie usuwa historyczny zapis już zarejestrowanego zdarzenia. Identyfikowalność anulowanego zdarzenia stanowi bowiem integralną część funkcji audytowej systemu.

Klauzule zabezpieczające dotyczące workflow alarmowego

Generowanie ostrzeżeń lub alarmów stanowi klasyfikację aplikacyjną, a nie bezwzględne poświadczenie zdarzenia. Istnienie workflow eskalacji nie jest równoznaczne z gwarancją, że interwencja zostanie zawsze uruchomiona, odebrana lub zakończona w oczekiwanym czasie. Opóźnienie, możliwość anulowania, deduplikacja i okresy karencji (cooldown) są narzędziami równoważenia szybkości reakcji, możliwości obsługi wyników fałszywie dodatnich i wydolności przepływu operacyjnego. Rozwiązania te **nie eliminują ani ryzyka niewłaściwych alarmów, ani ryzyka braku aktywacji.**
Skuteczność workflow zależy od prawidłowego działania urządzenia, dostępności łączności, poprawności konfiguracji, dostępności usług zdalnych oraz zdolności organizacyjnej jednostki nadzorującej.

Funkcja dobrowolnego SOS

System SAS obejmuje funkcję dobrowolnego SOS, umożliwiającą operatorowi jawne wezwanie pomocy, również w przypadku braku automatycznego wykrycia upadku, anomalii parametrów życiowych lub innego zdarzenia generowanego przez podsystemy monitorowania. Funkcja SOS stanowi zatem kanał bezpośredniego uruchomienia alarmu przez pracownika i jest niezbędnym komponentem architektury bezpieczeństwa, ponieważ pozwala obsługiwać sytuacje, w których zagrożenie jest subiektywnie odczuwane przez operatora, zanim jeszcze stanie się technicznie wykrywalne przez czujniki.
Funkcję można skonfigurować w różnych trybach pracy, tak aby dostosować ją do kontekstu ryzyka, charakteru wykonywanej czynności oraz rodzaju wymaganej reakcji organizacyjnej.

SOS głosowe

Tryb SOS głosowego jest przeznaczony dla wszystkich sytuacji, w których operator może jawnie wezwać pomoc, a urządzenie powinno lokalnie zasygnalizować, że wezwanie zostało uruchomione. W tym scenariuszu terminal może przekazywać wyraźne informacje zwrotne, takie jak potwierdzenia głosowe, dźwiękowe, haptyczne lub wizualne, aby poinformować pracownika, że wezwanie zostało przyjęte, a odpowiedni workflow został uruchomiony.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Typowym przypadkiem użycia jest operator, który znalazł się w trudnej sytuacji z powodu zasłabnięcia, urazu, zagubienia, izolacji, potrzeby pilnego wsparcia lub innej sytuacji krytycznej, w której jawne zasygnalizowanie alarmu nie zwiększa ryzyka. W takich okolicznościach lokalne potwierdzenie aktywacji jest przydatne z operacyjnego punktu widzenia, ponieważ pozwala osobie natychmiast zorientować się, że proces udzielania pomocy został uruchomiony.

SOS ciche

Tryb cichego SOS jest przeznaczony dla scenariuszy, w których uruchomienie alarmu nie powinno być widoczne na zewnątrz ani wytwarzać sygnałów dostrzegalnych dla osób trzecich. Konfiguracja ta ma szczególne znaczenie w sytuacjach napaści, groźby, przymusu, przemocy, próby kradzieży, wrogiego otoczenia lub, bardziej ogólnie, we wszystkich przypadkach, w których jawne zasygnalizowanie alarmu mogłoby zwiększyć zagrożenie dla operatora.
W tym trybie system może przyjąć wezwanie pomocy bez generowania rozpoznawalnych lokalnych informacji zwrotnych lub ograniczając je do form niedostrzegalnych dla otoczenia. Zdarzenie jest następnie przekazywane zgodnie ze skonfigurowanym workflow, z zachowaniem w miarę możliwości dyskrecji aktywacji, co pozwala Control Room lub jednostce nadzorującej odebrać zgłoszenie, zanim sprawca lub wrogie otoczenie się o nim zorientują.
Z punktu widzenia zastosowania ciche SOS stanowi odrębną funkcję w zakresie bezpieczeństwa osobistego, ponieważ zostało zaprojektowane dla sytuacji, w których niewidoczność alarmu jest niezbędnym wymogiem ochrony.

Opóźnienie umożliwiające anulowanie SOS

Funkcję SOS można skonfigurować z opóźnieniem umożliwiającym anulowanie lub bez niego. W pierwszym trybie system może przewidywać krótkie okno anulowania (abort), pozwalające operatorowi przerwać aktywację w przypadku niezamierzonego uruchomienia lub błędu obsługi. Konfiguracja ta jest szczególnie przydatna w sytuacjach, w których ryzyko przypadkowych aktywacji musi zostać ograniczone bez rezygnacji z dostępności funkcji.
W drugim trybie SOS może natomiast zostać skonfigurowane bez opóźnienia umożliwiającego anulowanie, tak aby zdarzenie było natychmiast przekazywane do backendu lub do Control Room. Ustawienie to jest szczególnie właściwe, gdy szybkość aktywacji ma bezwzględny priorytet lub gdy kontekst ryzyka sprawia, że jakiekolwiek opóźnienie wprowadzone przez okno potwierdzenia lub anulowania jest niewskazane.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Wybór między SOS z możliwością anulowania a natychmiastowym SOS zależy zatem od przypadku użycia, profilu ryzyka, wykonywanego zadania oraz przyjętych polityk organizacyjnych.

