



USINE SA

Chantier Usine

Version 1.0

Speedlink SA

1. Table des matières

2.	SUIVI DES RÉVISIONS.....	2
3.	CONTEXTE.....	2
4.	DESCRIPTIFS FONCTIONNELS.....	4
a)	PBX	4
b)	Call Flow	4
c)	Intégration de logiciels sur PC	4
d)	Postes fixes pour secrétaire/s	4
e)	Téléphonie Mobile DECT	4
f)	SIP-to-SIP Trunk.....	4
a)	Ligne 10 Gbit/s symétrique.....	5
b)	IP fixes.....	5
a)	Réseaux virtuels	5
b)	Réseaux Wi-Fi.....	5
1.	Wi-Fi Corporate	5
2.	Wi-Fi Guest.....	5
c)	RSTP (Rapid Spanning Tree Protocol).....	6
a)	IAM.....	6
b)	SMB pour partage de fichiers.....	6
c)	Gestion du parc informatique.....	6
d)	Systèmes de sauvegardes	7
e)	Salle de conférence	7
5.	EXIGENCES TECHNIQUES	8
a)	PROTECTION DES DONNÉES	8
1.	Politique pour employés.....	8
b)	SÉCURITÉ DES SYSTÈMES.....	8
1.	Sécurité physique	8
2.	Vlans :	8
3.	Chiffrement des appareils	9
4.	UTM :	9
5.	Liaison VPN client-to-site SSL	9
a)	Redondance électrique.....	10
1.	Systèmes avec criticité faible	10

IT - TÉLÉPHONIE - PLANIFICATION

Chemin de la Digestion 2 -

CP 12656 - 1259 Carotte 2/17 TVA N° CHE - 107.990.227 TVA

Tél/Fax : 022 400 44 44/24 E-mail : info@speedlink.ch

2.	Systèmes avec criticité modérée	11
3.	Systèmes avec criticité élevée	11
b)	Redondance des données	12
1.	Méthode d'organisation et sauvegarde des données	12
2.	Redondance du pare-feu	12
3.	Redondance des switches	12
a)	Câblage.....	12
b)	Wi-Fi	12
c)	DECT.....	12
a)	Volumes de stockage serveurs	13
b)	Capacité des switches.....	13
c)	Capacité du gestionnaire d'accès	13
a)	Audits.....	13
6.	CONTRAINTES ET LIMITATIONS.....	13
7.	CRITÈRES D'ÉVALUATION ET DE VALIDATION	14
8.	LIVRAISONS ATTENDUES (Speedlink SA).....	15
9.	SUIVI POST-IMPLÉMENTATION.....	15
10.	CONDITIONS CONTRACTUELLES.....	16

2. SUIVI DES RÉVISIONS

Version du document	Éditeur	Approbation par
1.0	Arthur LE GUENNEC	Speedlink SA

3. CONTEXTE

Projet Usine SA

Comme convenu à la suite de la rédaction et validation du cahier des charges, Speedlink SA fournit le descriptif de projet détaillé nécessaire à la planification et à l'exécution complète du projet conformément aux phases de planification et d'exécution des SIA.

L'installation ci-jointe concerne les espaces techniques de manufacture du rez-de-chaussée et les environnements de bureau du 1^{er} étage.

Description générale du projet :

- Localisation : Genève Carouge
- Dimension : Deux étages, espaces techniques et environnements de bureau, parking privé
- Capacité : Environ 80 employés au rez-de-chaussée et 20 employés au premier étage.
- Fonctionnalités principales : Productivité, administration, manufacture...

