Recommandation de la branche pour le marché suisse de l'électricité

ICT Continuity

(Information & Communication Technology Continuity)

Recommandations pour assurer la disponibilité constante des technologies de l'informatique et des télécommunications dans le contexte de la continuité de l'approvisionnement

ICT-Cont, édition 2011

Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Impressum et contact

Editeur
Association des entreprises électriques suisses AES
Hintere Bahnhofstrasse 10, Case postale
CH-5001 Aarau
Tél. +41 62 825 25 25
Fax +41 62 825 25 26
info@strom.ch
www.strom.ch

Auteurs de la première édition 2011

Christian Angele	SGSW	DSV
Norbert Bachmann	Swissgrid/WL ICT-I	Swissgrid
Mattia Bardelli	AET	ESI
Reto Bondolfi	ewz/WL ICT-I	Regionalwerke
Jean-Michel Bovet	Romande Energie	Regiogrid
Lorenz Cairoli	EBM	Regionalwerke
Raymond Cettou	SIG	Swisspower
Nisheet Singh	Swissgrid	Swissgrid
Adrian Schwammberger	AEW/WL ICT-I	Regionalwerke
Peter Waldegger	Axpo	Swisselectric

Conseil et réalisation

Dr. Adrian Marti	AWK
Reto Büttner	AWK

AWK Group AG
Leutschenbachstrasse 45
Postfach, CH-8050 Zurich
Tél. +41 (44) 305 95 11
www.awk.ch

Soutien complémentaire par
Werner Meier, Alpiq / Chef WL ICT-I-Energie
Ruedi Rytz, BWL
Sandfire AG, Bruchmattstrasse 12, CH-6003 Lucerne

Direction de projet AES
Peter Betz, mandant
Jean-Michel Notz, chef de projet

Chronologie de la recommandation de la branche ICT Continuity

Février 2011	Entrée en fonction du groupe de travail ICT Continuity
Juillet 2011	Projet prêt pour la consultation
Eté 2011	Consultation de la branche
Septembre-novembre 2011	Révision selon consultation
7 décembre 2011	Approbation par le Comité de l'AES

Ce document est un document de la branche pour le marché de l'électricité

Imprimé n° 1025f. Edition 2011. (Édition française, le texte original en allemand fait foi en cas de contestation)

Abréviations et termes

Abréviation	Description
OFAE	Office fédéral pour l'approvisionnement économique du pays
LPD	Loi fédérale sur la protection des données (loi sur la protection des données)
ICT (TIC)	Technologie de l'information et de la communication
Crise	Comportement imprévu de l'approvisionnement en énergie électrique avec plus de 50 MWh d'énergie non fournie en temps voulu.
Perturbation	Comportement imprévu de l'approvisionnement en énergie électrique
SCADA	Télésurveillance et acquisition de données (Supervisory Control and Data Acquisition)
LApEl	Loi fédérale sur l'approvisionnement en électricité (loi sur l'approvisionnement en électricité)
END	Energie non-distribuée
AES	Association des entreprises électriques suisses

Documents de référence

Titre	Auteur/éditeur	Date [1]	Lien/fichier
[1] Analyse des risques, domaine infrastructure ICT, secteur énergie électrique	Office fédéral pour l'approvisionnement économique du pays	18 janvier 2011	
[2] Transmission Code 2010	Swissgrid	23 novembre 2009	http://www.strom.ch/uploads/media/TC_CH_2010_de_01.pdf
[3] Distribution Code Suisse	AES	2011	http://www.strom.ch/uploads/media/DC_CH_2011_F.pdf
[4] Guide de bonnes pratiques (2010)	Business Continuity Institute BCI	2010	www.thebci.org
[5] Recommandations en matière de Business Continuity Management (BCM)	Association suisse des banquiers SwissBanking	2007	http://www.swissbanking.org/11107_d.pdf
[6] Recommandation de la branche de l'asut en matière de Business Continuity Management (BCM)	Association suisse des télécommunications asut	2009	http://www.asut.ch/content/content_renderer.php?id=263&s=1&lan=1
[7] Spécification technique TS 62351-1. Power systems management and associated information exchange – Data and communications security (gestion des systèmes de puissance et échanges d'informations associés – sécurité des données et de l'information)	Commission électrotechnique internationale CEI	2007 - 5	http://webstore.iec.ch/preview/info_iec62351-1%7Bed1.0%7Den.pdf
[8] Treatment of Information Security for Electric Power Utilities (Traitement de la sécurité de l'information pour les compagnies d'électricité), Brochure Technique N°419	Cigré	Juin 2010	http://www.cigre.org/

[1] Ou l'édition la plus actuelle

Sommaire

Index des figures

Index des tableaux

Avant-propos

La loi sur l'approvisionnement en électricité (LApEl) du 23.03.2007 et l'ordonnance sur l'approvisionnement en électricité (OApEl) du 14.03.2008 et du 12.12.2008 ont ouvert le marché électrique suisse aux clients finaux dont la consommation annuelle est supérieure à 100 MWh par site de consommation. 5 ans après l'entrée en vigueur de cette loi, les consommateurs finaux dont la consommation annuelle est inférieure à 100 MWh par site de consommation doivent aussi pouvoir, sur décision du conseil fédéral, accéder au réseau de manière non discriminatoire. Cette décision peut faire l'objet d'un référendum.

Fidèle au principe de subsidiarité (LApEl, art. 3, al. 1), la branche a créé dans le cadre du projet Merkur Access II, grâce à des spécialistes un ouvrage extensif de règlements, ceci indépendamment des développements politiques. Cet ouvrage concerne l'approvisionnement en électricité dans le marché libre de l'électricité. Avec celui-ci, l'économie électrique dispose d'une recommandation de la branche traitant de l'utilisation des réseaux électriques et de l'organisation du commerce de l'énergie.

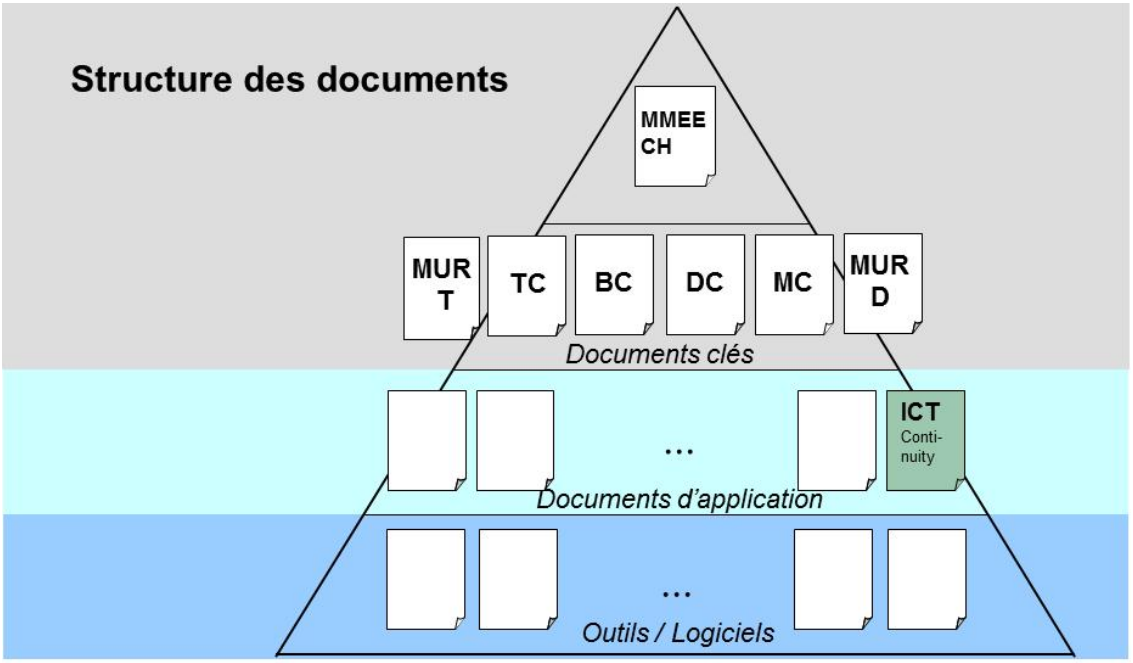
La LApEl et l'OApEl exigent la mise sur pied par les gestionnaires de réseau de directives pour divers faits matériels. Cette tâche a été remplie dans le cadre des documents de la branche. Les chapitres correspondants répartis dans divers documents sont indiqués au chapitre 7 du Modèle de marché pour le courant électrique - Suisse (MMEE).

