SERVICE CORRECTIONNEL DU CANADA
DIRECTION DES INSTALLATIONS
SYSTÈMES DE SÉCURITÉ ÉLECTRONIQUES

22 octobre 2014

EXIGENCES DE CONCEPTION

DE LA PLATEFORME DE COMMANDE ET DE CONTRÔLE, INCLUANT UN ENVIRONNEMENT DE DÉVELOPPEMENT D'APPLICATIONS ET DE PRESTATION DE SERVICES

Table des matières

Liste des sigles et acronymes

Les sigles et acronymes suivants figurent dans la présente spécification :

Sigle/acronyme	Signification
IPV	Interface de programmation d'applications
PEA	Procédure d'essai d'acceptation
BIFMA	Business & Industrial Furniture Manufacturers Association
CCAD	Communications, commande et acquisition de données
TCF	Télévision en circuit fermé
SIGE	Systèmes informatisés de gestion de l'entretien
DC	Directive du commissaire
SEC	Salle d'équipement commun
PIE	Protection des infrastructures essentielles
Logiciel	Commercial sur étagère
UCT	Unité centrale de traitement
ASC	Association canadienne de normalisation
SCC	Service correctionnel du Canada
CSV	Valeurs séparées par des virgules (format)
SCSP	Système de commande et de surveillance des portes
DSI	Directeur, Services d'ingénierie
EIA	Electronic Industries Association
GBE	Gestion des biens d'entreprise
SIAE	Système d'indication des alarmes de l'établissement
TFA	Taux de fausses alarmes
SDDC	Système de détection de dérangement des clôtures
UIS	Unité d'interface du SIAE
EFG	Équipement fourni par le gouvernement
IUG	Interface utilisateur graphique
IHM	Interface homme-machine
EDI	Environnement de développement intégré
IP	Protocole Internet
E/S	Entrées/sorties
PPCC	Poste principal de contrôle des communications
MSDE	Microsoft Database Engine
SDM	Système de détection de mouvement
TAI	Taux d'alarmes intempestives
NTP	Protocole de synchronisation réseau
OLE	Protocole de liaison et d'incorporation d'objets
ONVIF	Open Network Video Interface Forum
OPC	Contrôle de processus avec le protocole OLE
PA	Public Address (système de sonorisation)
PD	Probabilité de détection
SPDI	Système périmétrique de détection des intrusions
UIS	Unité d'intégration du sous-système périmétrique de détection des intrusions
DP	Demande de propositions
AP	Automate programmable
DAPP	Dispositif d'alarme personnel portatif

SLDAPP	Système de localisation du dispositif d'alarme personnel portatif
GISP	Gestion de l'information sur la sécurité physique
PBD	Protocole Bureau à distance
REST	Architecture de structure représentationnelle (service Web)
IRF	Identification par radiofréquence
RC	Rythme du changement
TD	Terminal à distance
ARS	Agent du renseignement de sécurité
SOAP	Protocole d'accès simple aux objets
EDT	Énoncé des travaux
SQL	Langage d'interrogation structuré
EST	Énoncé des spécifications techniques
TCP/IP	Protocole de contrôle de transmission/protocole Internet
SET	Salle de l'équipement des télécommunications
ASC	Alimentation sans coupure
V et C	Visites et correspondance
SIEV	Système d'interception et d'enregistrement des visites
SGV	Système de gestion vidéo

Tableau des définitions

La présente spécification fait usage des définitions suivantes :

N°	Terme	Exemple	Description	Fonction
1	Interface utilisateur d'administration		Moniteur et logiciel procurant aux administrateurs de système l'interactivité nécessaire à certaines tâches, dans un emplacement sécurisé.	Permet au personnel administratif de mettre en correspondance les utilisateurs inscrits avec les domaines fonctionnels auxquels ils ont le droit d'accéder et d'apporter des modifications.
2	Demande	Gestion des appels à partir des cellules, gestion de la sonorisation	Logiciel servant à ajouter une fonction de soutien d'applications pour un sous-système.	Fournit l'interface opérateur et la logistique de soutien permettant de gérer un sous-système (domaine de contrôle).
3	Écran de télévision en circuit fermé (TCF)	Système périmétrique de détection des intrusions (SPDI) ou écran de TCF pour les rangées	Écran d'ordinateur	Montre les images de la TCF à l'opérateur.
4	Client		Ordinateur monté sur bâti dans un emplacement sécurisé, à distance d'un poste de contrôle ou d'un bureau de contrôle.	Exécute le logiciel et prend en charge une ou des applications.
5	Données de configuration	Plans d'étage de l'établissement présentant le nombre de caméras, de portes, de cellules, etc., ainsi que l'emplacement des caméras. Nombres d'interfaces utilisateurs requises dans un poste.	Renseignements portant sur un établissement ou sur un système, généralement fournis par le Service correctionnel du Canada (SCC). Ils indiquent comment une application de sous-système doit être installée dans un établissement, un emplacement ou un poste.	Fournit les renseignements dont l'application du sous-système a besoin pour adapter ce dernier aux exigences particulières d'un établissement, d'un emplacement ou d'un poste.
6	Interface utilisateur de configuration		Moniteur et logiciel procurant l'interactivité nécessaire à certaines tâches, dans un emplacement sécurisé.	Permet aux fournisseurs ou au personnel qualifié d'ajouter, de supprimer et de modifier la configuration d'une application.
7	Autorité contractante		Travaux publics et Services gouvernementaux Canada (TPSGC) est responsable de toutes les questions d'ordre contractuel liées à la conception et à la mise en œuvre des systèmes.	
8	Entrepreneur		Entreprise du soumissionnaire retenu	

N°	Terme	Exemple	Description	Fonction
9	Console de contrôle	Poste principal de contrôle des communications (PPCC), poste de contrôle des unités résidentielles	Console généralement placée dans un poste de contrôle. Infrastructure de soutien physique pour les interfaces utilisateurs des opérateurs.	Réunit les interfaces utilisateurs ou les panneaux de commande utilisés par les membres du personnel pour s'acquitter de leurs responsabilités de gestion et pour interagir dans les domaines relevant de leur compétence.
10	Bureau de contrôle	Bureau de contrôle des unités résidentielles	Généralement situé dans un poste de contrôle ou un bureau. Infrastructure de soutien physique des interfaces utilisateurs des opérateurs.	Réunit les interfaces utilisateurs dont les membres du personnel ont besoin pour s'acquitter de leurs responsabilités de gestion et pour interagir dans les domaines relevant de leur compétence.
11	Domaine de contrôle	Appel à partir des cellules, tour de garde, système de sonorisation	Groupe d'appareils et d'objets physiques et virtuels nécessitant souvent du matériel spécialisé ou un logiciel pour exécuter un ensemble de fonctions.	Recueille de l'information ou active des capacités dans son domaine opérationnel.
12	Panneau de commande	Panneau de commande de la sonorisation, alarme incendie	Appareil matériel et logiciel constituant l'interface opérateur (appareil d'entrée-sortie) dans un poste de contrôle.	Permet aux opérateurs de gérer un ou des domaines.
13	Poste de contrôle	Poste de contrôle des unités résidentielles/PPCC	Salle ou emplacement généralement sécurisé dans un établissement.	Offre un espace où les membres du personnel peuvent s'acquitter de leurs responsabilités de gestion et interagir dans les domaines relevant de leurs compétences.
14	Équipement sur mesure		Équipement conçu et/ou fabriqué expressément pour un contrat donné.	
15	Responsable de la conception		Le directeur des systèmes électroniques de sécurité de SCC est responsable de tous les aspects techniques relatifs à la conception et à la mise en œuvre des systèmes.	
16	Appareil	Caméra de TCF, porte gérée, appareil de détection de la provenance des appels	Appareil spécialisé, comportant habituellement des composants matériels et logiciels.	Permet la collecte de données ou active les fonctions associées à un système ou un sous-système en particulier.
17	Interface utilisateur d'inscription		Moniteur et logiciel procurant l'interactivité nécessaire à certaines tâches, dans un emplacement sécurisé.	Permet au personnel désigné d'inscrire et de supprimer des utilisateurs dans les systèmes de commande, de contrôle, et d'acquisition de données.