Parties prenantes :

- Maître d'ouvrage et client : M. Marrocco
- Bureau d'architectes : Trigo21 SA
- Entreprise Générale d'électricité : STO SA
- Bureau d'ingénieurs conseils et entreprise IT & Telecom : Speedlink SA
- Groupe de déploiement de réseau fibre optique : CabeulComme SA
- Vidéo surveillance : Aquecisse Yooo SARL

IT - TÉLÉPHONIE - PLANIFICATION

Chemin de la Digestion 2 -

CP 12656 - 1259 Carotte 2/17 TVA N° CHE - 107.990.227 TVA

Tél/Fax : 022 400 44 44/24 E-mail : info@speedlink.ch

4. DESCRIPTIFS FONCTIONNELS

Téléphonie : Planification et installation d'un réseau téléphonique complet et opérationnel pour chaque collaborateur souhaité. Installation du PBX ainsi que des différentes interfaces de communication (softphones, postes IP fixes, réseau DECT...) et des différentes fonctionnalités.

a) PBX

L'installation et la configuration d'un PBX 3CX virtualisé dans l'hyperviseur ESXi du Dell PowerEdge R650.

b) Call Flow

Le call flow sera effectuée à la demande du client et des collaborateurs afin d'adopter une stratégie de réception et d'émission d'appels fonctionnelle, adéquate et efficace.

Les rôles de chaque collaborateur seront à établir dans un futur rendez-vous avec le maître d'ouvrage.

c) Intégration de logiciels sur PC

Installation des clients 3CX logiciels sur les postes des utilisateurs finaux.

d) Postes fixes pour secrétaire/s

Installation et configuration des postes Yealink T57W pour les secrétaires, avec des touches BLF préprogrammées et raccourcis souhaités

e) Téléphonie Mobile DECT

Pour simplifier les déplacements au RDC dans les espaces techniques pour les ouvriers, de la téléphonie mobile DECT sera à disposition pour chaque poste de travail.

2 antennes seront installées au plafond.

f) SIP-to-SIP Trunk

Pour permettre aux collaborateurs clients de téléphoner à des numéros externes fixes et mobiles en Suisse, une liaison SIP-to-SIP trunk Swisscom est prévue à cette effet.

Ce trunk disposera de 4 canaux.

Un SBC sera installé et configuré sur place sur le site du client.



Ouverture de ligne : Ouverture de ligne Swisscom Gigabit réalisée par nos soins.

a) Ligne 10 Gbit/s symétrique

Offre SBC Internet L incluant une connexion Internet haut-débit permettant à l'entreprise de bénéficier d'une connectivité à toute épreuve.

b) IP fixes

Pour que certains services puissent fonctionner, notamment le VPN, il est nécessaire de louer des IP fixes à l'ISP.

Ici. Un bloc de 4 IP fixes sera loué par mois pour un maximum de flexibilité.

Networking : Planification et installation des équipements réseaux permettant une connexion Internet filaire et sans-fil optimale pour les collaborateurs (CUC RJ45 et Wi-Fi).

a) Réseaux virtuels

Différents réseaux seront créés pour segmenter le réseau, le protéger, limiter le domaine de broadcasting, et gérer la QoS améliorant en conséquence sa performance.

Voir la sécurité des systèmes dans le chapitre des exigences techniques.

b) Réseaux Wi-Fi

La diffusion des réseaux Wi-Fi seront diffusés par des Unifi AC Pro 7.

Pour permettre une connectivité sans-fil pour les utilisateurs, 2 réseaux Wi-Fi seront mis en place :

1. Wi-Fi Corporate

Ce réseau Wi-Fi ne diffusera pas son SSID, afin que seules les personnes connaissant son existence puissent s'y connecter.

Réseau Wi-fi basé sur le VLAN 50 VDATA.

Les utilisateurs pourront accéder aux ressources d'entreprise via ce SSID.

2. Wi-Fi Guest

Pour répondre aux critères de sécurité de la norme ISO27001 section A13.1.1 et A13.1.3, il est nécessaire de séparer le réseau professionnel du réseau invité.

D'autres mesures, telles que la désactivation de l'intra-BSS, du DHCP guarding, et l'inspection active du réseau seront mises en œuvre.

Réseau Wi-Fi basé sur le VLAN 5000 VPUBLIC

Ce réseau sera soumis aux mêmes restrictions d'accès à Internet BPP (Business Productivity Protection), limitant les sites distractifs, pornographiques et illégaux.

c) RSTP (Rapid Spanning Tree Protocol)

Utilisé pour empêcher les boucles dans le réseau, le RSTP sera donc nécessaire dans notre infrastructure redondante.