Le modèle d'utilisation des réseaux de distribution (MURD – CH), le modèle d'utilisation des réseaux de transport (MURT – CH), le Transmission Code (TC – CH), le Balancing Concept (BC – CH), le Metering Code (MC – CH) et le Distribution Code (DC – CH) sont des documents clés.

En relation avec ces documents centraux, les documents d'application et divers «outils» sont élaborés par la branche.

Le présent document ICT Continuity est un document d'application.

Ni les documents de la branche ni les directives ne sont mentionnés dans la loi. En ce qui concerne les dispositions des documents de la branche qui font office de directives dans le sens de l'art. 27, al. 4 de l'OApEl, il s'agit là de normes d'autorégulation. En règle générale, les autorités et les tribunaux reprennent de cas en cas la solution proposée dans les directives de la branche sauf si elle s'avère inappropriée.
Les autres documents de la branche ont par principe un caractère contraignant pour les acteurs concernés dont le contrat mentionne ces documents de la branche comme partie intégrante du contrat (pour autant que les déclarations dans le contrat n'aillent pas à l'encontre de la législation sur l'approvisionnement en électricité). Il s'agit là de recommandations de la branche.



1. Résumé

(1) Le développement rapide des technologies de l'information et de la communication (TIC ou ICT) offre aux entreprises électriques des possibilités techniques insoupçonnées mais présente aussi de nouveaux défis et risques. Il est crucial pour la maîtrise d'évènements imprévus dans les systèmes en réseau que tous les acteurs importants agissent de manière coordonnée et que les propriétaires de systèmes de la branche définissent ensemble de manière préventive les dispositions nécessaires à la maîtrise d'évènements.

(2) Une norme minimale d'ICT Continuity Management (ICT-CM) est définie à cet effet dans la présente recommandation de la branche. Elle structure la stratégie ICT Continuity, l'analyse Business Impact, les plans ICT Continuity, les revues ICT Continuity, les tests ICT Continuity et les constantes améliorations. Cette norme minimale contient des analyses, des consignes et des instructions que chaque entreprise électrique doit formuler par écrit.

(3) Des recommandations d'action concrètes sont formulées pour les infrastructures critiques des entreprises électriques. Cette recommandation de la branche sert à la prévention de crises. Les infrastructures critiques d'ICT des entreprises électriques doivent être conçues de façon à ce que pour chaque évènement, il n'arrive quasi jamais que 50 MWh ou plus ne soient pas distribués en temps voulu (END énergie non-distribuée) [1].

(4) Cette recommandation de la branche vaut comme « Best Practice » pour les acteurs des niveaux de réseau 1 à 4. Les entreprises de la branche travaillant à des niveaux de réseau inférieurs sont tenues de mettre en œuvre cette recommandation autant que possible, conformément à leur implication dans le système. Voir aussi Figure 2, page 11.

(5) La Commission pour les questions juridiques de l'AES (REKO) souligne dans sa prise de position au sujet du présent document, que par le fait qu'il s'agit d'un document de la branche, son contenu constitue dorénavant une échelle que les autorités et tribunaux vont appliquer dans des cas concrets. Les gestionnaires de réseau seront donc bien inspirés d'appliquer toutes les mesures contenues dans ce document et de consigner ceci de manière accessible (mise en sûreté des preuves).

2. Situation initiale et objectifs

(1) Le développement rapide des technologies de l'information et de la communication (TIC ou ICT) offre aux entreprises électriques des possibilités techniques insoupçonnées, mais présente aussi de nouveaux défis et risques. A cause de l'interconnexion toujours plus forte au-delà du périmètre de l'entreprise et de la branche, une petite défaillance du système ou un évènement externe peuvent déjà conduire à l'effondrement des systèmes ICT, avec de sérieuses conséquences. La centralisation de plus en plus importante des systèmes de gestion augmente l'étendue des dommages en cas de perturbations dans ces systèmes.

(2) Les développements techniques actuels de l'infrastructure d'approvisionnement en électricité sont fortement marqués par l'interconnexion et la conduite de la production d'électricité, du stockage, des consommateurs électriques et des équipements d'exploitation dans les réseaux de transport et de distribution d'électricité. La création de réseaux électriques intelligents (en anglais Smart Grids) conduit à de nouvelles vulnérabilités des entreprises électriques, engendrées par exemple par:

- la communication bidirectionnelle avec des terminaux (Smart Meters)
- des systèmes de contrôle-commande associés à des zones de réseau toujours plus grandes
- la faible authentification des utilisateurs des systèmes de contrôle-commande
- une formation insuffisante des collaborateurs

(3) L'introduction sans cesse croissante d'infrastructures permettant la connexion à un réseau informatique et la télémaintenance augmente les possibilités d'attaques de l'extérieur, p. ex. par des pirates informatiques.

(4) Il faut aussi s'attendre à une importance grandissante du problème de la protection des données[2], amplifiée par une production toujours plus importante de données de clients, tout particulièrement dans le domaine du Smart Metering.

(5) La sécurité impérativement élevée des systèmes de contrôle-commande modernes est obtenue par:

- un concept de sécurité intégré et global
- des domaines de sécurité clairement définis et séparés (Security Domain Model)
- une stratégie de défense à plusieurs niveaux (prévenir, déceler, défendre et restaurer)
- une normalisation (n'utiliser que des technologies soigneusement testées et adaptées à l'approvisionnement en électricité)
- la mise en place d'une formation et d'une culture de la sécurité crédibles et vécues par le management.

(6) Il est crucial pour la maîtrise des perturbations imprévues dans les systèmes en réseau que tous les acteurs importants agissent de manière coordonnée et que les dispositions nécessaires soient préalablement définies.

(7) Le but de cette recommandation est de créer les conditions-cadre pour combattre les interruptions de l'activité de l'entreprise, protéger les processus critiques des répercussions de pannes importantes de l'infrastructure ICT et assurer leur continuité. Le processus le plus important et le plus critique des entreprises électriques est l'approvisionnement des clients en énergie électrique. La sécurité du personnel d'exploitation et d'entretien ainsi que des tiers doit toujours être assurée.