N°	Terme	Exemple	Description	Fonction
18	Interface utilisateur d'entretien		Moniteur et logiciel procurant l'interactivité nécessaire à certaines tâches, dans la salle d'équipement commune (SEC) ou dans le bureau du fournisseur de services d'entretien.	Permet au personnel de l'entretien d'interagir avec un ou des systèmes afin d'accomplir leurs tâches quotidiennes de dépannage et d'entretien des systèmes et sous-systèmes.
19	Avis	Avis indiquant l'ouverture ou la fermeture d'une porte, ou le déclenchement d'une alarme liée à un capteur.	Message affiché sur une interface utilisateur et/ou enregistré dans une base de données afin d'indiquer un changement d'état ou une commande lancée par un opérateur.	
20	Produit commercial		Équipement disponible sur le marché et livré avec des données de fiabilité recueillies sur le terrain, des manuels, des dessins techniques et une liste de prix des pièces de rechange.	
21	Interface utilisateur de l'opérateur	Affichage du SPDI, affichage du système de commande et de surveillance des portes	Moniteur et logiciel procurant l'interactivité nécessaire à certaines tâches (appareil d'entrée-sortie).	Permet à l'opérateur d'interagir avec un ou des systèmes afin d'accomplir ses tâches quotidiennes à la console de contrôle ou au bureau de contrôle.
22	Agent de projet		Employé du SCC ou contractuel choisi par le directeur des services d'ingénierie (DSI) à titre de responsable de l'exécution du projet.	
23	Interface utilisateur de rapports		Moniteur et logiciel procurant l'interactivité nécessaire à certaines tâches, dans un emplacement sécurisé.	Permet au personnel de gestion d'accéder aux rapports préconfigurés et de créer des rapports personnalisés.
24	Serveur	Enregistreur vidéo en réseau	Ordinateur monté sur bâti exécutant un logiciel, situé dans une salle d'équipement, telle qu'une SEC ou une salle d'équipement des télécommunications (SET).	Exécute le logiciel de prise en charge des applications de commande et de contrôle connectées à des sous-systèmes.
25	État		L'état d'un appareil tel qu'il est rapporté par un sous-système ou un système.	Fournit une représentation logique de l'état d'un appareil qui fait l'objet d'une surveillance ou d'un processus de gestion.
26	Sous-système	Appel à partir des cellules, tour de garde	Groupe d'appareils et d'objets physiques et virtuels nécessitant souvent du matériel spécialisé ou un logiciel pour exécuter un ensemble de fonctions connexes.	Recueille de l'information ou active des capacités dans son domaine opérationnel.

N°	Terme	Exemple	Description	Fonction
27	Système	SPDI	Groupe d'appareils et d'objets physiques et virtuels, y compris des appareils composant des sous-systèmes, nécessitant souvent du matériel spécialisé ou un logiciel pour exécuter un ensemble de fonctions connexes d'ordre général.	Recueille de l'information ou active des capacités dans son domaine opérationnel.
28	Interface utilisateur tactile	Interface utilisateur du système de commande et de surveillance des portes	Habituellement, un moniteur à écran ACL doté de la technologie d'écran tactile.	Permet à un opérateur de consulter les systèmes présentés sur le moniteur et d'interagir avec eux.
29	Poste de travail		Ordinateur monté sur bâti dans un emplacement sécurisé, à distance d'un poste de contrôle ou d'un bureau de contrôle.	Exécute le logiciel utilisé pour déployer les fonctions de commande et de contrôle.

1 Portée

La présente norme définit les exigences essentielles du Service correctionnel du Canada (SCC) en ce qui a trait à la conception et aux fonctionnalités de la plateforme de communications, de commande et d'acquisition de données (CCAD), incluant le développement d'applications et la prestation des services, qui sera déployée afin de prendre en charge les applications et les services nécessaires au déploiement de systèmes de commande et de contrôle de prochaine génération dans l'ensemble des postes de contrôle des établissements correctionnels fédéraux. La plateforme doit inclure :

- un environnement de développement intégré (EDI) à l'intérieur duquel sont créées des applications propres à chaque domaine et dont la disposition de l'interface utilisateur graphique fournie par le SCC est uniformisée et normalisée;
- un environnement d'exécution des applications en service;
- un environnement de prestation de services et de distribution d'applications permettant de configurer et de déployer celles-ci dans un réseau réparti;
- une infrastructure de sécurité qui communique les paramètres d'accès des utilisateurs et de portée du contrôle à la plateforme de systèmes et à ses applications, ainsi qu'aux systèmes et appareils de sécurité gérés;
- un environnement de traitement hautement disponible, fiable, redondant et robuste conçu de telle sorte que la défaillance d'un de ses éléments matériel ou logiciel ne désactive pas la plateforme et les applications en cours d'exécution;
- un cadre logiciel, avec outils et bibliothèques, qui simplifie le développement d'applications et la communication avec les appareils de sécurité sur place et à distance, ainsi qu'avec les systèmes de médiation répartis à l'intérieur d'un établissement correctionnel;
- un cadre logiciel capable de créer des plans d'intervention lorsqu'un appareil ou un utilisateur est à l'origine d'un événement ou déclenche une alarme;
- une base de données ou un fichier structuré et défini, contenant la configuration complète du système mis en œuvre à un endroit précis et qui peut être exportée à des fins de sauvegarde, de restauration ou de formation;
- un enregistreur de données ou une base de données d'historique, accessibles et centralisés, permettant la collecte, la gestion, le stockage et l'extraction en temps réel de données sur les alarmes et les événements détectés par le système.

2 Exigences générales relatives au logiciel de CCAD

Le logiciel de communications, de commande et d'acquisition de données (CCAD) sert avant tout à fournir un cadre de développement, ou environnement de développement intégré (EDI), pour que le Service correctionnel du Canada (SCC) puisse remplacer son vieux parc d'applications disparates de gestion de la sécurité et des opérations, ainsi que ses interfaces utilisateurs hétéroclites. La technologie de prochaine génération doit procurer des applications intuitives, faciles à utiliser et dont l'interface utilisateur graphique (IUG) en couleurs présente un aspect et une convivialité uniformes. Ces applications, conformes à une norme de conception de portée nationale, sont déployées dans de multiples sous-systèmes et établissements. L'IUG doit également s'afficher sur un écran tactile qui constitue le principal dispositif d'entrée de l'utilisateur.

Le logiciel de CCAD a pour but de créer à la fois un environnement de développement logiciel et un modèle de composants uniformes à tous les niveaux de la solution, des dispositifs d'extrémité jusqu'à la présentation de l'information. Ainsi, les développeurs peuvent travailler avec les mêmes outils dans un même environnement de programmation.

L'EDI du logiciel de CCAD doit comporter une interface homme-machine (IHM) qui prend en charge la connaissance de la situation, le contrôle de la surveillance et des processus, l'acquisition de données en temps réel, la gestion des alarmes et des événements, la collecte de données historiques, la production de rapports, la transmission locale et à distance de données télémétriques à n'importe quel sous-système de médiation ou dispositif de sécurité, ainsi que l'accès à l'Internet et aux intranets. Facile à utiliser et doté d'un environnement de développement orienté objet, le logiciel doit être compatible avec le cadre logiciel .NET développé par Microsoft et intégré aux différents systèmes d'exploitation Windows.

Le système doit être suffisamment souple pour le configurer aisément en fonction des besoins particuliers de l'utilisateur. Les intégrateurs de systèmes sur place, les ingénieurs en systèmes et les fournisseurs de service d'entretien doivent pouvoir également le modifier rapidement. De plus, il doit être doté des protocoles nécessaires pour empêcher l'accès non autorisé aux logiciels.

Le logiciel réunit une suite de composants modulaires commerciaux du même fabricant de logiciels. Ces composants doivent être étroitement intégrés les uns aux autres pour exécuter toutes les fonctions du système de CCAD. La suite doit comporter un système interactif (IHM) pour présenter et surveiller les alarmes, ainsi que pour contrôler les processus et gérer les dispositifs et les systèmes. Le logiciel de CCAD doit également fournir les outils nécessaires aux activités liées à l'administration, l'inscription, la configuration, l'entretien et la production de rapports.

Le logiciel doit également communiquer facilement avec des bases de données et des systèmes de modélisation et de simulation externes, comme ceux qui assurent la gestion des biens d'entreprise (GBE) et celle de l'entretien (SIGE).