Administration système : Planification et installation de systèmes de gestion des privilèges utilisateurs hybrides (lié aux systèmes d'accès physiques), serveur SMB pour partage de fichiers (collaboration), gestion du parc informatique, centralisateur de logs SIEM, et systèmes de sauvegardes temporelles et décentralisées.

a) IAM

La gestion des utilisateurs est primordiale au sein d'une entreprise, d'autant plus si l'accès aux locaux est intégré à cette gestion.

Un serveur Active Directory sera donc installé et configuré pour créer les groupes et utilisateurs nécessaires. Il sera synchronisé sur un tenant Microsoft de l'entreprise Usines SA pour une gestion hybride des accès aux ressources de l'entreprise.

b) SMB pour partage de fichiers

Le partage de fichiers sera géré par une machine virtuelle Windows Server 2022 ayant la fonctionnalité de partage de fichiers SMB.

Les permissions seront gérées par le même serveur et seront créées en fonction des besoins explicites du client.

c) Gestion du parc informatique

Grâce au contrat d'entretien et support premium business de Speedlink SA, Usines SA bénéficiera d'une gestion complète de leur parc informatique.

Cela inclut donc la gestion de la veille informatique, la gestion des vulnérabilités, et la surveillance des appareils.

d) Systèmes de sauvegardes

Afin de sauvegarder le serveur SMB, la VM Windows Server 2022 et la VM Ubuntu 3CX (ainsi que ses fichiers de configuration), nous utiliserons la fonctionnalité Active Backup de Synology.

La stratégie de sauvegarde est détaillé dans la section

Multimédia : Planification et installation de systèmes multimédia pour visio-conférence et réunions de groupes interactives.

e) Salle de conférence

La salle de conférence est conçue de manière à permettre une collaboration interactive au sein même de la pièce, mais aussi en ligne grâce à des services de communications dédiés à cela (voir software).

Un écran tactile intelligent Samsung Flip 2 WM65R sera installé dans la pièce, accompagné d'une webcam haute qualité et d'un téléphone confidentiel...

Une documentation sera également disponible pour les utilisateurs finaux.

5. EXIGENCES TECHNIQUES

Sécurité : Les solutions proposées par Speedlink SA doivent garantir la sécurité des données sensibles de l'entreprise, en incluant des mesures de protection avancées telles que la cryptographie, l'authentification multi-facteurs, du PAM ainsi que la confidentialité des données des collaborateurs / clients.

a) PROTECTION DES DONNÉES

Parler des certification, normes suisses etc etc... notions juridiques

1. Politique pour employés

Lors de la signature du contrat avec un nouveau collaborateur, faire signer à ce dernier une politique d'accès aux ressources informatiques d'entreprises et une politique d'utilisation de leurs outils informatiques (Poste fixe appartenant à l'entreprise, ou ordinateur portable BYOD...)

b) SÉCURITÉ DES SYSTÈMES

1. Sécurité physique

Sécurité des racks (fermés à clé, avec seul le personnel compétent y ayant accès).

2. Vlans :

- VDATA : ID-50, pour les ordinateurs des collaborateurs ainsi que les ressources partagées (fichiers, applications d'entreprise, imprimantes...). AVEC accès INTERNET
- VVOIP : ID-60, pour la téléphonie IP / DECT (incluant le PBX). AVEC accès INTERNET pour les appels EXTERNES.
- VCCTV : ID-70, pour le système de vidéo-surveillance (caméras IP + NVR). SANS accès INTERNET.
- VPUBLIC : ID-5000, pour les utilisateurs invités dans les locaux, n'ayant besoin que d'un accès à Internet. Pas d'accès accordés aux ressources et aucun communication inter-appareils. Connexion à la PASSERELLE SEULE (faisant aussi office de DNS). Réseau loggé.
- VMONITOR_1 : ID-999, pour la maintenance des serveurs sur des NIC hors ligne (PowerEdge et NAS Synology)
- VMONITOR_2 :

IT - TÉLÉPHONIE - PLANIFICATION

Chemin de la Digestion 2 -

CP 12656 - 1259 Carotte 2/17 TVA N° CHE - 107.990.227 TVA

Tél/Fax : 022 400 44 44/24 E-mail : info@speedlink.ch

3. Chiffrement des appareils

Pour limiter l'accès non autorisé aux données des employés, chaque poste fixe / mobile sera chiffré avec BitLocker.

