APLIKAČNÍ POZNÁMKY

SYSTÉM SAFE ALERT SYSTEM (SAS) SE SMARTWATCHEM H09

TECHNICKO-FUNKČNÍ POPIS, PŘÍPADY UŽITÍ, OMEZENÍ POUŽITÍ, OCHRANNÉ DOLOŽKY A OMEZENÍ ODPOVĚDNOSTI

Úvod

Systém SAS se smartwatchem H09 je technologická platforma na podporu provozní bezpečnosti personálu, určená pro prostředí, v nichž se pracovník může nacházet v podmínkách rizika, izolace, vystavení specifickým nebezpečím, potřeby vzdáleného monitorování, povinnosti dodržovat bezpečnostní postupy nebo nutnosti rychlého spuštění nouzových workflow.

Zařízení H09 není běžné spotřebitelské nositelné zařízení. Jedná se o specializovaný provozní terminál, navržený k provádění činností na pozadí, jako je monitorování, sběr signálů, klasifikace událostí, ověřování dodržování postupů, lokalizace operátora, místní interakce při kritických událostech a zapojení osoby do strukturovaného toku varování, eskalace, komunikace a auditu.

Systém není totožný pouze s nositelným terminálem, ale zahrnuje také softwarové moduly pro místní zpracování, mechanismy centralizované konfigurace, komunikační kanály, backendové služby, systémy záznamu a dohledatelnosti a případně Control Room nebo jinou organizační složku pověřenou dohledem nad událostmi a jejich řízením.

Systém představuje technologickou pomůcku pro provozní bezpečnost. Nepředstavuje zdravotnický prostředek, nepředstavuje zdravotnickou pomůcku, neprovádí diagnostiku, nenahrazuje lidský dohled a nenahrazuje podnikové postupy pro mimořádné události, dohled, prevenci a záchranu.

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

Obsah

4 ..... Povaha systému a určené použití
4 ..... Obecná funkční architektura
5 ..... Pokročilé architektury
5 ..... Obecný princip fungování
5 ..... Provozní heartbeat a stavová telemetrie
6 ..... Ochranné doložky týkající se provozního heartbeatu
6 ..... Detekce nehybnosti
6 ..... Ochranné doložky týkající se detekce nehybnosti
7 ..... Uživatelské rozhraní operátora
8 ..... Ochranné doložky týkající se uživatelského rozhraní operátora
8 ..... Pokročilé provozní stránky
9 ..... Ochranné doložky týkající se pokročilých provozních stránek
9 ..... Detekce pádu
11 ..... Ochranné doložky týkající se detekce pádu
11 ..... Monitorování vitálních funkcí
12 ..... Ochranné doložky týkající se monitorování vitálních funkcí
12 ..... Ověření přítomnosti na zápěstí
12 ..... Ochranné doložky týkající se ověření přítomnosti na zápěstí
13 ..... Workflow varování, alarmu, zpoždění, eskalace a zrušení
13 ..... Ochranné doložky týkající se alarmového workflow
14 ..... Funkce dobrovolného SOS
14 ..... Hlasové SOS
14 ..... Tiché SOS
14 ..... Zpoždění pro zrušení SOS
15 ..... Spuštění zvukového a obrazového záznamu
15 ..... Ochranné doložky týkající se funkce SOS
15 ..... Vícekanálová komunikace
16 ..... Zabezpečení komunikace
16 ..... Ochranné doložky týkající se adaptivní komunikace
16 ..... Adaptivní komunikace mezi Control Room a operátorem
16 ..... Ochranné doložky
17 ..... Výhradní víceuživatelská správa alarmů a organizace převzetí

17 ..... Ochranné doložky týkající se výhradní víceuživatelské správy alarmů
18 ..... Správa OOP bez Bluetooth pomocí QR code nebo výběru
19 Ochranné doložky týkající se OOP bez Bluetooth registrovaných pomocí QR nebo výběru
19 ..... Určování polohy a lokalizace operátora
20 .....Ochranné doložky týkající se určování polohy
20 ..... Asistovaná lokalizace pro záchranné týmy a podpora při dosažení cíle
20 ..... Ochranné doložky týkající se asistované lokalizace cíle
21 .....Konfigurovatelnost systému a závislost na případu užití
21 ..... Vzdálené aktualizace a rekonfigurace platformy
21 ..... Ochranné doložky týkající se aktualizací a rekonfigurace
21 ..... Automatická a tichá aktualizace aplikace v režimu OTA
22 .....Ochranné doložky týkající se aktualizace OTA
22 .....Obecné ochranné doložky týkající se konfigurace
23 ..... Stav nabíjení a pozastavení provozních funkcí
23 .....Ochranné doložky týkající se stavu nabíjení
23 .....Integrace smartwatche do bezpečnostního ekosystému
23 ..... Ochranné doložky týkající se integrace do ekosystému
23 .....Obecné ochranné doložky týkající se používání
23 ..... Doložky o nezdravotnické povaze
24 ..... Doložky o omezení odpovědnosti
24 .....Závěrečné prohlášení

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

Povaha systému a určené použití

Systém je určen k podpoře provozní bezpečnosti ve všech případech, kdy je užitečné:

- s vyšší pravděpodobností detekovat úrazové události nebo dynamiku odpovídající pádu;
- umožnit dobrovolné přivolání pomoci;
- monitorovat vitální funkce pro preventivní, nikoli však diagnostické účely;
- udržovat průběžný nebo téměř průběžný odhad polohy operátora;
- ověřovat soulad s požadavky na osobní ochranné prostředky vyžadované v daném provozním kontextu;
- spojovat události, polohu, stav zařízení a pravidla oblastí do jediného dohledového přehledu;
- spouštět toky komunikace, oznamování, eskalace a dohledatelnosti směrem ke vzdáleným systémům nebo kontrolním složkám.

Určené použití systému se tedy týká zmírňování rizika, zvýšení pravděpodobnosti zjištění neobvyklých stavů, podpory včasnosti organizačního zásahu a zlepšení dohledatelnosti událostí.

Systém není určen k tomu, aby nahrazoval preventivní povinnosti zaměstnavatele nebo představoval jediné bezpečnostní opatření pracovníka.

Obecná funkční architektura

Na nositelném terminálu probíhá sběr dat ze senzorů, místní zpracování, předběžná klasifikace událostí, interakce s operátorem, řízení předem stanovených workflow a shromažďování provozního kontextu. V backendu jsou uloženy konfigurace, profily, prahové parametry, komunikační logika, pravidla oblastí, seznamy OOP, zásady lokalizace, kritéria oznamování, archivační systémy a integrační kanály do Control Room. Na organizační úrovni dohledová složka přijímá události, vyhodnocuje je a spouští stanovené postupy.
Control Room nepředstavuje pouze organizační úroveň příjmu, vyhodnocování a řízení událostí generovaných nositelnými zařízeními, ale je aktivní a strukturální součástí architektury SAS jakožto centrální uzel orchestrace bezpečnostních stavů pracoviště. V tomto modelu je Control Room navržena také jako nativní zdroj alarmů, provozních oznámení a koordinačních povelů, které lze selektivně adresovat jednotlivým operátorům, týmům, homogenním skupinám nebo celému pracovišti v závislosti na probíhajícím scénáři, profilu příjemců, jejich logické nebo zeměpisné poloze a dostupnosti individuálního připojení.
Toto nastavení umožňuje platformě distribuovat téměř v reálném čase pokyny, výstražné stavy a pokyny k chování vyplývající z celkové situace na pracovišti. Patří sem například vydávání příkazů k evakuaci, svolávání na shromaždiště, spouštění postupů izolace nebo vzdálení se a šíření alarmů týkajících se událostí na pracovišti. Ve stejném provozním modelu může smartwatch navíc plnit roli terminálu pro přímé doručování příkazů, pokynů a

provozních zpráv odesílaných z backendu (které může zařízení také přečíst nahlas), takže obsah s příkazy nebo pokyny k chování je pro operátora okamžitě dostupný, aniž by nutně musel aktivně číst displej, což zvyšuje účinnost komunikace v dynamickém, hlučném nebo vysoce kritickém prostředí.
Toto nastavení činí platformu vhodnou k podpoře nejen hlášení událostí, které pracovník utrpěl, ale také koordinované distribuce aktivních ochranných opatření, včetně opatření zaměřených na dosažení konkrétních kolektivních ochranných prostředků, bezpečných míst, shromaždišť nebo únikových cest stanovených podle povahy zjištěného nebezpečí. Control Room jakožto logické centrum ekosystému SAS proto není pouhým konečným příjemcem alarmu, ale strukturální součástí dynamického řízení bezpečnosti pracoviště, schopnou generovat, korelovat a šířit provozní výstrahy v závislosti na celkovém stavu systému.

Pokročilé architektury

Control Room ekosystému SAS lze zpřístupnit podle různých architektonických modelů, aby se přizpůsobila infrastrukturním, organizačním a konektivním charakteristikám pracoviště nebo zákazníka. V první konfiguraci může být Control Room poskytována centralizovaně prostřednictvím cloudu Safe S.r.l., což umožňuje jednotnou správu zařízení, událostí, alarmových workflow, konfigurací a provozních interakcí i napříč více pracovišti nebo distribuovanými tenanty.
V prostředích, kde není k dispozici nepřetržité a/nebo stabilní připojení, lze tutéž architekturu provozovat on premises, aby byl systém funkční i při omezeních daných izolací sítě, požadavcích na místní autonomii nebo infrastrukturních zásadách, které vyžadují zachování kritických funkcí v rámci pracoviště. V této konfiguraci Safety control room a backend, který ji podporuje, fungují lokálně a zajišťují kontinuitu funkcí dohledu, správy alarmů, archivace, lokalizace a provozní koordinace i bez trvalého spojení s externími vzdálenými službami.
V případech, kdy zákazník již disponuje existující provozní Control Room, lze Safety control room ekosystému SAS aplikačně integrovat do stávající struktury, čímž se předejde vytváření odděleného prostředí a naopak se podpoří rozšíření schopností již používané Control Room. Tato integrace může probíhat prostřednictvím API zpřístupněných systémem, která umožňují obousměrnou správu alarmů, oznámení, provozních stavů a výše popsaných interakcí, a tím jak předávání událostí generovaných ekosystémem SAS do stávající Control Room, tak spouštění alarmů, workflow a povelů určených pro připojená zařízení a subsystémy přímo z této Control Room.