2.1 Prise en charge de normes et de protocoles universels

Le système de CCAD doit faciliter l'intégration des dispositifs d'extrémité, des systèmes ou serveurs de médiation (TD, AP, SCSP, TCF, systèmes de sonorisation, etc.) au moyen de normes et de protocoles universels, comme Modbus, le contrôle OPC et la PIE, appliqués à l'interface avec les produits de sécurité physique.

Le système de CCAD doit pourvoir se connecter aux dispositifs au moyen de services Web, par exemple au moyen du protocole SOAP de l'ONVIF et de l'architecture REST de la GISP.

2.2 Extensibilité

Comme il est peu probable que les fonctionnalités spécifiques du logiciel fourni satisfassent à toutes les exigences relatives au système de CCAD, le logiciel doit permettre à un intégrateur de système ou à un technicien en systèmes compétent d'en développer de nouvelles.

Des trousses d'outils évoluées doivent être disponibles pour permettre de développer des composants logiciels sur mesure et de les intégrer au logiciel de CCAD.

L'architecture logicielle doit pouvoir traiter 500 000 entrées/sorties et 50 nœuds dans un réseau réparti semblable à celui qui sera déployé dans de nombreux établissements correctionnels du SCC.

2.3 Compatibilité avec le système d'exploitation

Le logiciel précisé doit être accompagné d'une licence autorisant son utilisation avec la version la plus récente des systèmes d'exploitation suivants pris en charge par Microsoft sur le matériel approprié, quelle que soit la combinaison :

Microsoft Windows 7 ou Windows 8.x (édition professionnelle);

Microsoft Windows Server 2012 ou plus récent;

versions 32 bits et 64 bits du système d'exploitation, selon l'architecture matérielle.

Le logiciel doit également être compatible avec les tablettes qui utilisent ces systèmes d'exploitation.

S'il s'agit d'une version ultérieure du système d'exploitation, le fabricant doit produire une déclaration et une feuille de route ayant trait à sa prise en charge.

Le logiciel de CCAD doit être également compatible avec des environnements de machines virtuelles, dont Microsoft Hyper-V et VMware.

Le matériel doit être compatible avec des ordinateurs multi-cœurs et multiprocesseurs.

3 Exigences logicielles relatives à l'EDI

La présente section décrit les exigences relatives à l'environnement de développement intégré (EDI) nécessaire à la création et à la personnalisation de logiciels propres à chaque domaine et destinés au système de commande et de contrôle de prochaine génération du SCC.

3.1 Environnement de développement

L'EDI doit consister en une seule application intégrée capable de gérer tous les aspects du développement et de l'essai d'une application de CCAD.

L'EDI doit accommoder plusieurs utilisateurs à la fois, là où des développeurs d'applications doivent détenir les autorisations de sécurité afférentes aux divers rôles prédéfinis dans l'ensemble du système.

3.2 Authentification des utilisateurs

L'EDI doit pouvoir être configuré de manière à prendre en charge l'authentification des systèmes d'exploitation de Microsoft, par exemple les domaines Active Directory, afin de permettre aux développeurs d'applications d'accéder au système de CCAD et d'afficher, de configurer et de modifier des applications.

3.3 Contrôle intégré des révisions de logiciels

L'EDI doit permettre de gérer et de contrôler les modifications apportées par les développeurs au code source des applications et des éléments graphiques. L'historique des révisions doit faire état de chaque changement, soit le nom d'utilisateur de son auteur, l'horodatage du changement et un résumé de ce dernier.

L'EDI doit permettre aux développeurs d'applications détenant les droits de configuration nécessaires d'afficher une application en développement et de faire en sorte qu'une seule personne puisse modifier son code source à la fois.

3.4 Exemples et modèles d'applications destinées aux dispositifs gérés

L'EDI doit utiliser des concepts de modélisation d'objets pour permettre la conception d'applications qui intègrent les caractéristiques physiques de l'établissement correctionnel, y compris la topologie des lieux, le matériel et l'emplacement des ordinateurs. Le système doit permettre de développer des applications, des modules (entité autonomes) qui représentent des dispositifs réels, comme les capteurs périmétriques, les détecteurs de mouvement, les dispositifs d'alarme personnels portatifs, les caméras de TCF et leurs systèmes de commande, les commutateurs de signalisation d'ouverture de porte, les commandes de porte, les commandes d'alimentation, les lecteurs de carte IRF, les intercoms, les systèmes d'annonces aux haut-parleurs, les boutons-poussoirs, etc.

L'EDI doit permettre de créer des modèles d'application et de module destinés aux diverses applications de domaine et leur assigner une logique, des alarmes, des éléments de sécurité et des données historiques. Les modèles doivent être réutilisables et extensibles (des versions améliorées du modèle parent) pour répondre aux exigences particulières d'un dispositif ou d'un sous-sous-système.

Le système de CCAD doit permettre de créer des applications ou des modules représentant des dispositifs complexes, eux-mêmes composés de dispositifs plus petits et plus simples, en regroupant ou en combinant deux modèles d'application ou plus (p. ex., des portes configurées en série interverrouillable). Chaque modèle ajoute des attributs spécifiques et une logique au modèle parent de l'application ou du module.

Le modèle d'application ou de module doit permettre une configuration simple pour faire le suivi des modifications apportées aux valeurs des attributs ou aux états du dispositif et de consigner ces modifications dans un enregistreur de données (base de données des événements historiques).

Le modèle d'application ou de module doit permettre de configurer les attributs qui déclenchent ou génèrent des alarmes lorsque leur valeur reflète un changement de situation. Par exemple, l'EDI doit prendre en charge des alarmes axées sur des situations (états « faible-faible », « faible », « élevé » et « élevé-élevé », écart du taux de changement, etc.) et axées sur des événements (condition « vrai » ou « faux », échec de l'ouverture, échec de la fermeture, commandes conflictuelles, etc.) au moyen d'outils définis au préalable qui indiquent la marche à suivre au développeur d'applications tout au long du processus de définition de la configuration.

3.4.1 Modèles d'application ou de module – Sécurité

L'EDI doit permettre de configurer les éléments de sécurité intégrés aux modèles d'application ou de module destinés aux dispositifs. À tout le moins, les permissions opérationnelles d'exécution doivent permettre :

d'accorder ou de refuser le droit de visualiser, de modifier ou de supprimer un attribut d'application ou de module;

d'accorder ou de refuser le droit d'accuser réception d'une alarme dans l'environnement d'exécution;

de modifier des attributs de configuration pour permettre aux développeurs d'applications d'en modifier la valeur (p. ex., le registre d'un automate programmable qui définit une entrée discrète);

de modifier des attributs opérationnels pour permettre aux développeurs d'applications qui détiennent les permissions opérationnelles appropriées d'accomplir certaines tâches courantes, par exemple modifier un point de consigne, le mode de sortie et de commande d'un dispositif, commander un dispositif ou encore ouvrir une fenêtre de processus ou d'application et en afficher le contenu;

de modifier des attributs pour permettre aux développeurs d'applications d'apporter un réglage fin à l'attribut d'une application ou d'un module dans l'environnement d'exécution, par exemple, l'attribut qui définit les points de consigne d'une alarme ou la sensibilité d'un dispositif périmétrique de détection des intrusions.

3.4.2 Modèles d'application ou de module – Éléments graphiques et animations

Le modèle d'application ou de module doit permettre d'associer et de configurer une ou plusieurs représentations graphiques aux fins de visualisation. L'application de visualisation elle-même doit pouvoir être représentée par un modèle de module qui la contient. Veuillez consulter la section 3.7.2 qui décrit plus en détail la marche à suivre pour intégrer des éléments graphiques ou des animations à un modèle d'application ou de module.

3.4.3 Logique d'application et scripts

L'IDE doit permettre d'intégrer la logique et le comportement de l'application au moyen de scripts associés au changement de la valeur d'un attribut. Ainsi, le changement d'une valeur de l'application ou du module en cours d'utilisation entraîne l'exécution d'un script qui déclenche à son tour une action ou un processus spécifique ou encore qui génère un événement ou une alarme quelconque.

Le langage de script choisi doit permettre d'intégrer le cadre logiciel .NET (prononcer « dot NET ») de Microsoft. Les bibliothèques .NET sont distribuées à grande échelle par les fabricants de dispositifs de sécurité et de systèmes de médiation afin de faciliter l'intégration d'une logique de commande propre à chaque dispositif dans les logiciels.