Uruchamianie nagrywania audio i wideo

Funkcja SOS może ponadto, w zależności od konfiguracji projektowej, być powiązana z cichym uruchamianiem mechanizmów nagrywania audio i wideo. Możliwość ta pozwala powiązać ze zdarzeniem awaryjnym nie tylko zgłoszenie alarmowe, ale również równoczesne gromadzenie informacji przydatnych do zrozumienia scenariusza, rekonstrukcji zdarzenia, kwalifikacji bieżącego ryzyka oraz wspierania decyzji operacyjnych jednostki nadzorującej.
Z punktu widzenia zastosowania nagrywanie audio może być przydatne do rejestrowania odgłosów otoczenia, rozmów, sygnałów napaści, wołania o pomoc lub innych elementów kontekstowych, których nie można bezpośrednio wywnioskować z samych danych o stanie urządzenia. Nagrywanie wideo może dodać kolejny poziom kontekstu wizualnego, szczególnie istotny w przypadkach napaści, wtargnięcia, groźby lub złożonego zdarzenia operacyjnego.

Klauzule zabezpieczające dotyczące funkcji SOS

Funkcja SOS stanowi narzędzie dobrowolnego uruchamiania alarmu i nie gwarantuje sama w sobie pewnego odbioru, natychmiastowego przejęcia do obsługi ani faktycznej obsługi zdarzenia w każdych okolicznościach. Skuteczność funkcji zależy od dostępności urządzenia, łączności, konfiguracji workflow, osiągalności systemów zdalnych oraz istnienia struktury organizacyjnej zdolnej do odebrania i obsłużenia zdarzenia.
Ewentualne uruchomienie nagrywania audio lub wideo nie gwarantuje pełnego zarejestrowania zdarzenia ani bezwzględnej przydatności zebranego materiału. Jakość i faktyczna przydatność nagrań zależą od warunków otoczenia, położenia urządzenia, dostępności kanału audio-wideo, warunków oświetlenia, hałasu otoczenia oraz ciągłości działania systemu.
Funkcja SOS, również w najbardziej zaawansowanych trybach, nie zastępuje procedur awaryjnych, środków ochrony osobistej, zabezpieczeń, organizacji ratownictwa ani zakładowych protokołów postępowania w przypadku napaści i sytuacji awaryjnych.

Komunikacja wielokanałowa

System obsługuje funkcje komunikacji wielokanałowej, które mogą obejmować połączenia, powiadomienia asynchroniczne, komunikaty stanu oraz, jeżeli przewidziano, kanały zapasowe (fallback). Komunikacja nie jest traktowana jako funkcja dodatkowa, lecz jako podstawowy

komponent operacyjnego modelu bezpieczeństwa, ponieważ pozwala przekształcić lokalne wykrycie w zdarzenie, które mogą obsłużyć podmioty zdalne.
W przypadku dobrowolnego SOS operator może bezpośrednio wezwać pomoc. Typowym przypadkiem użycia jest pracownik, który mimo braku automatycznego wykrycia upadku lub odchylenia parametrów życiowych odczuwa zagrożenie, trudność lub sytuację krytyczną i prosi o pomoc. W tym scenariuszu system pełni funkcję terminala świadomego uruchomienia procedury awaryjnej. W innych przypadkach użycia komunikacja stanowi kontynuację automatycznego alarmu już sklasyfikowanego przez system. Urządzenie może wówczas zostać włączone w strategię nawiązywania kontaktu i powiadamiania Control Room lub innych skonfigurowanych podmiotów, z wykorzystaniem głównego dostępnego kanału oraz, w razie potrzeby, kanałów pomocniczych lub zapasowych (fallback).
Komunikacja między urządzeniem, backendem a Control Room nie musi być jednolita, lecz może być zarządzana zgodnie z adaptacyjnymi politykami, które różnicują wykorzystywane kanały i protokoły w zależności od charakteru danych, wymaganej częstotliwości aktualizacji, poziomu priorytetu zdarzenia, potrzeby ciągłości połączenia oraz oczekiwanego wpływu na zużycie energii terminala. Przy takim podejściu system może stosować różne strategie przesyłania heartbeat, telemetrii, alarmów, aktualizacji pozycji, żądań kontaktu, komunikatów asynchronicznych lub sesji komunikacji interaktywnej, tak aby zoptymalizować kompromis między szybkością, niezawodnością, ciągłością operacyjną i efektywnością energetyczną. Architektura ta pozwala uniknąć bezkrytycznego stosowania jednego schematu transmisji dla wszystkich klas informacji, stawiając zamiast tego na kontekstowe zarządzanie ruchem aplikacyjnym, spójne z funkcją bezpieczeństwa systemu oraz z ograniczeniami właściwymi dla urządzenia ubieralnego zasilanego z baterii.

Bezpieczeństwo komunikacji

Komunikacja między urządzeniem H09 a platformą jest chroniona szyfrowaniem TLS i wzajemnym uwierzytelnianiem (mTLS). Każde urządzenie posiada własny certyfikat cyfrowy X.509, wydany przez dedykowaną infrastrukturę PKI i podlegający automatycznemu odnawianiu. Kanały komunikacji wykorzystywane przez urządzenie, zarówno MQTT, jak i HTTPS, są szyfrowane. Dostęp użytkowników Control Room do platformy internetowej jest chroniony połączeniem HTTPS i uwierzytelnianiem dwuskładnikowym (TOTP).

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Klauzule zabezpieczające dotyczące komunikacji adaptacyjnej

Zastosowanie adaptacyjnej logiki komunikacji poprawia ogólną wydajność systemu, ale nie gwarantuje w sposób bezwzględny ciągłości, braku opóźnień ani pewnego doręczenia każdego komunikatu w każdych warunkach operacyjnych lub infrastrukturalnych.

