NOTES D'APPLICATION

SYSTÈME SAFE ALERT SYSTEM (SAS) AVEC SMARTWATCH H09

DESCRIPTION TECHNIQUE ET FONCTIONNELLE, CAS D'USAGE, LIMITES D'APPLICATION, CLAUSES DE SAUVEGARDE ET DE LIMITATION DE RESPONSABILITÉ

Préambule

Le système SAS avec smartwatch H09 est une plateforme technologique d'aide à la sécurité opérationnelle du personnel, destinée aux contextes dans lesquels le travailleur peut se trouver en situation de risque, d'isolement, d'exposition à des dangers spécifiques, de besoin de surveillance à distance, d'obligation de conformité à des procédures de sécurité ou de nécessité de déclenchement rapide de workflows d'urgence.

Le dispositif H09 n'est pas un wearable grand public ordinaire. Il s'agit d'un terminal opérationnel spécialisé, conçu pour assurer en arrière-plan des activités de surveillance, de collecte de signaux, de classification d'événements, de vérification de la conformité procédurale, de localisation de l'opérateur, d'interaction locale lors d'événements critiques et d'intégration de la personne dans un flux structuré d'alerte, d'escalade, de communication et d'audit.

Le système ne se limite pas au seul terminal porté : il comprend également les modules logiciels de traitement local, les logiques de configuration centralisée, les canaux de communication, les services backend, les systèmes d'enregistrement et de traçabilité et, le cas échéant, la control room ou toute autre structure organisationnelle chargée de la supervision et de la gestion des événements.

Le système constitue une aide technologique à la sécurité opérationnelle. Il ne constitue pas un dispositif médical, ne constitue pas un moyen de secours sanitaire, n'effectue aucun diagnostic, ne remplace pas la surveillance humaine et ne remplace pas les procédures internes d'urgence, de surveillance, de prévention et de secours.

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

Sommaire

4 ..... Nature du système et usage prévu
4 ..... Architecture fonctionnelle générale
5 ..... Architectures avancées
5 ..... Principe général de fonctionnement
6 ..... Heartbeat opérationnel et télémétrie d'état
6 ..... Clauses de sauvegarde relatives au heartbeat opérationnel
6 ..... Détection d'immobilité
7 ..... Clauses de sauvegarde relatives à la détection d'immobilité
7 ..... Interface opérateur
9 ..... Clauses de sauvegarde relatives à l'interface opérateur
9 ..... Pages opérationnelles avancées
10 ..... Clauses de sauvegarde relatives aux pages opérationnelles avancées
10 ..... Détection de chute
12 ..... Clauses de sauvegarde relatives à la détection de chute
12 ..... Surveillance des paramètres vitaux
13 ..... Clauses de sauvegarde relatives à la surveillance des paramètres vitaux
13 ..... Vérification de la présence au poignet
14 ..... Clauses de sauvegarde relatives à la vérification de la présence au poignet
14 ..... Workflow d'avertissement, d'alarme, de latence, d'escalade et d'annulation
15 ..... Clauses de sauvegarde relatives au workflow d'alarme
15 ..... Fonction SOS volontaire
15 ..... SOS vocal
16 ..... SOS silencieux
16 ..... Délai d'annulation du SOS
16 ..... Déclenchement de l'enregistrement audio et vidéo
17 ..... Clauses de sauvegarde relatives à la fonction SOS
17 ..... Communication multicanal
18 ..... Sécurité des communications
18 ..... Clauses de sauvegarde relatives à la communication adaptative
18 ..... Communication adaptative entre la Control Room et l'opérateur
18 ..... Clauses de sauvegarde
19 ..... Gestion exclusive multi-utilisateur des alarmes et organisation de la prise en charge

20 ..... Clauses de sauvegarde relatives à la gestion exclusive multi-utilisateur des alarmes
20 ..... Gestion des EPI non Bluetooth par QR code ou sélection
21 ..... Clauses de sauvegarde relatives aux EPI non Bluetooth avec QR code ou sélection
21 ..... Positionnement et localisation de l'opérateur
23 ..... Clauses de sauvegarde relatives au positionnement
23 ..... Localisation assistée des équipes de secours et aide pour rejoindre la cible
23 ..... Clauses de sauvegarde relatives à la localisation assistée de la cible
23 ..... Configurabilité du système et dépendance au cas d'usage
24 ..... Mises à jour à distance et reconfiguration de la plateforme
24 ..... Clauses de sauvegarde relatives aux mises à jour et à la reconfiguration
24 ..... Mise à jour automatique et silencieuse de l'application en mode OTA
25 ..... Clauses de sauvegarde relatives à la mise à jour OTA
25 ..... Clauses de sauvegarde générales relatives à la configuration
26 ..... État de charge et suspension des fonctions opérationnelles
26 ..... Clauses de sauvegarde relatives à l'état de charge
26 ..... Intégration de la smartwatch dans l'écosystème de sécurité
26 ..... Clauses de sauvegarde relatives à l'intégration dans l'écosystème
26 ..... Clauses générales de sauvegarde relatives à l'utilisation
27 ..... Clauses de non-médicalité
27 ..... Clauses de limitation de responsabilité
27 ..... Déclaration finale

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

Nature du système et usage prévu

Le système est destiné à soutenir la sécurité opérationnelle dans tous les cas où il s'avère utile de :

- détecter avec une probabilité accrue des événements traumatiques ou des dynamiques compatibles avec une chute ;
- permettre le déclenchement volontaire de demandes d'aide ;
- surveiller des paramètres vitaux à des fins préventives mais non diagnostiques ;
- maintenir une estimation continue, ou quasi continue, de la position de l'opérateur ;
- vérifier la conformité vis-à-vis des équipements de protection individuelle requis par le contexte opérationnel ;
- associer événements, position, état du dispositif et règles de zone dans un tableau de supervision unique ;
- déclencher des flux de communication, de notification, d'escalade et de traçabilité vers des systèmes distants ou des structures de contrôle.

L'usage prévu du système porte donc sur la réduction du risque, l'augmentation de la probabilité de détection de conditions anormales, le soutien à la rapidité organisationnelle de l'intervention et l'amélioration de la traçabilité des événements.

Le système n'est pas destiné à se substituer aux obligations de prévention de l'employeur ni à constituer l'unique mesure de sécurité du travailleur.

Architecture fonctionnelle générale

Le terminal porté assure l'acquisition des données des capteurs, le traitement local, la classification préliminaire des événements, l'interaction avec l'opérateur, la gestion de workflows prédéfinis et la collecte du contexte opérationnel. Le backend héberge les configurations, les profils, les paramètres de seuil, les logiques de communication, les règles de zone, les listes d'EPI, les politiques de localisation, les critères de notification, les systèmes d'historisation et les canaux d'intégration vers la control room. Au niveau organisationnel, la structure de supervision reçoit les événements, les évalue et déclenche les procédures prévues.

La control room ne représente pas seulement le niveau organisationnel de réception, d'évaluation et de gestion des événements générés par les dispositifs portés : elle constitue une partie active et structurelle de l'architecture SAS, en tant que nœud central d'orchestration des états de sécurité du site. Dans ce modèle, la control room est également conçue comme source native d'alarmes, de notifications opérationnelles et de commandes de coordination, adressables de manière sélective à des opérateurs individuels, à des équipes, à des groupes homogènes ou à l'ensemble du site, en fonction du scénario en

cours, du profil des destinataires, de leur position logique ou géographique et de la disponibilité de la connectivité individuelle.
Cette approche permet à la plateforme de diffuser en temps quasi réel des instructions, des états d'alerte et des consignes comportementales découlant de la situation globale du site. Cela comprend, par exemple, l'émission d'ordres d'évacuation, la convocation vers des points de rassemblement, le déclenchement de procédures de confinement ou d'éloignement et la diffusion d'alarmes relatives à des événements de site. Dans ce même modèle opérationnel, la smartwatch peut en outre jouer le rôle de terminal de remise directe d'ordres, d'instructions et de messages opérationnels envoyés par le backend (qui peuvent également être lus à voix haute par le dispositif), afin de rendre immédiatement accessibles à l'opérateur des contenus prescriptifs ou comportementaux sans nécessairement exiger une lecture active de l'écran, en renforçant l'efficacité de la communication dans des contextes dynamiques, bruyants ou hautement critiques.
Cette approche rend la plateforme apte à soutenir non seulement le signalement d'événements subis par le travailleur, mais aussi la diffusion coordonnée de mesures de protection actives, y compris celles visant à rejoindre des équipements de protection collective (EPC) spécifiques, des points sûrs, des points de rassemblement ou des itinéraires d'éloignement définis en fonction de la nature du danger détecté. La control room, en tant que centre logique de l'écosystème SAS, ne constitue donc pas un simple destinataire final de l'alarme, mais un composant structurel de pilotage dynamique de la sécurité du site, capable de générer, corréler et propager des alertes opérationnelles en fonction de l'état global du système.

Architectures avancées

La control room de l'écosystème SAS peut être mise à disposition selon différents modèles architecturaux, afin de s'adapter aux caractéristiques d'infrastructure, d'organisation et de connectivité du site ou du client. Dans une première configuration, la control room peut être fournie de manière centralisée via le cloud de Safe S.r.l., permettant une gestion unifiée des dispositifs, des événements, des workflows d'alarme, des configurations et des interactions opérationnelles, y compris sur plusieurs sites ou tenants distribués.
Pour les contextes dans lesquels une connectivité continue et/ou stable n'est pas disponible, la même architecture peut être exploitée on premises, de manière à rendre le système opérationnel même en présence de contraintes d'isolement réseau, d'exigences d'autonomie locale ou de politiques d'infrastructure imposant le maintien des fonctions critiques à l'intérieur du périmètre du site. Dans cette configuration, la Safety control room et

le backend qui la supporte fonctionnent localement, en maintenant la continuité des fonctions de supervision, de gestion des alarmes, d'historisation, de localisation et de coordination opérationnelle, même en l'absence de liaison permanente avec des services distants externes.
Lorsque le client dispose déjà d'une control room opérationnelle préexistante, la Safety control room de l'écosystème SAS peut être intégrée au niveau applicatif dans la structure existante, ce qui évite la création d'un environnement distinct et favorise au contraire l'extension des capacités de la control room déjà en service. Cette intégration peut s'effectuer au moyen des API exposées par le système, qui permettent la gestion bidirectionnelle des alarmes, des notifications, des états opérationnels et des interactions décrites précédemment, autorisant ainsi tant le transfert vers la control room existante des événements générés par l'écosystème SAS que le déclenchement, depuis cette même control room, d'alarmes, de workflows et de commandes destinés aux dispositifs et aux sous-systèmes connectés.
La plateforme SAS peut fonctionner soit comme control room complète, soit comme composant intégré d'une control room existante, en conservant dans les deux cas la même logique d'orchestration bidirectionnelle de la sécurité opérationnelle.