(8) Cette recommandation doit servir de base pour les planifications correspondantes et pour les préparatifs nécessaires à la maîtrise des perturbations ICT de manière à éviter ou du moins à diminuer les répercussions négatives sur la sécurité de l'approvisionnement.

(9) La recommandation de la branche se veut indépendante de l'état actuel de la technique, car celle-ci évolue rapidement. L'utilisation de la recommandation de la branche doit être adaptée individuellement à chaque entreprise. Une aide pour la mise en œuvre concrète de la recommandation de la branche se trouve au chapitre 8 «Autre bibliographie».

[2] Voir LApEI, art 10 et LPD

3. Champ d'application

(1) La présente autorégulation de l'AES s'adresse aux gestionnaires de réseaux. Les propriétaires et exploitants des niveaux de réseau 1 à 4 (voir chapitre 4.2 et Figure 2) sont tout particulièrement concernés. Cette recommandation est appliquée par la branche en tant que « Best Practice », spécifiquement pour les niveaux de réseau 1 à 4.

(2) Les membres de la branche qui se situent à des niveaux de réseau inférieurs sont tenus de mettre en œuvre cette recommandation, partout où cela est possible, de façon adaptée à leurs niveaux de réseau. Les gestionnaires des niveaux de réseau 5 à 7 doivent s'assurer qu'ils n'occasionnent pas de perturbation sur des niveaux de réseau supérieurs par le biais des systèmes de contrôle-commande interconnectés.

(3) Les niveaux de réseau inférieurs doivent tout particulièrement tenir compte de la protection des données.

(4) Cette autorégulation contient des recommandations («Best Practice») pour la mise en place d'un ICT Continuity Management spécifique à l'entreprise. Il faut en outre respecter les spécificités de chaque situation initiale, en particulier de la situation des risques de chaque entreprise.

4. Intégration

4.1. Structure des documents AES

(1) La présente recommandation de la branche est intégrée à titre de document d'application dans la structure des documents AES destinée au marché suisse de l'électricité.

(2) Le TC (Transmission Code) et le DC (Distribution Code) contiennent les règles techniques pour une exploitation de réseau et de système sûre. La présente recommandation est intégrée au niveau des documents d'application. Voir aussi l'avant-propos de ce document.

4.2. Définition d'un évènement important (crise)

(1) Pour le réseau de transport, les événements qui doivent être annoncés sont définis (Transmission Code [2] et Manuel de gestion opérationnelle de Swissgrid).

(2) Pour le réseau de distribution, le Distribution Code Suisse [3] fixe, aux chapitres 2.2.3 et 3.5 « Qualité du réseau » chiffre (6), la valeur-cible de 4 heures maximum d'interruption de l'approvisionnement par évènement chez un consommateur final pour les réseaux urbains avec plus de 10 000 raccordements. De telles interruptions d'approvisionnement ne doivent se produire que très rarement comme décrit [3] au chapitre 3.5 qualité du réseau chiffre (7) par les indicateurs SAIFI et SAIDI.

(3) C'est pourquoi une telle défaillance touchant plus de 10 000 raccordements pendant plus de 4 heures est définie comme une crise. Pour une puissance moyenne estimée à 1250 W par raccordement (sans gros consommateur), elle correspond à une puissance de défaillance de 12,5 MW et à une énergie non-distribuée (END) de 50 MWh.

(4) Dans le Distribution Code [3] chapitre 2.2.3 et 3.5 les valeurs-cibles sont limitées aux évènements internes à un réseau de distribution. Les évènements de très faible probabilité sont exclus, comme par exemple le délestage lié à la fréquence, les catastrophes naturelles ou le terrorisme.

(5) Aucune durée de défaillance admissible n'est quantifiée dans le Transmission Code [2].

(6) Il n'existe par conséquent aucune consigne concernant la fréquence admissible de défaillances dues à de tels évènements.

4.3. Sécurité de l'information, modèle de domaines

(1) Le haut degré de sécurité nécessaire aux systèmes de contrôle-commande modernes est obtenu par la définition de domaines de sécurité clairs et séparés (Security Domain Model).

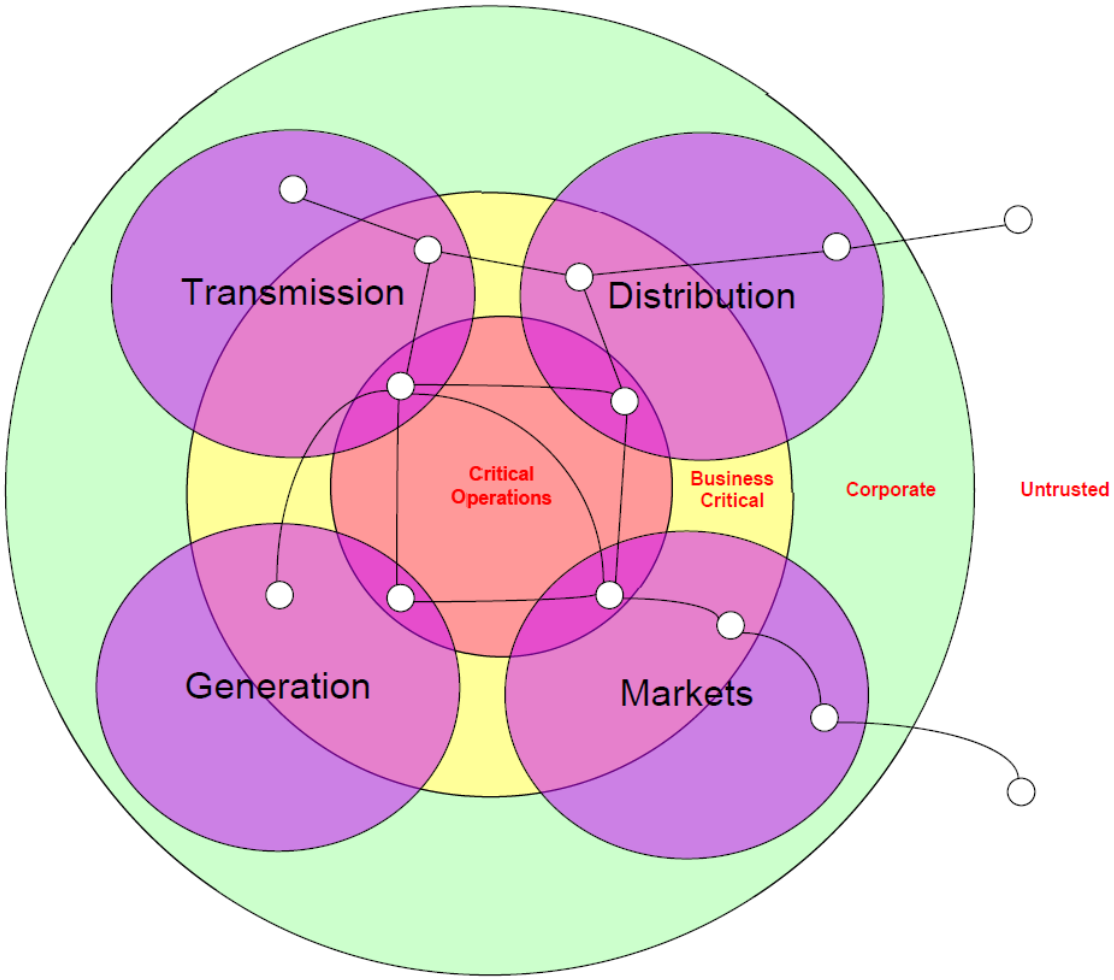


Figure 1: Sécurité de l'information, modèle de domaines (de [8])

