Sécurité
des
Unités Locales Intelligentes
WIT

MTR/002F • V1.0 • 02/2024

SOMMAIRE

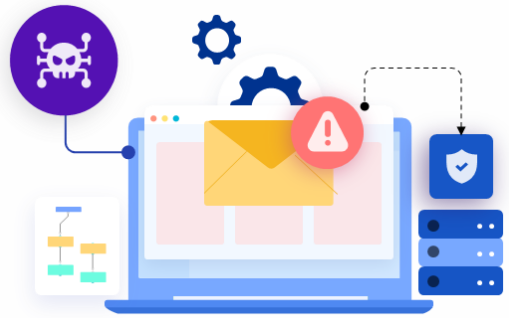
Introduction

Généralités

La sécurité a depuis toujours été un sujet important pour les équipements techniques des bâtiments, et elle l'est d'autant plus ces dernières années. Notre secteur d'activité est exposé, comme d'autres secteurs d'ailleurs, aux risques de cyberattaques. Tous nos clients sont concernés par la cybersécurité selon les enjeux de leurs métiers et les éventuelles contraintes réglementaires auxquelles ils sont soumis.

La cybersécurité pour WIT est un enjeu majeur inscrit dans la stratégie de l'entreprise dans la durée. Nous mettons en œuvre les recommandations de l'ANSSI dans le process industriel de conception, d'assemblage de nos produits et de leur mise en œuvre sur site.

Ce document permet de connaitre les mécanismes et habitudes à mettre en place pour sécuriser votre installation de GTEB.



Qu'est-ce que l'ANSSI ?

Service du Premier ministre, rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN), l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. Acteur majeur de la cyber sécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

La sécurité des accès

Premier maillon de la chaîne : l'accès au système doit être protégé des intrus et affecter les autorisations de chaque utilisateur selon ses droits.

La sécurité des données

Les données constituent le cœur des Unités Locales Intelligentes. Leur accès mais aussi leur intégrité et leur pérennité doivent être assurées.

La sécurité fonctionnelle

Socle et prérequis indispensable aux deux précédents ensembles : la sécurité fonctionnelle garantit un fonctionnement adapté à chaque situation.

Symboles du document

Ce symbole représente les actions conseillées par WIT, cela permet d'assurer le respect des bonnes pratiques conseillées par l'ANSSI.

Supports documentaires

Ce document est complémentaire à d'autres documents liés à la sécurité ou à l'utilisation de nos ULI, ils sont tous disponibles depuis notre site www.wit.fr espace **Téléchargement** :

Livret de sécurité - Les 13 bonnes pratiques de l'ANSSI
Présente les recommandations et bonnes pratiques de l'ANSSI pour les systèmes industriels.

Manuel Communications sécurisées
Détaille le fonctionnement des protocoles sécurisés dans nos ULI, tel que : HTTPs, FTPs et SMTPs

Manuel OpenVPN
Décrit comment configurer et utiliser l'OpenVPN (client et serveur) dans l'environnement REDY.

Manuel de paramétrage REDY

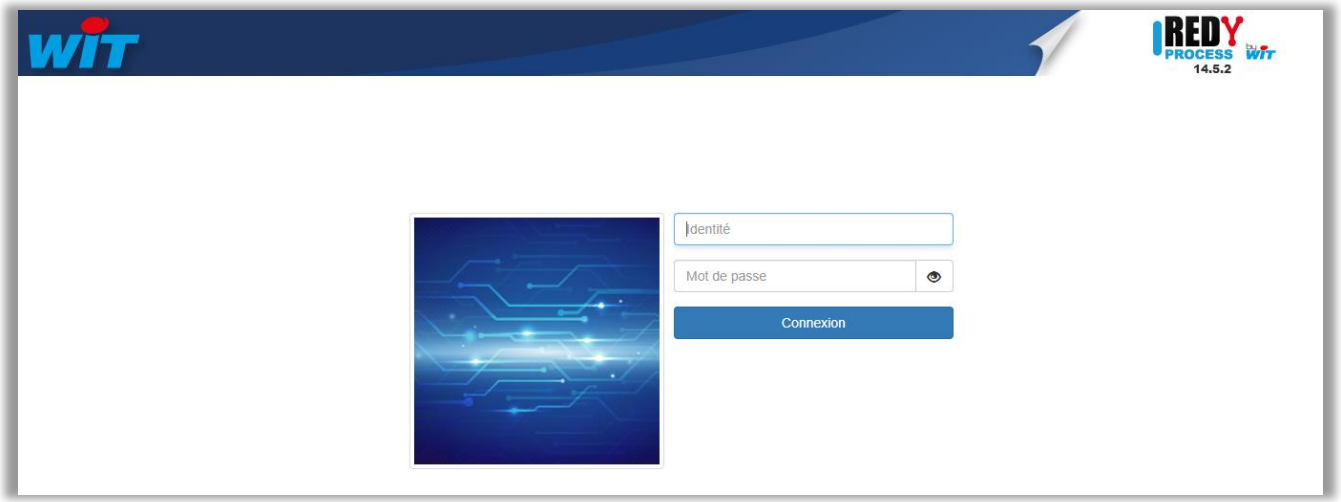
Permet de comprendre les fondamentaux du logiciel, son fonctionnement général et les configurations minimales requises.