Principe général de fonctionnement

Le système fonctionne selon une logique de surveillance non intrusive. Les principaux traitements s'effectuent en arrière-plan ; l'interaction directe avec l'opérateur intervient lorsqu'une situation méritant attention est détectée, lorsqu'un événement doit être confirmé ou annulé, lorsqu'une communication doit être déclenchée ou lorsque le système requiert une action procédurale spécifique.

Heartbeat opérationnel et télémétrie d'état

Le système prévoit la génération périodique de heartbeats opérationnels par le dispositif, entendus comme des « messages d'état » transmis au backend ou à la control room à des fins de supervision, de vérification de la joignabilité et de mise à jour de la situation opérationnelle du travailleur. Le heartbeat ne représente pas un simple signal de présence sur le réseau, mais un conteneur d'informations configurable pouvant inclure, selon le profil applicatif, le niveau de charge du dispositif, les principaux paramètres de connectivité, l'état de port et d'autres métadonnées utiles à la supervision.
D'un point de vue applicatif, le heartbeat permet à la plateforme de conserver une vision à jour de l'état du terminal et de son fonctionnement, même en l'absence d'alarmes explicites.

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

La control room peut ainsi distinguer plus efficacement l'absence d'événements de l'absence de joignabilité, la continuité normale de fonctionnement d'une dégradation potentielle du terminal, ainsi que les conditions de pleine opérabilité de celles dans lesquelles certaines fonctions sont temporairement limitées ou indisponibles (par exemple, absence de connexion Wi-Fi).
La périodicité, le contenu et le niveau de détail du heartbeat peuvent être configurés en fonction du cas d'usage, du contexte de risque, des contraintes de connectivité et des politiques énergétiques du système. Dans les scénarios ordinaires, la transmission peut être maintenue à des niveaux plus économes ; dans les scénarios hautement critiques ou en présence d'événements, le contenu ou la fréquence des messages d'état peuvent être adaptés afin d'accroître la capacité de supervision à distance.

Clauses de sauvegarde relatives au heartbeat opérationnel

La présence de heartbeats réguliers ne constitue pas une garantie absolue de pleine opérabilité de toutes les fonctions du dispositif, de même que l'absence temporaire de heartbeat n'équivaut pas automatiquement à une panne certaine ou à un état de danger de l'opérateur. La disponibilité de ces messages dépend de la connectivité, de l'état énergétique, de la configuration, de l'intégrité du dispositif et du bon fonctionnement de la chaîne de transmission.
Le heartbeat constitue un outil d'aide à la supervision opérationnelle et ne remplace pas les procédures de vérification, le contrôle organisationnel ou la gestion humaine des situations d'anomalies possibles.

Détection d'immobilité

Le système prévoit une fonction de détection de l'immobilité de l'opérateur. Le dispositif l'exécute en continu et en arrière-plan, conformément à la logique de surveillance non intrusive qui caractérise l'ensemble de l'architecture. La fonction repose sur l'analyse du mouvement du seul terminal porté, ce qui garantit en outre l'anonymisation du travailleur.
Lorsque le dispositif reste en absence totale de mouvement pendant un intervalle de temps prédéfini et configurable sur demande, fixé à 40 secondes dans la configuration d'usine, le système interprète cette condition comme potentiellement anormale et déclenche une alarme.
La gestion de l'événement est structurée en deux niveaux successifs. Dans une première phase, l'alarme est gérée localement sur le dispositif, qui offre à l'opérateur la possibilité de l'annuler dans les 10 premières secondes suivant son déclenchement. Cet intervalle permet

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

au travailleur de signaler activement que sa situation est normale et limite ainsi la propagation de signalements non pertinents vers la control room. Si l'alarme n'est pas annulée dans ce délai, l'événement est transmis à la control room. La control room le prend en charge, procède à sa vérification et déclenche, si nécessaire, les procédures prévues.
D'un point de vue applicatif, la détection d'immobilité permet à la plateforme d'intercepter des situations dans lesquelles l'opérateur pourrait ne pas être en mesure de déclencher lui-même une demande d'aide.
La fonction est entièrement configurable. Le contrôle d'immobilité peut être activé ou désactivé lors de la configuration initiale sans compromettre le fonctionnement général du dispositif. Les paramètres temporels qui déterminent le déclenchement de l'alarme et la fenêtre d'annulation peuvent être définis en fonction du cas d'usage, de la tâche exercée et du contexte opérationnel. Cela permet d'adapter la sensibilité de la fonction aux modalités de travail effectives, en évitant que des activités impliquant naturellement de longues périodes d'immobilité ne génèrent des alarmes injustifiées.

Clauses de sauvegarde relatives à la détection d'immobilité

La détection d'immobilité repose sur l'absence de mouvement du dispositif porté et non sur une évaluation directe de l'état physique de l'opérateur. Par conséquent, le déclenchement d'une alarme d'immobilité n'équivaut pas automatiquement à un état de danger ou de malaise de l'opérateur. De même, l'absence d'alarme ne constitue pas une garantie de son intégrité physique.
L'efficacité de la fonction dépend de son activation effective dans la configuration, des paramètres temporels définis, du port correct du dispositif, de son état énergétique et de la disponibilité de la connectivité nécessaire à la transmission de l'événement vers la control room.
La détection d'immobilité ne remplace pas les procédures de vérification, le contrôle organisationnel ou la gestion humaine des situations d'urgence possibles.

Interface opérateur

L'interface opérateur du dispositif H09 est conçue comme une interface épurée, robuste et orientée vers une utilisation rapide en contexte opérationnel, avec une attention particulière portée à la réduction de la charge cognitive, à la minimisation des déclenchements accidentels et à la possibilité d'utilisation y compris dans des conditions de stress, d'urgence ou d'attention réduite du travailleur. La conception générale de l'interface privilégie en effet la clarté fonctionnelle, la lisibilité immédiate de l'état du dispositif et la rapidité d'accès aux

fonctions critiques, en évitant les structures de navigation complexes ou incompatibles avec un terminal de sécurité porté.
Le dispositif dispose d'un écran tactile, d'une caméra frontale, d'un microphone et d'un haut-parleur, permettant non seulement l'interaction visuelle directe, mais aussi des fonctions de communication audio et, dans les contextes où cela est prévu, de support vidéo. Ces composants sont complétés par deux boutons physiques. Le premier est destiné aux fonctions d'allumage et d'extinction du terminal. Le second, identifié comme le bouton argenté, est associé à la fonction SOS (silencieux ou non) et au déclenchement du scan des équipements de protection individuelle (EPI).
Outre les boutons physiques, l'interface tactile met en œuvre des boutons virtuels supplémentaires, qui permettent d'étendre les fonctions disponibles sans introduire de complexité mécanique supplémentaire sur le dispositif. L'ensemble des boutons physiques et virtuels est configuré pour réduire le risque de déclenchements involontaires au moyen de logiques d'appui prolongé. Le début de l'appui est accompagné d'une brève vibration signalant le lancement de la séquence d'activation, tandis qu'une seconde brève vibration confirme la validité de l'appui et donc la prise en compte effective de la commande. Ce choix de conception poursuit un double objectif : d'une part, limiter les actions involontaires dues à des chocs, des frôlements ou des contacts accidentels ; d'autre part, fournir à l'opérateur un retour haptique immédiat, utile également lorsque l'attention visuelle portée à l'écran est réduite ou nulle.
Le système est conçu pour les personnes qui portent la montre sous leurs vêtements de travail et doivent pouvoir l'utiliser sans la regarder. Il est actif par défaut. En dehors d'une situation d'alarme, l'écran est noir et affiche uniquement, en haut à gauche, un cercle de couleur verte, qui permet de constater que la montre fonctionne correctement.
Sur le côté gauche, des icônes apparaissent chaque fois qu'une situation requiert l'attention :


Connexion Wi-Fi absente, seul le réseau mobile est disponible. Cette icône s'affiche uniquement si le dispositif a été configuré et connecté à un réseau Wi-Fi ; dans le cas contraire, elle ne s'affichera jamais.


Aucune connexion (ni Wi-Fi ni réseau mobile).


Réception GPS faible. Erreur de localisation estimée à environ 50 mètres.


Aucune réception GPS.


Batterie faible, inférieure à 30 %.

 Batterie faible, inférieure à 10 %.

 H09 mal porté.