Niveau de protection (relatif à l'exploitation)	Domaines	Couleur dans la Figure 1	Exemples
bas	ouvert (non fiable)	blanc	fournisseur/fabriquant, réseaux de tiers, Internet
moyen	confidentiel (entreprise)	vert	bureau ICT (général)
haut	critique pour les affaires (Business Critical)	jaune	bureau ICT (finances et personnel)
très haut	critique pour l'exploitation (Critical Operations)	rouge	processus ICT

Tableau 1: Aperçu des niveaux de protection

4.4. Niveaux de réseau importants

(1) Les niveaux de réseau importants peuvent être déduits du chapitre 4.2 Définition d'un évènement important (crise).

- Des perturbations dans les niveaux de réseau 1 à 4 peuvent conduire à une crise avec une quantité d'énergie non-distribuée (END) de plus de 50 MWh. De telles perturbations doivent être maîtrisées conformément à leur niveau.
- Les niveaux de réseau 5 à 7 sont concernés dans la mesure où il faut s'assurer qu'ils ne sont pas la cause de perturbations dans les niveaux de réseau supérieurs. Les systèmes de contrôle-commande interconnectés doivent notamment être pris en compte avec le danger de propagation d'un virus ou d'une attaque de pirates informatiques.

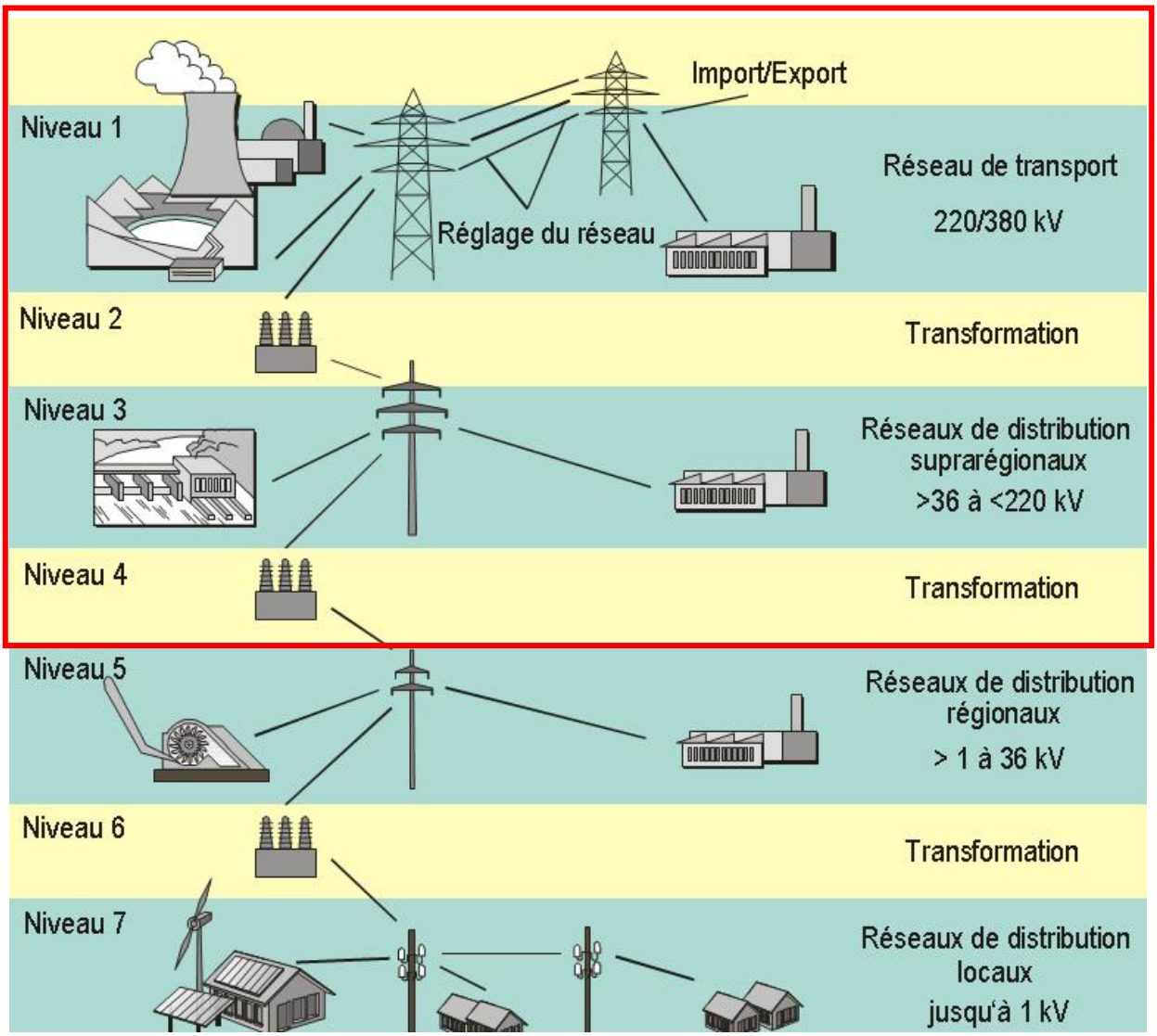


Figure 2: Niveaux de réseau importants

4.5. Relation avec l'analyse des risques du domaine infrastructure ICT du secteur Energie de l'approvisionnement économique du pays

(1) L'analyse des risques [1] constitue une base importante pour la présente recommandation de la branche. L'analyse confirme que les dommages potentiels sont plus élevés dans les réseaux de transport, car à cet endroit, les instabilités peuvent se propager sur de grands territoires.

(2) Six risques critiques ont été identifiés dans l'analyse des risques [1]. Ces six risques critiques reflètent la topologie actuelle des systèmes de contrôle-commande des entreprises électriques (voir Figure 3):

- Défaillance du système central de gestion du réseau / technique de conduite du réseau (SCADA)
- Défaillance d'une application critique de la conduite du réseau
- Défaillance du centre de calcul
- Défaillance des télécommunications et de l'infrastructure
- Défaillance des contrôle-commande des postes et centrales

(3) Etant donné que les probabilités estimées d'occurrence des risques ne permettent pas de déterminer le point de départ de l'évènement, une gestion active des risques identifiés est nécessaire.