Le stockage des clés BitLocker sera centralisé dans Entra ID.

4. UTM :

Les fonctionnalités UTM sont intégrées au pare-feu Fortigate 200F.

- Pare-feu applicatif : Accès restrictif à Internet, avec blocage des réseaux sociaux (Meta, Twitter...) et P2P
- URL et DNS threat filters : Blocage d'URLs et de requêtes DNS potentiellement dangereuses / illégales, ou ne favorisant pas la productivité (casino en ligne, sites pornographiques...)
- IPS / IDS : Inclus dans le pare-feu, la

5. Liaison VPN client-to-site SSL

Pour permettre aux employés de se connecter au réseau d'entreprise en dehors des locaux, une liaison VPN SSL est prévue à cet effet.

Les utilisateurs s'authentifieront à travers Entra ID SAML pour simplifier et centraliser la mémorisation des identifiants professionnels.

QoS : La QoS est importante autant dans le domaine de la téléphonie que dans un réseau IP classique d'entreprise. Cela permet de limiter la congestion du réseau et de prioriser des paquets selon son origine.

VLAN Data (VDATA)

- Priorité élevée (QoS 5)
- Trafic critique pour la productivité des employés
- Applications d'entreprise, partage de fichiers, etc.

VLAN VoIP (VVOIP)

- Priorité la plus élevée (QoS 7)
- Trafic voix en temps réel, très sensible aux délais
- Téléphonie IP, vidéoconférence

VLAN Public (VPUBLIC)

- Priorité basse (QoS 1)
- Trafic best-effort pour les invités
- Navigation web, courriels

VLAN Monitoring (VMONITOR_1, VMONITOR_2)

- Priorité moyenne à élevée (QoS 4)
- Trafic de gestion et de supervision des équipements réseau
- Accès à l'interface d'administration des équipements

Redondance et Disponibilité : L'infrastructure réseau doit être conçue pour assurer une redondance efficace et une disponibilité maximale des services, minimisant ainsi les temps d'arrêt et assurant une continuité opérationnelle.

a) Redondance électrique

Afin d'assurer l'alimentation en continu des différents systèmes, une redondance électrique est prévue par niveau de criticité.

Voir les niveaux ci-dessous :

1. Systèmes avec criticité faible

Les systèmes informatiques à criticité faible ne disposeront pas de redondance électrique.

Ces systèmes comprennent :

- Ordinateurs fixes
- Postes téléphoniques
- Antennes Wi-Fi
- Antennes DECT

IT - TÉLÉPHONIE - PLANIFICATION

Chemin de la Digestion 2 -

CP 12656 - 1259 Carotte 2/17 TVA N° CHE - 107.990.227 TVA

Tél/Fax : 022 400 44 44/24 E-mail : info@speedlink.ch

- Switchs

2. Systèmes avec criticité modérée

Les systèmes informatiques à criticité modérée disposeront d'une redondance électrique temporaire limitée, permettant une extinction sécurisée de ces derniers.

Ces systèmes comprennent :

- Serveur Dell PowerEdge R650
- 2x NAS Synology RackStation® RS1619xs+

3. Systèmes avec criticité élevée

Les systèmes informatiques à criticité élevée disposeront d'une redondance électrique étendue, permettant la continuité de leur fonctionnement lors d'une coupure électrique.

Ces systèmes comprennent :

- Gestionnaire d'accès physique Unifi Enterprise Access Hub (système à part)
- NVR + caméras IP

b) Redondance des données

1. Méthode d'organisation et sauvegarde des données

L'organisation des données dans les disques se fera selon le système RAID10.

Des backups quotidiennes des dossiers en partage, de la VM Windows Server 2022 et de la VM Ubuntu 3CX, seront effectuées sur le NAS avec Active Backup.