Pendant une alarme, deux grands boutons apparaissent à l'écran. En haut s'affiche le pouce vert, qui signifie « Tout OK », et en bas l'icône représentant un microphone. Le bouton « Tout OK », s'il est pressé dans les 10 secondes suivant l'envoi du SOS, permet d'annuler l'appel ; s'il est pressé une fois l'alarme partie, il permet de signaler à la Control Room que la situation est sous contrôle. Le microphone, quant à lui, lance un enregistrement d'ambiance et ne peut être utilisé qu'une fois l'alarme partie. Cet enregistrement reste actif tant que la Control Room ne s'est pas connectée au dispositif. Une fois la Control Room connectée, l'enregistrement est automatiquement arrêté et envoyé simultanément à la Control Room, qui l'affiche à l'écran. Lorsqu'un appel Teams est déclenché, l'interface s'adapte automatiquement en ouvrant, dans la partie inférieure de l'écran, une vue de rendu (render view) dédiée à la communication audiovisuelle. Cette zone est automatiquement amenée à l'affichage par défilement, afin d'offrir à l'opérateur la possibilité de voir son interlocuteur de la control room ou, en tout état de cause, la composante vidéo associée à la session de communication. À la fin de l'appel Teams, la vue de rendu disparaît et l'interface revient à sa configuration standard. Dans son ensemble, l'interface opérateur est donc conçue pour concilier immédiateté d'utilisation, robustesse face aux déclenchements involontaires, accès rapide aux fonctions critiques et adaptation dynamique aux workflows en cours, tout en conservant une structure simple et cohérente avec l'emploi du dispositif comme terminal de sécurité porté.

Clauses de sauvegarde relatives à l'interface opérateur

L'interface du dispositif est conçue pour réduire le risque de déclenchements accidentels et pour favoriser l'utilisation rapide des fonctions critiques, mais **elle ne peut éliminer de manière absolue la possibilité de déclenchements involontaires, d'appuis valides non effectués, d'erreurs d'interaction ou d'utilisation incorrecte dans des conditions opérationnelles particulièrement difficiles.** L'efficacité de l'interaction dépend également de facteurs externes tels que le port de gants, la position du bras, les conditions environnementales, les chocs, les vibrations, l'état d'attention de l'opérateur, l'intégrité de l'écran tactile, le fonctionnement des boutons physiques et l'état général du dispositif.
Les icônes et indicateurs d'état affichés à l'écran constituent une représentation synthétique des conditions opérationnelles détectées par le système et ne doivent pas être interprétés comme une garantie absolue de disponibilité continue de la fonction correspondante.

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

La disponibilité de la caméra frontale, du microphone, du haut-parleur ou de la vue de rendu d'appel ne garantit pas en soi la qualité, la continuité ou l'utilité effective de la communication audio-vidéo en toutes circonstances. Ces fonctions dépendent de la connectivité, de l'état du dispositif, des conditions environnementales, de la qualité du signal, de la configuration du système et de la disponibilité des services distants concernés.
L'interface opérateur, bien que conçue pour une utilisation rapide en contexte de sécurité, ne remplace pas l'information, la formation pratique, les procédures opérationnelles et les protocoles d'urgence. L'utilisation correcte des fonctions SOS, d'annulation (abort), de confirmation, de communication et d'enregistrement des EPI exige que le personnel ait été préalablement formé de manière cohérente avec le cas d'usage adopté.

Pages opérationnelles avancées

L'interface du dispositif peut être enrichie, selon la configuration appliquée, de pages opérationnelles dédiées à des besoins spécifiques de sécurité, de supervision ou d'aide à l'action. Ces pages ne constituent pas de simples écrans d'information génériques, mais des composants fonctionnels de l'architecture applicative, activables en fonction du profil de l'opérateur, du contexte de risque, de l'état du système ou du workflow en cours.
Parmi les configurations possibles figurent, à titre d'exemple, des pages dédiées à la consultation synthétique des paramètres vitaux, des pages d'aide à la navigation assistée vers des points de rassemblement ou des points sûrs dans des scénarios d'évacuation, ainsi que des pages destinées à localiser ou à rejoindre des EPC spécifiques ou d'autres éléments d'aide à la gestion des urgences présents sur le site, tels que des trousses de premiers secours, des défibrillateurs, des moyens de lutte contre l'incendie ou d'autres points d'intérêt opérationnels analogues.
Dans ces cas, le dispositif ne remplit pas seulement la fonction de générateur ou de récepteur d'alarmes, mais aussi celle de terminal d'aide contextuelle à l'action, capable de mettre à la disposition de l'opérateur des indications synthétiques et opérationnelles cohérentes avec la situation en cours.

Clauses de sauvegarde relatives aux pages opérationnelles avancées

Les « pages opérationnelles avancées » constituent des outils d'aide contextuelle et ne remplacent pas la formation, la connaissance du site, la signalisation de sécurité, les procédures d'urgence ou la coordination humaine. L'utilité effective des informations affichées dépend de l'exactitude de la configuration, de la qualité des données de contexte, de la disponibilité de la localisation et de la mise à jour des informations du backend.

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

Détection de chute

Le sous-système de détection de chute repose sur l'analyse accélérométrique et inertielle en temps réel, selon une logique multiphase qui ne réduit pas la décision à la présence d'un pic d'accélération isolé. Le système analyse au contraire une séquence dynamique globale compatible avec une possible chute réelle de la personne, en la distinguant des gestes brusques, des chocs occasionnels au poignet, des vibrations mécaniques, des activités professionnelles vigoureuses, des impacts non traumatiques, de la chute du seul dispositif ou de la simple immobilité du terminal.

La phase initiale de l'évaluation consiste à rechercher une condition plausible d'allègement gravitationnel, c'est-à-dire une réduction significative de l'accélération apparente compatible avec une perte d'appui. Cette phase n'est pas traitée comme une condition suffisante, mais comme un élément sentinelle qui déclenche une analyse plus approfondie. Pour être considérée comme pertinente, elle doit présenter une cohérence temporelle et ne pas pouvoir s'expliquer plus vraisemblablement comme du bruit, une oscillation aléatoire ou un mouvement dépourvu de portée traumatique.

Le système recherche ensuite la présence d'une phase d'impact cohérente, c'est-à-dire d'une variation accélérométrique compatible avec la conclusion d'une dynamique de chute. L'impact n'est pas non plus traité comme un critère autosuffisant, car tous les impacts ne correspondent pas à des chutes réelles et toutes les chutes ne produisent pas un impact net. Le rôle de l'impact est de renforcer la crédibilité de la séquence lorsque son amplitude et sa chronologie sont compatibles avec la phase précédente.

Cette analyse est complétée par une phase d'observation ultérieure, visant à évaluer la réduction de l'activité motrice ou une condition d'immobilité relative. L'immobilité n'est pas considérée comme un critère autonome et suffisant, puisqu'un dispositif immobile pourrait simplement être posé, retiré ou non porté. La réduction ultérieure de l'activité prend en revanche de la valeur lorsqu'elle survient après une dynamique déjà jugée significative et renforce l'hypothèse que l'événement observé a eu des effets réels sur la personne.

Le système évalue en outre la posture finale et la variation d'orientation du terminal, en les considérant comme des facteurs de cohérence supplémentaires. Ces éléments peuvent contribuer à distinguer une véritable chute d'un simple geste brusque, d'un choc isolé ou d'une vibration incompatible avec un événement traumatique.

La logique de classification fait également intervenir des mécanismes d'hystérésis, une validation multi-échantillons, des fenêtres temporelles d'observation, des pénalisations pour les profils incompatibles avec un événement réel et des critères de robustesse visant à réduire les déclenchements injustifiés. En particulier, la vérification que le dispositif est

effectivement porté permet d'atténuer le risque que la chute du seul terminal soit interprétée comme une chute de la personne, sans pour autant l'éliminer de manière absolue.
D'un point de vue applicatif, le cas d'usage type est celui du travailleur qui subit une perte soudaine d'équilibre ou un malaise avec effondrement dont la dynamique est suffisamment marquée pour produire une séquence d'allègement, d'impact puis de réduction du mouvement. Dans ce scénario, le système peut générer un avertissement (warning) local, enregistrer l'événement, le transmettre aux systèmes centraux et, en l'absence d'annulation, déclencher la procédure d'escalade prévue.
Un deuxième cas d'usage concerne l'événement ambigu ou limite, dans lequel la dynamique détectée présente certains éléments compatibles avec une chute, mais pas une cohérence complète. Dans ces circonstances, le système peut adopter une classification prudente, solliciter une interaction de l'opérateur ou déclencher des workflows moins agressifs, selon la configuration appliquée.
Un troisième cas d'usage concerne le faux positif typique du poignet, dans lequel des activités physiques vigoureuses, des chocs répétés ou des mouvements rapides génèrent des profils partiellement similaires à une chute. Dans ces cas, l'architecture multiphase, la vérification post-événement et la possibilité d'annuler l'avertissement constituent les principaux outils de limitation du bruit décisionnel.
Malgré le niveau d'élaboration de l'analyse multiphase, la présence de mécanismes de validation progressive, de pénalisation des profils incohérents et de modulation du risque final, le sous-système de détection ne peut éliminer de manière absolue la possibilité de faux positifs ou de faux négatifs. La complexité du phénomène biomécanique réel, le positionnement du capteur au poignet, la variabilité individuelle des mouvements, la nature non parfaitement déterministe des chutes réelles et la nécessité de fonctionner sur un dispositif embarqué à faible consommation rendent inhérente l'existence d'une marge résiduelle d'erreur décisionnelle. L'analyse multiphase accroît la robustesse du modèle et réduit la dépendance à des pics isolés ou à des critères trop simplistes, mais elle ne fait pas du système un classificateur infaillible de l'événement traumatique. En termes applicatifs, le modèle est donc conçu pour accroître la probabilité d'interception correcte des chutes compatibles avec les signaux observables, et non pour garantir la reconnaissance certaine et universelle de tout événement possible.
Le sous-système de détection de chute adopte une logique explicitement optimisée pour des dispositifs wearables embarqués à faible consommation, dans laquelle l'équilibre entre précision de détection, rapidité de décision, consommation énergétique, occupation mémoire et soutenabilité du calcul constitue un choix de conception structurel et non une limite accidentelle de l'implémentation. Dans ce contexte, la fréquence d'échantillonnage