Komunikacja adaptacyjna między Control Room a operatorem

W przypadkach przewidzianych w konfiguracji system może umożliwiać otwarcie kanału komunikacji przez Control Room bez konieczności uprzedniej ręcznej akceptacji przez operatora na urządzeniu. Tryb ten ma szczególne znaczenie w sytuacjach, w których pracownik nie jest w stanie szybko wejść w interakcję z terminalem lub w których szybkość nawiązania kontaktu stanowi priorytetowy wymóg operacyjny.
W tym kontekście różne rodzaje komunikacji mogą podlegać zróżnicowanym zasadom. Sesje komunikacji oparte na Teams lub równoważnych kanałach mogą być zarządzane przez Control Room jako integralna część workflow udzielania pomocy i nadzoru, natomiast inne tradycyjne połączenia głosowe mogą podlegać odmiennym trybom obsługi w zależności od zastosowanej konfiguracji, przypadku użycia oraz dostępności powiązanych usług.

Klauzule zabezpieczające

Możliwość zdalnego otwarcia kanału komunikacji nie gwarantuje sama w sobie pełnej zrozumiałości rozmowy, ciągłej dostępności audio lub wideo ani faktycznej możliwości interakcji operatora w każdych okolicznościach. Jakość sesji zależy od łączności, stanu urządzenia, warunków otoczenia, hałasu, konfiguracji oraz dostępności zaangażowanych usług zdalnych.
Zastosowanie wielu kanałów pełni funkcję odporności aplikacyjnej. Celem jest zmniejszenie prawdopodobieństwa, że pojedynczy punkt awarii uniemożliwi przejęcie zdarzenia do obsługi. Obecność wielu kanałów komunikacji nie gwarantuje bezwzględnego doręczenia, ciągłej dostępności ani pewnego nawiązania kontaktu w każdych okolicznościach. Komunikacja zależy od zasięgu radiowego, stanu sieci, usług podmiotów trzecich, konfiguracji, integralności backendu, stanu urządzenia oraz dostępności odbiorców.
Uruchomienie SOS lub innych kanałów alarmowych nie zastępuje struktury organizacyjnej ratownictwa i nie stanowi gwarancji, że wezwanie zostało odebrane, zrozumiane lub obsłużone w oczekiwanym czasie.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Wyłączna wieloużytkownikowa obsługa alarmów i organizacja przejmowania zdarzeń

System stosuje logikę wyłącznej wieloużytkownikowej obsługi alarmów, mającą zapewnić, że każde zdarzenie jest w danym momencie obsługiwane przez jednego operatora Control Room, co pozwala uniknąć nakładania się działań, równoległych interwencji, dublowania czynności lub niejasności co do odpowiedzialności operacyjnej. W tym modelu, gdy alarm zostaje przeniesiony ze stanu nowego zgłoszenia do stanu przejęcia do obsługi operacyjnej, przestaje być dostępny na aktywnej liście pozostałych operatorów i zostaje tym samym przypisany wyłącznie do osoby, która rozpoczęła jego obsługę.
Architektura ta pozwala zachować przejrzystą identyfikowalność odpowiedzialności operacyjnej za zdarzenie w fazie interwencji, zmniejszając ryzyko, że kilku operatorów będzie jednocześnie działać w odniesieniu do tego samego alarmu w sposób nieskoordynowany, nadmiarowy lub wzajemnie się zakłócający.
Jeżeli operator, który przejął alarm, przerwie jego obsługę, nie doprowadzając go do przewidzianego zamknięcia workflow, zdarzenie może zostać zwolnione i przywrócone do stanu ponownej dostępności, stając się ponownie widoczne dla pozostałych operatorów Control Room i możliwe do ponownego przypisania. Przy takim podejściu system łączy wyłączność przejęcia z możliwością zwolnienia i ponownego przypisania, aby zachować zarówno porządek operacyjny, jak i odporność organizacyjną w przypadku porzucenia obsługi, niedostępności, przekazania odpowiedzialności lub potrzeby redystrybucji obciążenia.
System może ponadto przewidywać, że alarm pozostający w stanie „NEW" bez przejęcia do obsługi w określonym maksymalnym czasie, skonfigurowanym tak, aby zapewnić niezbędną szybkość reakcji odpowiednią do przypadku użycia, automatycznie uruchamia wewnętrzną eskalację w Control Room do właściwych kierowników lub osób odpowiedzialnych. W tej konfiguracji nieprzejęcie zdarzenia w oczekiwanym oknie czasowym nie pozostaje ograniczone wyłącznie do operacyjnego poziomu pierwszej linii, lecz uruchamia kolejny poziom uwagi organizacyjnej, mający na celu ograniczenie ryzyka opóźnień niezgodnych z protokołami usługi lub z krytycznością zdarzenia.
Control Room jest zorganizowana z obsadą operacyjną dobraną tak, aby zapewnić możliwie największą, racjonalnie osiągalną szybkość przejmowania alarmów i obsługi powiązanych procedur. Struktura jednostki nadzorującej, liczba operatorów, poziomy eskalacji i podział odpowiedzialności mogą być określane w zależności od liczby obsługiwanych obiektów, poziomu ryzyka, liczby urządzeń oraz protokołów operacyjnych klienta.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Workflow interwencji powiązany z alarmem nie musi być jednolity na całej platformie, lecz może być różnicowany dla poszczególnych tenantów, obiektów lub innych jednostek organizacyjnych przewidzianych w architekturze aplikacyjnej. Takie zróżnicowanie pozwala dostosować do protokołów klienta procedury ewakuacji, reguły eskalacji, kryteria priorytetu, odbiorców powiadomień, sposoby zwalniania lub ponownego przypisywania zdarzeń oraz, bardziej ogólnie, zachowanie operacyjne Control Room w zależności od specyfiki obsługiwanego środowiska.
W tym kontekście system nie narzuca jednego abstrakcyjnego modelu interwencji, lecz pozwala dostosować cykl życia alarmu do procedur zakładowych, planów awaryjnych, logiki obiektu oraz reguł organizacyjnych, które w praktyce określają przejmowanie i obsługę zdarzenia.