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

Platforma SAS může fungovat jak jako kompletní Control Room, tak jako integrovaná součást stávající Control Room, přičemž v obou případech zachovává stejnou logiku obousměrné orchestrace provozní bezpečnosti.

Obecný princip fungování

Systém funguje na principu neinvazivního monitorování. Hlavní zpracování probíhá na pozadí; k přímé interakci s operátorem dochází, když je zjištěna situace vyžadující pozornost, když je třeba událost potvrdit nebo zrušit, když je třeba zahájit komunikaci nebo když systém vyžaduje konkrétní procedurální úkon.

Provozní heartbeat a stavová telemetrie

Systém počítá s tím, že zařízení pravidelně generuje provozní heartbeat, chápaný jako „stavové zprávy“ odesílané do backendu nebo do Control Room za účelem dohledu, ověření dosažitelnosti a aktualizace provozního přehledu o pracovníkovi. Heartbeat nepředstavuje pouhý signál přítomnosti v síti, ale konfigurovatelný informační kontejner, který může v závislosti na aplikačním profilu obsahovat stav nabití zařízení, hlavní parametry připojení, stav nošení a další metadata užitečná pro dohled.
Z aplikačního hlediska heartbeat umožňuje platformě udržovat aktuální přehled o stavu terminálu a jeho provozuschopnosti i v nepřítomnosti výslovných alarmů. Control Room tak může účinněji rozlišovat mezi absencí událostí a absencí dosažitelnosti, mezi běžnou kontinuitou provozu a možnou degradací terminálu, jakož i mezi stavy plné provozuschopnosti a stavy, kdy jsou některé funkce dočasně omezené nebo nedostupné (například bez připojení Wi-Fi).
Periodicitu, obsah a úroveň podrobnosti heartbeatu lze konfigurovat podle případu užití, rizikového kontextu, omezení konektivity a energetických zásad systému. V běžných scénářích lze přenos udržovat na konzervativnější úrovni; ve vysoce kritických scénářích nebo při výskytu událostí lze obsah nebo frekvenci stavových zpráv upravit tak, aby se zvýšila schopnost vzdáleného dohledu.

Ochranné doložky týkající se provozního heartbeatu

Přítomnost pravidelného heartbeatu nepředstavuje absolutní záruku plné provozuschopnosti všech funkcí zařízení, stejně jako dočasná absence heartbeatu automaticky neznamená jistou poruchu nebo stav ohrožení operátora. Dostupnost těchto zpráv závisí na konektivitě, energetickém stavu, konfiguraci, integritě zařízení a správném fungování přenosového řetězce.

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

Heartbeat je nástrojem na podporu provozního dohledu a nenahrazuje ověřovací postupy, organizační kontrolu ani lidské řešení situací možných anomálií.

Detekce nehybnosti

Systém zahrnuje funkci detekce nehybnosti operátora. Zařízení ji vykonává nepřetržitě a na pozadí v souladu s logikou neinvazivního monitorování, která charakterizuje celou architekturu. Funkce je založena na analýze pohybu pouze nositelného terminálu, což dále zajišťuje anonymizaci pracovníka. Pokud zařízení zůstane zcela bez pohybu po předem stanovenou dobu, konfigurovatelnou na vyžádání a činící v továrním nastavení 40 sekund, systém tento stav vyhodnotí jako potenciálně neobvyklý a spustí alarm.
Řízení události probíhá ve dvou po sobě jdoucích úrovních. V první fázi je alarm řešen lokálně na zařízení, které operátorovi umožňuje jej zrušit během prvních 10 sekund od jeho spuštění. Tento interval umožňuje pracovníkovi aktivně oznámit, že je v pořádku, a omezuje tak předávání irelevantních hlášení do Control Room. Pokud alarm není v tomto časovém okně zrušen, je událost předána do Control Room. Control Room ji převezme, ověří a v případě potřeby spustí stanovené postupy.
Z aplikačního hlediska detekce nehybnosti umožňuje platformě zachytit situace, v nichž operátor nemusí být schopen sám přivolat pomoc.
Funkce je plně konfigurovatelná. Kontrolu nehybnosti lze při počáteční konfiguraci zapnout nebo vypnout, aniž by to omezilo celkovou funkčnost zařízení. Časové parametry určující spuštění alarmu a okno pro zrušení lze definovat podle případu užití, vykonávané pracovní činnosti a provozního kontextu. To umožňuje přizpůsobit citlivost funkce skutečnému způsobu práce a zabránit tomu, aby činnosti, které ze své podstaty zahrnují dlouhá období bez pohybu, vyvolávaly nežádoucí alarmy.

Ochranné doložky týkající se detekce nehybnosti

Detekce nehybnosti je založena na absenci pohybu nošeného zařízení, nikoli na přímém hodnocení fyzického stavu operátora. V důsledku toho spuštění alarmu nehybnosti automaticky neznamená stav ohrožení nebo nevolnosti operátora. Stejně tak absence alarmu nepředstavuje záruku jeho bezpečí.
Účinnost funkce závisí na jejím skutečném zapnutí v konfiguraci, nastavených časových parametrech, správném nošení zařízení, jeho energetickém stavu a dostupnosti konektivity potřebné k přenosu události do Control Room.
Detekce nehybnosti nenahrazuje ověřovací postupy, organizační kontrolu ani lidské řešení situací možné nouze.

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

Uživatelské rozhraní operátora

Uživatelské rozhraní operátora zařízení H09 je navrženo jako jednoduché, robustní rozhraní zaměřené na rychlé použití v provozním kontextu, se zvláštním důrazem na snížení kognitivní zátěže, minimalizaci náhodných aktivací a možnost použití i ve stresu, ve spěchu nebo při omezené pozornosti pracovníka. Celková koncepce rozhraní totiž upřednostňuje funkční přehlednost, okamžitou čitelnost stavu zařízení a rychlý přístup ke kritickým funkcím a vyhýbá se složitým navigačním strukturám nebo strukturám neodpovídajícím nositelnému bezpečnostnímu terminálu.

Zařízení je vybaveno dotykovou obrazovkou, přední kamerou, mikrofonem a reproduktorem, což umožňuje nejen přímou vizuální interakci, ale také funkce zvukové komunikace a tam, kde je to stanoveno, i podporu videa. Tyto komponenty doplňují dvě fyzická tlačítka. První slouží k zapnutí a vypnutí terminálu. Druhé, označované jako stříbrné tlačítko, je spojeno s funkcí SOS (tichou i hlasitou) a se spuštěním skenování osobních ochranných prostředků (OOP).

Vedle fyzických tlačítek obsahuje dotykové rozhraní další virtuální tlačítka, která umožňují rozšířit dostupné funkce bez zavádění dalších mechanických prvků do zařízení. Soubor fyzických a virtuálních tlačítek je nakonfigurován tak, aby pomocí logiky dlouhého stisku snižoval riziko neúmyslných aktivací. Zahájení stisku doprovází krátká vibrace signalizující začátek aktivační sekvence, zatímco další krátká vibrace potvrzuje platnost stisku, a tedy skutečné přijetí povelu. Toto konstrukční řešení sleduje dvojí cíl: na jedné straně omezit neúmyslné úkony způsobené nárazy, otřením nebo náhodným dotykem, na druhé straně poskytnout operátorovi okamžitou haptickou zpětnou vazbu, užitečnou i v situacích, kdy je vizuální pozornost věnovaná displeji omezená nebo žádná.

Systém je určen pro osoby, které nosí hodinky pod pracovním oděvem a musí je umět používat, aniž by se na ně dívaly. Ve výchozím nastavení je aktivní. Mimo alarmovou situaci je obrazovka černá a zobrazuje pouze, vlevo nahoře, zelený kroužek, který slouží k ověření, že hodinky správně fungují.

Na levé straně se zobrazí ikony pokaždé, když nastane situace vyžadující pozornost:


Chybí připojení Wi-Fi, k dispozici je pouze mobilní síť. Tato ikona se na obrazovce zobrazí pouze tehdy, pokud bylo zařízení nakonfigurováno a připojeno k síti Wi-Fi; v opačném případě se tato ikona nikdy nezobrazí.


Bez připojení (Wi-Fi ani mobilní síť).


Slabý příjem GPS. Odhadovaná chyba lokalizace kolem 50 metrů.


Žádný příjem GPS.

 Slabá baterie, pod 30 %.

 Slabá baterie, pod 10 %.

 H09 není správně nasazeno.