accélérométrique n'est pas poussée vers les valeurs maximales théoriquement possibles, mais maintenue à un niveau compatible avec une surveillance continue sur dispositif porté, afin de préserver l'autonomie opérationnelle, la stabilité du système et la soutenabilité de la charge de traitement sur le long terme.
L'adoption d'une fréquence d'échantillonnage modérée présente des avantages importants : elle réduit la consommation des capteurs et du CPU, limite la pression sur les callbacks des capteurs, contient le trafic interne de données, réduit le risque d'accumulation de traitements en attente (backlog) et rend plus soutenable une surveillance continue pendant toute la durée du poste. Ce choix favorise en outre une meilleure compatibilité avec une architecture embarquée dans laquelle le dispositif doit assurer simultanément d'autres fonctions, telles que la communication, la localisation, la gestion des workflows d'alarme, l'interaction avec l'utilisateur et le contrôle de l'état opérationnel général.
En contrepartie de ces avantages, une fréquence d'échantillonnage peu élevée implique aussi des compromis techniques précis. En particulier, elle réduit la résolution temporelle avec laquelle sont observés les transitoires les plus rapides, peut rendre moins détaillée la reconstitution fine d'événements impulsionnels de très courte durée et peut diminuer la sensibilité à des micro-profils extrêmement rapides ou peu persistants. Pour compenser cette limite, le système ne fonde pas sa décision sur un seul échantillon, mais adopte une logique par fenêtres temporelles et validation multi-échantillons, dans laquelle l'événement est interprété comme une structure dynamique globale et non comme une succession de pics (spikes) élémentaires.
En résumé, le sous-système de détection de chute est conçu selon une logique de compromis maîtrisé : la fréquence accélérométrique est choisie de manière à rendre soutenable la surveillance continue sur wearable, tandis que le traitement par lots (batching) et l'analyse par fenêtres sont adoptés pour renforcer la robustesse sémantique, réduire le bruit et contenir le coût de calcul. Le résultat n'est pas un modèle orienté vers une réactivité brute maximale, mais un modèle orienté vers la meilleure fiabilité opérationnelle compatible avec les contraintes réelles d'un dispositif embarqué porté au poignet.

Clauses de sauvegarde relatives à la détection de chute

Le sous-système de détection de chute constitue un outil d'aide à la sécurité des personnes et ne garantit pas la reconnaissance certaine de tout événement traumatique. Peuvent ne pas être interceptés les chutes lentes, les effondrements progressifs, les glissades avec appui partiel, les événements à dynamique atypique, les événements avec un mouvement résiduel significatif du poignet ou les événements survenus alors que le dispositif n'était pas correctement porté.

Le système ne garantit ni l'absence de faux positifs ni l'absence de faux négatifs. La détection dépend de la dynamique de l'événement, de la position du dispositif, de l'état de port, des conditions opérationnelles et de la configuration appliquée.
La non-détection d'une chute ou la génération d'une alarme injustifiée ne constituent pas, en elles-mêmes, une preuve automatique de dysfonctionnement certain ni un fondement de responsabilité objective du fabricant ou du fournisseur.
Le sous-système de détection de chute ne remplace pas la surveillance humaine, les procédures internes d'urgence, l'évaluation des risques, la formation du personnel, les mesures de prévention, les EPI spécialisés ou les autres moyens de sécurité prévus par le contexte opérationnel.

Surveillance des paramètres vitaux

Le système intègre un sous-système de surveillance des paramètres vitaux, destiné à détecter des conditions physiologiques potentiellement anormales pendant l'activité professionnelle. La surveillance est conçue comme une **fonction préventive non diagnostique** et repose sur la collecte de paramètres vitaux pouvant être acquis par le dispositif porté, transformés en indicateurs applicatifs d'attention ou de risque.
Le traitement des paramètres vitaux ne se limite pas à l'évaluation de la valeur instantanée de chaque mesure. Chaque paramètre est au contraire considéré dans le temps comme une série chronologique, sur laquelle le système peut établir des moyennes, des statistiques progressives, des indicateurs de variabilité, des écarts par rapport au comportement habituel, des conditions de persistance et des critères de stabilité du signal. Cette approche permet de distinguer plus efficacement les oscillations transitoires de faible importance des anomalies répétées ou persistantes.
Le système peut donc identifier différentes situations applicatives.

- Le travailleur présente un paramètre qui dépasse un seuil d'attention de manière stable » ou significativement anormale par rapport à son profil historique. Le système peut générer un avertissement » (warning), à traiter selon le workflow configuré.
- L'anomalie ne découle pas tant de la valeur absolue que de l'écart significatif par rapport à la moyenne individuelle. Dans ce scénario, la fonction de surveillance est particulièrement utile pour les dispositifs attribués de manière permanente au même opérateur, car l'historique personnel améliore la sensibilité aux altérations qui ne sont pas nécessairement extrêmes en valeur absolue mais significatives au regard du comportement physiologique ordinaire de la personne.
- Plusieurs paramètres concomitants présentent des écarts modérés mais cohérents. Le système peut alors agréger les contributions des différents modules dans une évaluation globale

du risque, en traitant la situation de manière plus systémique et moins dépendante d'une mesure isolée.

La surveillance des paramètres vitaux interagit en outre avec la vérification de la présence au poignet. L'acquisition de ces valeurs n'a en effet de signification technique que si le dispositif est vraisemblablement porté et si le contact avec le corps est suffisamment fiable. À défaut, la valeur informative de la donnée peut diminuer sensiblement.

Clauses de sauvegarde relatives à la surveillance des paramètres vitaux

La surveillance des paramètres vitaux a pour finalité l'aide à la sécurité opérationnelle et non des finalités diagnostiques, thérapeutiques ou cliniques. Le système n'est pas un dispositif médical, ne produit pas de comptes rendus médicaux, ne remplace pas les évaluations médicales et ne peut être utilisé comme seul outil pour confirmer, exclure ou traiter une pathologie.

Les mesures au poignet peuvent être influencées par de multiples facteurs, notamment un contact non optimal avec la peau, le mouvement du membre, un serrage inadapté du dispositif, la perfusion périphérique, la transpiration, la température ambiante, les conditions de luminosité ou de signal, l'état du capteur, le retrait du dispositif ou une utilisation incorrecte.

La présence d'une alarme n'équivaut pas à la confirmation d'un malaise ou d'une pathologie ; l'absence d'alarme n'équivaut pas à l'exclusion de conditions cliniques significatives. La responsabilité de l'évaluation clinique incombe aux professionnels de santé compétents.

Vérification de la présence au poignet

La vérification de la présence au poignet est une fonction transversale de l'architecture SAS, puisqu'elle influe sur la qualité d'interprétation de plusieurs sous-systèmes, notamment les paramètres vitaux, la chute et la gestion de certains workflows d'alarme. Son objectif est de distinguer les conditions dans lesquelles le dispositif est vraisemblablement porté de celles dans lesquelles il pourrait être posé, retiré ou utilisé de manière non conforme à l'usage prévu.

D'un point de vue applicatif, cette fonction est particulièrement importante dans trois scénarios.

1. Elle évite que des paramètres vitaux recueillis en l'absence de port effectif soient interprétés comme informatifs.
2. Elle réduit le risque que la chute du seul terminal soit confondue avec une chute du travailleur.
3. Elle contribue à qualifier avec une plus grande fiabilité certains événements d'état ou d'inactivité.

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

La vérification ne correspond pas à une détection physique absolue du fait que le dispositif se trouve effectivement au poignet. Elle est le résultat d'une classification logicielle fondée sur les signaux disponibles et améliore donc la robustesse globale du système sans pouvoir prétendre à une certitude totale.

Clauses de sauvegarde relatives à la vérification de la présence au poignet

La classification du dispositif comme porté ou non porté constitue une estimation applicative et non une preuve absolue de l'état matériel du terminal. Des classifications ne correspondant pas parfaitement à la situation réelle peuvent donc se produire.
L'utilité de cette fonction est de **réduire** les erreurs d'interprétation et les déclenchements injustifiés, **et non de les éliminer de manière absolue.**

Workflow d'avertissement, d'alarme, de latence, d'escalade et d'annulation

Le système SAS adopte un workflow de gestion des événements structuré, progressif et différenciable par classe d'événement. Le pipeline ne se limite pas à l'émission d'une notification : il comprend l'acquisition de l'événement, sa classification, la vérification de sa recevabilité, une éventuelle latence, le signalement local, l'enregistrement, la notification à distance, l'annulation éventuelle par l'opérateur et l'escalade éventuelle vers la structure de surveillance.
Lorsqu'une fonction du système produit un événement pertinent, le dispositif peut d'abord générer un avertissement local au moyen d'une notification à l'écran, d'un signal sonore, d'un message vocal ou d'une vibration, afin d'informer directement l'opérateur et de lui permettre une première réaction. Parallèlement, l'événement peut déjà être enregistré et transmis aux systèmes distants à des fins d'audit, de journalisation et de traçabilité.
Selon la configuration, l'événement peut être soumis à une latence applicative. La latence remplit une fonction technique et organisationnelle précise : elle laisse un intervalle utile pour l'annulation éventuelle d'un faux positif, permet une première vérification locale et réduit la transmission indiscriminée d'événements non encore confirmés.
La latence n'équivaut pas à une perte de l'événement, mais à sa rétention temporaire et qualifiée au sein du workflow.
Si l'événement n'est pas annulé dans les délais prévus (10 secondes), le système peut procéder à l'escalade vers les destinataires distants configurés. L'escalade peut suivre des

politiques différenciées selon le type d'alarme, le degré de priorité, le profil de l'opérateur, le contexte de la zone ou d'autres critères applicatifs.
Le système intègre en outre des mécanismes de déduplication et de temporisation (cooldown), qui évitent la répétition excessive d'événements de même nature dans des fenêtres temporelles rapprochées. Cette fonction est essentielle lorsqu'une même anomalie génère plusieurs déclencheurs consécutifs, car elle évite la surcharge d'informations du backend, de l'opérateur et de la control room.
Un cas d'usage type est celui de l'alarme de chute avec avertissement local et fenêtre d'annulation. Si l'opérateur est conscient et que l'événement est faux, il peut interrompre le workflow. S'il n'intervient pas, le système poursuit avec l'escalade. Un deuxième cas d'usage concerne des événements qui, sans présenter de dynamique traumatique, nécessitent une notification et une éventuelle vérification à distance. Un troisième cas d'usage concerne les alarmes procédurales ou de conformité, qui peuvent suivre des flux différents, moins orientés vers l'urgence immédiate et davantage vers la prise en charge organisationnelle.
L'annulation par l'opérateur interrompt l'escalade ultérieure, mais n'efface pas nécessairement la trace historique de l'événement déjà enregistré. La traçabilité de l'événement annulé fait en effet partie intégrante de la fonction d'audit du système.