Klauzule zabezpieczające dotyczące wyłącznej wielożytkownikowej obsługi alarmów

Wyłączna wielożytkownikowa obsługa alarmów poprawia porządek operacyjny, identyfikowalność odpowiedzialności i ograniczenie wzajemnych zakłóceń między operatorami, ale nie gwarantuje sama w sobie bezwzględnego braku opóźnień, niewłaściwego zwolnienia, nieoptymalnych ponownych przypisań ani nieciągłości w obsłudze zdarzenia. Skuteczność mechanizmu zależy od prawidłowej konfiguracji workflow, dostępności personelu dyżurnego, ciągłości działania systemów backendowych oraz jakości organizacji operacyjnej Control Room.
Wewnętrzna eskalacja alarmu nieprzejętego do obsługi w skonfigurowanym maksymalnym czasie stanowi organizacyjny środek zabezpieczający mający na celu ograniczenie ryzyka braku szybkiej reakcji, ale nie gwarantuje sama w sobie, że każde zdarzenie zostanie przejęte lub obsłużone bez opóźnienia w każdych okolicznościach. Jej skuteczność zależy od właściwego dobrania obsady, dostępności zaangażowanych osób odpowiedzialnych, konfiguracji progów czasowych oraz ciągłości działania platformy.
Różnicowanie workflow według tenanta, obiektu lub protokołu klienta zwiększa zgodność platformy z rzeczywistymi procedurami awaryjnymi i koordynacyjnymi, ale wymaga odpowiedniego etapu projektowania, konfiguracji, walidacji i utrzymania reguł. Niekompletne, niespójne lub nieaktualne konfiguracje mogą wpływać na prawidłowy przebieg cyklu życia alarmu oraz na spójność między zachowaniem systemu a procedurami klienta.
System zapewnia ustrukturyzowane wsparcie operacyjnej obsługi alarmów, ale nie zastępuje nadzoru człowieka, szkolenia operatorów Control Room, właściwego zwymiarowania usługi, protokołów interwencji klienta ani odpowiedzialności organizacyjnej związanej z zarządzaniem sytuacjami awaryjnymi.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Obsługa ŚOI bez Bluetooth za pomocą QR code lub wyboru z listy

System obsługuje również rejestrację ŚOI bez Bluetooth poprzez skanowanie QR code lub, w przewidzianych przypadkach, poprzez wybór z listy w interfejsie urządzenia. Funkcja ta pozwala rozszerzyć kontrolę proceduralną również na środki ochrony, które z przyczyn organizacyjnych muszą być rejestrowane ręcznie na początku zmiany lub przed określoną czynnością.

W najprostszym przypadku użycia pracownik rejestruje wymagany ŚOI, skanując odpowiedni QR code. W alternatywnym przypadku użycia pracownik wybiera z listy na urządzeniu właściwy ŚOI lub zestaw proceduralny. W obu przypadkach system zapisuje dokonaną rejestrację jako element zgodności aplikacyjnej.

Istotną cechą tej funkcji jest to, że weryfikacja braku ŚOI bez Bluetooth niekoniecznie następuje w pierwszej chwili rozpoczęcia zmiany. System może bowiem przewidywać początkowe okno przeznaczone na prawidłową rejestrację, tak aby brak natychmiastowej rejestracji nie generował przedwczesnych alarmów, gdy procedura wejścia jest jeszcze w toku.

Typowym przypadkiem użycia jest pracownik, który przed rozpoczęciem czynności musi zadeklarować lub zarejestrować środki ochrony. Jeżeli system nie wykryje, w skonfigurowanych warunkach i czasie, rejestracji wymaganych ŚOI, może wygenerować alarm niezgodności, pojedynczy lub powtarzany, zgodnie z logiką zdefiniowaną centralnie. Funkcja ta ma zatem charakter przede wszystkim proceduralny: ma na celu wzmocnienie przestrzegania zasad rozpoczęcia czynności lub wejścia do obszaru oraz dostarczenie platformie aplikacyjnego dowodu, że wymagany krok został wykonany.

Obowiązkowe wyposażenie w ŚOI bez Bluetooth jest konfigurowalne na wielu poziomach i może być definiowane w zależności od tenanta, poszczególnego obiektu operacyjnego, przydzielonego zadania, profilu poszczególnego operatora oraz, bardziej ogólnie, reguł organizacyjnych mających zastosowanie do danego przypadku użycia. W zaawansowanym podejściu projektowym konfiguracja ta może ponadto zostać zintegrowana na poziomie backendu z systemami legacy lub istniejącymi aplikacjami do zarządzania pozwoleniami na pracę, uprawnieniami operacyjnymi, procedurami dostępu do obszarów lub czynności oraz innymi ograniczeniami organizacyjnymi, tak aby kontrola ŚOI była spójna z ogólnymi ramami uprawnień obowiązującymi na obiekcie.

Wybór z listy lub skanowanie QR code ŚOI nie musi być przewidziane jako krok obowiązkowy we wszystkich konfiguracjach aplikacyjnych systemu. W zależności od przyjętego modelu

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

organizacyjnego, poziomu integracji projektowej oraz reguł zdefiniowanych dla obiektu procedura może bowiem być obowiązkowa, opcjonalna lub w ogóle niewymagana.