Sécurité des accès

Identifiants

L'accès aux ULI est sécurisé par une demande d'identification à deux paramètres :

- Un nom d'utilisateur.
- Un mot de passe.



Nom d'utilisateur

- Chaque nom d'utilisateur est unique.
- Une vérification automatique d'unicité est réalisée à chaque création d'un nouvel utilisateur.
- Un nom d'utilisateur peut être composé de 1 à 65 caractères. Lettres, chiffres et/ou caractères spéciaux.

Mot de passe

- Un mot de passe sécurisé peut être composé de 12 à 15 caractères. Lettres, chiffres et caractères spéciaux.
- La casse (majuscule/minuscule) des lettres est prise en compte.

Un délai d'attente de une minute est présent suite à la saisie de trois mauvais noms d'utilisateur ou mots de passe.

Symbolique

Identifiants par défaut

Lorsque les identifiants par défaut sont toujours utilisés, un symbole est présent en haut à droite de la page de l'ULI REDY :

Il est fortement recommandé de modifier les identifiants par défaut, ces identifiants ne doivent être utilisées qu'en phase d'installation.
Les identifiants par défaut sont renseignés dans les documentations techniques de mise en service.
Ce sont donc les premiers identifiants qu'un individu utilisera pour tenter d'accéder au système.
Lorsque le site est en exploitation, cette symbolique ne doit jamais apparaitre.

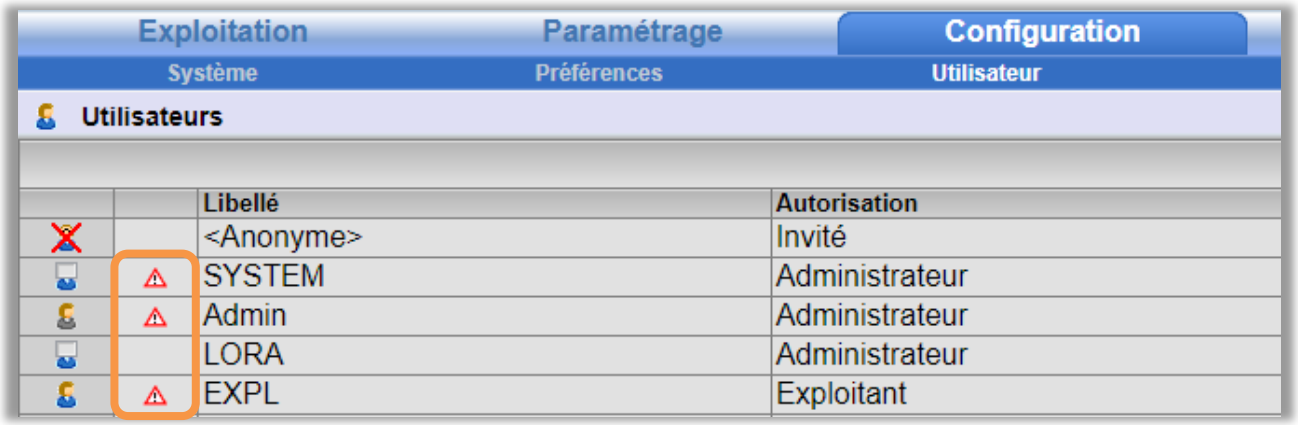
Sécurité des mots de passes

Lorsqu'un des mots de passes est trop faible, la symbolique suivante apparait en haut à droite de la page de l'ULI REDY :

Cela ne doit arriver que lorsqu'un ancien paramétrage effectué en version inférieure à la V14.0.0 est chargé dans une ULI REDY supérieure ou égale à la V14.0.0.

Mot de passe « obsolète »

Une symbolique d'avertissement apparait au bout de 6 mois sur les utilisateurs (Configuration / Utilisateur), cela ne bloque pas l'identifiant en question mais avertit l'administrateur que le mot de passe devrait être changé pour plus de sécurité :



		Libellé	Autorisation
		<Anonyme>	Invité
	⚠	SYSTEM	Administrateur
	⚠	Admin	Administrateur
		LORA	Administrateur
	⚠	EXPL	Exploitant

Niveaux utilisateurs

Chaque utilisateur est associé à un « niveau utilisateur » autorisant ou non certaines fonctionnalités. Les ULI WIT disposent de 4 niveaux :

Niveau 1 - Invité	*Lecture seule (par défaut).*
Niveau 2 - Exploitant	*Lecture et commande des paramètres d'exploitation (consignes, planning, etc.).*
Niveau 3 - Installateur	*Modification du paramétrage, des écrans graphiques.*
Niveau 4 - Administrateur	*Accès à l'ensemble du système.*

Chaque niveau reprend les autorisations du niveau précédent.