Clauses de sauvegarde relatives au workflow d'alarme

La génération d'avertissements ou d'alarmes constitue une classification applicative et non une certification absolue de l'événement. L'existence d'un workflow d'escalade ne constitue pas une garantie que l'intervention sera toujours déclenchée, reçue ou menée à bien dans les délais souhaités.
La latence, la possibilité d'annulation, la déduplication et les temporisations sont des outils d'équilibre entre rapidité, gestion des faux positifs et soutenabilité du flux opérationnel. Ces choix **n'éliminent ni le risque d'alarmes injustifiées ni le risque de non-déclenchement.**
L'efficacité du workflow dépend du bon fonctionnement du dispositif, de la disponibilité de la connectivité, de l'exactitude de la configuration, de la présence des services distants et de la capacité organisationnelle de la structure de surveillance.

Fonction SOS volontaire

Le système SAS intègre une fonction SOS volontaire destinée à permettre à l'opérateur de demander explicitement assistance, même en l'absence de détection automatique de chute, d'anomalie des paramètres vitaux ou d'autre événement généré par les sous-systèmes de surveillance. La fonction SOS représente donc un canal de déclenchement direct de l'alarme

par le travailleur et constitue un composant essentiel de l'architecture de sécurité, puisqu'elle permet de gérer des situations dans lesquelles le danger est perçu subjectivement par l'opérateur avant même d'être techniquement détectable par les capteurs.
La fonction peut être configurée selon différents modes opérationnels, de manière à s'adapter au contexte de risque, à la nature de l'activité exercée et au type de réaction organisationnelle requis.

SOS vocal

Le mode SOS vocal est conçu pour tous les cas dans lesquels l'opérateur peut déclencher ouvertement une demande d'aide et où il est souhaitable que le dispositif produise une indication locale du déclenchement effectué. Dans ce scénario, le terminal peut fournir des retours explicites, tels que des confirmations vocales, sonores, haptiques ou visuelles, afin d'informer le travailleur que la demande a été prise en compte et que le workflow correspondant a été lancé.
Le cas d'usage type est celui d'un opérateur en difficulté en raison d'un malaise, d'un accident, d'une désorientation, d'un isolement, d'un besoin d'assistance urgent ou de toute autre situation critique dans laquelle la manifestation ouverte de l'alarme n'entraîne pas d'aggravation du risque. Dans ces circonstances, la confirmation locale du déclenchement constitue un élément utile sur le plan opérationnel, car elle permet à la personne de percevoir immédiatement le lancement du processus d'assistance.

SOS silencieux

Le mode SOS silencieux est conçu pour des scénarios dans lesquels le déclenchement de l'alarme ne doit pas être rendu visible à l'extérieur ni produire de signaux perceptibles par des tiers. Cette configuration est particulièrement pertinente en cas d'agression, de menace, de coercition, de violence, de tentative de vol, de contexte hostile ou, plus généralement, dans tous les cas où une manifestation explicite de l'alarme pourrait accroître le danger pour l'opérateur.
Dans ce mode, le système peut prendre en compte la demande d'aide sans générer de retours locaux reconnaissables, ou en limitant ces retours à des formes non perceptibles par l'environnement extérieur. L'événement est alors transmis selon le workflow configuré, en préservant autant que possible la discrétion du déclenchement et en permettant à la control room ou à la structure de surveillance de recevoir le signalement sans que l'auteur des faits ou le contexte hostile n'en aient immédiatement connaissance.

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

D'un point de vue applicatif, le SOS silencieux constitue une fonction distincte sur le plan de la sécurité des personnes, puisqu'il est conçu pour des contextes dans lesquels la discrétion de l'alarme représente une exigence essentielle de protection.

Délai d'annulation du SOS

La fonction SOS peut être configurée avec ou sans délai d'annulation. Dans un premier mode, le système peut prévoir une brève fenêtre d'annulation (abort), permettant à l'opérateur d'interrompre le déclenchement en cas d'activation involontaire ou d'erreur de manipulation. Cette configuration est particulièrement utile dans les contextes où le risque de déclenchements accidentels doit être limité sans renoncer à la disponibilité de la fonction. Dans un second mode, le SOS peut au contraire être configuré sans délai d'annulation, de manière à transmettre immédiatement l'événement au backend ou à la control room. Ce réglage est particulièrement approprié lorsque la rapidité du déclenchement a une priorité absolue ou lorsque le contexte de risque rend inopportun tout retard introduit par une fenêtre de confirmation ou d'annulation.
Le choix entre un SOS annulable et un SOS immédiat dépend donc du cas d'usage, du profil de risque, de la tâche et des politiques organisationnelles adoptées.

Déclenchement de l'enregistrement audio et vidéo

La fonction SOS peut en outre être associée, selon la configuration du projet, au déclenchement silencieux de mécanismes d'enregistrement audio et vidéo. Cette possibilité permet d'associer à l'événement d'urgence non seulement un signalement d'alarme, mais aussi une collecte simultanée d'éléments d'information utiles à la compréhension du scénario, à la reconstitution de l'événement, à la qualification du risque en cours et à l'aide aux décisions opérationnelles de la structure de surveillance.
D'un point de vue applicatif, l'enregistrement audio peut s'avérer utile pour capter des bruits ambiants, des dialogues, des signes d'agression, des appels à l'aide ou d'autres éléments contextuels qui ne peuvent être déduits immédiatement des seules données d'état du dispositif. L'enregistrement vidéo peut ajouter un niveau supplémentaire de contextualisation visuelle, particulièrement pertinent en cas d'agression, d'intrusion, de menace ou d'événement opérationnel complexe.

Clauses de sauvegarde relatives à la fonction SOS

La fonction SOS constitue un outil de déclenchement volontaire de l'alarme et ne garantit pas, en soi, la réception certaine, la prise en charge immédiate ou la gestion effective de l'événement en toutes circonstances. L'efficacité de la fonction dépend de la disponibilité du

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

dispositif, de la connectivité, de la configuration du workflow, de la joignabilité des systèmes distants et de la présence d'une structure organisationnelle capable de recevoir et de traiter l'événement.
Le déclenchement éventuel d'enregistrements audio ou vidéo ne garantit ni la captation complète de l'événement ni l'exploitabilité absolue des éléments recueillis. La qualité et l'utilité effective des enregistrements dépendent du contexte environnemental, du positionnement du dispositif, de la disponibilité du canal audio-vidéo, des conditions de luminosité, du bruit ambiant et de la continuité de fonctionnement du système.
La fonction SOS, même dans ses modes les plus avancés, ne remplace pas les procédures d'urgence, les mesures de protection des personnes, les moyens de sécurité, l'organisation des secours ou les protocoles internes de gestion des agressions et des urgences.

Communication multicanal

Le système prend en charge des fonctions de communication multicanal, pouvant inclure des appels, des notifications asynchrones, des messages d'état et, le cas échéant, des canaux de secours (fallback). La communication n'est pas traitée comme une fonction accessoire, mais comme un composant fondamental du modèle opérationnel de sécurité, puisqu'elle permet de transformer la détection locale en un événement gérable par des intervenants distants.
Dans le cas du SOS volontaire, l'opérateur peut déclencher directement une demande d'aide. Le cas d'usage type est celui du travailleur qui, même en l'absence de détection automatique de chute ou d'écart des paramètres vitaux, perçoit un danger, une difficulté ou une situation critique et demande assistance. Dans ce scénario, le système remplit la fonction de terminal de déclenchement conscient de l'urgence. Dans d'autres cas d'usage, la communication représente la suite d'une alarme automatique déjà classifiée par le système. Le dispositif peut alors s'inscrire dans une stratégie de contact et de notification vers la control room ou d'autres destinataires configurés, en utilisant le canal principal disponible et, si nécessaire, des canaux d'appoint ou de secours.
La communication entre le dispositif, le backend et la control room n'est pas nécessairement uniforme, mais peut être gérée selon des politiques adaptatives qui différencient les canaux et les protocoles utilisés en fonction de la nature de la donnée, de la fréquence de mise à jour requise, du niveau de priorité de l'événement, du besoin de continuité de la liaison et de l'impact énergétique attendu sur le terminal. Dans cette approche, le système peut adopter des stratégies différentes pour la transmission des heartbeats, de la télémétrie, des alarmes, des mises à jour de position, des demandes de contact, des messages asynchrones ou des

sessions de communication interactive, afin d'optimiser le compromis entre rapidité, fiabilité, continuité opérationnelle et soutenabilité énergétique.
Cette architecture permet d'éviter le recours indiscriminé à un schéma de transmission unique pour toutes les classes d'information, en privilégiant au contraire une gestion contextuelle du trafic applicatif cohérente avec la fonction de sécurité du système et avec les limites propres à un dispositif porté fonctionnant sur batterie.

Sécurité des communications

Les communications entre le dispositif H09 et la plateforme sont protégées par un chiffrement TLS et une authentification mutuelle (mTLS). Chaque dispositif dispose de son propre certificat numérique X.509, délivré par une infrastructure PKI dédiée et soumis à un renouvellement automatique. Les canaux de communication utilisés par le dispositif, MQTT comme HTTPS, sont chiffrés. L'accès à la plateforme web par les utilisateurs de la Control Room est protégé par une connexion HTTPS et une authentification à deux facteurs (TOTP).