Klauzule zabezpieczające dotyczące ŚOI bez Bluetooth rejestrowanych za pomocą QR lub wyboru z listy

Rejestracja za pomocą QR code lub wyboru z listy stanowi aplikacyjny dowód odnotowania w systemie i **nie jest bezwzględnym dowodem faktycznego fizycznego posiadania, prawidłowego noszenia, przydatności technicznej ani ciągłego używania ŚOI przez cały czas trwania zmiany**.

Pozycjonowanie i lokalizacja operatora

Funkcja pozycjonowania nie opiera się na jednym źródle, lecz na polityce wieloczujnikowej zaprojektowanej w celu utrzymania możliwie najbardziej wiarygodnego oszacowania pozycji operatora, aktywowanej wyłącznie w przypadku alarmu, w zróżnicowanych środowiskach, ze szczególnym uwzględnieniem kompromisu między dokładnością, ciągłością danych i efektywnością energetyczną urządzenia noszonego na ciele.
Lokalizacja łączy informacje pochodzące z wielu dostępnych technologii, w tym GNSS (Global Navigation Satellite System), wspomaganych usług lokalizacyjnych, dostawców lokalizacji łączonej (fused), IMU (Inertial Measurement Unit), inercyjnej nawigacji zliczeniowej (dead-reckoning), WiFi fingerprinting, Bluetooth fingerprinting oraz, jeżeli są dostępne, RTLS (Real-Time Location System) lub innych źródeł kontekstowych. Końcowe oszacowanie wynika z połączenia tych danych w jednym modelu fuzji, tak aby ograniczyć zależność od pojedynczego źródła i zwiększyć odporność danych.
Podstawową zasadą podsystemu jest stosowanie strategii akwizycji oportunistycznej. System nie wymusza w każdej chwili maksymalnej aktywności odbiornika pozycji, lecz najpierw ocenia, czy w pamięci podręcznej (cache) jest już dostępny niedawny i wystarczająco wiarygodny fix pozycji. Gdy natomiast cache nie jest już uznawany za odpowiedni, system przystępuje do nowej aktywnej akwizycji.
Aktywna akwizycja nie przebiega jednakowo we wszystkich warunkach. Strategia może bowiem dostosowywać się do kontekstu, preferując różne tryby w zależności od stanu operacyjnego urządzenia, jakości dostępnego sygnału, ewentualnego stanu alarmowego, prawdopodobnego charakteru scenariusza (wewnątrz lub na zewnątrz budynków) oraz wymaganego poziomu dokładności. W ten sposób system dąży do najlepszej równowagi między precyzją a efektywnością energetyczną.

Kolejnym istotnym elementem jest walidacja spójności fixów pozycji. Pozycja kandydująca nie jest akceptowana automatycznie tylko dlatego, że jest dostępna, lecz może zostać porównana z poprzednią pozycją, deklarowaną dokładnością, wiekiem pomiaru oraz wiarygodnością ruchu wynikającego z przejścia od jednego fixa do drugiego. Pozwala to ograniczyć skoki pozycji niezgodne z rzeczywistym ruchem osoby oraz zmniejszyć skutki sporadycznych błędów dostawcy lub pogorszonych warunków radiowych.
Architektura ta umożliwia różne przypadki użycia. Na otwartym terenie zewnętrznym system może z większą niezawodnością opierać się na źródłach satelitarnych lub na dostawcach lokalizacji łączonej, uzyskując stosunkowo bezpośrednie oszacowanie. Wewnątrz budynków lub w strefach ekranowanych lokalizacja może w większym stopniu zależeć od informacji inercyjnych, odcisków radiowych (fingerprint) lub reguł obszarowych. W stanie alarmowym system może zwiększyć częstotliwość aktualizacji, aby ślad operacyjny był bardziej przydatny dla jednostki nadzorującej. W warunkach zwykłego użytkowania może natomiast stosować bardziej zachowawcze polityki w celu zachowania autonomii i ogólnej ciągłości działania urządzenia.
Zarządzanie pozycjonowaniem realizowane jest zwykle w ujęciu projektowym, konfigurowanym w zależności od cech obiektu operacyjnego i faktycznie dostępnej infrastruktury. Przy takim podejściu podsystem lokalizacji może zostać zintegrowany, jeżeli są one dostępne i odpowiednio skonfigurowane, z sieciami WiFi, mapami odcisków radiowych (fingerprinting), logiką obszarową, odniesieniami topologicznymi obiektu oraz dodatkowymi źródłami kontekstowymi umożliwiającymi zwiększenie odporności oszacowania pozycji, w szczególności w środowiskach wewnątrz budynków lub mieszanych.
Polityka lokalizacji nie jest zatem z konieczności jednolita, lecz jest określana w zależności od przypadku użycia, wymaganego poziomu dokładności, ograniczeń energetycznych urządzenia, dostępności infrastruktury lokalnej oraz stopnia ciągłości śledzenia uznanego za niezbędny w danym kontekście aplikacyjnym.
W konfiguracji podstawowej system wykorzystuje wyłącznie usługi lokalizacji łączonej udostępniane przez Google Play Services, stosując adaptacyjne zarządzanie żądaniami pozycji. W tej konfiguracji wymagany poziom dokładności, częstotliwość aktualizacji i intensywność wyszukiwania są dynamicznie dostosowywane w zależności od stanu operacyjnego urządzenia i wykrytego kontekstu, na przykład z rozróżnieniem warunków zwykłych od sytuacji alarmowych, scenariuszy wewnątrz budynków od scenariuszy na zewnątrz, faz normalnego monitorowania od faz, w których wymagana jest większa szybkość przekazywania informacji do systemów zdalnych.
Również w tej konfiguracji podstawowej lokalizacja jest zatem zarządzana zgodnie z kryteriami równowagi między dokładnością, ciągłością danych i efektywnością energetyczną,

z pominięciem sztywno jednolitych podejść i z preferencją dla strategii adaptacyjnej, spójnej z funkcją bezpieczeństwa systemu oraz z ograniczeniami operacyjnymi terminala noszonego na ciele.