Le langage de script doit être facile à programmer grâce à une syntaxe et des instructions courantes qui ne requièrent qu'un minimum de connaissances des autres langages de programmation. Le développeur d'applications doit être en mesure de modifier les scripts d'instructions logiques pendant que le système surveille le processus (en cours d'exécution).

Le langage de script doit prendre en charge la configuration de la logique du système dans les modèles d'application ou de module pour surveiller l'état de chaque attribut dans le système et exécuter des fonctions spécifiques en fonction du type et de l'état de l'alarme.

L'environnement de script doit prendre en charge la configuration des applications ou des modules d'un dispositif de commande en fonction de l'état de ce dernier et de l'attribut défini par le développeur d'applications ou du résultat d'une expression comportant plusieurs noms d'attribut d'objet, y compris des attributs discrets, des états d'alarme, comme « faible », « faible-faible », « élevé », « élevé-élevé », ou l'équivalent d'une valeur spécifique.

Le système doit prendre en charge la configuration de scripts de commande d'application pour modifier l'état de points discrets, afficher des fenêtres, etc. Une telle logique d'application doit également permettre de démarrer et d'arrêter d'autres programmes, comme Microsoft Excel, Microsoft Word, le logiciel Crystal Reports et d'autres applications Windows.

3.5 Déploiement des modèles d'application ou de module destinés aux dispositifs

L'EDI doit permettre de déployer les modèles d'application ou de module destinés aux dispositifs, depuis l'environnement de développement vers l'environnement d'exécution. Le déploiement d'une instance du modèle d'application ou de module active l'objet et le rend opérationnel.

Tous les composants instanciés de l'application ou du module doivent être configurés et déployés depuis l'EDI vers les postes de travail et les serveurs cibles.

3.6 Utilitaire d'importation et d'exportation

L'EDI doit prendre en charge l'importation et l'exportation des données de configuration des applications destinées aux dispositifs. Le fichier ainsi produit doit être lisible par l'utilisateur, par exemple un fichier CSV (*comma separated value*), ou dans d'autres formats qui lui permettent d'en modifier le contenu.

Il doit être possible de modifier une ou plusieurs instances des dispositifs de même type (c'est-à-dire issus du même modèle) à partir d'un fichier CSV ou formaté en colonnes multiples qui contiennent des valeurs correspondant aux attributs de l'objet.

3.7 Exigences logicielles du développement de l'IHM

La présente section décrit les exigences relatives au développement technique de toutes les fonctions logicielles du système d'interface homme-machine (IHM). Ce développement englobe l'affichage en couleurs, la configuration de la base de données historiques et en temps réel, les alarmes, les communications avec les dispositifs de terrain et la configuration des applications des serveurs et des systèmes clients présents sur le réseau de CCAD.

3.7.1 Prise en charge de plusieurs langues

L'EDI du système de CCAD doit permettre de développer une application dont la langue d'affichage peut être modifiée dynamiquement en cours d'exécution.

Le système doit prendre en charge toutes les langues disponibles dans la version courante du système d'exploitation.

Le logiciel doit permettre de choisir au moins entre deux langues (le français et l'anglais).

Les chaînes de caractères des objets textuels accompagnés d'images doivent s'afficher en différentes langues. Lorsque l'utilisateur ouvre une application, la langue d'affichage est définie en fonction des préférences locales du système.

Il doit être possible de configurer les messages d'alarme pour s'afficher dans la langue sélectionnée.

Les chaînes de caractères non traduites dans la langue sélectionnée doivent s'afficher dans la langue par défaut de l'IHM.

3.7.2 Environnement de développement de l'IHM

L'EDI du système de CCAD doit comprendre des logiciels permettant d'agencer les éléments visuels des interfaces utilisateurs graphique (IUG), c'est-à-dire les écrans et les fenêtres de l'interface homme-machine (IHM). À l'exécution du système, les symboles graphiques doivent représenter l'état actuel d'une application ou d'un module au moyen d'animations liées aux valeurs des attributs des dispositifs (données opérationnelles). L'IHM doit présenter aux utilisateurs une vue réaliste des processus du système de CCAD.

L'EDI du système de CCAD doit permettre l'importation d'images de plan d'étage (en format vectoriel) représentant l'aménagement des bâtiments de l'établissement correctionnel. L'EDI doit être doté d'outils pour animer les plans d'étage avec des symboles représentant des portes, des barrières, des caméras vidéo, des microphones et d'autres dispositifs. L'animation du symbole doit changer de manière à représenter en temps réel l'état opérationnel du dispositif qui lui est associé.

Les développeurs d'applications doivent pouvoir définir des écrans graphiques pendant que le système surveille le processus.

3.7.2.1 Éditeur graphique intégré

L'EDI doit comprendre un éditeur graphique. Celui-ci regroupe divers outils de dessin de base permettant de créer des objets graphiques simples et complexes. La boîte à outils doit permettre de dessiner des lignes, des rectangles, des polygones, des ellipses, des cercles, des courbes ouvertes et fermées, ainsi que des arcs et des tartes à deux et à trois points, en plus de remplir les formes graphiques et le texte.

L'éditeur graphique doit permettre d'assigner divers attributs à ces objets graphiques, comme la couleur du trait et du remplissage, la taille et l'orientation, en plus de les

rendre statique ou dynamique. Il doit être possible de redimensionner les éléments textuels, de choisir la police TrueType et de les afficher en caractères gras, italiques et soulignés. Redimensionnables, tous les objets peuvent être déplacés dans toutes les directions, un pixel à la fois ou en les faisant glisser avec la souris. Un nuancier comptant 48 couleurs prédéfinies doit être fourni.

L'utilisateur doit pouvoir définir, exporter et importer sa propre palette de couleurs choisies parmi 16,7 millions de nuances. Le système doit également permettre à l'utilisateur de choisir la couleur et le type de remplissage des objets et de l'arrière-plan, soit un remplissage plein, à un, deux et trois gradients de couleur, à motif, texturé ou sans remplissage.

3.7.2.1.1 Modification et manipulation des éléments graphiques

L'éditeur graphique doit prendre en charge les fonctions normalisées de manipulation des objets, tel que couper, copier, coller et supprimer. Des outils d'alignement doivent être disponibles pour faciliter le bon positionnement et l'agencement adéquat des objets. L'éditeur doit être doté des commandes nécessaires pour aligner les objets à gauche, à droite, en haut, en bas et au centre, ainsi que pour espacer les objets sur les axes horizontal et vertical, les déplacer à l'avant-plan ou à l'arrière-plan, les faire pivoter, les grouper et les dissocier.

L'éditeur graphique doit permettre de grouper les éléments graphiques de manière à les traiter comme s'ils ne forment qu'une seule entité. Il doit toutefois permettre de modifier l'un des éléments du groupe tout en maintenant l'intégrité de ce dernier.

L'environnement de développement graphique doit prendre en charge la copie d'un ou de plusieurs objets ou symboles graphiques animés, d'une fenêtre ou d'un écran à l'autre sans rien perdre des caractéristiques, des liens et des attributs de l'animation. Il doit également être possible d'importer des fenêtres d'une autre application de cette même façon.

L'éditeur graphique doit permettre d'importer une série d'icônes ou d'éléments graphiques fournis par le SCC et associés à des objets complexes liés à la sécurité, aux opérations et aux communications, comme les capteurs périmétriques, les détecteurs de mouvement, les dispositifs d'alarme personnels portatifs, les caméras de TCF et leurs systèmes de commande, les commutateurs de signalisation d'ouverture de porte, les commandes de porte, les commandes d'alimentation, les lecteurs de carte IRF, les intercoms, les systèmes de sonorisation, les boutons-poussoirs, etc.

Tous ces objets graphiques complexes doivent être redimensionnables dans n'importe quelle taille et pouvoir s'animer dynamiquement et en temps réel en fonction des données reçues et des actions de l'utilisateur.

L'éditeur graphique doit permettre de créer des couches d'objets de manière à activer ceux qui répondent à certaines conditions dans le déroulement du processus. Il doit également permettre de contrôler et de visualiser l'ordre de ces couches d'éléments graphiques.

3.7.2.2 Importation de fichiers d'images

L'éditeur graphique de l'EDI doit aussi permettre à l'utilisateur d'importer des fichiers de dessin et d'image dans les formats BMP, JPEG, EMF, TIF, PNG et ICO.