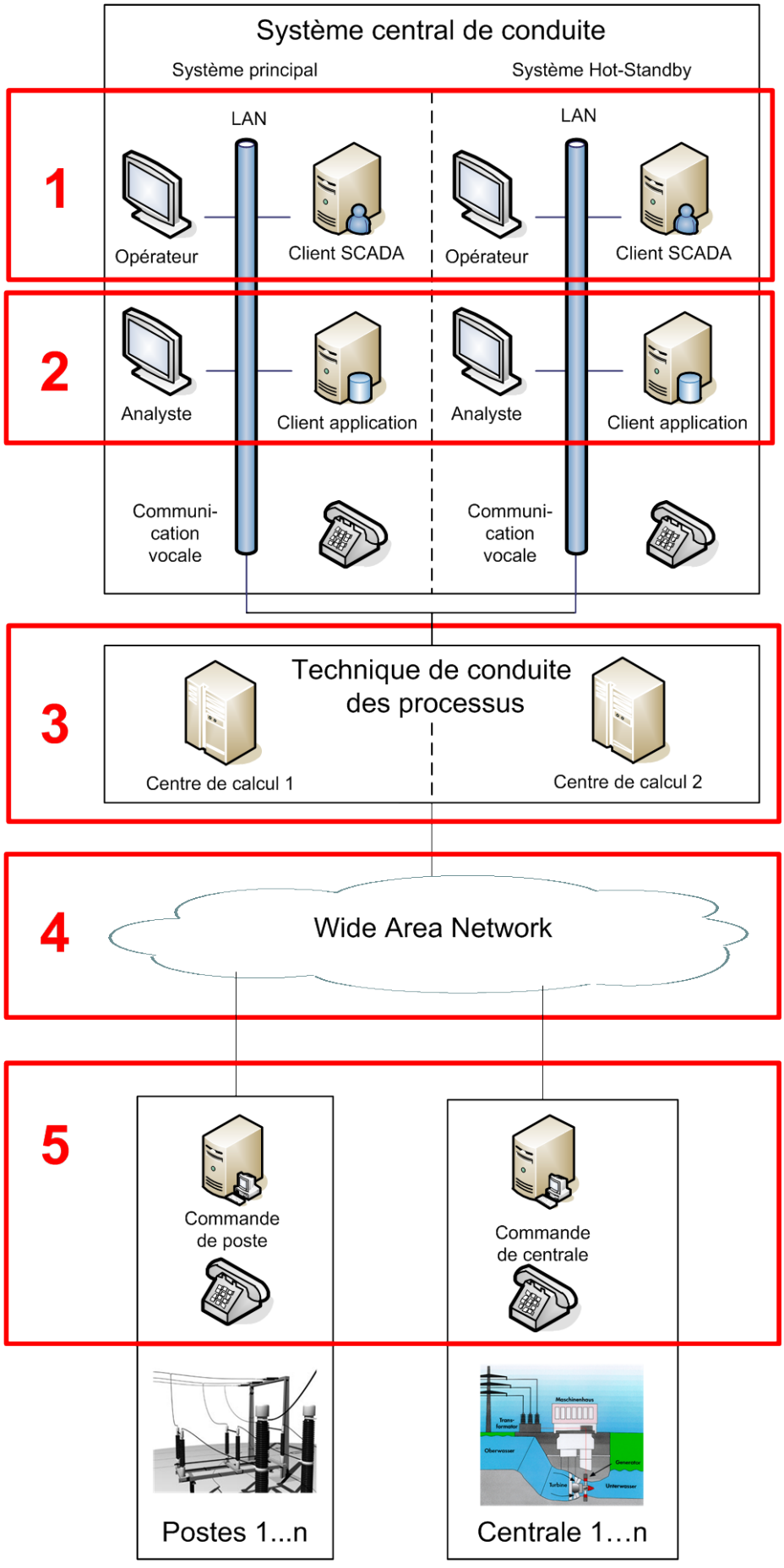


Figure 3: Infrastructures critiques dans le contrôle-commande, la communication de données et la communication vocale

5. Domaines d'application/scénarios

(1) Les entreprises électriques ont toutes des scénarios potentiellement importants à prendre en compte qui pourraient conduire l'entreprise ou la branche à une crise. Comme défini au chapitre 4.2, on entend par «crise» un comportement non planifié de l'approvisionnement en énergie électrique impliquant plus de 50 MWh d'énergie non livrée en temps voulu. La maîtrise de plus petites «perturbations» de moins de 50 MWh d'énergie non livrée en temps voulu ne fait pas l'objet de cette recommandation.

(2) L'apparition de crises peut avoir différentes origines.

(3) Des causes involontaires de situations de crise peuvent être par exemple:

- des évènements «accidentels» tels qu'un incendie ou une explosion
- des catastrophes naturelles, comme p. ex. une inondation ou un tremblement de terre
- une négligence du personnel d'exploitation
- une défaillance du personnel, p. ex. due à une pandémie
- une défaillance de la domotique et/ou de l'approvisionnement en énergie (p. ex. électricité)
- une panne de systèmes ou d'infrastructures IT (erreur de matériel ou de logiciel)
- une défaillance des systèmes de communication ou des fournisseurs de télécommunication
- une défaillance des fournisseurs externes (cf. Outsourcing/Cloud Computing) comme p. ex. fournisseur d'informations.

(4) Des causes intentionnelles de situations de crise peuvent être par exemple:

- des collaborateurs fâchés
- le vandalisme
- l'espionnage industriel, les attaques terroristes ou le sabotage (explosif ou vandalisme)
- des attaques sur le Net - Cyber Attac (p. ex. virus ou piratage informatique)

(5) Il est du devoir de chaque entreprise d'identifier ses situations de menace spécifiques dans le cadre de l'ICT Continuity Management. Les risques identifiés (scénarios) et l'analyse Business Impact servent de base commune pour élaborer les plans d'ICT Continuity (voir point 6.3).

(6) Les évènements qui surviennent peuvent par exemple avoir pour conséquence que les collaborateurs/collaboratrices et/ou les infrastructures (en particulier l'infrastructure de conduite, les télécommunications, les bâtiments ou les places de travail) ne sont plus opérationnels pour les fonctions critiques de l'entreprise. De la même manière, des problèmes avec les services informatiques ou les fournisseurs d'infrastructure peuvent conduire à des défaillances d'approvisionnement intolérables. Une attention particulière doit être prêtée aux réactions en chaîne et aux dépendances réciproques, telle que la défaillance des télécommunications nécessaires au rétablissement de l'approvisionnement en électricité due à une panne de courant.

(7) L'ICT Continuity Management doit assurer même en cas de crise le respect des prescriptions légales, régulatoires, contractuelles et internes.

6. Recommandations: Norme minimale ICT Continuity Management (ICT-CM)

Remarques préalables

(1) Au début de l'introduction d'un ICT Continuity Management, un domaine (Scope) et une ligne directrice (Policy) doivent être définis puis approuvés par la direction de l'entreprise. Cette ligne directrice décrit les piliers de l'ICT Continuity Management et expose le mandat de la direction de l'entreprise pour la mise en œuvre. Dans le cadre de la gestion du programme, les budgets et les ressources humaines sont aussi mis à disposition pour l'introduction et le maintien de l'ICT Continuity Management. La direction doit nommer un responsable pour l'élaboration et la mise en œuvre de la ligne directrice ainsi qu'un ou plusieurs responsables pour l'introduction des mesures nécessaires.

(2) Pour s'assurer l'intégration de l'ICT Continuity Management dans la culture de l'entreprise, les collaborateurs concernés sont accompagnés dans toutes les phases du cycle par le biais de formations et de mesures renforçant leur prise de conscience. Ces mesures ont pour but de stimuler l'acquisition des connaissances et l'acceptation de ce management.