Droits des Administrateurs

Seul les utilisateurs ayant des droits Administrateurs ont la possibilité de créer/modifier/supprimer des utilisateurs. Il peuvent notamment personnaliser l'accès à chaque donnée (mesure, consigne, processus, …) pour être en consultation et/ou en pilotage pour chaque utilisateur par des profils (groupes) d'utilisateurs. Ces profils permettent à la fois de sécuriser l'accès aux données et de simplifier leur exploitation. Le nombre de profils peut être de 1000 par Unité Locale Intelligente.

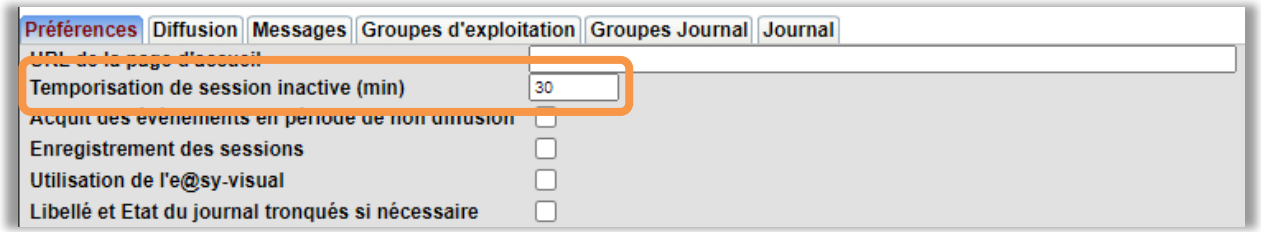
Ils sont les garants de la gestion des droits et de la sécurité des Utilisateurs.

Le niveau d'accès **Administrateur** ne permet pas de voir les codes d'accès des autres utilisateurs.

Afin de suivre les bonnes pratiques de l'ANSSI, nous conseillons aux Administrateurs de modifier les codes d'accès des utilisateurs en les informant tous les 6 mois.

Déconnexion automatique

Lorsque la session d'un utilisateur est inactive durant un temps donné, la session de cet utilisateur est automatiquement fermée. Ceci permet de réduire le risque que cette session soit utilisée par une autre personne de manière non désirée.
Le temps de session (30 min par défaut) peut être personnalisé pour chaque utilisateur, pour une meilleure sécurité d'accès, nous conseillons de ne pas modifier la temporisation par défaut :



Journal des actions utilisateurs

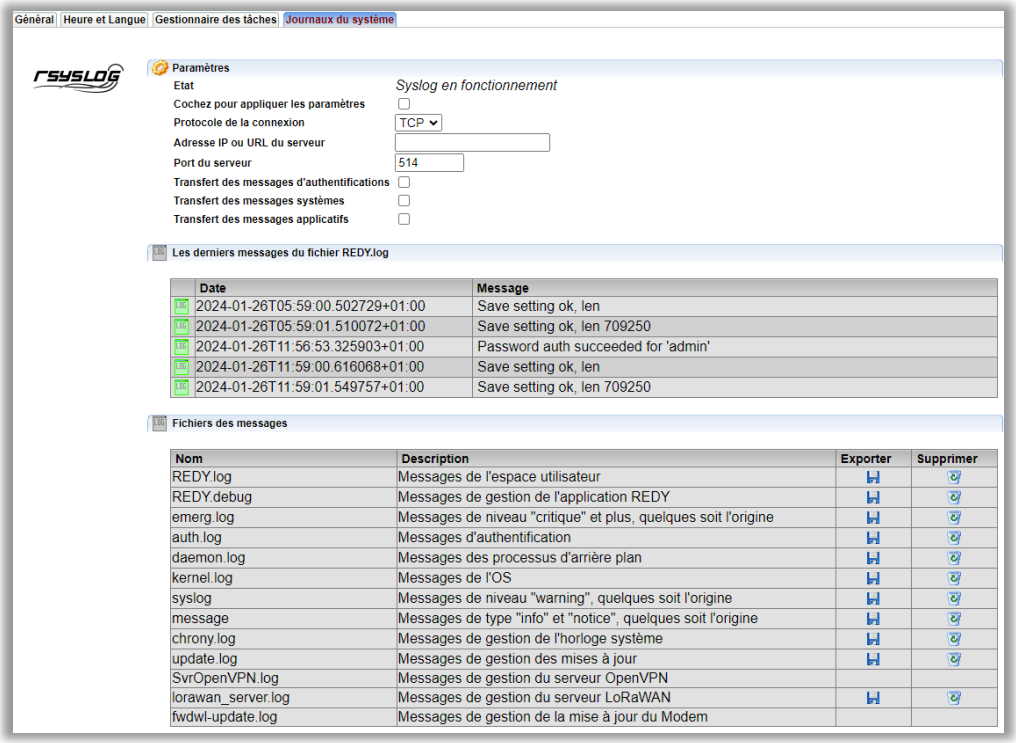
Les changements de consignes peuvent être tracés dans le journal des l'ULI, cela demandera à l'installateur de la programmer dans chaque ressources concernées (onglet Témoins).
Les sessions des utilisateurs (connexions, déconnexions et actions) peuvent aussi être enregistrées de manière horodatée dans un journal appelé : journal des sessions.
Le journal des sessions peut être activé/désactivé pour chaque utilisateur (Configuration / Utilisateur):

```
20190111121350  Connexion  Pierre :System.User.U00001
20190111121359  Créer      Variable analogique :easy.RESS.R00011
20190111121402  Déconnexion
```