3.7.2.3 Incorporation d'une logique aux éléments graphiques

L'éditeur graphique de l'EDI doit permettre d'intégrer une logique et un comportement spécifique aux éléments graphiques au moyen d'un script.

Le script doit accepter les appels systèmes à la bibliothèque .NET.

La programmation de scripts avec l'éditeur graphique doit comprendre une option permettant d'afficher ou de masquer l'élément graphique à partir d'attributs nommés et créés par l'utilisateur (p. ex., si une valeur est « True », « False » ou « On False ») ou à la suite du changement de la valeur d'un attribut de l'objet de l'application. Le développeur d'applications doit pouvoir définir les attributs des types de données suivants du dispositif local ou externe : nombre entier, chaîne de caractères, opérateur booléen, virgule flottante, double, horodatage et temps écoulé.

Un seul objet composite doit pouvoir intégrer un nombre virtuellement illimité de symboles graphiques, jusqu'à concurrence d'une fenêtre entière de symboles. Les symboles doivent être reliés à des applications ou des modules, ou faire référence à d'autres attributs des variables de l'IHM ou du script. Les modifications apportées au symbole graphique doivent se propager dans toutes les instances de ce symbole.

3.7.2.4 Importation et exportation d'éléments graphiques

La trousse d'outils graphiques personnalisés créée avec l'éditeur graphique doit permettre d'importer et d'exporter tant les symboles graphiques que la logique et le comportement qui leur sont assignés au moyen des scripts.

3.7.2.5 Animation graphique

L'éditeur graphique doit prendre en charge au moins la configuration des animations précisées ci-après. Les objets graphiques doivent s'animer en fonction de critères définis par l'utilisateur et composés de noms d'attribut de dispositifs dans le système. Cela inclut l'utilisation d'expressions contenant des fonctions mathématiques et l'état de valeurs analogiques et discrètes dans le système.

Animation par la couleur

La couleur du symbole graphique doit changer en fonction de références exprimées en valeurs analogiques ou discrètes, ou en chaînes de caractères, au moyen de scripts ou par association à des changements de la valeur d'un attribut de l'objet de l'application. Il ne doit pas y avoir de limite fixe quant au nombre de changements de couleur d'un même symbole. Le pourcentage de la couleur de remplissage appliqué à l'objet doit être déterminé en associant cette valeur à celle d'un attribut de l'objet de l'application.

Animation par clignotement

L'objet graphique doit pouvoir clignoter en fonction de n'importe quelle expression, alarme ou événement discret, ou encore d'un groupe d'alarmes désigné. Le clignotement doit être réglable selon trois vitesses, soit lent, moyen et rapide.

Visibilité et transparence

La visibilité et la transparence de chaque symbole graphique doivent être associées à une option d'attribut pour activer celles-ci en fonction de l'état d'un point, d'une alarme ou d'un niveau de sécurité d'opérateur, qu'il soit discret ou analogique.

Dimensions, emplacement et orientation
Le système doit permettre d'animer les symboles en les redimensionnant, les déplaçant et les faisant pivoter en fonction d'un changement apporté à un nom d'étiquette ou hiérarchique.

3.7.3 Sommaire et historique des alarmes

La configuration des alarmes doit intégrer des paramètres permettant de leur appliquer des codes de couleur en fonction de leur état et de leur niveau de priorité. Ces codes de couleur doivent également s'appliquer aux divers états d'une alarme (alarme avec ou sans accusé de réception et alarme remise à l'état normal sans accusé de réception). L'utilisateur doit pouvoir choisir parmi 32 couleurs pour afficher chacun de ces états d'un alarme.

Les alarmes doivent s'afficher en temps réel ou sous la forme d'un historique. Le même objet doit communiquer avec le processus en service ou avec la base de données de l'historique des alarmes.

3.7.4 Aide incorporée

L'aide contextuelle doit appuyer l'élaboration des écrans et fenêtres de l'IHM de l'application. Les développeurs d'applications doivent pouvoir obtenir de l'aide immédiate sur tous les sujets touchant la configuration par l'intermédiaire d'une seule touche de fonction.

3.7.5 Gestion des applications de l'IHM

L'EDI du système de CCAD doit intégrer un logiciel qui facilite la gestion et le déploiement des applications de l'IHM dans les postes de travail cibles.

Le logiciel de gestion et de déploiement des applications de l'IHM doit propager tout changement apporté à une application de visualisation dans l'ensemble des postes de travail qui l'hébergent à l'échelle du système de CCAD. Le gestionnaire d'applications doit permettre de modifier dynamiquement la résolution des fenêtres de l'application. Cela permet de développer des affichages graphiques en fonction de la résolution du poste de travail et de les adapter rapidement pour leur procurer un aspect et une convivialité uniformes.

3.7.5.1 Gestion des applications réparties dans le réseau

Le logiciel de CCAD doit fournir des fonctions normalisées qui facilitent la configuration, l'utilisation, le dépannage et la maintenance de l'application en permettant de la déployer sans effort dans les environnements de réseau.

Le logiciel de gestion doit permettre de développer une seule application principale et de la tenir à jour dans le réseau. L'EDI doit permettre de distribuer automatiquement cette application principale dans tous les nœuds du réseau de CCAD et de propager les modifications qui lui sont apportées dans toutes ses instances présentes dans le système.

3.7.5.2 Notification du système client au sujet des applications modifiées

Lorsqu'un nœud client est déployé avec une application de l'IHM, il doit en conserver une copie sur son disque dur local et être enregistré à titre de développeur de cette application. Lorsqu'une modification de l'application est détectée, chaque nœud d'utilisateur enregistré doit en être informé par une notification. L'EDI doit permettre au développeur d'applications de définir la façon dont le nœud client est informé de tels changements. Le nœud client doit charger automatiquement la nouvelle version de l'application, indiquer au développeur d'applications de charger ou d'ignorer les modifications, ou ignorer automatiquement ces modifications. Si le réseau connaît une défaillance entre le dépôt et le nœud client, ce dernier doit continuer d'utiliser la dernière version déployée. Lorsque le réseau est rétabli, le système déploie l'application modifiée chez le nœud client.

4 Environnement d'exécution

La présente section décrit les diverses fonctions de l'interface utilisateur du système combinées en mode d'exécution.

4.1 Gestion des alarmes

Un service de gestionnaire des alarmes doit détecter et signaler les alarmes et prendre simultanément en charge au moins 200 affichages clients. Si une « tempête » d'alarmes survient (c.-à-d. lorsque des centaines ou des milliers d'alarmes sont détectées en une seconde), le gestionnaire d'alarmes doit signaler au système client, et afficher à son écran, jusqu'à 1000 nouvelles alarmes dans les 10 secondes suivant leur détection.

Le système doit pouvoir détecter et consigner les types d'alarmes suivants, ainsi qu'envoyer des notifications à leur sujet :

les ressources du système, comme l'utilisation de l'UC, limite de mémoire atteinte, etc.;

l'état du réseau, comme la connectivité IP, les embouteillages qui ralentissent le débit de transmission et de réception, etc.;

les conditions environnementales susceptibles de perturber le fonctionnement de systèmes ou de dispositifs;

les alarmes associés à des domaines spécifiques, comme l'accès aux portes, des portes forcées, une panne de caméra vidéo, la fermeture d'un poste de contrôle, etc.;

les actions des utilisateurs, par exemple un comportement inhabituel caractérisé par un nombre excessif de tentatives d'ouverture de session.

Les alarmes doivent être consignées dans une base de données, de préférence Microsoft SQL Server ou Microsoft Database Engine (MSDE). Les événements ainsi enregistrés incluent le déclenchement, la remise à l'état normal et l'accusé de réception des alarmes. Outre ces renseignements, la date et l'heure, le groupe, le type de données (valeur réelle/nombre entier/opérateur booléen), le type (« faible-faible », « faible », « élevé », « élevé-élevé », l'écart du taux de changement, le disque, etc.), le nom de l'opérateur, le nœud de l'opérateur à l'origine de l'accusé de réception, et le niveau de priorité des alarmes doivent également être consignés dans la base de données.

Un service de purge des alarmes doit être disponible afin de purger automatiquement et, facultativement, archiver les alarmes demeurées en ligne plus longtemps qu'un nombre de jours définis au préalable.