(3) Au cours de la première phase, les exigences posées par un Business Continuity Management (BCM) à l'informatique sont mises en évidence. Les différents départements ont calculé le temps d'interruption maximal tolérable pour leurs applications et leurs systèmes. Sur cette base, les priorités et le temps pour le remplacement sont définis dans le cadre de l'ICT Continuity. Puis un ajustage est effectué entre la situation réelle et la situation visée par le biais des mesures déjà en place de l'ICT Continuity (analyse de l'écart). Lors de cette analyse, aussi bien les mesures techniques que celles d'ordre organisationnel sont prises en considération, comme par exemple: quels sont les collaborateurs avec les connaissances correspondantes pour les équipes d'ICT Continuity et quelles sont les mesures visant à augmenter la disponibilité des applications et des systèmes.

(4) Il existe un large spectre d'agresseurs potentiels qui connaissent à la perfection les technologies de transmission et de distribution, ainsi que celles de gestion et de contrôle des réseaux de transport et de distribution, et cela avec les méthodes d'intrusion correspondantes. Des erreurs de fonctionnement des logiciels peuvent être à l'origine de ces points faibles donnant lieu à des comportements erronés imprévus, tout comme des défauts du matériel ou des pannes de réseaux informatiques.

6.1. Analyse de Business Impact

(1) Chaque entreprise détermine ses ressources et ses processus critiques. Une analyse de Business Impact doit être réalisée sur la base des scénarios définis dans la phase stratégique. Chacune des répercussions sur les processus critiques des affaires y est évaluée lorsque ces scénarios surviennent.

(2) Cette évaluation inclut aussi les dépendances réciproques entre les secteurs d'activité (processus en amont et en aval) et les dépendances de fournisseurs externes (Outsourcing).

(3) L'analyse des risques [1] a été réalisée en mettant l'accent sur les défaillances importantes du point de vue de l'économie nationale. Les infrastructures critiques (ressources) y sont identifiées. Ceci doit servir de point de départ pour l'analyse de Business Impact spécifique à l'entreprise. Pour garantir l'ICT-Continuity, l'accent est mis sur la technique de l'information et de la communication de l'entreprise.

(4) L'analyse de Business Impact doit avoir au moins pour résultat:

- l'identification des processus et des processus auxiliaires qui jouent un rôle clé dans la production des prestations de l'entreprise.
- le laps de temps maximal tolérable jusqu'à la restauration des processus d'affaire critiques.

- l'envergure minimale des ressources (de remplacement) (bâtiments, collaborateurs, IT/données, fournisseurs externes) qui doivent être disponibles en cas de crise pour atteindre le degré de restauration souhaité.

(5) Dans le cadre de la réalisation d'une analyse de Business Impact, les exigences d'intégrité et de confidentialité des processus sont souvent recensées conjointement à leur disponibilité.

(6) La fréquence à laquelle l'analyse de Business Impact est actualisée dépend de la situation de risque de chaque entreprise.

6.2. Stratégie ICT Continuity

(1) La stratégie ICT Continuity fixe les principes de base avec lesquels l'entreprise veut atteindre les objectifs de restauration définis dans son analyse de Business Impact. Les scénarios importants exposés sur lesquels la planification repose doivent aussi intervenir dans le cadre de la définition de la stratégie.

(2) Cette stratégie doit exister sous forme écrite.

(3) Les menaces qui ressortent particulièrement des processus critiques qui mettent à disposition les prestations essentielles pour notre société doivent être prises en considération globalement et de manière réaliste.

(4) Le but doit être que les mises en danger spécifiques à l'IT ne se répercutent pas négativement sur les processus télécommandés. Pour les systèmes existants, il faut opter pour la meilleure sécurité possible. Des critères de sécurité supplémentaires devraient être si possible implémentés surtout pour les nouveaux systèmes, en vue de réduire encore davantage les risques au niveau de la technique d'information. Les nouvelles solutions implémentées ne doivent pas être à l'origine de nouveaux risques ou de défauts dans les systèmes.

6.3. Plans d'ICT Continuity

(1) Un résultat de l'analyse de Business Impact est l'identification des processus et des processus auxiliaires qui jouent un rôle clé dans la fourniture des prestations de l'entreprise. En cas de crise, la restauration de la capacité de fonctionnement des systèmes ICT pour l'exécution des processus critiques pour les affaires est hautement prioritaire du point de vue d'ICT-Continuity.

(2) Des plans d'ICT-Continuity décrivant les démarches nécessaires à la restauration doivent être établis pour les systèmes ICT identifiés comme critiques pour les affaires.

(3) Les plans correspondants doivent contenir au moins:

- la description du cas d'utilisation (scénario déclencheur)
- la démarche ou le catalogue de mesures avec les priorités et les ressources de remplacement nécessaires.
- l'organisation de crise avec les responsabilités et les compétences.

(4) Il faut fixer des intervalles de temps réguliers dans lesquels les plans d'ICT Continuity doivent être actualisés. Des changements significatifs dans l'architecture IT ou dans l'activité de l'exploitation peuvent aussi nécessiter une révision des plans.

6.4. Rapports d'ICT Continuity

(1) Les rapports d'ICT Continuity comportent un inventaire des documents de planification importants et une évaluation permettant de savoir si les documents correspondent aux critères de vérification définis. Il est conseillé de définir des critères de vérification cohérents et des processus clairs pour le contrôle et la correction des points en suspens.

6.5. Tests d'ICT Continuity

(1) Les tests d'ICT Continuity vérifient la mise en œuvre de la planification et l'efficacité de l'organisation de gestion de crises. Les thèmes centraux et la périodicité de chacun des tests doivent être fixés en fonction de l'évaluation des risques (cf. analyse de Business Impact). Les tests réalisés doivent être proches de la réalité et adaptés à la situation des risques. La capacité de l'entreprise à maîtriser les situations de crise peut être améliorée par le rassemblement des résultats des tests et en particulier par des tests coordonnés des détenteurs de processus et des responsables ICT.

(2) Il est recommandé de coordonner chaque activité de test au moyen d'une planification systématique des tests, de régler l'établissement des rapports de manière homogène et de définir un processus de contrôle et de correction des points faibles. La norme ISO 27002 donne de précieuses indications sur les domaines potentiels à protéger et à tester.

(3) Un plan d'exercice pratique et de test doit être élaboré et approuvé par la direction de l'entreprise. Outre la précision correcte concernant la documentation, il est fortement recommandé de documenter les risques potentiels de l'exécution déjà lors de la planification et de les communiquer à la direction. La question est donc entre autres de savoir ce qui s'est passé durant l'exercice pratique et comment les participants y sont préparés. Des risques peuvent être par exemple évités lors de la réalisation du test en utilisant un contexte isolé et un backup des données.

(4) Les exercices et les tests prévus doivent être réalisés en collaboration avec les départements. Lors de chaque exercice, les objectifs doivent être fixés et vérifiés pour chaque département ainsi que pour l'ICT Continuity Management. Le test concernant les ressources techniques – indépendamment des exercices des départements – est simplement recommandé comme mesure de soutien. Comme pour d'autres standards (par exemple BS 25999, BSI 100-4), il est recommandé d'augmenter avec le temps le degré de difficulté et la complexité des exercices: du test écrit au test physique live de toute la chaîne d'une application en tenant compte de toutes les ressources et de tous les utilisateurs. Une fois que les exigences minimales d'un test, nommé ici tests d'ICT Continuity, sont définies, vient la phase des indications «standard» pour la réalisation du test. Après cette phase, les contenus minimaux font l'objet d'un rapport qui est envoyé à la personne ayant demandé l'exercice.