Klauzule zabezpieczające dotyczące pozycjonowania

Pozycja dostarczana przez system jest oszacowaniem technicznym uzyskanym w drodze fuzji danych z wielu czujników i kryteriów walidacji programowej. Nie stanowi bezwzględnego, ciągłego i nieomylnego pomiaru rzeczywistej pozycji operatora w każdej chwili.
Jakość oszacowania zależy od kontekstu (wewnątrz lub na zewnątrz budynków), zasięgu satelitarnego, zakłóceń powodowanych przez artefakty lub wielodrogowość (multipath), jakości sygnału radiowego, dostępności źródeł pomocniczych, dynamiki ruchu, stanu energetycznego urządzenia, konfiguracji oraz warunków otoczenia.
System nie gwarantuje ciągłej lokalizacji, jednolitej dokładności we wszystkich środowiskach, braku opóźnień, braku dryfu ani stałej dostępności wszystkich źródeł pozycji. **Dane o pozycji należy interpretować jako pomoc operacyjną, a nie jako bezwzględną pewność.**

Wspomagana lokalizacja dla zespołów ratowniczych i wsparcie w dotarciu do celu

W zaawansowanych konfiguracjach projektowych podsystem lokalizacji może być wykorzystywany do wspierania dotarcia do celu operacyjnego przez osoby wyznaczone do interwencji, weryfikacji lub udzielenia pomocy.
Funkcja ta ma szczególne znaczenie w środowiskach złożonych, rozległych, wewnątrz budynków lub o ograniczonej widoczności, w których sama dostępność abstrakcyjnej pozycji nie jest wystarczająca, a konieczne jest wspieranie operacyjnej koordynacji dotarcia do celu.

Klauzule zabezpieczające dotyczące wspomaganej lokalizacji celu

Również w zaawansowanych konfiguracjach wspomaganej lokalizacji system zapewnia wsparcie operacyjne, a nie bezwzględną gwarancję szybkiego, precyzyjnego lub wolnego od błędów dotarcia do osoby lub punktu docelowego. Skuteczność zależy od jakości infrastruktury obiektu, dostępności źródeł lokalizacji, spójności mapowania oraz rzeczywistych warunków otoczenia.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Konfigurowalność systemu i zależność od przypadku użycia

System SAS jest w wysokim stopniu konfigurowalny. Parametry progowe, logika alarmów, czasy opóźnienia, polityki komunikacji, kryteria lokalizacji, reguły obszarowe, wykazy ŚOI, częstotliwości aktualizacji i zachowania interfejsu mogą być dostosowywane do przypadku użycia i personalizowane dla tenanta, obiektu, grupy, stanowiska, zespołu, aż po poziom indywidualny.
Ta konfigurowalność stanowi jedną z głównych zalet platformy, ponieważ pozwala stosować ją w różnych kontekstach bez sprowadzania wszystkich sytuacji operacyjnych do jednego standardowego modelu. Jednocześnie sprawia ona, że system w dużym stopniu zależy od poprawności zastosowanej konfiguracji. Dobrze zaprojektowana funkcja, lecz sparametryzowana w sposób niespójny z obiektem, ryzykiem i organizacją, może dawać niezadowalające rezultaty aplikacyjne.

Zdalne aktualizacje i rekonfiguracja platformy

Konfigurowalność platformy obejmuje również możliwość zdalnej aktualizacji parametrów, reguł, profili aplikacyjnych, stron operacyjnych, wymaganego wyposażenia, polityk lokalizacji, logiki ostrzeżeń i innych elementów funkcjonalnych systemu, tak aby dostosować zachowanie urządzenia i backendu do zmian zachodzących na obiekcie, w procedurach lub w przyjętym modelu organizacyjnym. Możliwość ta pozwala utrzymywać system w zgodności z kontekstem operacyjnym bez konieczności wykonywania lokalnych ręcznych interwencji na każdym terminalu, z wyjątkiem przypadków, w których konkretna architektura wdrożenia lub polityki klienta przewidują inne tryby.

Klauzule zabezpieczające dotyczące aktualizacji i rekonfiguracji

Czynności aktualizacji i rekonfiguracji zwiększają zdolność adaptacji systemu, ale wymagają odpowiedniego zarządzania cyklem życia aplikacji, walidacji zmian oraz kontroli spójności między wdrożoną konfiguracją a rzeczywistym przypadkiem użycia. Zmiany nieprawidłowo zwalidowane lub niespójne z kontekstem mogą zmienić zachowanie operacyjne systemu.

Automatyczna i cicha aktualizacja aplikacji w trybie OTA

System może obsługiwać procedury aktualizacji aplikacji w trybie OTA (Over-The-Air), umożliwiające zdalną dystrybucję nowych wersji oprogramowania bez konieczności

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

lokalnych ręcznych interwencji na poszczególnych urządzeniach. W tej konfiguracji aktualizacja APK może być przeprowadzana automatycznie i bezgłośnie, zgodnie z politykami bezpieczeństwa, uprawnieniami systemowymi i trybami wdrażania przewidzianymi w przyjętej architekturze.

Możliwość ta pełni podwójną rolę aplikacyjną. Z jednej strony stanowi narzędzie rozwojowego utrzymania, ponieważ pozwala dystrybuować ulepszenia funkcjonalne, poprawki, optymalizacje, dostosowania w zakresie kompatybilności, udoskonalenia algorytmów, aktualizacje interfejsu oraz ulepszenia logiki komunikacji, lokalizacji lub obsługi alarmów. Z drugiej strony stanowi również ważny element wspierający personalizacje projektowe, ponieważ pozwala w kontrolowany sposób wprowadzać, aktualizować lub dostosowywać komponenty oprogramowania specyficzne dla danego klienta, obiektu, stanowiska lub konkretnego wdrożonego przypadku użycia.