Les alarmes doivent pouvoir être imprimées sur une imprimante locale ou réseau. L'impression varie selon le nœud et peut inclure toutes les alarmes, uniquement les alarmes sans ou avec accusé de réception, les alarmes appartenant à un ou plusieurs groupes en particulier, les alarmes dont le niveau de priorité varie de *x* à *y*, ou encore les alarmes provenant de plusieurs fournisseurs d'alarmes.

Lorsque des alarmes sont générées, le gestionnaire d'alarmes doit permettre d'envoyer aux opérateurs clés des courriels contenant un sommaire des alarmes auxquelles il faut donner suite.

4.2 Architecture répartie

L'environnement d'exécution doit reposer sur une architecture de système répartie de type poste-à-poste. Cette architecture doit pouvoir accepter un nombre variable de nœuds, d'un seul nœud autonome à plus de 50 nœuds. Elle doit intégrer un modèle à ordinateurs multiples vu comme un unique espace de nommage réparti dans l'environnement d'exécution et qui ne nécessite pas de duplication des données entre deux nœuds.

4.3 Visionneuse de données en cours d'exécution

Le système doit comporter un outil permettant d'afficher en temps réel l'état, la qualité et la valeur de n'importe quel attribut d'application ou de module.

4.4 Reprise du système de CCAD

Le système logiciel de CCAD doit assurer la haute disponibilité de toutes les fonctions dans une environnement normal. Les exigences à l'égard de cette haute disponibilité s'appliquent également à la consignation des données de traitement historiques.

Dans une configuration redondante, il doit y avoir un système principal et un système de reprise qui gère le système principal actif et un système secondaire en cas de défaillance. Le système doit exécuter des données actives et les synchroniser avec le système de reprise. Si l'exécution des données ou la communication avec le système actif connaît une défaillance, le système de reprise doit prendre la relève, ainsi qu'assurer l'exécution et la communication à l'intérieur du système.

Étant donné le grand nombre de dispositifs que doit gérer le système de CCAD, celui-ci doit prendre en charge la configuration redondante du partage de la charge des applications entre plusieurs serveurs jusqu'à ce qu'une défaillance se produise.

4.4.1 Défaillances définies

Le système de CCAD doit détecter les événements dans les objets du système et du réseau de CCAD :

échec de communication avec un seul dispositif ou système de médiation;

échec de communication avec plusieurs dispositifs ou systèmes de médiation;

échec de communication avec la logique de l'application;

échec de l'imprimante des alarmes (hors ligne, bac à feuilles vide) et défaillance du gestionnaire des alarmes;

échec de communication avec l'enregistreur de données;

écart de la vitesse de collecte de l'enregistreur de données;

espace disque faible dans tous les enregistreurs de données sur le réseau.

Le système de CCAD doit détecter toutes les défaillances possibles et permettre de récupérer les données du système client sans l'intervention de l'opérateur.

4.4.2 Redondance des applications du poste de travail (IHM)

Le système doit permettre à des applications de reprise de prendre la relève des applications actives qui connaissent une défaillance d'exécution ou avec lesquelles il est impossible de communiquer. Il ne doit pas être nécessaire de configurer individuellement les systèmes de reprise. En temps normal, le serveur principal et les applications qu'il héberge doivent être actifs. Le serveur de secours et les applications

qu'il héberge doivent être maintenus en état d'attente et synchronisés avec le nœud actif auquel ils sont appariés.

Les postes de travail sur lesquels sont exécutées des applications de visualisation doivent pouvoir basculer automatiquement vers un poste de travail redondant. L'opérateur ne doit pas être obligé d'intervenir. Le système doit prendre en charge l'exécution de logiciels de visualisation et les outils de développement technique au niveau des sessions de service de terminal, tout en appliquant le modèle de sécurité du système d'exploitation configuré.

4.4.3 Redondance des alarmes

Le système doit permettre de traiter les alarmes à partir des applications de reprise du dispositif qui ont pris la relève des applications actives du même dispositif, qui ont connu une défaillance d'exécution ou avec lesquelles il est impossible de communiquer. Il ne doit pas être nécessaire de configurer individuellement les alarmes dans les applications de reprise du dispositif. À l'instar de la redondance des applications du poste de travail (IHM), les applications du dispositif doivent être affectées à un système principal qui, en retour, s'assure que les applications de reprise sont créées et déployées en mode de reprise pour traiter les alarmes.

4.4.4 Redondance des communications

Les serveurs actifs et de reprise doivent être interconnectés par des canaux de message redondants qui assurent leur relève réciproque en cas d'interruption.

4.4.5 Redondance du stockage dans les enregistreurs de données

Le système doit assurer le stockage des données historiques provenant des applications et des modules actifs. Si une application ou un module principal actif connaît une défaillance, une application ou un module de reprise doit être activé et prendre la relève pour fournir les données historiques à stocker. Il ne doit pas être nécessaire de configurer individuellement le stockage de données historiques des objets de reprise.

Si un enregistreur de données est hors ligne ou impossible à joindre, les moteurs qui prennent en charge les applications ou les modules actifs doivent stocker localement les données historiques et transmettre les données dans la mémoire tampon à l'enregistreur de données lorsque le serveur d'enregistreurs est disponible. Les moteurs principaux et de reprise doivent synchroniser le stockage des données historiques dans la mémoire tampon.

4.5 Sécurité dans l'environnement d'exécution

La sécurité de l'accès est primordiale dans l'environnement d'exécution.

L'environnement d'exécution doit pouvoir être configuré au moyen d'une interface d'administration qui permet d'accorder ou de refuser aux opérateurs l'accès aux fonctionnalités du système en fonction de leurs compétences, rôles et responsabilités.

C'est le logiciel de CCAD, et non l'application développée, qui doit imposer ces contraintes touchant la sécurité.

4.5.1 Modifications de données dans l'environnement d'exécution

Les modifications apportées aux valeurs des applications destinées aux dispositifs dans l'environnement d'exécution doivent faire l'objet d'une autorisation de sécurité. Les permissions configurées dans l'EDI doivent être vérifiées automatiquement dans l'environnement d'exécution. Cette vérification doit également porter sur l'identité et les permissions d'accès de l'auteur de la demande de changement dans l'environnement d'exécution.

Les demandes d'authentification rejetées doivent être consignées.

Le fabricant doit publier ses lignes directrices en matière de sécurité pour aider à sécuriser le système de CCAD en entier.

4.5.2 Piste de vérification dans l'environnement d'exécution

Le système doit pouvoir être configuré de manière à ce que toute modification apportée à une variable dans l'environnement d'exécution doit créer une piste de vérification qui fait état du code d'identification et du nom complet du développeur d'applications, ainsi que des valeurs actuelle et précédente de la variable.

Tout attribut configuré aux fins de la vérification doit créer une piste de vérification qui fait état du code d'identification et du nom complet du développeur d'applications, du nom d'utilisateur et du nom complet du vérificateur, ainsi que des valeurs actuelle et précédente de l'attribut.

4.5.3 Sécurité des postes de travail

Le poste de travail doit être régi par le modèle de sécurité défini au niveau des profils et des groupes d'utilisateurs du système de CCAD.

Le logiciel doit appliquer un modèle de sécurité des données hiérarchique qui prévoit que la permission de modifier un point de consigne ou toute autre valeur est établie dans la base de données de configuration. Tout changement apporté à ce modèle doit être visible sur les postes de travail de tous les opérateurs sans modifier ces postes de travail.

Le système de sécurité doit pouvoir désactiver l'accès à chacun des contrôles Microsoft Windows (menu Fichier, fermer, réduire, etc.) et des raccourcis-claviers (CTRL-Échap, ALT-Tab, etc.) et empêcher d'accéder au système de l'extérieur au moyen de la combinaison de touches CTRL-ALT-Suppr).

4.5.4 Consignation des actions de l'opérateur

Toutes les actions de l'opérateur doivent être consignées dans un enregistreur d'événements. Celui-ci doit enregistrer chaque ouverture et fermeture de session, chaque modification d'un point de consigne ou chaque commande envoyée à un dispositif.

Chaque événement doit être consigné avec la date, l'heure, le nom de l'opérateur qui a ouvert la session et le type d'action qu'il a effectuée (modification d'un point de consigne, modification d'un état, etc.).

4.5.5 Consignation des changements de valeur

Tout attribut peut également être configuré de manière à déclencher un événement. Ce dernier doit être consigné dès que l'attribut change de valeur.

Les événements doivent être consignés avec la date et l'heure où ils se sont produits, et avec leur niveau de priorité.