Clauses de sauvegarde relatives à la communication adaptative

L'adoption de logiques de communication adaptatives améliore l'efficacité globale du système, mais ne garantit pas de manière absolue la continuité, l'absence de retard ou la remise certaine de chaque message dans toutes les conditions opérationnelles ou d'infrastructure.

Communication adaptative entre la Control Room et l'opérateur

Dans les cas prévus par la configuration, le système peut permettre l'ouverture du canal de communication par la control room sans exiger d'acceptation manuelle préalable de la part de l'opérateur sur le dispositif. Ce mode est particulièrement pertinent dans les contextes où le travailleur n'est pas en mesure d'interagir rapidement avec le terminal ou dans lesquels la rapidité d'établissement du contact constitue une exigence opérationnelle prioritaire.
Dans ce cadre, les différents types de communication peuvent suivre des logiques différenciées. Les sessions de communication fondées sur Teams ou sur des canaux équivalents peuvent être pilotées par la control room comme partie intégrante du workflow d'assistance et de supervision, tandis que d'autres communications vocales traditionnelles peuvent suivre des modes de gestion différents selon la configuration appliquée, le cas d'usage et la disponibilité des services associés.

Clauses de sauvegarde

La possibilité d'ouverture à distance du canal de communication ne garantit pas, en soi, la parfaite intelligibilité de la conversation, la disponibilité continue de l'audio ou de la vidéo ou la possibilité effective d'interaction de l'opérateur en toutes circonstances. La qualité de la session dépend de la connectivité, de l'état du dispositif, des conditions environnementales, du bruit, de la configuration et de la disponibilité des services distants concernés.
Le recours à une pluralité de canaux a une fonction de résilience applicative. L'objectif est de réduire la probabilité qu'un point de défaillance unique rende impossible la prise en charge de l'événement. La présence de plusieurs canaux de communication ne garantit pas une remise absolue, une disponibilité continue ou l'établissement certain du contact en toutes circonstances. La communication dépend de la couverture radio, de l'état des réseaux, des services tiers, de la configuration, de l'intégrité du backend, de l'état du dispositif et de la disponibilité des destinataires.
Le déclenchement du SOS ou d'autres canaux d'urgence ne remplace pas la structure organisationnelle des secours et ne constitue pas une garantie que la demande a été reçue, comprise ou traitée dans les délais attendus.

Gestion exclusive multi-utilisateur des alarmes et organisation de la prise en charge

Le système adopte une logique de gestion exclusive multi-utilisateur des alarmes, visant à garantir que chaque événement soit pris en charge, à un moment donné, par un seul opérateur de la control room, en évitant les chevauchements, les interventions concurrentes, la duplication des activités ou toute ambiguïté quant à la responsabilité opérationnelle. Dans ce modèle, lorsqu'une alarme passe de l'état de nouveau signalement à un état de prise en charge opérationnelle, elle cesse d'être disponible dans la liste active des autres opérateurs et se trouve ainsi associée de manière exclusive à la personne qui en a lancé la gestion.
Cette architecture permet de conserver une traçabilité claire de la responsabilité opérationnelle de l'événement pendant la phase d'intervention, en réduisant le risque que plusieurs opérateurs agissent simultanément sur la même alarme par des actions non coordonnées, redondantes ou interférant mutuellement.
Si l'opérateur qui a pris en charge l'alarme interrompt sa gestion sans la mener jusqu'à la clôture prévue du workflow, l'événement peut être libéré et remis dans un état de nouveau disponible, redevenant ainsi visible pour les autres opérateurs de la control room et pouvant à nouveau être attribué. Dans cette approche, le système combine l'exclusivité de la prise en

charge avec la possibilité de libération et de réattribution, afin de préserver à la fois l'ordre opérationnel et la résilience organisationnelle en cas d'abandon, d'indisponibilité, de transfert de responsabilité ou de nécessité de réaffectation de la charge.
Le système peut en outre prévoir qu'une alarme restée à l'état « NEW » sans prise en charge dans un délai maximal prédéfini, configuré de manière à garantir la rapidité nécessaire au regard du cas d'usage, déclenche automatiquement une escalade interne à la control room vers les dirigeants ou responsables compétents. Dans cette configuration, l'absence de prise en charge de l'événement dans la fenêtre temporelle attendue ne reste pas confinée au seul niveau opérationnel de premier niveau, mais déclenche un niveau supplémentaire d'attention organisationnelle, visant à réduire le risque de retards incompatibles avec les protocoles de service ou avec la criticité de l'événement.
La control room est organisée avec une couverture opérationnelle dimensionnée pour permettre la plus grande rapidité raisonnablement atteignable dans la prise en charge des alarmes et dans la gestion des procédures correspondantes. La structure de surveillance, le nombre d'opérateurs, les niveaux d'escalade et la répartition des responsabilités peuvent être définis en fonction du nombre de sites desservis, du niveau de risque, du nombre de dispositifs et des protocoles opérationnels du client.
Le workflow d'intervention associé à une alarme n'est pas nécessairement uniforme sur l'ensemble de la plateforme, mais peut être différencié par tenant, par site ou selon d'autres subdivisions organisationnelles prévues par l'architecture applicative. Cette différenciation permet d'adapter fidèlement aux protocoles du client les procédures d'évacuation, les règles d'escalade, les critères de priorité, les destinataires de la notification, les modalités de libération ou de réattribution de l'événement et, plus généralement, le comportement opérationnel de la control room en fonction des spécificités du contexte desservi.
Dans ce cadre, le système n'impose pas un modèle d'intervention abstrait unique, mais permet d'adapter le cycle de vie de l'alarme aux procédures internes, aux plans d'urgence, aux logiques de site et aux règles organisationnelles qui régissent concrètement la prise en charge et la gestion de l'événement.

Clauses de sauvegarde relatives à la gestion exclusive multi-utilisateur des alarmes

La gestion exclusive multi-utilisateur des alarmes améliore l'ordre opérationnel, la traçabilité de la responsabilité et la réduction des interférences entre opérateurs, mais ne garantit pas en soi l'absence absolue de retards, de libérations inappropriées, de réaffectations non optimales ou de discontinuités dans la gestion de l'événement. L'efficacité du mécanisme dépend de la configuration correcte du workflow, de la disponibilité du personnel de

surveillance, de la continuité des systèmes backend et de la qualité de l'organisation opérationnelle de la control room.
L'escalade interne d'une alarme non prise en charge dans le délai maximal configuré constitue une mesure organisationnelle de sauvegarde visant à réduire le risque de défaut de rapidité, mais ne garantit pas en soi que chaque événement soit pris en charge ou géré sans retard en toutes circonstances. Son efficacité dépend du dimensionnement correct de la surveillance, de la disponibilité des responsables concernés, de la configuration des seuils temporels et de la continuité de la plateforme.
La différenciation du workflow par tenant, par site ou par protocole client améliore l'adéquation de la plateforme aux procédures effectives d'urgence et de coordination, mais exige une phase appropriée de conception, de configuration, de validation et de maintenance des règles. Des configurations incomplètes, incohérentes ou non mises à jour peuvent affecter la bonne exécution du cycle de vie de l'alarme et la cohérence entre le comportement du système et les procédures du client.
Le système fournit une aide structurée à la gestion opérationnelle des alarmes, mais ne remplace pas la surveillance humaine, la formation des opérateurs de la control room, le dimensionnement correct du service, les protocoles d'intervention du client ou les responsabilités organisationnelles liées à la gestion des urgences.

Gestion des EPI non Bluetooth par QR code ou sélection

Le système prend également en charge l'enregistrement d'EPI non Bluetooth par scan de QR code ou, dans les cas prévus, par sélection dans une liste sur l'interface du dispositif. Cette fonction permet d'étendre le contrôle procédural à des équipements qui, par choix organisationnel, doivent être enregistrés manuellement en début de poste ou avant une activité déterminée.
Dans le cas d'usage le plus simple, le travailleur enregistre l'EPI requis en scannant le QR code correspondant. Dans un cas d'usage alternatif, le travailleur sélectionne dans la liste du dispositif l'EPI ou le kit procédural pertinent. Dans les deux cas, le système mémorise l'acquisition effectuée en tant qu'élément de conformité applicative.
Une caractéristique importante de cette fonction est que la vérification de l'absence d'EPI non Bluetooth ne coïncide pas nécessairement avec le tout premier instant de la prise de poste. Le système peut en effet prévoir une fenêtre initiale dédiée à l'enregistrement correct, afin d'éviter que l'absence d'acquisition immédiate ne génère des alarmes prématurées alors que la procédure d'entrée est encore en cours.

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

Le cas d'usage type est celui du travailleur qui doit déclarer ou enregistrer ses équipements avant de commencer l'activité. Si le système ne détecte pas, dans les conditions et les délais configurés, l'acquisition des EPI requis, il peut générer une alarme de non-conformité, unique ou répétée, selon la logique définie de manière centralisée.
Cette fonction a donc une portée essentiellement procédurale : elle vise à renforcer le respect des règles d'entrée en activité ou en zone et à fournir à la plateforme une preuve applicative de l'accomplissement de l'étape requise.
La dotation obligatoire en EPI non Bluetooth est configurable à plusieurs niveaux et peut être définie en fonction du tenant, du site opérationnel, de la tâche attribuée, du profil de chaque opérateur et, plus généralement, des règles organisationnelles applicables au cas d'usage spécifique. Dans une logique de projet avancée, cette configuration peut en outre être intégrée au niveau du backend avec des systèmes legacy ou des applications préexistantes de gestion des permis de travail, des autorisations opérationnelles, des procédures d'accès aux zones ou aux activités et d'autres contraintes organisationnelles, afin de rendre le contrôle des EPI cohérent avec le cadre d'autorisation global du site.
La sélection ou le scan des QR codes des EPI n'est pas nécessairement prévu comme une étape obligatoire dans toutes les configurations applicatives du système. Selon le modèle organisationnel adopté, le niveau d'intégration du projet et les règles définies pour le site, la procédure peut en effet être rendue obligatoire, facultative ou ne pas être requise du tout.