Z operacyjnego punktu widzenia cicha aktualizacja pozwala skrócić czas propagacji zmian, szybciej ujednolicić flotę urządzeń, ograniczyć potrzebę ręcznych rekonfiguracji w terenie oraz zachować większą spójność między wersją oprogramowania, konfiguracją backendu i ogólną architekturą aplikacyjną. W rozproszonym ekosystemie, takim jak SAS, funkcja ta w istotny sposób przyczynia się do sterowalności platformy, zarówno w środowiskach scentralizowanych, jak i on premises lub zarządzanych hybrydowo.

Aktualizacja OTA może ponadto służyć wspieraniu stopniowego rozwoju systemu w czasie, umożliwiając rozszerzanie integracji z ekosystemem bezpieczeństwa, wprowadzanie nowych funkcji, rozbudowę stron operacyjnych, zmianę logiki interakcji z Control Room lub dostosowanie do szczególnych wymagań projektowych pojawiających się w cyklu życia rozwiązania.

Ze względu na ciągłość operacyjną i efektywność energetyczną aktualizacja OTA jest zazwyczaj odkładana do pierwszego ładowania po udostępnieniu nowej wersji, tak aby zminimalizować wpływ na bieżące czynności, uniknąć zakłóceń funkcji operacyjnych urządzenia podczas zmiany oraz ograniczyć wpływ procesu aktualizacji na pozostały czas pracy baterii. Przy takim podejściu moment udostępnienia i moment faktycznej instalacji niekoniecznie się pokrywają, ponieważ architektura preferuje logikę dystrybucji zgodną z rzeczywistym użytkowaniem terminala w terenie.

W tej perspektywie automatycznej i cichej aktualizacji nie należy rozumieć wyłącznie jako technicznego narzędzia dystrybucji oprogramowania, lecz jako **strukturalny komponent utrzymywalności i kontrolowanego rozwoju platformy**, zdolny do wspierania zarówno standardowego rozwoju produktu, jak i zarządzania profilami aplikacyjnymi oraz specyficznymi personalizacjami.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com

Klauzule zabezpieczające dotyczące aktualizacji OTA

Dostępność mechanizmów automatycznej i cichej aktualizacji nie gwarantuje sama w sobie, że każda aktualizacja zostanie z powodzeniem rozesłana, pobrana, zainstalowana lub uruchomiona w każdych okolicznościach. Skuteczność procesu zależy od dostępności łączności, stanu urządzenia, kompatybilności rozsyłanej wersji, prawidłowego zarządzania cyklem wydań, dostępności niezbędnej przestrzeni, polityk bezpieczeństwa terminala oraz prawidłowej integracji między backendem, pakietem aplikacji i architekturą wdrożenia. Odłożenie instalacji do kolejnego ładowania zwykle zmniejsza wpływ na działalność operacyjną i autonomię urządzenia, ale nie gwarantuje samo w sobie, że aktualizacja zostanie zastosowana natychmiast po udostępnieniu lub w jednolitym przedziale czasu w całej flocie terminali. Faktyczny moment instalacji może zależeć od rzeczywistych cykli użytkowania i ładowania, dostępności łączności w przewidzianym momencie, stanu terminala oraz przyjętych reguł dystrybucji.
Aktualizacja oprogramowania, choć służy rozwojowemu doskonaleniu i kontrolowanemu zarządzaniu personalizacjami, wymaga odpowiednich procedur walidacji, weryfikacji i zarządzania wydaniami. Zmiany nieprawidłowo zwalidowane lub niespójne z kontekstem operacyjnym mogą wpływać na zachowanie aplikacyjne systemu, ciągłość niektórych funkcji lub spójność z konfiguracjami obiektu.
Obecność funkcji zdalnej aktualizacji **nie eliminuje konieczności planowania cyklu utrzymania, kontroli rozsyłanych wersji, weryfikacji po wydaniu oraz organizacyjnego nadzoru nad wprowadzonymi zmianami**. Również w przypadku cichej aktualizacji należy zapewnić spójność między rozwojem oprogramowania, wymaganiami przypadku użycia, konfiguracją backendu i procedurami operacyjnymi klienta.

Ogólne klauzule zabezpieczające dotyczące konfiguracji

System może być używany wyłącznie w konfiguracjach spójnych z kontekstem operacyjnym, stanowiskiem pracy, procedurami zakładowymi oraz celami, dla których został wdrożony. Niekompletne, niespójne, niezwalidowane lub nieaktualne konfiguracje mogą znacznie zmienić czułość, swoistość, szybkość i przydatność generowanych informacji.

Stan ładowania i zawieszenie funkcji operacyjnych

Gdy urządzenie zostanie trwale podłączone do ładowania w sposób przewidziany na zakończenie zmiany lub na czas odstawienia, system automatycznie zawiesza funkcje monitorowania i generowania zdarzeń, aby uniknąć niewłaściwej interpretacji stanu terminala w warunkach niezgodnych z normalnym noszeniem na nadgarstku. W tej

konfiguracji przejście do stanu ładowania nie oznacza wyłącznie uzupełnienia energii, lecz może również stanowić aplikacyjny wskaźnik wyjścia urządzenia ze zwykłego kontekstu użytkowania.