Během alarmu se na obrazovce zobrazí dvě velká tlačítka. Nahoře se zobrazí zelený palec označující „Vše OK“, dole ikona mikrofonu. Tlačítko „Vše OK“ může po stisknutí do 10 sekund od odeslání SOS volání zrušit, zatímco po stisknutí po spuštění alarmu umožňuje sdělit Control Room, že situace je pod kontrolou. Mikrofon naopak spouští záznam okolního zvuku a lze jej použít pouze po spuštění alarmu. Tento záznam bude aktivní, dokud se Control Room se zařízením nespojí. Jakmile se Control Room připojí, záznam se automaticky zastaví a současně odešle do Control Room, která jej zobrazí na obrazovce.
Při zahájení hovoru Teams se rozhraní automaticky přizpůsobí a ve spodní části obrazovky otevře render view vyhrazený pro audiovizuální komunikaci. Tato oblast se automaticky posune do zobrazení, aby operátor mohl vidět kontaktní osobu z Control Room nebo obecně video složku spojenou s komunikační relací. Po ukončení hovoru Teams render view zmizí a rozhraní se vrátí do standardní konfigurace. Celkově je tedy uživatelské rozhraní operátora navrženo tak, aby kombinovalo okamžitost použití, odolnost vůči neúmyslným aktivacím, rychlý přístup ke kritickým funkcím a dynamické přizpůsobení probíhajícím workflow, při zachování jednoduché struktury odpovídající použití zařízení jako nositelného bezpečnostního terminálu.

Ochranné doložky týkající se uživatelského rozhraní operátora

Rozhraní zařízení je navrženo tak, aby snižovalo riziko náhodných aktivací a usnadňovalo rychlé použití kritických funkcí, avšak **nemůže absolutně vyloučit možnost neúmyslných aktivací, neplatných stisků, chyb při interakci nebo nesprávného použití za zvlášť náročných provozních podmínek.** Účinnost interakce závisí také na vnějších faktorech, jako je používání rukavic, poloha paže, okolní podmínky, nárazy, vibrace, stav pozornosti operátora, neporušenost dotykové obrazovky, funkčnost fyzických tlačítek a celkový stav zařízení.
Ikony a stavové indikátory zobrazené na obrazovce představují zjednodušené znázornění provozních podmínek zjištěných systémem a nesmějí být vykládány jako absolutní záruka nepřetržité dostupnosti příslušné funkce.
Dostupnost přední kamery, mikrofonu, reproduktoru nebo render view hovoru sama o sobě nezaručuje kvalitu, kontinuitu ani skutečnou užitečnost audio-video komunikace za všech

okolností. Tyto funkce závisejí na konektivitě, stavu zařízení, okolních podmínkách, kvalitě signálu, konfiguraci systému a dostupnosti zapojených vzdálených služeb.
Uživatelské rozhraní operátora, ačkoli je navrženo pro rychlé použití v bezpečnostním kontextu, nenahrazuje školení, výcvik, provozní postupy ani nouzové protokoly. Správné používání funkcí SOS, zrušení (abort), potvrzení, komunikace a registrace OOP vyžaduje, aby byl personál předem poučen způsobem odpovídajícím přijatému případu užití.

Pokročilé provozní stránky

Rozhraní zařízení lze v závislosti na použité konfiguraci rozšířit o provozní stránky určené pro specifické potřeby bezpečnosti, dohledu nebo podpory činnosti. Tyto stránky nepředstavují pouhé obecné informační obrazovky, ale funkční součásti aplikační architektury, které lze aktivovat v závislosti na profilu operátora, rizikovém kontextu, stavu systému nebo probíhajícím workflow.
Mezi možné konfigurace patří například stránky určené ke stručnému přehledu vitálních funkcí, stránky na podporu asistované navigace ke shromaždištím nebo bezpečným místům při evakuaci a také stránky zaměřené na vyhledání nebo dosažení konkrétních kolektivních ochranných prostředků či jiných prvků na podporu řešení mimořádných událostí přítomných na pracovišti, jako jsou lékárničky, defibrilátory, protipožární vybavení nebo obdobná provozně významná místa.
V takových případech zařízení neplní pouze funkci generátoru nebo přijímače alarmů, ale také funkci terminálu kontextové podpory činnosti, schopného poskytnout operátorovi stručné a praktické pokyny odpovídající aktuální situaci.

Ochranné doložky týkající se pokročilých provozních stránek

„Pokročilé provozní stránky“ představují nástroje kontextové podpory a nenahrazují školení, znalost pracoviště, bezpečnostní značení, nouzové postupy ani lidskou koordinaci. Skutečná užitečnost zobrazených informací závisí na správnosti konfigurace, kvalitě kontextových dat, dostupnosti lokalizace a aktuálnosti informací v backendu.

Detekce pádu

Subsystém detekce pádu je založen na analýze dat z akcelerometru a inerciálních senzorů v reálném čase s vícefázovou logikou, která nezužuje rozhodnutí na přítomnost jediné špičky zrychlení. Systém naopak analyzuje celkovou dynamickou sekvenci odpovídající možnému skutečnému pádu osoby a odlišuje ji od prudkých gest, příležitostných nárazů zápěstí,

mechanických vibrací, intenzivních pracovních činností, neúrazových nárazů, pádu samotného zařízení nebo prosté nehybnosti terminálu.
Počáteční fáze vyhodnocení spočívá v hledání věrohodného stavu gravitačního odlehčení, tj. výrazného snížení zdánlivého zrychlení odpovídajícího ztrátě opory. Tato fáze není považována za postačující podmínku, ale za kontrolní prvek, který spouští hlubší analýzu. Aby byla považována za relevantní, musí vykazovat časovou konzistenci a nesmí být lépe vysvětlitelná jako šum, náhodné kmitání nebo pohyb bez úrazového významu.
Následně systém hledá konzistentní fázi nárazu, tj. změnu zrychlení odpovídající ukončení dynamiky pádu. Ani náraz není považován za samostatně postačující kritérium, protože ne všechny nárazy odpovídají skutečným pádům a ne všechny pády způsobí zřetelný náraz. Úlohou nárazu je zvýšit věrohodnost sekvence, pokud amplitudou a časováním odpovídá předchozí fázi.
Tuto analýzu doplňuje fáze následného pozorování, jejímž cílem je vyhodnotit snížení pohybové aktivity nebo stav relativní nehybnosti. Nehybnost není považována za samostatné a postačující kritérium, protože nehybné zařízení může být jednoduše odložené, sundané nebo nenošené. Snížená následná aktivita však nabývá na významu, pokud nastane po dynamice již vyhodnocené jako významná, a posiluje hypotézu, že pozorovaná událost měla na osobu skutečné následky.
Systém dále hodnotí konečnou polohu těla a změnu orientace terminálu a považuje je za doplňkové faktory konzistence. Tyto prvky mohou pomoci odlišit skutečný pád od prostého prudkého gesta, ojedinělého nárazu nebo vibrace neodpovídající úrazové události.
V klasifikační logice se uplatňují také mechanismy hystereze, vícevzorkové validace, časová okna pozorování, penalizace vzorců neslučitelných se skutečnou událostí a kritéria robustnosti zaměřená na omezení nežádoucích aktivací. Zejména ověření, zda je zařízení skutečně nošeno, umožňuje zmírnit riziko, že pád samotného terminálu bude vyhodnocen jako pád osoby, aniž by jej však absolutně vylučovalo.
Z aplikačního hlediska je typickým případem užití pracovník, který náhle ztratí rovnováhu nebo zkolabuje s dynamikou dostatečně výraznou na to, aby vznikla sekvence odlehčení, nárazu a následného omezení pohybu. V takovém scénáři může systém vygenerovat místní varování (warning), zaznamenat událost, předat ji centrálním systémům a v případě, že nedojde ke zrušení, spustit stanovený postup eskalace.
Druhý případ užití se týká nejednoznačné nebo hraniční události, u níž zjištěná dynamika vykazuje některé prvky odpovídající pádu, nikoli však úplnou konzistenci. Za těchto okolností může systém v závislosti na použité konfiguraci přistoupit k opatrné klasifikaci, vyžádat si interakci operátora nebo spustit méně agresivní workflow.

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

Třetí případ užití se týká falešně pozitivního výsledku typického pro zápěstí, kdy intenzivní fyzická aktivita, opakované nárazy nebo rychlé pohyby vytvářejí vzorce částečně podobné pádu. V těchto případech představují hlavní nástroje omezení rozhodovacího šumu vícefázová architektura, ověření po události a možnost zrušení varování.
Navzdory propracovanosti vícefázové analýzy, přítomnosti mechanismů postupné validace, penalizace nekonzistentních vzorců a modulace konečného rizika nemůže subsystém detekce absolutně vyloučit možnost falešně pozitivních nebo falešně negativních výsledků. Složitost skutečného biomechanického jevu, umístění senzoru na zápěstí, individuální variabilita pohybů, ne zcela deterministická povaha skutečných pádů a nutnost fungovat na vestavěném (embedded) zařízení s nízkou spotřebou činí existenci zbytkové míry rozhodovací chyby přirozenou. Vícefázová analýza zvyšuje robustnost modelu a snižuje závislost na jednotlivých špičkách nebo příliš zjednodušených kritériích, nečiní však ze systému neomylný klasifikátor úrazové události. Z aplikačního hlediska je proto model navržen tak, aby zvyšoval pravděpodobnost správného zachycení pádů odpovídajících pozorovatelným signálům, nikoli aby zaručoval jisté a univerzální rozpoznání každé možné události.
Subsystém detekce pádu využívá logiku výslovně optimalizovanou pro vestavěná nositelná zařízení s nízkou spotřebou, v níž rovnováha mezi přesností detekce, rychlostí rozhodnutí, spotřebou energie, nároky na paměť a výpočetní zátěží představuje strukturální konstrukční volbu, nikoli náhodné omezení implementace. V tomto kontextu není vzorkovací frekvence akcelerometru zvyšována na teoreticky možné maximální hodnoty, ale je udržována na úrovni slučitelné s nepřetržitým monitorováním na nositelném zařízení, aby byla zachována provozní výdrž, stabilita systému a únosnost výpočetní zátěže v dlouhodobém horizontu. Použití střední vzorkovací frekvence přináší významné výhody: snižuje spotřebu senzorů a CPU, omezuje zátěž senzorových callbacků, omezuje interní datový provoz, snižuje riziko nahromadění nezpracovaných dat (backlog) a činí nepřetržité monitorování po celou dobu směny lépe udržitelným. Tato volba navíc podporuje lepší slučitelnost s vestavěnou architekturou, v níž musí zařízení současně vykonávat další funkce, jako je komunikace, lokalizace, řízení alarmových workflow, interakce s uživatelem a kontrola celkového provozního stavu.
Proti těmto výhodám s sebou nízká vzorkovací frekvence nese i konkrétní technické kompromisy. Zejména snižuje časové rozlišení, s nímž jsou pozorovány nejrychlejší přechodové jevy, může zhoršit podrobnou rekonstrukci velmi krátkých impulzních událostí a může snížit citlivost na mimořádně rychlé nebo málo trvalé mikrovzorce. K vyrovnání tohoto omezení systém nezakládá rozhodnutí na jediném vzorku, ale využívá logiku časových oken a