Il est conseillé d'actionner les sessions des utilisateurs uniquement pour une visibilité de **7 jours** maximum pour **20 utilisateurs** maximum, cela afin d'éviter la surcharge mémoire liée à la multitude de fichiers créés.
Les fichiers de sessions peuvent être supprimés dans **Configuration/Utilisateurs/Session/Onglet Enregistrement**.

Journal RSyslog

Les messages Rsysolg permettent une traçabilité des évènements d'administration de l'ULI REDY.
Afin d'éviter toute malveillance en supprimant cette traçabilité, les messages Rsyslog peuvent être envoyés à un serveur Rsyslog compatible, le serveur Rsysolg est activé par défaut :



Paramètres du Rsyslog

Etat	Affiche l'état du moteur Rsyslog (fonctionne en permanence)
Cocher pour appliquer les paramètres	Permet de valider les paramètres réseaux et les préférences saisies
Protocole de connexion	Protocole utilisé pour transmettre les messages (TCP ou UDP)
Adresse IP ou URL du serveur	Adresse IP du serveur Rsyslog recevant les messages du REDY
Port du serveur	Port du serveur Rsyslog
Transfert des messages d'authentifications	Choix de transmettre les messages d'authentifications
Transfert des messages systèmes	Choix de transmettre les messages systèmes
Transfert des messages applicatifs	Choix de transmettre les messages applicatifs

Les derniers messages du fichier REDY.log

Tableaux indiquant les 5 derniers messages du Rsyslog

Fichiers des messages

Tableaux indiquant les messages disponibles, les messages peuvent être exportés ou supprimés.
La lecture des messages est destinée à un usage avancé.

Nous vous conseillons de vous assurer :

- Que la DSI du site dispose d'une politique de gestion de mots de passe définie pour l'ULI et que celle-ci a été mise en œuvre.
- De définir strictement les personnes autorisées sur les systèmes (Identifications et autorisations) et en réduisant au strict minimum les administrateurs.
- D'activer la journalisation via des protocoles tel que Syslog ou SNMP.
- D'envoyer les données RSyslog vers un serveur RSyslog compatible.
- De centraliser les journaux et en assurer le stockage et la sauvegarde.
- De définir une stratégie de conservation de ces journaux.
- Que la DSI a bien mis en place un système de sauvegarde pour ces journaux.

Disponibilité

Remontée en temps réel des indisponibilités

Les automates peuvent monitorer des erreurs de communication et ainsi remonter les alarmes correspondantes.
Les Unités Locales Intelligentes WIT assurent une surveillance permanente de leur état de fonctionnement et de ses périphériques :

- Présence secteur.
- Tension batterie.
- Tension UC.
- Mémoire restante (%).
- Temps de cycle min, max et moyen (ms).
- Etat des bus de communication.
- Statistiques sur les trames émises et reçues.
- Date et heure de la dernière initialisation de l'UC.

Lorsque l'état d'un des paramètres surveillés est diagnostiqué anormal, l'ULI est en mesure de diffuser une alerte et si besoin basculer vers un état de repli.

Stratégie de secours

L'ULI peut être équipée de plusieurs moyens de communication (voir paragraphe 6) permettant un basculement selon la disponibilité. Cela permet donc un mode de repli.

Sauvegarde des données

Les données

Dans l'ULI REDY

Les données acquises, archivées et traitées sous forme de Trace, Journal, Bilan, Flux sont sauvegardées dans une mémoire permanente. Cette mémoire conserve l'intégralité des données sur coupure d'alimentation et redémarrage du système. Les données peuvent être exportées en différents formats de manière à pouvoir être sauvegardées sur un support externe et traitées par des logiciels/services par un tiers. La sauvegarde des données est automatisée tous les jours à minuit.

Dans l'ULI e@sy

Les données acquises, archivées et traitées sous forme de **Trace** et **Journal**, sont sauvegardées dans une mémoire RAM. Cette mémoire ne conserve pas les données sur coupure d'alimentation et redémarrage du système. Néanmoins, ces données peuvent être exportées en différents formats de manière à pouvoir être sauvegardées sur un support externe et traitées par des logiciels/services par un tiers.
Les données de **Bilan** et de **Flux** sont sauvegardées dans une mémoire permanente. Cette mémoire conserve l'intégralité de ces données sur coupure d'alimentation et redémarrage du système. Les données peuvent être exportées en différents formats de manière à pouvoir être sauvegardées sur un support externe et traitées par des logiciels/services par un tiers.