Clauses de sauvegarde relatives aux EPI non Bluetooth avec QR code ou sélection

L'enregistrement par QR code ou par sélection constitue une preuve applicative d'acquisition dans le système et **non une preuve absolue de la possession matérielle effective, du port correct, de l'adéquation technique ou du maintien continu de l'EPI pendant toute la durée du poste**.

Positionnement et localisation de l'opérateur

La fonction de positionnement ne repose pas sur une source unique, mais sur une politique multicapteur conçue pour maintenir une estimation aussi robuste que possible de la position de l'opérateur, avec une activation exclusivement en cas d'alarme, dans des environnements hétérogènes, avec une attention particulière portée au compromis entre précision, continuité de la donnée et soutenabilité énergétique du dispositif porté.
La localisation intègre des informations provenant de plusieurs technologies disponibles, notamment GNSS (Global Navigation Satellite System), services de localisation assistée,

fournisseurs de localisation fusionnée, IMU (Inertial Measurement Unit), navigation à l'estime (dead-reckoning) inertielle, WiFi fingerprinting, Bluetooth fingerprinting et, le cas échéant, RTLS (Real-Time Location System) ou d'autres sources contextuelles. L'estimation finale résulte de la combinaison de ces contributions dans un cadre de fusion unique, afin de limiter la dépendance à une source unique et d'améliorer la résilience de la donnée.
Un principe fondamental du sous-système est l'adoption de stratégies d'acquisition opportuniste. Le système ne force pas à tout moment l'activation maximale du récepteur de position, mais vérifie d'abord s'il existe un fix récent et suffisamment fiable déjà disponible en cache. Lorsque le cache n'est plus considéré comme adéquat, le système procède à une nouvelle acquisition active.
L'acquisition active n'est pas uniforme dans toutes les conditions. La stratégie peut en effet s'adapter au contexte, en privilégiant différents modes selon l'état opérationnel du dispositif, la qualité du signal disponible, l'éventuel état d'alarme, la nature vraisemblablement intérieure ou extérieure du scénario et le niveau de précision requis. Le système recherche ainsi le meilleur équilibre entre précision et soutenabilité énergétique.
Un autre élément essentiel est la validation de la cohérence des fix. La position candidate n'est pas acceptée automatiquement du seul fait qu'elle est disponible, mais peut être comparée à la position précédente, à la précision déclarée, à l'ancienneté de la mesure et à la plausibilité du mouvement impliqué par le passage d'un fix à l'autre. Cela permet d'atténuer les sauts de position incompatibles avec le déplacement réel de la personne et de réduire les effets d'erreurs sporadiques du fournisseur ou de conditions radio dégradées.
Cette architecture permet plusieurs cas d'usage. En environnement extérieur dégagé, le système peut s'appuyer avec une plus grande fiabilité sur les sources satellitaires ou sur les fournisseurs de position fusionnée, et obtenir ainsi une estimation relativement directe. En environnement intérieur ou dans des zones masquées, la localisation peut dépendre davantage des informations inertielles, des empreintes radio ou des règles de zone. En état d'alarme, le système peut intensifier le rythme des mises à jour afin de rendre la trace opérationnelle plus utile à la structure de surveillance. En conditions d'utilisation ordinaires, il peut au contraire adopter des politiques plus économes afin de préserver l'autonomie et la continuité générale du dispositif.
La gestion du positionnement est normalement abordée selon une approche projet, configurée en fonction des caractéristiques du site opérationnel et des infrastructures effectivement disponibles. Dans cette approche, le sous-système de localisation peut être intégré, lorsqu'ils sont présents et correctement configurés, avec des réseaux WiFi, des cartes d'empreintes radio (fingerprinting), des logiques de zone, des références topologiques du site

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

et d'autres sources contextuelles propres à améliorer la robustesse de l'estimation de position, en particulier dans les environnements intérieurs ou mixtes.
La politique de localisation n'est donc pas nécessairement unique, mais est définie en fonction du cas d'usage, du niveau de précision requis, des contraintes énergétiques du dispositif, de la disponibilité d'infrastructures locales et du degré de continuité du suivi jugé nécessaire dans le contexte applicatif.
Dans la configuration de base, le système utilise exclusivement les services de localisation fusionnée fournis par Google Play Services, avec une gestion adaptative des demandes de position. Dans cette configuration, le niveau de précision requis, la fréquence de mise à jour et l'intensité de la recherche sont modulés dynamiquement en fonction de l'état opérationnel du dispositif et du contexte détecté, par exemple en distinguant les conditions ordinaires des situations d'alarme, les scénarios intérieurs des scénarios extérieurs, les phases de surveillance normale des phases dans lesquelles une plus grande réactivité de l'information vers les systèmes distants est requise.
Même dans cette configuration de base, la localisation est donc gérée selon des critères d'équilibre entre précision, continuité de la donnée et soutenabilité énergétique, en évitant les approches rigidement uniformes et en privilégiant au contraire une stratégie adaptative cohérente avec la fonction de sécurité du système et avec les limites opérationnelles d'un terminal porté.

Clauses de sauvegarde relatives au positionnement

Le positionnement fourni par le système est une estimation technique obtenue par fusion multicapteur et critères de validation logicielle. Il ne constitue pas une mesure absolue, continue et infaillible de la position réelle de l'opérateur à chaque instant.
La qualité de l'estimation dépend du contexte intérieur ou extérieur, de la couverture satellitaire, des perturbations induites par des artefacts ou par les trajets multiples (multipath), de la qualité du signal radio, de la disponibilité des sources auxiliaires, de la dynamique du mouvement, de l'état énergétique du dispositif, de la configuration et des conditions environnementales.
Le système ne garantit pas une localisation continue, une précision uniforme dans tous les environnements, l'absence de retard, l'absence de dérive ou la disponibilité permanente de toutes les sources de position. **La donnée de position doit être interprétée comme une aide opérationnelle et non comme une certitude absolue.**

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

Localisation assistée des équipes de secours et aide pour rejoindre la cible

Dans des configurations de projet avancées, le sous-système de localisation peut être utilisé pour aider les personnes chargées de l'intervention, de la vérification ou des secours à rejoindre une cible opérationnelle.
Cette fonction revêt une importance particulière dans les contextes complexes, étendus, intérieurs ou à visibilité réduite, dans lesquels la simple disponibilité d'une position abstraite ne suffit pas et où il est au contraire nécessaire de soutenir la coordination opérationnelle de l'approche.

Clauses de sauvegarde relatives à la localisation assistée de la cible

Même dans les configurations avancées de localisation assistée, le système fournit une aide opérationnelle et non une garantie absolue d'atteinte rapide, précise ou exempte d'erreur de la personne ou du point à rejoindre. L'efficacité dépend de la qualité des infrastructures du site, de la disponibilité des sources de localisation, de la cohérence de la cartographie et des conditions environnementales réelles.

Configurabilité du système et dépendance au cas d'usage

Le système SAS est hautement configurable. Les paramètres de seuil, les logiques d'alarme, les délais de latence, les politiques de communication, les critères de localisation, les règles de zone, les listes d'EPI, les fréquences de mise à jour et les comportements de l'interface peuvent être adaptés au cas d'usage et personnalisés par tenant, par site, par groupe, par tâche, par équipe et jusqu'au niveau individuel.
Cette configurabilité constitue l'un des principaux atouts de la plateforme, puisqu'elle permet de l'appliquer dans des contextes différents sans réduire toutes les situations opérationnelles à un modèle standard unique. Elle rend toutefois le système fortement dépendant de l'exactitude de la configuration appliquée. Une fonction bien conçue mais paramétrée de manière incohérente par rapport au site, au risque et à l'organisation peut produire des résultats applicatifs insatisfaisants.

Mises à jour à distance et reconfiguration de la plateforme

La configurabilité de la plateforme s'étend également à la possibilité de mettre à jour à distance des paramètres, des règles, des profils applicatifs, des pages opérationnelles, des

dotations requises, des politiques de localisation, des logiques d'avertissement et d'autres éléments fonctionnels du système, afin d'adapter le comportement du dispositif et du backend à l'évolution du site, des procédures ou du modèle organisationnel adopté. Cette capacité permet de maintenir le système en adéquation avec le contexte opérationnel sans nécessairement exiger des interventions manuelles locales sur chaque terminal, sauf dans les cas où l'architecture de déploiement spécifique ou les politiques du client prévoient des modalités différentes.

Clauses de sauvegarde relatives aux mises à jour et à la reconfiguration

Les opérations de mise à jour et de reconfiguration améliorent l'adaptabilité du système, mais exigent une gouvernance appropriée du cycle de vie applicatif, une validation des modifications et un contrôle de la cohérence entre la configuration déployée et le cas d'usage réel. Des modifications non correctement validées ou incohérentes avec le contexte peuvent altérer le comportement opérationnel du système.