vícevzorkové validace, v níž je událost interpretována jako celková dynamická struktura, nikoli jako sled elementárních špiček (spike).
Stručně řečeno, subsystém detekce pádu je navržen podle logiky řízeného kompromisu: frekvence akcelerometru je zvolena tak, aby bylo nepřetržité monitorování na nositelném zařízení udržitelné, zatímco dávkové zpracování (batching) a analýza v oknech slouží k obnovení sémantické robustnosti, omezení šumu a snížení výpočetních nákladů. Výsledkem není model zaměřený na maximální surovou reaktivitu, ale model zaměřený na nejlepší provozní spolehlivost dosažitelnou při skutečných omezeních vestavěného zařízení nošeného na zápěstí.

Ochranné doložky týkající se detekce pádu

Subsystém detekce pádu představuje nástroj na podporu osobní bezpečnosti a nezaručuje jisté rozpoznání každé úrazové události. Nemusí být zachyceny pomalé pády, postupné kolapsy, uklouznutí s částečnou oporou, události s atypickou dynamikou, události s výrazným zbytkovým pohybem zápěstí nebo události, k nimž došlo při nesprávně nošeném zařízení.
Systém nezaručuje absenci falešně pozitivních ani absenci falešně negativních výsledků. Detekce závisí na dynamice události, poloze zařízení, stavu nošení, provozních podmínkách a použité konfiguraci.
Nezjištění pádu nebo vygenerování nežádoucího alarmu samo o sobě nepředstavuje automatický důkaz jisté poruchy ani základ objektivní odpovědnosti výrobce nebo dodavatele.
Subsystém detekce pádu nenahrazuje lidský dohled, podnikové postupy pro mimořádné události, hodnocení rizik, školení personálu, preventivní opatření, specializované OOP ani jiná bezpečnostní opatření stanovená pro daný provozní kontext.

Monitorování vitálních funkcí

Systém obsahuje subsystém monitorování vitálních funkcí určený k detekci potenciálně neobvyklých fyziologických stavů během pracovní činnosti. Monitorování je navrženo jako **preventivní, nediagnostická funkce** a je založeno na sběru vitálních parametrů, které může nošené zařízení snímat a které jsou převáděny na aplikační ukazatele pozornosti nebo rizika. Zpracování vitálních funkcí se neomezuje na vyhodnocení okamžité hodnoty jednotlivého měření. Každý parametr je naopak posuzován v čase jako časová řada, na jejímž základě může systém sestavovat průměry, průběžné statistiky, ukazatele variability, odchylky od obvyklého chování, podmínky přetrvávání a kritéria stability signálu. Tento přístup umožňuje

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

účinněji rozlišovat mezi přechodnými výkyvy malého významu a opakovanými nebo přetrvávajícími anomáliemi.

Systém tak může rozpoznat různé aplikační situace.

- U pracovníka se vyskytuje parametr, který trvale překračuje práh pozornosti nebo je výrazně neobvyklý vzhledem k jeho vlastnímu historickému profilu. Systém může vygenerovat „varování“ (warning), které se řeší podle nakonfigurovaného workflow.
- Anomálie nevyplývá ani tak z absolutní hodnoty, jako spíše z výrazné odchylky od individuálního průměru. V tomto scénáři je funkce monitorování zvláště užitečná u zařízení trvale přidělených stejnému operátorovi, protože osobní historie zvyšuje citlivost na změny, které nemusejí být extrémní v absolutní hodnotě, ale jsou významné vzhledem k běžnému fyziologickému chování dané osoby.
- Více souběžných parametrů vykazuje mírné, ale konzistentní odchylky. Systém pak může příspěvky jednotlivých modulů agregovat do celkového hodnocení rizika a posuzovat situaci systémověji a méně závisle na jediném izolovaném měření.

Monitorování vitálních funkcí dále spolupracuje s ověřením přítomnosti na zápěstí. Snímání těchto hodnot má totiž technický význam pouze tehdy, je-li zařízení pravděpodobně nošeno a kontakt s tělem je dostatečně spolehlivý. Nejsou-li tyto podmínky splněny, může se informační hodnota dat výrazně snížit.

Ochranné doložky týkající se monitorování vitálních funkcí

Monitorování vitálních funkcí slouží k podpoře provozní bezpečnosti a nemá diagnostické, terapeutické ani klinické účely. Systém není zdravotnickým prostředkem, nevydává zdravotnické nálezy, nenahrazuje lékařské posouzení a nesmí být používán jako jediný nástroj k potvrzení, vyloučení nebo léčbě chorobného stavu.

Měření na zápěstí mohou být ovlivněna řadou faktorů, mimo jiné neoptimálním kontaktem s pokožkou, pohybem končetiny, nesprávným utažením zařízení, periferní perfuzí, pocením, okolní teplotou, světelnými podmínkami nebo podmínkami signálu, stavem senzoru, sundáním zařízení nebo jeho nesprávným používáním.

Výskyt alarmu neznamená potvrzení nevolnosti nebo onemocnění; absence alarmu neznamená vyloučení klinicky významných stavů. Odpovědnost za klinické posouzení nesou příslušné zdravotnické subjekty.

Ověření přítomnosti na zápěstí

Ověření přítomnosti na zápěstí je průřezovou funkcí architektury SAS, protože ovlivňuje kvalitu interpretace ve více subsystémech, mimo jiné u vitálních funkcí, pádu a řízení některých alarmových workflow. Jeho účelem je rozlišit stavy, kdy je zařízení pravděpodobně nošeno, od

stavů, kdy může být odložené, sundané nebo používané způsobem neodpovídajícím určenému použití.

Z aplikačního hlediska je tato funkce zvláště důležitá ve třech scénářích.

1. Zabraňuje tomu, aby byly vitální funkce zaznamenané bez skutečného nošení zařízení považovány za vypovídající.
2. Snižuje riziko, že pád samotného terminálu bude zaměněn za pád pracovníka.
3. Přispívá ke spolehlivějšímu vyhodnocení některých stavových událostí nebo událostí nečinnosti.

Ověření není totožné s absolutním fyzickým zjištěním, že je zařízení skutečně na zápěstí. Je výsledkem softwarové klasifikace založené na dostupných signálech, a proto zvyšuje celkovou robustnost systému, aniž by však mohlo mít hodnotu plné jistoty.

Ochranné doložky týkající se ověření přítomnosti na zápěstí

Klasifikace zařízení jako nošeného nebo nenošeného představuje aplikační odhad, nikoli absolutní důkaz skutečného stavu terminálu. Může tedy dojít ke klasifikacím, které zcela neodpovídají skutečné situaci.

Užitečnost této funkce spočívá ve **snižování** chyb interpretace a nežádoucích aktivací, **nikoli v jejich absolutním vyloučení.**

Workflow varování, alarmu, zpoždění, eskalace a zrušení

Systém SAS využívá strukturované, postupné a podle třídy události rozlišitelné workflow řízení událostí. Zpracovatelský řetězec (pipeline) nekončí zobrazením oznámení, ale zahrnuje zachycení události, klasifikaci, ověření přípustnosti, případné zpoždění, místní signalizaci, záznam, vzdálené oznámení, možné zrušení operátorem a případnou eskalaci k dohledové složce.

Pokud funkce systému vyvolá relevantní událost, může zařízení nejprve vygenerovat místní varování (warning) formou oznámení na displeji, zvukové nebo hlasové signalizace či vibrace, aby operátora přímo informovalo a umožnilo mu první reakci. Současně může být událost již zaznamenána a odeslána do vzdálených systémů pro účely auditu, logování a dohledatelnosti.

V závislosti na konfiguraci může událost podléhat aplikačnímu zpoždění. Zpoždění plní přesně vymezenou technickou a organizační funkci: ponechává časový interval pro případné zrušení falešně pozitivního výsledku, umožňuje první místní ověření a omezuje plošné předávání dosud nepotvrzených událostí.

Zpoždění neznamená ztrátu události, ale její dočasné kontrolované pozdržení v rámci workflow.