Le paramétrage

Nous conseillons de mettre en place une stratégie de sauvegarde grâce aux possibilités offertes par l'ULI et notamment un export et une sauvegarde lors d'une modification du paramétrage.
Lors d'une sauvegarde du paramétrage réalisée par l'utilisateur, l'ULI conserve automatiquement la version antérieure à la version sauvegardée. Au démarrage de l'automate, si la sauvegarde en cours est corrompue, l'ULI utilisera automatiquement la version antérieure déjà sauvegardée. L'ULI maitrise ses Utilisateurs et vérifie l'intégrité du fichier de paramétrage au démarrage.

Nous vous conseillons de vous assurer :

- D'avoir une gestion des utilisateurs maitrisée, c'est-à-dire diminuer le plus strictement possible l'élévation des privilèges des utilisateurs ayant accès au paramétrage.
- De s'assurer qu'aucune injection de code malveillant ne soit exécutée par les systèmes.
- De sécuriser l'accessibilité aux systèmes, que ce soit en accès physique ou via les réseaux (LAN, Wi-Fi, 3G ou 4G).
- Que les accès administrateurs et installateurs soient connus et divulgués uniquement aux personnes concernées.
- Que les accès via réseaux soient connus et maitrisés.
- Que les échanges de fichier via FTP ou FTPs soient réalisés de manière ponctuels et contrôlés.

L'Applicative ULI

Il est possible de sauvegarder les versions Applicative antérieures de l'ULI. En cas de problème, il est possible (mais non conseillé) de revenir à la version antérieure.
OS (Operating System) : Il est possible de sauvegarder les OS antérieurs de l'ULI. En cas de problème, il est possible (mais non conseillé) de revenir à la version antérieure.

Le système

Le noyau de l'ULI REDY (appelé OS), intègre un codage de sécurité de 2048 bits.
En cas de corruption de l'OS de l'ULI et après 3 tentatives de démarrage infructueuses, l'ULI bascule automatiquement sur un second OS.
Après le démarrage réussi de ce nouvel OS, celui-ci répare le premier OS afin de s'assurer lui-même en cas de nouvelle corruption.

Nous vous conseillons de vous assurer :

- D'effectuer des sauvegardes régulières et automatisées, de la structure des programmes et des données.
- D'avoir un accès simple à ces sauvegardes horodatées, cela permet une restauration de l'installation rapide et fluide.
- Qu'au minimum les sauvegardes de la structure et des données soient réalisées automatiquement à une fréquence cohérente avec l'usage de paramétrage de l'installation.
- Que l'export et le stockage des fichiers soient réalisés à minima dans deux localisations différentes facilement accessibles et sécurisés.

Maintien en condition de sécurité

Attaques par déni de service

Afin de limiter les attaques par déni de service, il est recommandé de changer les ports d'origine. Cependant pour une sécurité renforcée, nous recommandons d'effectuer l'exploitation du site en activant la Synapps comme point d'accès unique. Cela permet de traiter plus efficacement ces attaques qui peuvent rendre inaccessible le système.

Couverture antivirale à jour et surveillée des composants Windows

Les postes utilisateurs ayant accès aux ULIs doivent être protégés.

Nous vous conseillons de vous assurer que les postes utilisateurs ayant accès aux ULIs ont :

- Leur antivirus actifs et à jour, que leurs bases de données soient automatiquement mises à jour.
- Un système d'exploitation à jour des derniers correctifs de sécurité.
- Si les équipements ne possèdent pas d'antivirus, l'installation peut être protégée en amont par des équipements spécialisés.

Veille et scan de vulnérabilité

Nous réalisons régulièrement des tests de vulnérabilité sur nos produits. Ces tests intrinsèques ne peuvent suffirent et donc, des tests au niveau de l'architecture doivent être effectués par le RSSI.

Contrôle et Test

La sécurité fonctionnelle constitue la capacité d'un système à maintenir son fonctionnement, alerter en cas de dysfonctionnement mineur et rétablir son fonctionnement de manière autonome en cas de dysfonctionnement majeur.

Contrôle d'intégrité des fichiers

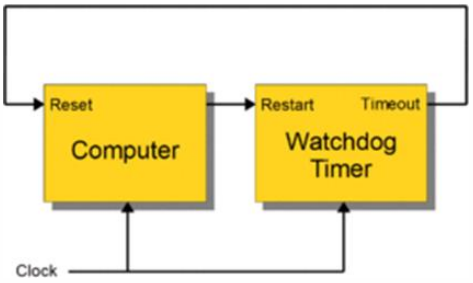
Avant d'être importé, tout fichier est soumis à un contrôle d'intégrité par l'ULI WIT pour vérifier que ce fichier n'altère pas son fonctionnement.
Les principaux fichiers concernés par ce contrôle d'intégrité sont :

- Logiciel : OS (Operating System), applicative UC, logiciels PLUG.
- Paramétrage : Total ou partiel.