Klauzule zabezpieczające dotyczące stanu ładowania

Podłączenie urządzenia do ładowania powoduje zawieszenie niektórych funkcji operacyjnych; w związku z tym terminal znajdujący się w tym stanie nie może być uznawany za w pełni równoważny urządzeniu noszonemu i aktywnemu podczas normalnej zmiany roboczej.

Integracja smartwatcha z ekosystemem bezpieczeństwa

Smartwatch H09 nie został pomyślany jako odizolowany terminal, lecz jako osobisty węzeł szerszego ekosystemu bezpieczeństwa, w którym wartość operacyjna wynika z integracji urządzeń indywidualnych, rozproszonych czujników, infrastruktury obiektu, systemów nadzoru oraz zaawansowanych modułów oprogramowania do interpretacji kontekstu. W tej architekturze urządzenie noszone na ciele może działać zarówno jako źródło zdarzeń i danych, jak i jako punkt końcowy odbioru ostrzeżeń, alarmów, instrukcji operacyjnych, stanów kontekstowych i treści wspierających pochodzących z pozostałej części ekosystemu.

Klauzule zabezpieczające dotyczące integracji z ekosystemem

Integracja smartwatcha z dodatkowymi elementami sprzętowymi i programowymi ekosystemu bezpieczeństwa poszerza dostępny obraz informacyjny i możliwości koordynacji operacyjnej, ale nie gwarantuje sama w sobie bezwzględnej kompletności, nieprzerwanej ciągłości ani nieomylnej poprawności odwzorowania ryzyka. Ogólna skuteczność zależy od jakości i dostępności zintegrowanych podsystemów, poprawności interfejsów, spójności projektowej architektury, stanu utrzymania infrastruktury, dostępności łączności oraz prawidłowej konfiguracji reguł korelacji.

Ogólne klauzule zabezpieczające dotyczące użytkowania

System musi zostać włączony w ustrukturyzowany model organizacyjny obejmujący szkolenie personelu, procedury awaryjne, nadzór, konserwację urządzeń, kontrolę konfiguracji, okresową weryfikację prawidłowego użytkowania oraz dostępność jednostki nadzorującej, jeżeli została przewidziana.
System nie nadaje się do pełnienia funkcji jedynego zabezpieczenia pracownika. Musi być uzupełniony o środki ludzkie, techniczne, organizacyjne i proceduralne wymagane w danym kontekście.

Niewłaściwe użytkowanie, nienoszenie urządzenia, wyłączenie funkcji, ingerencja w oprogramowanie, niezgodne konfiguracje, użytkowanie w nieodpowiednich środowiskach lub brak konserwacji mogą znacznie obniżyć skuteczność aplikacyjną systemu.

Klauzule dotyczące niemedycznego charakteru systemu

System SAS ze smartwatchem H09 nie jest wyrobem medycznym, nie jest systemem monitorowania klinicznego, nie jest narzędziem diagnostycznym, nie jest środkiem terapeutycznym i nie jest certyfikowanym systemem ratującym życie.
Parametry życiowe, dane behawioralne, oszacowania upadku i klasyfikacje generowane przez oprogramowanie należy interpretować jako techniczne wskaźniki wspierające bezpieczeństwo operacyjne, a nie jako dokumentację medyczną, dowody kliniczne lub zaświadczenia diagnostyczne.

Klauzule ograniczenia odpowiedzialności

System nie gwarantuje uniwersalnego wykrywania każdego zdarzenia urazowego, parametru życiowego, zdarzenia proceduralnego lub kontekstowego. Nie gwarantuje braku wyników fałszywie dodatnich, braku wyników fałszywie ujemnych, bezwzględnej ciągłości usługi, pewnego doręczenia każdej komunikacji, stałej dostępności danych o pozycji ani bezwzględnej fizycznej weryfikacji faktycznej obecności ŚOI. Ewentualne niewykrycie zdarzenia, niedoskonała klasyfikacja sytuacji, opóźnienie powiadomienia, brak rejestracji ŚOI, niedokładność pozycji lub chwilowa niedostępność funkcji nie stanowią same w sobie automatycznego dowodu pewnej wadliwości działania ani odpowiedzialności na zasadzie ryzyka producenta lub dostawcy.
Na organizacji użytkującej spoczywa odpowiedzialność za określenie właściwego przypadku użycia, walidację konfiguracji, przeszkolenie personelu, utrzymanie sprawności systemu, przygotowanie procedur awaryjnych oraz uzupełnienie systemu o wszystkie niezbędne środki dodatkowe.

Oświadczenie końcowe

System SAS ze smartwatchem H09 jest platformą technologiczną wspierającą bezpieczeństwo operacyjne.
System został zaprojektowany w celu zwiększenia prawdopodobieństwa wychwycenia zdarzeń krytycznych, wzmocnienia zgodności z procedurami, poprawy możliwości zdalnego nadzoru oraz wspierania organizacji reagowania. Działa jednak w granicach właściwych dla urządzenia noszonego na nadgarstku, czujników nieklinicznych, wnioskującej logiki

programowej, infrastruktury komunikacyjnej nie zawsze w pełni kontrolowalnej oraz zmiennego rzeczywistego kontekstu operacyjnego.

Z tych powodów system nie stanowi wyrobu medycznego, nie zastępuje nadzoru człowieka, nie zastępuje zakładowych procedur awaryjnych i nie gwarantuje w sposób bezwzględny wykrycia, klasyfikacji, przesłania ani przejęcia do obsługi każdego zdarzenia w każdych okolicznościach.

Safe s.r.l. Unipersonale
Via Pastore n. 14 · 25046 Cazzago S. Martino (BS) · +39 030 7751504
Capitale Sociale Euro 1.000.000,00 i.v. · C.F. 01604520989 · Partita IVA 03223860176 · Iscrizione REA e CCIAA di Brescia 329091
info@safesafety.com · www.safesafety.com