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

Pokud událost není zrušena ve stanovené lhůtě (10 sekund), může systém přistoupit k eskalaci na nakonfigurované vzdálené cíle. Eskalace se může řídit odlišnými zásadami podle typu alarmu, stupně priority, profilu operátora, kontextu oblasti nebo jiných aplikačních kritérií.
Systém dále obsahuje mechanismy deduplikace a ochranné prodlevy (cooldown), které zabraňují nadměrnému opakování stejnorodých událostí v krátkých časových oknech. Tato funkce je nezbytná v případech, kdy stejná anomálie vyvolá více po sobě jdoucích spouštěčů, protože zabraňuje informačnímu přetížení backendu, operátora a Control Room.
Typickým případem užití je alarm pádu s místním varováním a oknem pro zrušení. Je-li operátor při vědomí a událost je falešná, může workflow přerušit. Pokud nezasáhne, systém pokračuje v eskalaci. Druhý případ užití se týká událostí, které sice nemají úrazovou dynamiku, ale vyžadují oznámení a případné vzdálené ověření. Třetí případ užití se týká procedurálních alarmů nebo alarmů souladu, které se mohou řídit odlišnými toky, méně zaměřenými na okamžitou nouzi a více na organizační převzetí.
Zrušení ze strany operátora zastaví další eskalaci, ale nemusí nutně vymazat historický záznam již zaznamenané události. Dohledatelnost zrušené události je totiž nedílnou součástí auditní funkce systému.

Ochranné doložky týkající se alarmového workflow

Generování varování nebo alarmů představuje aplikační klasifikaci, nikoli absolutní osvědčení události. Existence workflow eskalace neznamená záruku, že zásah bude vždy zahájen, přijat nebo dokončen v požadovaném čase.
Zpoždění, možnost zrušení, deduplikace a ochranné prodlevy (cooldown) jsou nástroji vyvažování mezi včasností, zvládnutelností falešně pozitivních výsledků a udržitelností provozního toku. Tato řešení **nevylučují ani riziko nežádoucích alarmů, ani riziko nespuštění.**
Účinnost workflow závisí na správném fungování zařízení, dostupnosti konektivity, správnosti konfigurace, dostupnosti vzdálených služeb a organizační schopnosti dohledové složky.

Funkce dobrovolného SOS

Systém SAS obsahuje funkci dobrovolného SOS, která operátorovi umožňuje výslovně požádat o pomoc i bez automatické detekce pádu, anomálie vitálních funkcí nebo jiné události generované monitorovacími subsystémy. Funkce SOS tak představuje kanál přímého spuštění alarmu pracovníkem a je nezbytnou součástí bezpečnostní architektury, protože umožňuje řešit situace, v nichž operátor subjektivně vnímá nebezpečí dříve, než je technicky zjistitelné senzory.

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

Funkci lze konfigurovat v různých provozních režimech, aby se přizpůsobila rizikovému kontextu, povaze vykonávané činnosti a typu požadované organizační reakce.

Hlasové SOS

Režim hlasového SOS je určen pro všechny případy, kdy operátor může otevřeně přivolat pomoc a kdy je vhodné, aby zařízení místně signalizovalo, že k aktivaci došlo. V tomto scénáři může terminál poskytovat výslovnou zpětnou vazbu, například hlasové, zvukové, haptické nebo vizuální potvrzení, aby pracovníka informoval, že žádost byla přijata a příslušné workflow bylo spuštěno.
Typickým případem užití je operátor, který se ocitne v potížích v důsledku nevolnosti, úrazu, ztráty orientace, izolace, potřeby naléhavé pomoci nebo jiné kritické situace, v níž otevřené vyhlášení alarmu nezvyšuje riziko. Za těchto okolností je místní potvrzení aktivace z provozního hlediska užitečné, protože osobě umožňuje okamžitě vnímat, že proces poskytnutí pomoci byl zahájen.

Tiché SOS

Režim tichého SOS je určen pro scénáře, v nichž spuštění alarmu nemá být navenek patrné ani vytvářet signály vnímatelné třetími osobami. Tato konfigurace má zvláštní význam v situacích napadení, výhrůžky, nátlaku, násilí, pokusu o odcizení, nepřátelského prostředí nebo obecně ve všech případech, kdy by zjevné vyhlášení alarmu mohlo zvýšit nebezpečí pro operátora.
V tomto režimu může systém přijmout žádost o pomoc, aniž by generoval rozpoznatelnou místní zpětnou vazbu, nebo tuto zpětnou vazbu omezit na formy, které okolí nevnímá. Událost je pak předána podle nakonfigurovaného workflow, přičemž je v maximální možné míře zachována diskrétnost aktivace a Control Room nebo dohledová složka může hlášení přijmout, aniž by o tom útočník nebo nepřátelské prostředí okamžitě věděli.
Z aplikačního hlediska představuje tiché SOS samostatnou funkci v oblasti osobní bezpečnosti, protože je navrženo pro situace, v nichž je nepatrnost alarmu zásadním ochranným požadavkem.

Zpoždění pro zrušení SOS

Funkci SOS lze konfigurovat se zpožděním pro zrušení nebo bez něj. V prvním režimu může systém poskytovat krátké okno pro zrušení (abort), které operátorovi umožní přerušit aktivaci v případě neúmyslného spuštění nebo chyby obsluhy. Tato konfigurace je zvláště užitečná v prostředích, kde je třeba omezit riziko náhodných aktivací, aniž by se rezignovalo na dostupnost funkce.

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

Ve druhém režimu lze SOS naopak nakonfigurovat bez zpoždění pro zrušení, aby byla událost okamžitě předána do backendu nebo do Control Room. Toto nastavení je zvláště vhodné tehdy, má-li rychlost aktivace absolutní prioritu nebo činí-li rizikový kontext nevhodným jakékoli zdržení způsobené oknem pro potvrzení nebo zrušení.
Volba mezi SOS s možností zrušení a okamžitým SOS tedy závisí na případu užití, rizikovém profilu, pracovní činnosti a přijatých organizačních zásadách.

Spuštění zvukového a obrazového záznamu

Funkci SOS lze dále v závislosti na projektové konfiguraci spojit s tichým spuštěním mechanismů zvukového a obrazového záznamu. Tato možnost umožňuje spojit s mimořádnou událostí nejen alarmové hlášení, ale také souběžný sběr informací užitečných pro pochopení situace, rekonstrukci události, posouzení probíhajícího rizika a podporu provozních rozhodnutí dohledové složky.
Z aplikačního hlediska může být zvukový záznam užitečný k zachycení okolních zvuků, rozhovorů, známek napadení, volání o pomoc nebo jiných kontextových prvků, které nelze přímo vyvodit pouze ze stavových dat zařízení. Obrazový záznam může přidat další úroveň vizuálního kontextu, zvláště významnou v případech napadení, vniknutí, výhrůžky nebo složité provozní události.

Ochranné doložky týkající se funkce SOS

Funkce SOS představuje nástroj dobrovolného spuštění alarmu a sama o sobě nezaručuje jisté přijetí, okamžité převzetí ani skutečné vyřízení události za všech okolností. Účinnost funkce závisí na dostupnosti zařízení, konektivitě, konfiguraci workflow, dosažitelnosti vzdálených systémů a existenci organizační struktury schopné událost přijmout a zpracovat.
Případné spuštění zvukového nebo obrazového záznamu nezaručuje úplné zachycení události ani absolutní použitelnost pořízeného materiálu. Kvalita a skutečná užitečnost záznamů závisí na okolním prostředí, umístění zařízení, dostupnosti audio-video kanálu, světelných podmínkách, okolním hluku a provozní kontinuitě systému.
Funkce SOS ani v nejpokročilejších režimech nenahrazuje nouzové postupy, opatření osobní ochrany, bezpečnostní opatření, organizaci záchrany ani podnikové protokoly pro řešení napadení a mimořádných událostí.

Vícekanálová komunikace

Systém podporuje funkce vícekanálové komunikace, které mohou zahrnovat hovory, asynchronní oznámení, stavové zprávy a tam, kde je to stanoveno, záložní kanály (fallback).

Komunikace není považována za doplňkovou funkci, ale za základní součást provozního modelu bezpečnosti, protože umožňuje přeměnit místní detekci na událost, kterou mohou řešit vzdálené subjekty.
V případě dobrovolného SOS může operátor přímo přivolat pomoc. Typickým případem užití je pracovník, který i bez automatické detekce pádu nebo odchylky vitálních funkcí vnímá nebezpečí, potíže nebo kritickou situaci a žádá o pomoc. V tomto scénáři systém plní funkci terminálu pro vědomé vyhlášení nouze. V jiných případech užití představuje komunikace pokračování automatického alarmu již klasifikovaného systémem. Zařízení se pak může zapojit do strategie navázání kontaktu a oznámení směrem ke Control Room nebo jiným nakonfigurovaným subjektům s využitím hlavního dostupného kanálu a v případě potřeby podpůrných nebo záložních kanálů (fallback).
Komunikace mezi zařízením, backendem a Control Room nemusí být jednotná, ale lze ji řídit podle adaptivních zásad, které rozlišují používané kanály a protokoly podle povahy dat, požadované frekvence aktualizace, úrovně priority události, potřeby kontinuity spojení a očekávaného energetického dopadu na terminál. Při tomto nastavení může systém uplatňovat různé strategie pro přenos heartbeatu, telemetrie, alarmů, aktualizací polohy, žádostí o kontakt, asynchronních zpráv nebo interaktivních komunikačních relací, aby optimalizoval kompromis mezi včasností, spolehlivostí, provozní kontinuitou a energetickou udržitelností.
Tato architektura umožňuje vyhnout se plošnému používání jediného přenosového schématu pro všechny třídy informací a naopak upřednostňuje kontextové řízení aplikačního provozu odpovídající bezpečnostní funkci systému a omezením nositelného zařízení napájeného z baterie.

Zabezpečení komunikace

Komunikace mezi zařízením H09 a platformou je chráněna šifrováním TLS a vzájemnou autentizací (mTLS). Každé zařízení má vlastní digitální certifikát X.509 vydaný vyhrazenou infrastrukturou PKI, který podléhá automatické obnově. Komunikační kanály používané zařízením, MQTT i HTTPS, jsou šifrované. Přístup uživatelů Control Room k webové platformě je chráněn připojením HTTPS a dvoufaktorovým ověřením (TOTP).