Les fichiers de configuration du PBX virtuel 3CX seront aussi sauvegardés hebdomadairement.

Le RTO sera donc minimal.

Des backups hebdomadaires hors ligne seront effectuées sur un autre NAS hors-ligne avec Snapshot Replication.

2. Redondance du pare-feu

Le pare-feu Fortigate 200F (FW-FG1) est répliqué en permanence vers un autre Fortigate 200F (FW-FG2). Les liens optiques vers le SWR-1183 et le SW2-1183 étant déjà établis, il suffira donc seulement d'une intervention d'un technicien pour connecter le FW-FG2 sur la prise OTO si le FW-FG1 tombe.

3. Redondance des switches

La configuration des switches n'étant pas complexe et ne changeant pas, le fichier de configuration initiale après la remise du projet sera sauvegardé pour chaque switch.

Évolutivité : Les équipements et les solutions déployés doivent être évolutifs pour s'adapter aux besoins futurs de l'entreprise, permettant une expansion aisée sans compromettre la performance du système.

a) Câblage

La disposition des boîtes de sol est pensée de façon à favoriser la modification des plans de bureaux et ainsi l'évolutivité de ces derniers.

b) Wi-Fi

Étant donné que les Unifi AC Pro 7 sont les derniers APs de la marque Ubiquiti sur le marché, la capacité de charge ainsi que les technologies incluses seront supportées sur le long terme.

c) DECT

Comme pour le Wi-Fi, le réseau DECT mis en place sur site inclue les dernières technologies disponibles sur le marché, assurant donc un support long-terme et l'intégration de nouvelles technologies et appareils si besoin.

IT - TÉLÉPHONIE - PLANIFICATION

Chemin de la Digestion 2 -

CP 12656 - 1259 Carotte 2/17 TVA N° CHE - 107.990.227 TVA

Tél/Fax : 022 400 44 44/24 E-mail : info@speedlink.ch

Gestion de la Capacité : Une gestion proactive de la capacité des équipements réseau et des systèmes informatiques doit être mise en place pour anticiper les besoins croissants en termes de bande passante et de stockage (volume).

a) Volumes de stockage serveurs

Afin de préserver une marge de manœuvre et éviter une saturation des disques de stockage, le serveur possédant 8 bays HDD SATA 3,5 pouces, il hébergera 8 disques de 12TB chacun.

Des archivages hors-ligne sur bandes LTO sont proposées dans notre contrat de maintenance Business Platinum.

Vous pouvez en demander max. 2 par an.

b) Capacité des switches

L'anticipation est la clé d'une évolutivité informatique saine.

Étant le cœur du réseau, les switches garderont min. 30% de marge libre quant à leur capacité de ports garantissant l'«agrandissement» de l'infrastructure et une longévité accrue.

c) Capacité du gestionnaire d'accès

Le gestionnaire d'accès permet de gérer jusqu'à 8 portes.

Dans cette installation, seulement 5 seront utilisées, laissant donc une marge conséquente si le client souhaite installer de nouveaux accès physiques.

Conformité aux Normes : Toutes les solutions techniques mises en œuvre doivent être conformes aux normes et réglementations en vigueur dans le secteur, garantissant ainsi la conformité légale et la sécurité des opérations.

a) Audits

Afin de garantir la conformité des systèmes informatiques aux nouvelles recommandations et/ou exigences de sécurité, il est important, selon les certifications, de renouveler ces dernières à minima tous les 2 ans.

Cybersafe & ISO 27001 (performées par Speedlink)

6. CONTRAINTES ET LIMITATIONS

IT - TÉLÉPHONIE - PLANIFICATION

Chemin de la Digestion 2 -

CP 12656 - 1259 Carotte 2/17 TVA N° CHE - 107.990.227 TVA

Tél/Fax : 022 400 44 44/24 E-mail : info@speedlink.ch



Speedlink

- **Budget** : Budget libre.
- **Délais** : Le chantier doit être achevée pour début 2026.

Contraintes et spécifications émises par Speedlink SA :

- Le câblage informatique sera effectué par l'entreprise STO SA. Il devra être de catégorie 6A minimum, testé et certifié au préalable avant toute intervention de notre part.
- Les fournitures informatiques de travail telles que les claviers, souris, sont comprises dans le coût des ordinateurs.