Par ailleurs, un contrôle de compatibilité est réalisé entre l'OS et l'applicatif lors des mises-à-jour.
Le fichier de paramétrage ne contient aucun script d'exécution externe type Injection SQL ou JavaScript.

Watchdog

Un Watchdog (chien de garde) est une fonction qui assure le rétablissement de l'ULI WIT lorsque celle-ci dépasse un temps de réponse système anormalement long. Cette situation peut se présenter par exemple, lorsque l'écriture d'un Script crée une boucle permanente :



Etat de repli

Lorsque la communication entre l'Unité Centrale et les entrées/sorties de l'ULI est interrompue (bus sectionné, perte d'alimentation ou redémarrage de l'UC), un état de repli peut être configuré pour chaque sortie (T.O.R. et Analogique).
Cette fonction permet de définir l'état de fonctionnement dégradé (état de repli) des équipements dans ces situations. Exemples : allumage des éclairages, ouverture ou fermeture des accès, …etc.

Nous vous conseillons, afin d'assurer un minimum de continuité de service de :

- Paramétrer les valeurs de repli cohérentes sur les sorties (DO et AO). Cette action est réalisable dès le niveau 3 Installateur.
- Forcer les sorties (DO et AO) le nécessitant en fonction de la criticité de la situation. Cette action est réalisable dès le niveau 2 Exploitant.

Alimentation secourue

L'alimentation secourue permet le maintien temporaire du fonctionnement de l'ULI en cas d'interruption de l'alimentation principale. Les ULI WIT dispose de leur propre système de recharge et de surveillance d'état de leur alimentation de secours (batterie), ceci contribuant à l'optimisation budgétaire de l'installation, à minimiser l'encombrement des armoires électriques ainsi qu'à améliorer la maintenance préventive et corrective. Par le paramétrage il est possible de générer des alertes en cas de coupure secteur.

Nous vous conseillons de :

- Installer des batteries de secours sur les embases demandant un secours en cas de coupure secteur, elles doivent être calibrée de manière proportionnelle à la charge et à la durée de secours calculée, action à réaliser par l'installateur.
- Programmer des alertes sur défaut batterie ou secteur afin d'alerter l'exploitant, action à réaliser par l'installateur.

Diffusion d'alertes

En cas de dysfonctionnement de l'installation et/ou de son environnement technique, il est primordial d'être alerté en temps réel pour agir de manière réactive. Les ULI WIT disposent de plusieurs moyens de communication des alertes :

- SMS
- Email
- SIA sur IP (télésurveilleurs)
- PC de supervision, local ou distant.
- EMI-UCP
- ESPA 4.4.4
- Imprimante fil de l'eau (type EPSON LX 300+)
- Via Script (Flux RSS 1)

La diffusion d'alertes peut être personnalisée selon un planning d'astreinte propre à chaque utilisateur.

Nous vous conseillons de :

- Paramétrer un planning d'astreinte pour chaque utilisateur le nécessitant.
- Choisir le canal de diffusion le plus approprié, par exemple, pour une alarme intrusion ou feu, ne pas choir l'alarme de type mail.

Actions à réaliser par le niveau 4 Administrateur.

Maintenance et mise en service

Préambule

Son objectif est de définir une politique cohérente entre les besoins techniques et la réalité terrain afin de maîtriser l'ensemble des risques.
La connexion à distance sur les équipements et ordinateurs distants est obligatoire en cas de dépannage ou de mise en service à distance.

Les types de connexions

Les connexions à distance sur les machines :

- Réseau VPN.
- Bureau à distance.
- TeamViewer/Teams/Skype.

Les connexions à distance sur les ULI :

- Réseau VPN (par l'infrastructure ou OpenVPN intégré en client ou serveur).
- Réseau public (ADSL ou GSM).

Les bonnes pratiques

Charte informatique Client-Fournisseur :

- Une procédure d'accès à distance doit être validée entre le fournisseur et le client
- Le fournisseur sollicite l'autorisation du client avant tout accès à distance.
- L'accès à distance ne doit être mis en place que temporairement.
- Le fournisseur sensibilisera le client des risques potentiels sur l'installation en cas de cyber malveillance.

Pour sécuriser toute connexion entrante, le client doit :

- Privilégier les connexions VPN.
- Filtrer par adresse IP toute connexion entrante.
- Tracer les connexions dans l'ULI.
- Fermer les ports non utilisés dans l'ULI.

Protection des flux de données

Chiffrement (Encryptage)

Le chiffrement est le bloc de construction de base de la sécurité des données et le moyen le plus simple et le plus important pour s'assurer que les informations de l'ULI ne puissent pas être volées et lues par quelqu'un qui souhaite les utiliser à des fins malveillantes.
Le chiffrement (ou encryptage) est la conversion des données d'un format lisible à un format codé qui peut uniquement être lu ou traité après déchiffrement.
Les principes du chiffrement se basent sur la notion d'algorithmes de chiffrement et de « clés ». Lorsque l'information est envoyée, elle est chiffrée à l'aide d'un algorithme et peut être décodée uniquement à l'aide de la clé appropriée.
Les ULI disposent de fonction de chiffrement pour les trois principales communications :

HTTPS	Hyper Text Transfert Protocole Secure Protocole employé pour accéder au serveur web de l'ULI et à son API ainsi que dans les communications inter-ULI (eShare) et l'accès aux applications RIA.
FTPS	File Transfert Protocole Secure Protocole employé dans le transfert de fichier avec l'ULI
SMTPS	Simple Mail Transfert Protocole Secure Protocole employé dans la diffusion d'email de l'ULI.