Ochranné doložky týkající se adaptivní komunikace

Použití adaptivní komunikační logiky zlepšuje celkovou efektivitu systému, ale absolutně nezaručuje kontinuitu, absenci zpoždění ani jisté doručení každé zprávy za všech provozních nebo infrastrukturních podmínek.

Adaptivní komunikace mezi Control Room a operátorem

V případech stanovených konfigurací může systém podporovat otevření komunikačního kanálu ze strany Control Room, aniž by vyžadoval předchozí ruční přijetí operátorem na zařízení. Tento režim má zvláštní význam v situacích, kdy pracovník není schopen s terminálem včas interagovat nebo kdy je rychlost navázání kontaktu prioritním provozním požadavkem.
V tomto rámci se mohou různé typy komunikace řídit odlišnou logikou. Komunikační relace založené na Teams nebo na rovnocenných kanálech může řídit Control Room jako nedílnou součást workflow pomoci a dohledu, zatímco jiné tradiční hlasové hovory se mohou řídit odlišnými způsoby obsluhy v závislosti na použité konfiguraci, případu užití a dostupnosti souvisejících služeb.

Ochranné doložky

Možnost vzdáleného otevření komunikačního kanálu sama o sobě nezaručuje plnou srozumitelnost rozhovoru, nepřetržitou dostupnost zvuku nebo obrazu ani skutečnou možnost interakce operátora za všech okolností. Kvalita relace závisí na konektivitě, stavu zařízení, okolních podmínkách, hluku, konfiguraci a dostupnosti zapojených vzdálených služeb.
Použití více kanálů plní funkci aplikační odolnosti. Cílem je snížit pravděpodobnost, že jediné místo selhání znemožní převzetí události. Přítomnost více komunikačních kanálů nezaručuje absolutní doručení, nepřetržitou dostupnost ani jisté navázání kontaktu za všech okolností. Komunikace závisí na rádiovém pokrytí, stavu sítí, službách třetích stran, konfiguraci, integritě backendu, stavu zařízení a dostupnosti příjemců.
Spuštění SOS nebo jiných nouzových kanálů nenahrazuje organizační strukturu záchrany a nepředstavuje záruku, že žádost byla přijata, pochopena nebo vyřízena v očekávaném čase.

Výhradní víceuživatelská správa alarmů a organizace převzetí

Systém uplatňuje logiku výhradní víceuživatelské správy alarmů, jejímž cílem je zajistit, aby každou událost v daném okamžiku převzal jediný operátor Control Room, a předejít tak překrývání, souběžným zásahům, zdvojování činností nebo nejasnostem v provozní odpovědnosti. V tomto modelu, jakmile je alarm převeden ze stavu nového hlášení do stavu provozního převzetí, přestává být dostupný v aktivním seznamu ostatních operátorů a je tak výhradně přiřazen osobě, která zahájila jeho řešení.

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

Tato architektura umožňuje zachovat jasnou dohledatelnost provozní odpovědnosti za událost během fáze zásahu a snižuje riziko, že by více operátorů současně jednalo ve vztahu k témuž alarmu nekoordinovaně, nadbytečně nebo vzájemně rušivě.
Pokud operátor, který alarm převzal, jeho řešení přeruší, aniž by jej dovedl ke stanovenému uzavření workflow, může být událost uvolněna a vrácena do opět dostupného stavu, takže se znovu zobrazí ostatním operátorům Control Room a lze ji znovu přidělit. Při tomto nastavení systém kombinuje výhradnost převzetí s možností uvolnění a opětovného přidělení, aby zachoval jak provozní pořádek, tak organizační odolnost v případě opuštění, nedostupnosti, předání odpovědnosti nebo potřeby přerozdělení zátěže.
Systém může dále stanovit, že alarm, který zůstane ve stavu „NEW“ bez převzetí po předem stanovenou maximální dobu, nakonfigurovanou tak, aby byla zajištěna potřebná včasnost s ohledem na případ užití, automaticky spustí interní eskalaci v rámci Control Room na příslušné vedoucí pracovníky nebo odpovědné osoby. V této konfiguraci nezůstává nepřevzetí události v očekávaném časovém okně omezeno pouze na provozní úroveň první linie, ale aktivuje další úroveň organizační pozornosti s cílem snížit riziko zpoždění neslučitelných s protokoly služby nebo s kritičností události.
Control Room je organizována s provozním pokrytím dimenzovaným tak, aby podporovalo maximální rozumně dosažitelnou včasnost převzetí alarmů a řízení souvisejících postupů. Struktura dohledové složky, počet operátorů, úrovně eskalace a rozdělení odpovědností lze stanovit podle počtu obsluhovaných pracovišť, úrovně rizika, počtu zařízení a provozních protokolů zákazníka.
Workflow zásahu spojené s alarmem nemusí být jednotné na celé platformě, ale lze jej rozlišovat podle jednotlivých tenantů, jednotlivých pracovišť nebo jiných organizačních členění stanovených aplikační architekturou. Toto rozlišení umožňuje přizpůsobit protokolům zákazníka evakuační postupy, pravidla eskalace, kritéria priority, příjemce oznámení, způsoby uvolnění nebo opětovného přidělení události a obecně provozní chování Control Room podle specifik obsluhovaného prostředí.
V tomto rámci systém nevnucuje jediný abstraktní model zásahu, ale umožňuje přizpůsobit životní cyklus alarmu podnikovým postupům, havarijním plánům, logice pracoviště a organizačním pravidlům, kterými se převzetí a řešení události v praxi řídí.

Ochranné doložky týkající se výhradní víceuživatelské správy alarmů

Výhradní víceuživatelská správa alarmů zlepšuje provozní pořádek, dohledatelnost odpovědnosti a omezení vzájemného rušení operátorů, ale sama o sobě nezaručuje absolutní absenci zpoždění, nesprávného uvolnění, neoptimálního přerozdělení nebo přerušení v řešení události. Účinnost mechanismu závisí na správné konfiguraci workflow,

dostupnosti dohledového personálu, kontinuitě backendových systémů a kvalitě provozní organizace Control Room.
Interní eskalace alarmu, který nebyl převzat v nakonfigurované maximální době, představuje organizační ochranné opatření zaměřené na snížení rizika nedostatečné včasnosti, ale sama o sobě nezaručuje, že každá událost bude za všech okolností převzata nebo vyřízena bez zpoždění. Její účinnost závisí na správném dimenzování dohledové složky, dostupnosti zapojených odpovědných osob, konfiguraci časových prahů a kontinuitě platformy.
Rozlišení workflow podle tenanta, pracoviště nebo protokolu zákazníka zlepšuje soulad platformy se skutečnými nouzovými a koordinačními postupy, ale vyžaduje odpovídající fázi návrhu, konfigurace, validace a údržby pravidel. Neúplné, nekonzistentní nebo neaktualizované konfigurace mohou ovlivnit správný průběh životního cyklu alarmu a soulad mezi chováním systému a postupy zákazníka.
Systém poskytuje strukturovanou podporu provozní správy alarmů, ale nenahrazuje lidský dohled, školení operátorů Control Room, správné dimenzování služby, zásahové protokoly zákazníka ani organizační odpovědnost za řešení mimořádných událostí.

Správa OOP bez Bluetooth pomocí QR code nebo výběru

Systém podporuje také registraci OOP bez Bluetooth naskenováním QR code nebo v příslušných případech výběrem ze seznamu v rozhraní zařízení. Tato funkce umožňuje rozšířit procedurální kontrolu i na ochranné prostředky, které je nutné z organizačních důvodů registrovat ručně na začátku směny nebo před určitou činností.
V nejjednodušším případě užití pracovník zaregistruje požadovaný OOP naskenováním příslušného QR code. V alternativním případě užití pracovník vybere ze seznamu v zařízení příslušný OOP nebo procedurální sadu. V obou případech systém uloží provedenou registraci jako prvek aplikačního souladu.
Důležitou vlastností této funkce je, že ověření absence OOP bez Bluetooth nemusí nutně proběhnout v prvním okamžiku zahájení směny. Systém totiž může stanovit počáteční okno vyhrazené pro správnou registraci, aby chybějící okamžitá registrace nevyvolávala předčasné alarmy, zatímco vstupní postup ještě probíhá.
Typickým případem užití je pracovník, který musí před zahájením činnosti deklarovat nebo zaregistrovat ochranné prostředky. Pokud systém v nakonfigurovaných podmínkách a lhůtách nezjistí registraci požadovaných OOP, může vygenerovat alarm nesouladu, jednorázový nebo opakovaný, podle centrálně definované logiky.

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

Tato funkce má tedy především procedurální význam: jejím cílem je posílit dodržování pravidel pro zahájení činnosti nebo vstup do oblasti a poskytnout platformě aplikační doklad o tom, že požadovaný krok byl proveden.
Povinná výbava OOP bez Bluetooth je konfigurovatelná na více úrovních a lze ji definovat podle tenanta, jednotlivého provozního pracoviště, přidělené pracovní činnosti, profilu jednotlivého operátora a obecně podle organizačních pravidel platných pro konkrétní případ užití. V rámci pokročilého projektového přístupu lze tuto konfiguraci navíc na úrovni backendu integrovat se staršími (legacy) systémy nebo existujícími aplikacemi pro správu pracovních povolení, provozních oprávnění, postupů přístupu do oblastí nebo k činnostem a dalších organizačních omezení, aby byla kontrola OOP v souladu s celkovým rámcem oprávnění na pracovišti.
Výběr nebo naskenování QR code OOP nemusí být stanoveno jako povinný krok ve všech aplikačních konfiguracích systému. V závislosti na přijatém organizačním modelu, úrovni projektové integrace a pravidlech stanovených pro pracoviště může být postup povinný, volitelný nebo zcela nevyžadovaný.