5 Postes de travail et applications propres à chaque domaine (IHM)

5.1 Postes de travail – Généralités

Le système de CCAD doit être compatible avec des ordinateurs disponibles commerciaux et leur système d'exploitation.

Le fabricant du système de CCAD doit offrir à titre de produits standard inscrits sur sa liste de prix standard divers panneaux d'IHM avec le logiciel de CCAD déjà installé.

Le système de CCAD doit prendre en charge l'affichage sur plusieurs écrans.

Si la suite de logiciels du système de CCAD ne les intègre pas déjà, celui-ci doit permettre de développer diverses applications destinées aux postes de travail et offrant les interfaces utilisateurs suivantes : opérateur, inscription, administration, diagnostics et rapports statistiques, configuration et déploiement, maintenance.

Le poste de travail de CCAD doit permettre d'ouvrir une session dans le système au moyen d'une carte IRF ou à partir de l'interface utilisateur, et de fermer la session en cours après un délai d'inactivité prédéfini.

5.1.1 Poste de travail client léger

Aucune installation de logiciel d'IHM du système de CCAD ne doit être nécessaire sur le poste de travail client léger de l'opérateur, à l'exception du micrologiciel du poste de travail ou du logiciel nécessaire pour ouvrir une session de Bureau à distance. L'IHM du système de CCAD doit prendre en charge la version la plus récente des systèmes d'exploitation Microsoft Windows capable de prendre en charge le protocole Bureau à distance (PBD) pour afficher l'IHM d'une application.

Aucune modification de l'IHM du système de CCAD ne doit être nécessaire pour que ce dernier puisse fonctionner avec une configuration client léger. La même application exécutée sur un poste de travail doté de toutes les fonctions (client lourd) doit également s'exécuter dans une session de services de terminal (Bureau à distance).

Une interface de gestion du parc de terminaux clients légers doit être fournie et offrir des fonctions de surveillance à distance, de redémarrage, de basculement et de reproduction du contenu de l'écran.

Le poste de travail client léger doit prendre en charge l'affichage sur plusieurs écrans.

5.2 Poste de travail d'opérateur

L'opérateur du système de CCAD doit pouvoir exécuter toutes les commandes de surveillance et de supervision depuis son poste de travail. Parmi les commandes les plus courantes, on retrouve la modification des points de consigne des boucles de contrôle, les accusés de réception des alarmes et le réglage de leurs points de consigne, la commutation des modes automatique et manuel et les mises sous et hors tension des appareils sur le terrain, ainsi que le balayage de l'état sous et hors tension des points et des dispositifs.

L'opérateur du système de CCAD doit pouvoir accéder à tous les attributs des dispositifs et à tous les affichages graphiques du système de CCAD à partir de n'importe quel poste de travail présent sur le réseau sans être obligé d'identifier l'enregistreur de données ou le serveur dans lequel se trouve le point ou l'affichage.

L'opérateur du système de CCAD doit pouvoir exécuter toutes les commandes de surveillance et de supervision depuis un poste de travail ou un environnement client léger.

5.3 Poste de travail d'inscription

Le système de CCAD doit permettre d'intégrer un système d'inscription par carte IRF pour que les représentants d'établissement concernés puissent ajouter, modifier ou supprimer la carte IRF d'un utilisateur.

Le poste de travail d'inscription doit permettre d'assigner les groupes de sécurité prédéfinis du système de CCAD à l'utilisateur d'une carte IRF qui assume divers rôles opérationnels pour lui permettre d'accéder aux différents postes de travail.

5.4 Poste de travail d'administration

Le poste de travail d'administration du système de CCAD doit permettre d'ajouter ou de supprimer des utilisateurs déjà inscrits et de leur attribuer des privilèges. Un utilisateur qui assume un rôle quelconque ou qui appartient à un groupe en particulier doit hériter de tous les privilèges attribués au groupe de sécurité.

Le poste de travail d'administration du système de CCAD doit permettre de créer différents groupes de sécurité que l'on peut attribuer aux utilisateurs. Les groupes de sécurité permettent aux utilisateurs non seulement d'accéder aux postes de travail, mais aussi de voir, d'utiliser ou de modifier ceux-ci en fonction de leur rôle opérationnel dans l'établissement correctionnel.

5.5 Poste de travail d'analyse des données et de production de rapports statistiques

Le logiciel de CCAD doit inclure des outils logiciels clients conviviaux pour produire en temps réel des rapports d'analyse des tendances et des données historiques. Ce logiciel d'analyse client est utilisé par le personnel d'ingénierie, de maintenance et de supervision dont les membres ont besoin des renseignements que fournit le système de CCAD mais pas d'accéder aux applications propres aux divers domaines (c.-à-d. les postes de travail d'opérateur, d'inscription, d'administration et de configuration). Les outils clients doivent pouvoir accéder aux données stockées dans les enregistreurs présents dans le réseau de CCAD.

Les membres du personnel d'ingénierie, de maintenance et de supervision doivent utiliser un mot de passe pour ouvrir une session et accéder au serveur de base de données. Ils n'ont pas à savoir où se trouve le serveur dans le réseau, mais uniquement son nom. Les logiciels d'analyse des données doivent intégrer des outils évolués d'analyse des tendances et de production de rapports sous forme de feuilles de calcul ou en format libre.

Les outils clients doivent être disponibles sous forme de programmes autonomes ou d'applets incorporées dans l'affichage de l'IHM du système de CCAD, de sorte que le poste de travail doté de toutes les fonctions et le poste de travail d'opérateur en lecture seule présentent les mêmes capacités.

Le système doit permettre de créer des rapports d'analyse des tendances et statistiques fondés sur les interrogations de la base de données des enregistreurs.

Le système doit intégrer des outils qui facilitent la production de rapports personnalisés en permettant de sélectionner l'un ou l'autre des attributs des dispositifs gérés, une heure ou une date, un événement ou une alarme en particulier, l'action d'un utilisateur, etc.

Le système de CCAD doit permettre de créer et d'enregistrer des rapports personnalisés sous forme de modèles pouvant être réutilisés.

Le système doit prendre en charge le langage SQL standard pour interroger la base de données des enregistreurs.

Le système de CCAD doit intégrer des outils pour exporter les données des rapports statistiques et d'analyse des tendances en fichiers aux formats Microsoft Excel et Word, .pdf et .csv.

5.6 Poste de travail de configuration et de déploiement

L'interface utilisateur de configuration et de déploiement doit permettre aux intégrateurs et aux représentants désignés de configurer tous les paramètres variables des diverses applications propres aux domaines, y compris de créer des dispositions d'écran, des cartes, des dispositifs de sécurité, des systèmes de médiation, etc.

Le poste de travail doit également permettre de déployer des applications et des dispositifs dans des serveurs et des postes de travail distants (qui deviennent actifs ou « en service »).

5.7 Poste de travail de maintenance

L'interface utilisateur de maintenance doit permettre à l'opérateur désigné d'accéder à tous les services, outils et menus de maintenance et de diagnostic du système de CCAD.

L'interface utilisateur de maintenance doit lui permettre d'accéder à toutes les fonctions associées aux autres interfaces utilisateurs, sauf à l'interface utilisateur d'administration.

L'interface utilisateur de maintenance doit intégrer des utilitaires pour visualiser en temps réel l'état et les valeurs opérationnelles des attributs de n'importe quel objet d'une application que gère la plateforme.

6 Enregistreur de données (dépôt de données historiques)

Le logiciel du système de CCAD doit intégrer une base de données relationnelles en temps réel (dépôt de données historiques) pour assurer le stockage de données opérationnelles à long terme. L'enregistreur de données doit permettre de stocker les données en temps réel et historiques de chaque nom d'étiquette, qu'il soit analogique, discret ou composé d'une chaîne de caractères. L'enregistreur de données doit également stocker des données de sommaire, d'événement, d'alarme et de configuration.

La base de données de l'enregistreur doit acquérir et stocker les données de traitement à pleine résolution. Elle doit intégrer les tables d'extensions normalisées des données en temps réel, ainsi qu'un jeu d'outils clients pour analyser les données et produire des rapports semblables à ceux qui ont été décrits dans les sections précédentes.