(5) Afin de garantir la mise à jour régulière de tous les documents de l'ICT Continuity, il est primordial que les mesures pour la gestion des changements et le contrôle de tous les documents et notes importants pour le management de l'ICT Continuity soient standardisés. Pour faire le point sur l'ICT Continuity Management, il est recommandé de prévoir des exigences semblables au BS 25999 pour le BCM. A titre d'exemple, il faudrait introduire ces passages:

- **Input**: niveau service interne, résultats des audits importants, stade d'application des mesures préventives et correctives.
- **Output**: adaptation des exigences au niveau du budget, le cas échéant, adapter le scope, mesures pour adapter la stratégie ou la procédure.

(6) Il est fortement recommandé d'effectuer des tests d'intrusion SCADA. Pour réaliser de tels tests correspondant aux attentes du donneur d'ordre, il faut que les buts soient convenus de manière claire. Si les buts poursuivis ne peuvent pas être atteints de manière efficiente, la personne qui teste devrait le mentionner durant la phase préparatoire et recommander des processus alternatifs comme une révision informatique ou un conseil en matière de sécurité informatique. Les objectifs qui peuvent être atteints lors d'un test d'intrusion SCADA peuvent être répartis en 4 groupes:

- renforcement de la sécurité des systèmes techniques
- identification des points faibles
- confirmation de la sécurité informatique par une tierce personne externe
- renforcement de la sécurité organisationnelle et personnelle de l'infrastructure

(7) Les résultats d'un test d'intrusion IT ne devraient pas seulement contenir une liste des points faibles, mais également des propositions de solutions concrètes pour y remédier.

(8) Dans le cadre d'un test d'intrusion SCADA, les mesures de sécurité informatiques logiques, comme par exemple les mots de passe, devraient être vérifiées, tout comme les mesures physiques telles que les systèmes de contrôle d'accès. Il arrive fréquemment que seules les mesures de sécurité logiques fassent l'objet d'une vérification car la majeure partie peut être testée à distance par le biais du réseau informatique ce qui demande moins de travail. D'autre part, la probabilité d'attaques sur des mesures de sécurité informatiques logiques est considérée comme bien plus élevée.

6.6. Amélioration continue

(1) L'ICT Continuity Management est un processus itératif. Les résultats des exercices et des tests effectués, mais aussi l'évaluation des évènements importants doivent servir à l'amélioration continue de l'ICT Continuity Management.

(2) Les mesures suivantes peuvent contribuer à cette amélioration:

- Mise en place d'une banque de données nationale protégée concernant la vulnérabilité dont les informations sont régulièrement transmises aux gestionnaires des niveaux de réseau 1 à 4. La banque de données comprend des informations visant à reconnaître, repousser et traiter les menaces de composants qui sont utilisés dans les infrastructures et les processus critiques des réseaux électriques de transport et de distribution suisses. Pour la mise sur pied de la banque de données, il est recommandé de s'accorder avec les offices de surveillance et les autorités de sécurité.
- Etablissement d'un rapport national de situation ENERGIE, comme instrument de conduite, avec interfaces vers les plateformes et outils d'échange d'informations importants pour la sécurité informatique (par exemple MELANI, centrale d'enregistrement et d'analyse de la sûreté de l'information qui publie un rapport de situation), ainsi que vers les nouvelles initiatives (par ex. stratégie de défense nationale cybernétique).
- Incitations économiques pour le développement national des technologies stratégiques et techniques, afin d'empêcher tout «inconnu» d'avoir accès aux structures et aux systèmes, ainsi que mise sur pied d'une banque de données normatives d'équipements – basée sur la banque de données concernant la vulnérabilité (« label de qualité » en matière de sécurité informatique).

7. Recommandations d'action pour la mise en œuvre de la norme minimale ICT-CM

7.1. Introduction

(1) Les recommandations d'action sont structurées en fonction des risques critiques identifiés au chapitre 4.5, Figure 3. Elles sont formulées de manière adaptées pour différentes infrastructures.

(2) Les infrastructures critiques des entreprises électriques doivent être protégées contre les pannes selon les définitions du chapitre 4.2.

(3) Au niveau national, cela signifie un laps de temps maximal de 25 secondes sans surveillance pour une puissance d'environ 7 GW. La disponibilité conforme au niveau de réseau peut être résolue par une redondance correspondante (systèmes de secours).

(4) Pour un réseau de distribution d'une puissance de 500 MW par exemple, le laps de temps sans surveillance se monte à 6 minutes et pour une seul poste d'une puissance par exemple de 50 MW, il est au maximum d'une heure. Plus la puissance raccordée est faible, plus les mesures non techniques sont adéquates (recours à du personnel) pour remédier aux perturbations.

(5) Comme mentionné au chapitre 4.3, la création de domaines de sécurité séparés par des interfaces contrôlées est un concept possible pour la sécurisation des infrastructures critiques des entreprises électriques.

(6) L'ensemble de l'infrastructure ICT et les systèmes ICT doivent présenter un temps d'autonomie adapté à chaque niveau de réseau, en particulier aux niveaux 1 à 4, cela en exploitation tant normale que perturbée du réseau électrique.

(7) Les applications critiques doivent être exploitées sur des infrastructures ICT et des systèmes ICT propres.