Mise à jour automatique et silencieuse de l'application en mode OTA

Le système peut prendre en charge des procédures de mise à jour de l'application en mode OTA (Over-The-Air), destinées à permettre la distribution à distance de nouvelles versions du logiciel sans exiger d'intervention manuelle locale sur chaque dispositif. Dans cette configuration, la mise à jour de l'APK peut être gérée de manière automatique et silencieuse, selon les politiques de sécurité, les privilèges système et les modalités de déploiement prévus par l'architecture adoptée.
Cette capacité joue un double rôle applicatif. D'une part, elle constitue un outil de maintenance évolutive, puisqu'elle permet de distribuer des améliorations fonctionnelles, des corrections, des optimisations, des adaptations de compatibilité, des affinements des algorithmes, des mises à jour de l'interface et des améliorations des logiques de communication, de localisation ou de gestion des alarmes. D'autre part, elle représente également un élément important d'appui aux personnalisations de projet, puisqu'elle permet d'introduire, de mettre à jour ou d'adapter de manière maîtrisée des composants logiciels spécifiques à un client, à un site, à une tâche ou au cas d'usage particulier mis en œuvre.
D'un point de vue opérationnel, la mise à jour silencieuse permet de réduire les délais de propagation des modifications, d'uniformiser plus rapidement le parc de dispositifs, de limiter la nécessité de reconfigurations manuelles sur le terrain et de maintenir une plus grande cohérence entre la version logicielle, la configuration du backend et l'architecture

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

applicative globale. Dans un écosystème distribué tel que SAS, cette fonction contribue de manière significative à la gouvernabilité de la plateforme, tant dans les contextes centralisés que dans les contextes on premises ou à gestion hybride.
La mise à jour OTA peut en outre être utilisée pour accompagner l'évolution incrémentale du système dans le temps, en permettant de suivre l'élargissement des intégrations avec l'écosystème de sécurité, l'introduction de nouvelles fonctionnalités, l'extension des pages opérationnelles, la modification des logiques d'interaction avec la control room ou l'adaptation à des exigences de projet spécifiques apparaissant au cours du cycle de vie de la solution.
Pour des raisons de continuité opérationnelle et de soutenabilité énergétique, la mise à jour OTA est généralement reportée à la première phase de charge suivant la publication de la nouvelle version, afin de réduire au minimum l'impact sur les activités en cours, d'éviter les interférences avec les fonctions opérationnelles du dispositif pendant le poste et de limiter les effets du processus de mise à jour sur l'autonomie résiduelle de la batterie. Dans cette approche, le moment de la publication et celui de l'installation effective ne coïncident pas nécessairement, car l'architecture privilégie une logique de distribution compatible avec l'utilisation réelle du terminal sur le terrain.
Dans cette perspective, la mise à jour automatique et silencieuse ne doit pas être comprise uniquement comme un outil technique de distribution logicielle, mais comme un **composant structurel de la maintenabilité et de l'évolution maîtrisée de la plateforme**, capable de soutenir aussi bien l'évolution standard du produit que la gestion de profils applicatifs et de personnalisations spécifiques.

Clauses de sauvegarde relatives à la mise à jour OTA

La disponibilité de mécanismes de mise à jour automatique et silencieuse ne garantit pas, en soi, que chaque mise à jour sera distribuée, téléchargée, installée ou rendue opérationnelle avec succès en toutes circonstances. L'efficacité du processus dépend de la disponibilité de la connectivité, de l'état du dispositif, de la compatibilité de la version distribuée, de la bonne gestion du cycle de publication, de la disponibilité de l'espace nécessaire, des politiques de sécurité du terminal et de l'intégration correcte entre le backend, le paquet applicatif et l'architecture de déploiement.
Le report de l'installation à la phase de charge suivante réduit normalement l'impact sur l'exploitation et sur l'autonomie du dispositif, mais ne garantit pas en soi que la mise à jour sera appliquée immédiatement après sa publication ou dans un délai uniforme sur l'ensemble du parc de terminaux. Le calendrier effectif de l'installation peut dépendre des

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

cycles réels d'utilisation et de recharge, de la disponibilité de la connectivité au moment prévu, de l'état du terminal et des règles de distribution adoptées.
La mise à jour logicielle, bien qu'elle vise l'amélioration évolutive et la gestion maîtrisée des personnalisations, exige des procédures appropriées de validation, de vérification et de gouvernance de la publication. Des modifications non correctement validées ou incohérentes avec le contexte opérationnel peuvent affecter le comportement applicatif du système, la continuité de certaines fonctions ou la cohérence avec les configurations de site.
La présence de fonctionnalités de mise à jour à distance **n'élimine pas la nécessité de planifier le cycle de maintenance, de contrôler les versions déployées, de procéder à des vérifications après publication et d'assurer une supervision organisationnelle des modifications introduites**. Même en présence d'une mise à jour silencieuse, il reste nécessaire d'assurer la cohérence entre l'évolution logicielle, les exigences du cas d'usage, la configuration du backend et les procédures opérationnelles du client.

Clauses de sauvegarde générales relatives à la configuration

Le système doit être utilisé uniquement dans des configurations cohérentes avec le contexte opérationnel, la tâche, les procédures internes et les finalités pour lesquelles il a été adopté. Des configurations incomplètes, incohérentes, non validées ou non mises à jour peuvent altérer considérablement la sensibilité, la spécificité, la rapidité et l'utilité des informations produites.

État de charge et suspension des fonctions opérationnelles

Lorsque le dispositif est placé durablement en charge selon les modalités prévues pour la fin du poste ou pour le rangement opérationnel, le système suspend automatiquement les fonctions de surveillance et de génération d'événements, afin d'éviter des interprétations erronées du terminal dans des conditions incompatibles avec son utilisation normale au poignet. Dans cette configuration, le passage à l'état de charge ne correspond pas seulement à une recharge énergétique, mais peut également constituer un indicateur applicatif de sortie du contexte d'utilisation ordinaire du dispositif.

Clauses de sauvegarde relatives à l'état de charge

La mise en charge du dispositif entraîne la suspension de certaines fonctions opérationnelles ; par conséquent, le terminal ne doit pas être considéré comme pleinement équivalent à un

dispositif porté et actif pendant le poste de travail normal lorsqu'il se trouve dans cette condition.

Intégration de la smartwatch dans l'écosystème de sécurité

La smartwatch H09 est conçue non pas comme un terminal isolé, mais comme le nœud personnel d'un écosystème de sécurité plus large, dans lequel la valeur opérationnelle découle de l'intégration entre dispositifs individuels, capteurs distribués, infrastructures de site, systèmes de supervision et modules logiciels avancés d'interprétation du contexte. Dans cette architecture, le dispositif porté peut agir à la fois comme source d'événements et de données et comme point terminal de réception d'avertissements, d'alarmes, d'instructions opérationnelles, d'états contextuels et de contenus d'aide provenant du reste de l'écosystème.

Clauses de sauvegarde relatives à l'intégration dans l'écosystème

L'intégration de la smartwatch avec d'autres éléments matériels et logiciels de l'écosystème de sécurité élargit le cadre informatif disponible et les possibilités de coordination opérationnelle, mais ne garantit pas en soi l'exhaustivité absolue, la continuité ininterrompue ou l'exactitude infaillible de la représentation du risque. L'efficacité globale dépend de la qualité et de la disponibilité des sous-systèmes intégrés, de l'exactitude des interfaces, de la cohérence de conception de l'architecture, de l'état de maintenance des infrastructures, de la disponibilité de la connectivité et de la configuration correcte des règles de corrélation.

Clauses générales de sauvegarde relatives à l'utilisation

Le système doit être intégré dans un modèle organisationnel structuré, comprenant la formation du personnel, des procédures d'urgence, la supervision, la maintenance des dispositifs, le contrôle des configurations, la vérification périodique de l'utilisation correcte et la disponibilité d'une structure de surveillance, le cas échéant.
Le système n'est pas apte à constituer l'unique moyen de sécurité du travailleur. Il doit être complété par les mesures humaines, techniques, organisationnelles et procédurales requises par le contexte spécifique.
L'utilisation inappropriée, le défaut de port, la désactivation des fonctions, l'altération du logiciel, les configurations non conformes, l'utilisation dans des environnements incompatibles ou le défaut de maintenance peuvent réduire de manière significative l'efficacité applicative du système.

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

Clauses de non-médicalité

Le système SAS avec smartwatch H09 n'est pas un dispositif médical, n'est pas un système de surveillance clinique, n'est pas un outil de diagnostic, n'est pas un moyen thérapeutique et n'est pas un système de sauvetage certifié.
Les paramètres vitaux, les données comportementales, les estimations de chute et les classifications générées par le logiciel doivent être interprétés comme des indicateurs techniques d'aide à la sécurité opérationnelle et non comme des comptes rendus médicaux, des preuves cliniques ou des certifications diagnostiques.

Clauses de limitation de responsabilité

Le système ne garantit pas la détection universelle de tout événement traumatique, paramètre vital, événement procédural ou contextuel. Il ne garantit pas l'absence de faux positifs, l'absence de faux négatifs, la continuité absolue du service, la remise certaine de chaque communication, la disponibilité permanente de la donnée de position ou la vérification matérielle absolue de la présence effective des EPI. L'éventuelle non-détection d'un événement, la classification imparfaite d'une situation, le retard d'une notification, le défaut d'enregistrement d'un EPI, l'inexactitude de la position ou l'indisponibilité temporaire d'une fonction ne constituent pas, à eux seuls, une preuve automatique de dysfonctionnement certain ni un fondement de responsabilité objective du fabricant ou du fournisseur.
Il incombe à l'organisation utilisatrice de définir le cas d'usage approprié, de valider la configuration, de former le personnel, de maintenir le système en bon état de fonctionnement, de mettre en place des procédures d'urgence et de compléter le système par toutes les mesures complémentaires nécessaires.

Déclaration finale

Le système SAS avec smartwatch H09 est une plateforme technologique d'aide à la sécurité opérationnelle.
Le système est conçu pour accroître la probabilité d'interception des événements critiques, renforcer la conformité procédurale, améliorer la capacité de supervision à distance et soutenir l'organisation de la réponse. Il fonctionne toutefois dans les limites propres à un dispositif porté au poignet, à des capteurs non cliniques, à des logiques logicielles inférentielles, à une infrastructure de communication pas toujours entièrement maîtrisable et à un contexte opérationnel réel variable.

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

Pour ces raisons, le système ne constitue pas un dispositif médical, ne remplace pas la surveillance humaine, ne remplace pas les procédures internes d'urgence et ne garantit pas de manière absolue la détection, la classification, la transmission ou la prise en charge de tout événement en toutes circonstances.

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