L'enregistreur de données doit pouvoir s'exécuter en mode autonome sans être connecté au système de CCAD ou être configuré par ce dernier. Malgré des contraintes physiques incontournables, comme l'espace disque disponible, il ne doit pas y avoir de limite quant à la quantité de données à stocker en ligne. De plus, la performance du système ne doit être affectée par le stockage à long terme des données. L'âge des données ne peut non plus affecter la vitesse de leur extraction. Ainsi, l'extraction des données enregistrées pendant deux heures voilà deux ans doit prendre autant de temps que si elles l'avaient été la veille.

L'enregistreur de données doit commencer automatiquement l'acquisition des données d'attribut du dispositif après que la configuration de ce dernier a été enregistrée dans la base de données.

6.1 Acquisition et analyses des données des postes de travail distants

L'enregistreur de données doit pouvoir être configuré dans un site distant pour acquérir localement des données. Il doit pouvoir transmettre ces données à un deuxième enregistreur dans une architecture de réseau hiérarchisée. Il doit être possible de stocker les données localement dans le site distant et de les analyser avec les outils clients du fabricant.

Le système doit permettre de regrouper des données et de les transmettre à un enregistreur de données de deuxième niveau en vue d'une analyse approfondie.

Le système doit permettre à plusieurs enregistreurs de données distants de transmettre leurs données, regroupées ou brutes, à un seul enregistreur de deuxième niveau, ou encore d'envoyer des données de même nature à plusieurs systèmes de deuxième niveau.

L'enregistreur doit accepter les données provenant d'un site distant déconnecté du réseau et dont la connexion est rétablie par la suite (augmentations fortes et subites du trafic IP). Les données doivent être stockées dans un système de collecte distant qui, une fois la connectivité du réseau rétablie, les achemine à l'enregistreur sans que l'opérateur n'intervienne dans le processus.

Le système doit permettre de configurer une architecture d'enregistreurs de données de manière à empêcher la perte de renseignements causée par une défaillance de la connexion au réseau.

6.1.1 Configuration des systèmes d'événements

L'enregistreur de données doit intégrer un sous-système qui surveille et enregistre les événements système ou issus de processus. Il doit également réagir à ces événements en déclenchant une action quelconque lorsqu'il les détecte. Cette détection survient lorsque l'événement remplit certains critères prédéfinis et configurables. L'enregistreur doit ensuite le consigner dans la base de données historiques et déclencher les actions désignées configurables en fonction de la nature de l'événement détecté. L'enregistreur doit consigner les attributs de l'événement, dont la date et l'heure où il s'est produit, ainsi que les critères auxquels cet événement satisfait.

6.2 Gestion du stockage sur disque

L'enregistreur de données ne doit pas nécessiter d'outils spécialisés pour assurer la gestion du stockage sur disque. Il doit permettre d'archiver et de récupérer des fichiers de données historiques au moyen des techniques de copie standard de Microsoft Windows. Il doit également permettre de récupérer certaines données archivées sans obliger l'utilisateur à extraire la totalité de l'archive.

L'enregistreur de données doit intégrer un mécanisme qui transfère automatiquement à un dispositif secondaire les fichiers en cours d'utilisation qui se trouvent sur un disque dont la capacité maximale est presque atteinte. Les fichiers et l'espace libre du dispositif secondaire doivent également être surveillés, de telle sorte que lorsque le plafond de capacité défini par le développeur d'applications est atteint, les fichiers les plus anciens sont supprimés automatiquement pour préserver l'intégrité du système. Les fichiers de données historiques ne doivent jamais être supprimés dans le dispositif de stockage principal si un dispositif secondaire approprié a été configuré.

7 Garantie, maintenance et soutien

Le fabricant doit offrir un programme de maintenance et de soutien de son logiciel pour faire en sorte que l'utilisateur puisse en profiter pleinement pour toute sa durée de vie utile. Le programme doit couvrir le logiciel par une garantie de base et inclure une garantie prolongée visant les besoins prioritaires et la distribution des mises à niveau disponibles. Un service téléphonique de soutien doit être accessible au moyen d'un numéro sans frais durant les heures normales de travail. Le fabricant doit également offrir le soutien par courriel ou sur un site Web prévu à cette fin.

7.1 Soutien de la garantie

Le fabricant du logiciel doit garantir son produit pendant 90 jours à compter de sa livraison. Au cours de cette période, le fabricant doit fournir gratuitement un service téléphonique de soutien durant les heures normales de travail. Le service doit être accessible en composant un numéro de téléphone sans frais. Le fabricant doit corriger rapidement tout défaut du logiciel.

7.2 Services prolongés de soutien et de maintenance du logiciel

Une fois écoulée la période de garantie de 90 jours, l'utilisateur doit continuer d'accéder au service de soutien par télécopieur, courriel ou site Web. L'utilisateur doit bénéficier en tout temps des dernières versions, du service de soutien et d'une garantie à long terme du logiciel offerts par le fabricant dans le cadre d'un programme prolongé à frais annuels fixes.

7.2.1 Mises à niveau du logiciel

Le programme de soutien prolongé du fabricant doit prévoir que l'utilisateur recevra les versions les plus récentes et les mises à niveau du logiciel de CCAD lorsqu'elles sont disponibles. Pour assurer la qualité de son soutien, le fabricant doit tenir à jour les licences d'utilisation visant la même version du logiciel. Si l'installation d'une mise à jour logicielle entraîne des incompatibilités avec des objets d'applications et des applications de l'IHM, le fabricant doit en dresser la liste puis élaborer un plan de développement adéquat pour les résoudre. Chacune des mises à niveau doit d'abord être mise à l'essai et approuvée avant son déploiement dans l'environnement de production.

Le programme de soutien doit prévoir l'accès à un site Web sécurisé où l'utilisateur peut télécharger sur un support de données (p. ex., un disque optique) les nouvelles versions du logiciel, les correctifs, individuels ou en trousse, et tout autre fichier de soutien connexe.

7.2.2 Soutien des correctifs des systèmes d'exploitation

Le fabricant doit faire l'essai et assurer le soutien des correctifs que publie Microsoft pour ses systèmes d'exploitation. Le fabricant doit avoir une politique établie en matière de soutien de tels correctifs de sécurité.

7.2.3 Service de soutien par téléphone

Le programme de soutien prolongé doit comprendre la prestation de services par téléphone durant les heures normales de travail. Ces services sont assurés par un technicien préposé au soutien technique possédant une certification du fabricant du logiciel obtenue en vertu d'un programme d'essais de soutien. Quelqu'un doit répondre en tout temps (24/7) aux demandes d'assistance et la durée des appels ne doit pas être limitée. Un système de soutien par boîte vocale n'est pas acceptable.

7.2.4 Service de soutien par courriel

Le programme de soutien prolongé doit inclure la prestation de services en une journée ouvrable ou moins lorsque la demande d'assistance a priorité sur celles des demandeurs qui ne sont pas couverts par une garantie de soutien du fabricant. Le courriel doit préciser les coordonnées du centre de soutien technique certifié le plus près. Le soutien électronique doit également inclure un accès élargi à une page Web de services techniques évolués. Le programme de soutien prolongé doit inclure l'accès en temps réel à une base de données de suivi des appels dans laquelle sont consignés les problèmes actuels et passés, et permettre également de créer de nouveaux dossiers de problème qui sont attribués sur-le-champ à un technicien préposé au soutien technique en vue de leur résolution.

7.2.5 Service de soutien par Internet

Le fabricant du logiciel doit avoir un site Web axé sur le soutien et le développement où le visiteur peut se renseigner sur le logiciel SCADA, connaître les pratiques exemplaires concernant sa mise en œuvre et consulter les forums des utilisateurs.

7.2.6 Bulletins et soutien technique

Au moins deux fois par année, le fabricant du logiciel doit fournir un bulletin et un média électronique contenant des notes techniques destinées à tous les utilisateurs couverts par le programme de garantie prolongée. Le support de données doit contenir un sommaire complet des notes techniques, des alertes techniques, des applications, des utilitaires d'application, des utilitaires de diagnostic, des pilotes, des scripts, des fonctions de script et des conseils utiles susceptibles de simplifier le travail du développeur d'applications.

7.3 Rétrocompatibilité du logiciel

Le fabricant du logiciel doit démontrer qu'il a assuré la rétrocompatibilité et fourni un chemin de migration ininterrompu de ses produits pendant au moins 10 ans afin de protéger l'investissement en ingénierie de ses clients. La migration des anciennes applications vers les versions les plus récentes du logiciel doit se faire facilement et sans modification de nature technique.