Ochranné doložky týkající se OOP bez Bluetooth registrovaných pomocí QR nebo výběru

Registrace pomocí QR code nebo výběru představuje aplikační doklad o zaznamenání v systému a **nikoli absolutní důkaz skutečného fyzického držení, správného nošení, technické vhodnosti ani nepřetržitého používání OOP po celou dobu směny**.

Určování polohy a lokalizace operátora

Funkce určování polohy není založena na jediném zdroji, ale na vícesenzorové strategii navržené tak, aby udržovala co nejrobustnější odhad polohy operátora, aktivované výhradně v případě alarmu, v různorodých prostředích, se zvláštním důrazem na kompromis mezi přesností, kontinuitou dat a energetickou udržitelností nositelného zařízení.
Lokalizace kombinuje informace z více dostupných technologií, mimo jiné GNSS (Global Navigation Satellite System), asistovaných polohových služeb, poskytovatelů fúzované polohy, IMU (Inertial Measurement Unit), inerciálního výpočtu polohy (dead-reckoning), WiFi fingerprinting, Bluetooth fingerprinting a tam, kde jsou k dispozici, RTLS (Real-Time Location System) nebo jiných kontextových zdrojů. Konečný odhad vychází z kombinace těchto příspěvků v jediném fúzním rámci, aby se omezila závislost na jediném zdroji a zvýšila odolnost dat.

Základním principem subsystému je použití strategií oportunistického získávání polohy. Systém nevynucuje v každém okamžiku maximální aktivitu přijímače polohy, ale nejprve vyhodnotí, zda je v mezipaměti (cache) již k dispozici nedávný a dostatečně spolehlivý fix polohy. Pokud mezipaměť již není považována za vyhovující, přistoupí systém k novému aktivnímu získání polohy.

Aktivní získávání polohy neprobíhá za všech podmínek stejně. Strategie se totiž může přizpůsobit kontextu a upřednostnit různé režimy podle provozního stavu zařízení, kvality dostupného signálu, případného stavu alarmu, pravděpodobné povahy scénáře (uvnitř budov nebo venku) a požadované úrovně přesnosti. Systém tak hledá nejlepší rovnováhu mezi přesností a energetickou udržitelností.

Dalším zásadním prvkem je validace konzistence fixů polohy. Kandidátní poloha není přijata automaticky jen proto, že je k dispozici, ale může být porovnána s předchozí polohou, deklarovanou přesností, stářím měření a věrohodností pohybu vyplývajícího z přechodu od jednoho fixu k druhému. To umožňuje zmírnit skoky polohy neslučitelné se skutečným pohybem osoby a omezit dopady ojedinělých chyb poskytovatele nebo zhoršených rádiových podmínek.

Tato architektura umožňuje různé případy užití. V otevřeném venkovním prostředí se systém může s vyšší spolehlivostí opírat o satelitní zdroje nebo poskytovatele fúzované polohy a získat poměrně přímý odhad. Uvnitř budov nebo ve stíněných zónách může lokalizace ve větší míře záviset na inerciálních informacích, rádiových otiscích (fingerprint) nebo pravidlech oblastí. Ve stavu alarmu může systém zvýšit frekvenci aktualizací, aby byla provozní stopa pro dohledovou složku užitečnější. Za běžného používání může naopak uplatňovat konzervativnější zásady, aby zachoval výdrž a celkovou kontinuitu provozu zařízení.

Řízení určování polohy se obvykle řeší projektovým přístupem, konfigurovaným podle charakteristik provozního pracoviště a skutečně dostupné infrastruktury. Při tomto přístupu lze subsystém lokalizace integrovat, jsou-li k dispozici a vhodně nakonfigurovány, se sítěmi WiFi, mapami rádiových otisků (fingerprinting), logikou oblastí, topologickými referencemi pracoviště a dalšími kontextovými zdroji vhodnými ke zvýšení robustnosti odhadu polohy, zejména uvnitř budov nebo ve smíšených prostředích.

Strategie lokalizace tedy nemusí být nutně jednotná, ale je stanovena s ohledem na případ užití, požadovanou úroveň přesnosti, energetická omezení zařízení, dostupnost místní infrastruktury a míru kontinuity sledování považovanou v daném aplikačním kontextu za nezbytnou.

V základní konfiguraci systém využívá výhradně služby fúzované lokalizace poskytované Google Play Services a uplatňuje adaptivní správu požadavků na polohu. V této konfiguraci se požadovaná úroveň přesnosti, frekvence aktualizace a intenzita vyhledávání dynamicky

upravují podle provozního stavu zařízení a zjištěného kontextu, například s rozlišením běžných podmínek a alarmových situací, scénářů uvnitř budov a venku, fází běžného monitorování a fází, v nichž je vyžadována vyšší informační reaktivita směrem ke vzdáleným systémům.
I v této základní konfiguraci je tedy lokalizace řízena podle kritérií rovnováhy mezi přesností, kontinuitou dat a energetickou udržitelností, přičemž se vyhýbá rigidně jednotným přístupům a upřednostňuje adaptivní strategii odpovídající bezpečnostní funkci systému a provozním omezením nositelného terminálu.

Ochranné doložky týkající se určování polohy

Poloha poskytovaná systémem je technickým odhadem získaným vícesenzorovou fúzí a softwarovými validačními kritérii. Nepředstavuje absolutní, nepřetržité a neomylné měření skutečné polohy operátora v každém okamžiku.
Kvalita odhadu závisí na kontextu (uvnitř budov nebo venku), satelitním pokrytí, rušení způsobeném artefakty nebo vícecestným šířením (multipath), kvalitě rádiového signálu, dostupnosti pomocných zdrojů, dynamice pohybu, energetickém stavu zařízení, konfiguraci a okolních podmínkách.
Systém nezaručuje nepřetržitou lokalizaci, jednotnou přesnost ve všech prostředích, absenci zpoždění, absenci driftu ani trvalou dostupnost všech zdrojů polohy. **Údaj o poloze je třeba vykládat jako provozní pomůcku, nikoli jako absolutní jistotu.**

Asistovaná lokalizace pro záchranné týmy a podpora při dosažení cíle

V pokročilých projektových konfiguracích lze subsystém lokalizace využít k podpoře dosažení provozního cíle osobami pověřenými zásahem, ověřením nebo záchranou.
Tato funkce má zvláštní význam ve složitých, rozlehlých, vnitřních prostředích nebo v prostředích s omezenou viditelností, kde pouhá dostupnost abstraktní polohy nestačí a je naopak nutné podporovat provozní koordinaci dosažení cíle.

Ochranné doložky týkající se asistované lokalizace cíle

I v pokročilých konfiguracích asistované lokalizace poskytuje systém provozní podporu, nikoli absolutní záruku rychlého, přesného nebo bezchybného dosažení osoby nebo cílového bodu.
Účinnost závisí na kvalitě infrastruktury pracoviště, dostupnosti lokalizačních zdrojů, konzistenci mapování a skutečných okolních podmínkách.

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

Konfigurovatelnost systému a závislost na případu užití

Systém SAS je vysoce konfigurovatelný. Prahové parametry, logiku alarmů, doby zpoždění, komunikační zásady, kritéria lokalizace, pravidla oblastí, seznamy OOP, frekvence aktualizací a chování rozhraní lze přizpůsobit případu užití a personalizovat podle tenanta, pracoviště, skupiny, pracovní činnosti, týmu až po individuální úroveň.
Tato konfigurovatelnost představuje jednu z hlavních předností platformy, protože umožňuje její použití v různých kontextech, aniž by všechny provozní situace zužovala na jediný standardní model. Zároveň však činí systém silně závislým na správnosti použité konfigurace. Dobře navržená funkce, která je však parametrizována nekonzistentně s pracovištěm, rizikem a organizací, může vést k neuspokojivým aplikačním výsledkům.

Vzdálené aktualizace a rekonfigurace platformy

Konfigurovatelnost platformy zahrnuje také možnost vzdáleně aktualizovat parametry, pravidla, aplikační profily, provozní stránky, požadovanou výbavu, zásady lokalizace, logiku varování a další funkční prvky systému, aby bylo možné přizpůsobit chování zařízení a backendu vývoji pracoviště, postupů nebo přijatého organizačního modelu. Tato schopnost umožňuje udržovat systém v souladu s provozním kontextem, aniž by nutně vyžadovala místní ruční zásahy na každém terminálu, s výjimkou případů, kdy konkrétní architektura nasazení nebo zásady zákazníka stanoví jiný postup.

Ochranné doložky týkající se aktualizací a rekonfigurace

Činnosti aktualizace a rekonfigurace zlepšují přizpůsobivost systému, ale vyžadují odpovídající řízení aplikačního životního cyklu, validaci změn a kontrolu souladu mezi distribuovanou konfigurací a skutečným případem užití. Změny, které nejsou správně validovány nebo neodpovídají kontextu, mohou změnit provozní chování systému.