La version de TLS (Transport Layer Security) utilisée est en version 1.2.

Authenticité & Certificats

L'utilisation de certificats TLS/ SSL exige la mise en place d'une chaîne de certification au sein des postes accédant à l'équipement. Cette chaine de certification peut être crée :

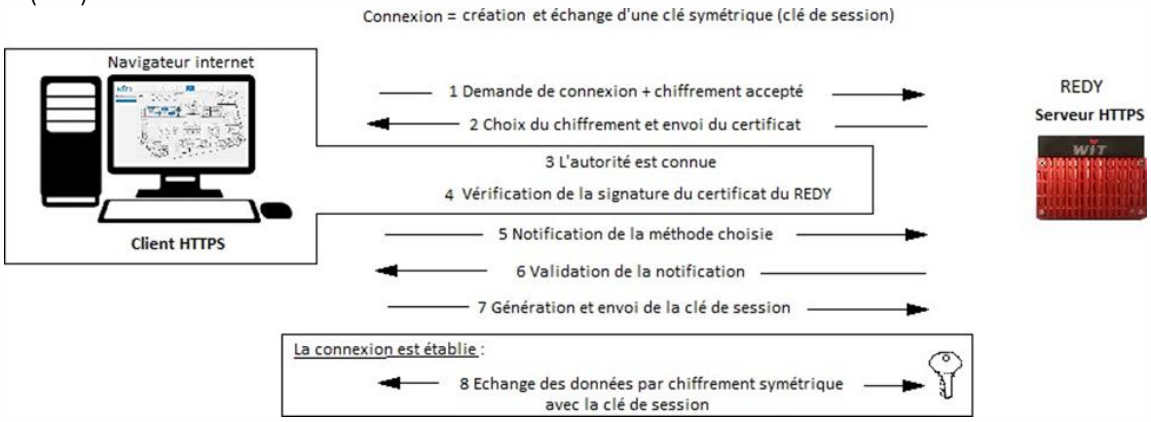
- A partir d'un certificat émit par une autorité de certification reconnue, importé et utilisé dans nos équipements REDY.
- Par la création manuelle d'un certificat et l'import du certificat racine sur tous les postes accédant à l'équipement.

Ce certificat peut être importé ou généré par nos équipements REDY.
Il a une durée d'1 an, après quoi il est nécessaire de le renouveler.
Dans le cas d'un import de certificat, le Domain Name (DN) doit être utilisé pour accéder à l'équipement, qui nécessite l'enregistrement DNS de ce nom sur le Serveur DNS opérant sur le réseau.
L'utilisation de certificats auto-générés par nos équipements doit s'accompagner d'une campagne de déploiement de ce certificat sur les postes de travail, afin de garantir l'authenticité des connexions sécurisées.

Pour plus d'informations sur les connexions sécurisés, se référer à la documentation **Manuel Communications sécurisées** sur www.wit.fr.

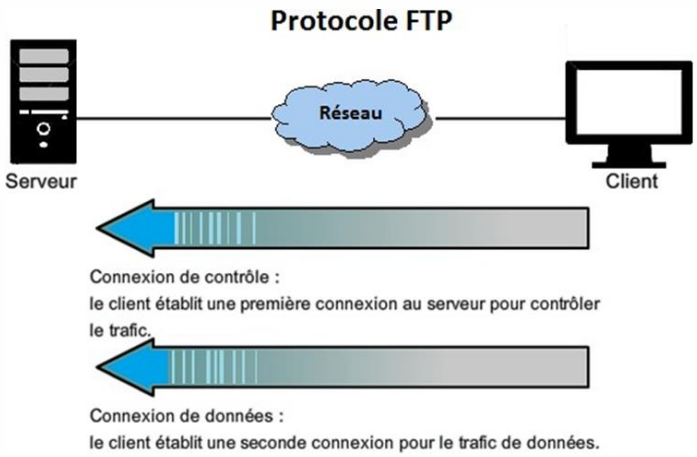
HTTPS

HTTPS permet de sécuriser la connexion et les échanges HTTP grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable. Il garantit la confidentialité et l'intégrité des données envoyées par l'utilisateur (notamment des informations entrées dans les formulaires) et reçues du serveur (ULI) :



FTPS

Le File Transfer Protocol Secure, abrégé FTPS est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP, variante du FTP, sécurisé avec les protocoles SSL ou TLS. Il permet au visiteur de vérifier l'identité du serveur auquel il accède grâce à un certificat d'authentification. Il permet également de chiffrer la communication :



Deux méthodes existent pour invoquer le chiffrement SSL/TLS en FTP : « explicite » ou « implicite ». Les ULI WIT utilisent le mode « implicite ».