7. CRITÈRES D'ÉVALUATION ET DE VALIDATION

- **Conformité aux exigences** : Les solutions doivent répondre précisément aux besoins spécifiés par le client.
- **Disponibilité et sécurité** : Les systèmes installés doivent garantir la sécurité des données, ainsi que leur disponibilité.
- **Productivité** : Les solutions doivent contribuer à augmenter la productivité des collaborateurs au sein des bureaux ainsi que dans les espaces techniques.
- **Redondance électrique** : Les solutions doivent garantir la redondance électrique des appareils mis en réseau afin de pouvoir procéder à une extinction normale de ces derniers.
- **Redondance des données** : Les solutions doivent garantir la redondance des systèmes en cas de panne, incluant donc un RTO minimal ainsi qu'un RPO optimal pour une perte de données minimal.

8. LIVRAISONS ATTENDUES (Speedlink SA)

- Plans techniques et architecturaux comprenant les solutions de Speedlink SA
- Mise en place des appareils de networking dans les étages
- Ouverture de ligne sur le BEP Swisscom au RDC (local technique).
- Mise en place, configuration des serveurs et configuration de la gouvernance des identités
- Installation des end-devices et provisioning.
- Installation et configuration de la vidéo-surveillance et gestion d'accès physique.
- Rédaction du document pour l'OCIRT.
- Effectuation des premiers tests par Speedlink SA
- Effectuation des tests avec les collaborateurs d'Usine SA
- Formation des collaborateurs
- Livraison de la documentation des différents systèmes et services
- Contrat de maintenance ainsi que contrat d'infrastructure managée totale (SOC, inventaires, veille technologique EOL, support user, dépannage rapide prioritaire... voir conditions lors de la signature du contrat)

9. SUIVI POST-IMPLÉMENTATION

Après la mise en œuvre du projet, il est essentiel de mettre en place un suivi post-implémentation pour :

- **Évaluation des Performances** : Mesurer l'efficacité des solutions mises en place, recueillir les retours d'expérience des utilisateurs et identifier les opportunités d'amélioration continue.
- **Maintenance et Support** : Définir les procédures de maintenance préventive, les niveaux de support disponibles et les modalités de résolution des problèmes techniques pour assurer le bon fonctionnement des systèmes déployés.
- **Formation Continue** : Organiser des sessions de formation pour le personnel afin de garantir une utilisation optimale des nouvelles technologies et systèmes mis en place.
- **Évaluation de la Satisfaction Client** : Collecter les retours clients pour évaluer leur satisfaction par rapport aux solutions déployées et identifier d'éventuels besoins supplémentaires ou ajustements.

IT - TÉLÉPHONIE - PLANIFICATION

Chemin de la Digestion 2 -

CP 12656 - 1259 Carotte 2/17 TVA N° CHE - 107.990.227 TVA

Tél/Fax : 022 400 44 44/24 E-mail : info@speedlink.ch

10. CONDITIONS CONTRACTUELLES

Il est expressément stipulé que ce document est considéré comme la propriété intellectuelle exclusive de Speedlink SA. Son accès et sa diffusion sont strictement limités au maître d'ouvrage et aux parties prenantes du projet. Toute reproduction, divulgation ou utilisation non autorisée est formellement interdite.

Dans l'éventualité où Speedlink SA subirait un préjudice résultant de la violation des termes de ce document par une partie tierce, des indemnisations appropriées et toutes mesures nécessaires seront prises pour protéger les droits et intérêts de Speedlink SA, conformément aux lois en vigueur.

11. CONTRAT DE MAINTENANCE

Speedlink SA propose différents niveaux de support et de maintenance à long terme pour les entreprises.

IT - TÉLÉPHONIE - PLANIFICATION

Chemin de la Digestion 2 -

CP 12656 - 1259 Carotte 2/17 TVA N° CHE - 107.990.227 TVA

Tél/Fax : 022 400 44 44/24 E-mail : info@speedlink.ch



Speedlink