Automatická a tichá aktualizace aplikace v režimu OTA

Systém může podporovat postupy aktualizace aplikace v režimu OTA (Over-The-Air), které umožňují vzdálenou distribuci nových verzí softwaru bez nutnosti místních ručních zásahů na jednotlivých zařízeních. V této konfiguraci lze aktualizaci APK provádět automaticky a tiše v souladu s bezpečnostními zásadami, systémovými oprávněními a způsoby nasazení stanovenými přijatou architekturou.
Tato schopnost plní dvojí aplikační roli. Na jedné straně představuje nástroj rozvojové údržby, protože umožňuje distribuovat funkční vylepšení, opravy, optimalizace, úpravy kompatibility,

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

zdokonalení algoritmů, aktualizace rozhraní a vylepšení logiky komunikace, lokalizace nebo správy alarmů. Na druhé straně je také důležitým prvkem podpory projektových přizpůsobení, protože umožňuje kontrolovaně zavádět, aktualizovat nebo upravovat softwarové komponenty specifické pro jednotlivého zákazníka, pracoviště, pracovní činnost nebo konkrétní implementovaný případ užití.
Z provozního hlediska tichá aktualizace umožňuje zkrátit dobu šíření změn, rychleji sjednotit flotilu zařízení, omezit potřebu ručních rekonfigurací v terénu a udržet větší soulad mezi verzí softwaru, konfigurací backendu a celkovou aplikační architekturou. V distribuovaném ekosystému, jako je SAS, tato funkce významně přispívá k řiditelnosti platformy, a to jak v centralizovaných prostředích, tak v prostředích on premises nebo s hybridní správou.
Aktualizaci OTA lze dále využít k podpoře postupného vývoje systému v čase, což umožňuje doprovázet rozšiřování integrací s bezpečnostním ekosystémem, zavádění nových funkcí, rozšiřování provozních stránek, úpravy logiky interakce s Control Room nebo přizpůsobení specifickým projektovým požadavkům, které vyvstanou během životního cyklu řešení.
Z důvodu provozní kontinuity a energetické udržitelnosti se aktualizace OTA obvykle odkládá na první nabíjení následující po vydání nové verze, aby se minimalizoval dopad na probíhající činnosti, předešlo se rušení provozních funkcí zařízení během směny a omezily se dopady procesu aktualizace na zbývající výdrž baterie. Při tomto nastavení se okamžik vydání a okamžik skutečné instalace nemusejí nutně shodovat, protože architektura upřednostňuje logiku distribuce slučitelnou se skutečným používáním terminálu v terénu.
Z tohoto pohledu nelze automatickou a tichou aktualizaci chápat pouze jako technický nástroj distribuce softwaru, ale jako **strukturální součást udržovatelnosti a řízeného vývoje platformy**, schopnou podporovat jak standardní vývoj produktu, tak správu aplikačních profilů a specifických přizpůsobení.

Ochranné doložky týkající se aktualizace OTA

Dostupnost mechanismů automatické a tiché aktualizace sama o sobě nezaručuje, že každá aktualizace bude za všech okolností úspěšně distribuována, stažena, nainstalována nebo uvedena do provozu. Účinnost procesu závisí na dostupnosti konektivity, stavu zařízení, kompatibilitě distribuované verze, správném řízení cyklu vydávání, dostupnosti potřebného úložného prostoru, bezpečnostních zásadách terminálu a správné integraci mezi backendem, aplikačním balíčkem a architekturou nasazení.
Odložení instalace na následující nabíjení obvykle snižuje dopad na provoz a na výdrž zařízení, ale samo o sobě nezaručuje, že aktualizace bude použita ihned po vydání nebo v jednotném intervalu na celé flotile terminálů. Skutečné načasování instalace může záviset na

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

reálných cyklech používání a nabíjení, dostupnosti konektivity v předpokládaném okamžiku, stavu terminálu a přijatých pravidlech distribuce.
Aktualizace softwaru, ačkoli slouží k rozvojovému zlepšování a řízené správě přizpůsobení, vyžaduje odpovídající postupy validace, ověřování a řízení vydávání. Změny, které nejsou správně validovány nebo neodpovídají provoznímu kontextu, mohou ovlivnit aplikační chování systému, kontinuitu některých funkcí nebo soulad s konfiguracemi pracoviště.
Přítomnost funkcí vzdálené aktualizace **nevylučuje nutnost plánování cyklu údržby, kontroly distribuovaných verzí, ověření po vydání a organizačního dohledu nad zavedenými změnami**. I v případě tiché aktualizace je nadále nutné zajistit soulad mezi vývojem softwaru, požadavky případu užití, konfigurací backendu a provozními postupy zákazníka.

Obecné ochranné doložky týkající se konfigurace

Systém smí být používán pouze v konfiguracích odpovídajících provoznímu kontextu, pracovní činnosti, podnikovým postupům a účelům, pro které byl zaveden. Neúplné, nekonzistentní, nevalidované nebo neaktualizované konfigurace mohou výrazně změnit citlivost, specificitu, včasnost a užitečnost poskytovaných informací.

Stav nabíjení a pozastavení provozních funkcí

Je-li zařízení trvale připojeno k nabíjení způsobem stanoveným pro ukončení směny nebo pro uložení mimo provoz, systém automaticky pozastaví funkce monitorování a generování událostí, aby se předešlo nesprávné interpretaci terminálu v podmínkách neslučitelných s běžným nošením na zápěstí. V této konfiguraci neznamená přechod do stavu nabíjení pouze doplnění energie, ale může také představovat aplikační indikátor opuštění běžného kontextu používání zařízení.

Ochranné doložky týkající se stavu nabíjení

Připojení zařízení k nabíjení má za následek pozastavení některých provozních funkcí; terminál, který se nachází v tomto stavu, proto nesmí být považován za plně rovnocenný zařízení nošenému a aktivnímu během běžné pracovní směny.

Integrace smartwatche do bezpečnostního ekosystému

Smartwatch H09 není koncipován jako izolovaný terminál, ale jako osobní uzel širšího bezpečnostního ekosystému, v němž provozní hodnota vyplývá z integrace individuálních zařízení, distribuovaných senzorů, infrastruktury pracoviště, dohledových systémů a pokročilých softwarových modulů pro interpretaci kontextu. V této architektuře může

nositelné zařízení působit jak jako zdroj událostí a dat, tak jako koncový bod pro příjem varování, alarmů, provozních pokynů, kontextových stavů a podpůrného obsahu pocházejícího z ostatních částí ekosystému.

Ochranné doložky týkající se integrace do ekosystému

Integrace smartwatche s dalšími hardwarovými a softwarovými prvky bezpečnostního ekosystému rozšiřuje dostupný informační přehled a možnosti provozní koordinace, ale sama o sobě nezaručuje absolutní úplnost, nepřerušenou kontinuitu ani neomylnou správnost znázornění rizika. Celková účinnost závisí na kvalitě a dostupnosti integrovaných subsystémů, správnosti rozhraní, projektové konzistenci architektury, stavu údržby infrastruktury, dostupnosti konektivity a správné konfiguraci korelačních pravidel.

Obecné ochranné doložky týkající se používání

Systém musí být začleněn do strukturovaného organizačního modelu zahrnujícího školení personálu, nouzové postupy, dohled, údržbu zařízení, kontrolu konfigurací, pravidelné ověřování správného používání a dostupnost dohledové složky, je-li stanovena.
Systém není způsobilý představovat jediné bezpečnostní opatření pracovníka. Musí být doplněn lidskými, technickými, organizačními a procedurálními opatřeními, která vyžaduje konkrétní kontext.
Nesprávné používání, nenošení zařízení, vypnutí funkcí, neoprávněné zásahy do softwaru, nevyhovující konfigurace, používání v nevhodném prostředí nebo zanedbání údržby mohou výrazně snížit aplikační účinnost systému.

Doložky o nezdravotnické povaze

Systém SAS se smartwatchem H09 není zdravotnickým prostředkem, není systémem klinického monitorování, není diagnostickým nástrojem, není terapeutickou pomůckou a není certifikovaným systémem pro záchranu života.
Vitální funkce, behaviorální data, odhady pádu a klasifikace generované softwarem je třeba vykládat jako technické ukazatele na podporu provozní bezpečnosti, nikoli jako lékařské zprávy, klinické důkazy nebo diagnostická osvědčení.

Doložky o omezení odpovědnosti

Systém nezaručuje univerzální detekci každé úrazové, vitální, procedurální nebo kontextové události. Nezaručuje absenci falešně pozitivních výsledků, absenci falešně negativních výsledků, absolutní kontinuitu služby, jisté doručení každé komunikace, trvalou dostupnost údaje o poloze ani absolutní fyzické ověření skutečné přítomnosti OOP. Případné nezjištění

události, nedokonalá klasifikace situace, zpoždění oznámení, chybějící registrace OOP, nepřesnost polohy nebo dočasná nedostupnost funkce samy o sobě nepředstavují automatický důkaz jisté poruchy ani objektivní odpovědnost výrobce nebo dodavatele. **Uživatelská organizace nese odpovědnost za stanovení správného případu užití, validaci konfigurace, školení personálu, udržování systému v provozuschopném stavu, přípravu nouzových postupů a doplnění systému o všechna nezbytná doplňková opatření.**

Závěrečné prohlášení

Systém SAS se smartwatchem H09 je technologická platforma na podporu provozní bezpečnosti.
Systém je navržen tak, aby zvyšoval pravděpodobnost zachycení kritických událostí, posiloval dodržování postupů, zlepšoval schopnost vzdáleného dohledu a podporoval organizaci reakce. Funguje však v mezích vlastních zařízení nošenému na zápěstí, neklinickým senzorům, inferenční softwarové logice, komunikační infrastruktuře, kterou nelze vždy plně kontrolovat, a proměnlivému reálnému provoznímu kontextu.
Z těchto důvodů systém nepředstavuje zdravotnický prostředek, nenahrazuje lidský dohled, nenahrazuje podnikové postupy pro mimořádné události a absolutně nezaručuje detekci, klasifikaci, přenos ani převzetí každé události za všech okolností.

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