Implicite : L'échange est crypté dès que la liaison client / serveur est établie.

Explicite : La connexion se fait en clair et l'échange des données est crypté après l'authentification.

SMTPS

Le Simple Mail Transfer Protocol Secure (SMTPS) est une méthode permettant de sécuriser le protocole SMTP (envoi d'emails) avec la sécurité de la couche de transport. Il est destiné à assurer l'authentification des partenaires de communication ainsi que l'intégrité et la confidentialité des données.
Deux méthodes existent pour invoquer le chiffrement SSL/TLS en SMTP : « explicite » ou « implicite ».
Les ULI WIT peuvent utiliser les deux modes.

Implicite : L'échange est crypté dès que la liaison client / serveur est établie.
Explicite : La connexion se fait en clair et l'échange des données est crypté après l'authentification.

Nous vous conseillons de vous assurer :

- D'activer impérativement le HTTPS pour des accès externes. D'activer le HTTP uniquement sur une configuration sécurisée et maitrisée (Réseau Privé entre un PC et un Système Industriel).
- D'installer et d'activer uniquement les protocoles et services nécessaires.
- Dans le cas d'activation de protocoles ou de services supplémentaires de changer la configuration par défaut notamment au niveau des ports d'accès.
- Idéalement, donner accès au système uniquement et de manière ponctuelle à l'administrateur et dans les autres cas à des utilisateurs sans privilèges et sans accès aux paramètres critiques.
- Que les protocoles et services vulnérables et non sécurisés ne sont pas activés (ex : Telnet)
- Que si des services ou des protocoles non sécurisés sont actifs de les répertorier pour mettre en place les mesures.

Maitrise des flux de données

Il y a de nombreuses manières de se connecter sur une ULI, notamment par : Ethernet (LAN), WIFI, USB, GSM (3G/4G).
Afin de maitriser les flux de données, chaque réseau est cloisonné. Un signal entrant par un réseau ne pourra pas atteindre un autre réseau.
Exemple : un signal entrant par le réseau 4G ne pourra pas être routé vers le réseau Ethernet (LAN).

Pare-feu

Les Unités Locales Intelligentes (ULI) WIT sont dotées d'un pare-feu natif. Ce pare-feu bloque automatiquement toutes les connexions sur les ports IP non-autorisés (programmé par l'installateur).
Les connexions considérés comme critiques telles que FTP-SSDP-WOP sont fermées par défaut.
Les connexions Telnet ou SSH-SFTP sont aussi fermées par défaut et peuvent être activées de manière ponctuelle (non sauvegardé dans le paramétrage).

Accès physiques

La sécurisation des accès physiques à l'Unité Locale Intelligente (ULI) est à prendre en considération dans la sécurité globale de l'installation.
Cette sécurisation peut être réalisée par des moyens traditionnels (porte à clé) ou par des moyens plus modernes : contrôle d'accès avec identification des personnes (lecteur de badges + ventouse/gâche électrique ou serrure sans-fil). Cette seconde solution offre également l'avantage de pouvoir suivre les accès aux locaux techniques.
La détection d'intrusion aux locaux techniques est un moyen efficace de parfaire la sécurité des accès physiques en alertant de manière instantanée tout accès non-autorisé. Pour ce faire, l'ULI WIT dispose d'entrées pouvant accueillir des capteurs à boucle équilibrée.

Nous vous conseillons de vous assurer :

- Que l'accès aux bus terrains est sécurisé en vérifiant que les accès à ce bus ne soient, par exemple, pas accessibles en dehors du bâtiment (câbles externes non isolés, …).
- De vérifier l'installation au niveau des câblages internes et externes.
- De mettre en œuvre la détection de sabotages tels que :
  - La mise en court-circuit du capteur (boucle fermée).
  - La section du câble (boucle ouverte).
  - L'ouverture ou la détérioration du capteur (boucle équilibrée).
- De vérifier pour les sites sensibles, de sécuriser l'accès aux équipements en libérant l'accès à distance uniquement sur une plage horaire définie par l'Administrateur Système.
- Mettre en place une détection d'ouverture de l'armoire par contact sec.

Media amovibles

L'OS de l'ULI REDY permet une discrimination active des périphériques USB non connus du système.
La sélection est effectuée avec les ID Vendor/Product de chaque device USB.
Il est recommandé d'utiliser des médias amovibles (clefs USB, disques durs externes, etc.) dédiés au site d'utilisation.

Nous vous conseillons de vous assurer :

- Que les périphériques connectés sont bien exploités dans l'ULI.
- De désactiver l'alimentation des ports USB dans le cas où ils ne seraient pas utilisés (fonctionnement par défaut).

Pour tout renseignement complémentaire, notre support technique se tient à votre disposition par e-mail à hot-line@wit.fr ou par téléphone au +33 (0)4 93 19 37 30