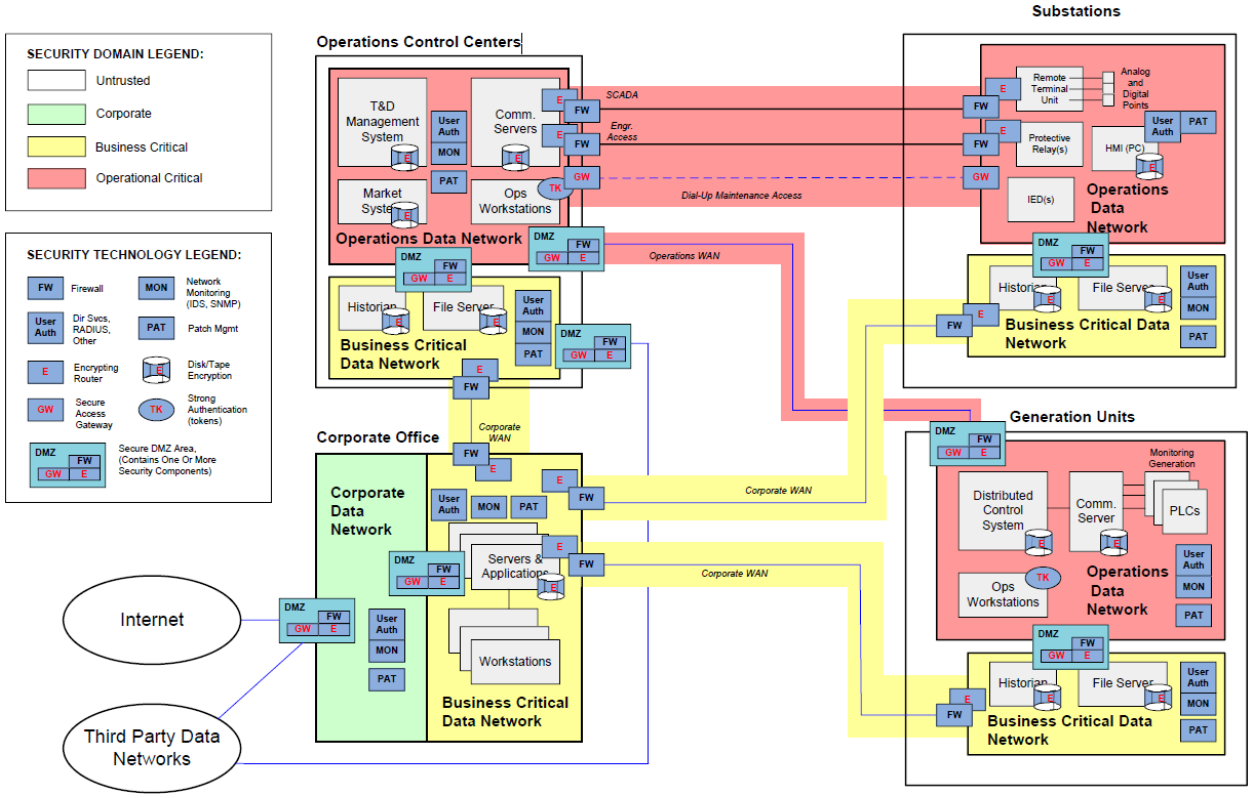


Figure 4: Exemple ICT axé sur la sécurité, création de domaines de sécurité (source [8])

(8) Afin de conserver leur capacité de fonctionnement, la fiabilité et la sécurité (intégrité) des éléments ou composants qui ont été installés par le passé sans que les entreprises en aient pris conscience, doivent être examinés et évalués de manière suffisante.

(9) Les menaces spécifiques à l'informatique ne doivent pas se répercuter négativement sur les processus télécommandés. Pour les systèmes existants, il faut opter pour la meilleure sécurité possible. Des critères de sécurité supplémentaires devraient être implémentés dans les nouveaux systèmes afin de diminuer encore les risques au niveau de la technique d'information. Les nouvelles solutions implémentées ne doivent cependant pas être à l'origine de nouveaux risques ou de défauts dans les systèmes.

(10) Il faut en outre tenir compte des points suivants:

a. Si possible pas d'accès externe (par ex. internet, intranet, maintenance) au réseau de contrôle des processus.

b. Les accès externes inévitables doivent être accordés de manière extrêmement restrictive et bien surveillés, compte tenu de la protection nécessaire très élevée des systèmes de contrôle des processus.

c. Limitation technique du trafic sur le réseau informatique dans la proportion nécessaire aux systèmes de contrôle; forte segmentation des réseaux de contrôle (par exemple par des portails spécifiques de sécurité (murs pare-feu - firewalls)); management restrictif des relations de communication autorisées.

d. Les systèmes et composants de contrôle des processus devraient:

- posséder seulement les caractéristiques de performance nécessaires à l'exploitation (surtout pas de fonctionnalités présentant un risque pour le contrôle des processus)
- être robustes par rapport aux perturbations et attaques
- disposer de mécanismes d'authentification fiables et spécifiques au système

e). Disponibilité à long terme de pièces de rechange, mises à jour et maintenance du système – en fonction de la durée de vie de l'infrastructure des processus; possibilité de migration aussi ouvertes que possible.

f). Possibilités d'intégrer les rajouts [patches] nécessaires (ce qui représente souvent un réel défi, en particulier pour les systèmes soumis aux exigences 24/7/365); la disponibilité rapide de patches de sécurité testés devrait être un des critères pour le choix du fabricant de la technique de conduite des processus.

7.2. Système central de conduite du réseau / technique de conduite (SCADA)

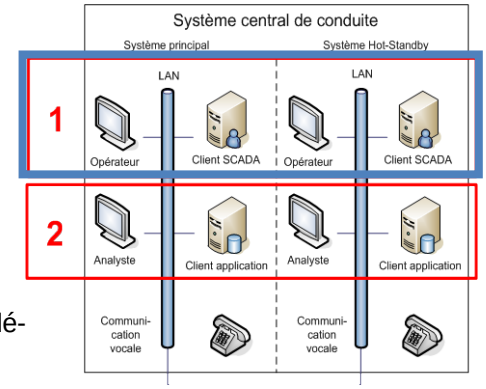
7.2.1. Directive quantifiée

(1) L'énergie non-distribuée (END) ne doit pas dépasser 50 MWh par évènement au niveau du système central de conduite du réseau électrique / de la technique de conduite (SCADA).

7.2.2. Recommandation

(1) Le système central de conduite du réseau électrique doit être conçu fonctionnellement de manière totalement redondante. Le système redondant doit être placé dans un lieu géographiquement distinct.

(2) Un système central de conduite du réseau / de technique de conduite (SCADA) avec peu d'ouvrages contrôlés peut avoir recours à des mesures alternatives (p. ex. faible éloignement, acheminement d'alarmes vers d'autres sites décentralisés ou commande locale rapide sur site).



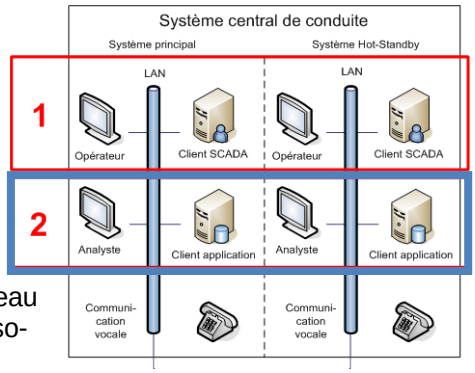
7.3. Applications critiques de conduite du réseau

7.3.1. Directive quantifiée

(1) L'END non analysée par des applications critiques de conduite du réseau (p. ex. sans calcul possible de sécurité (n-1)) ne doit pas dépasser 50 MWh par évènement.

7.3.2. Recommandation

(1) La disponibilité des applications critiques de conduite du réseau doit être conçue selon les exigences correspondantes. Des solutions de rechange manuelles doivent en outre être disponibles.



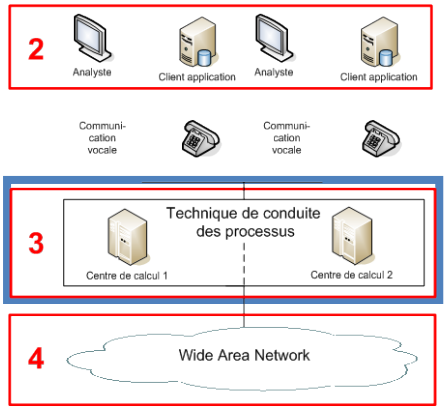
7.4. Centres de calcul

7.4.1. Directive quantifiée

(1) L'END au niveau des centres de calcul ne doit pas dépasser 50 MWh par évènement.

7.4.2. Recommandation

(1) Les centres de calcul doivent fonctionner de manière totalement redondante et, dans la mesure du possible, être placés dans deux locaux différents du site. S'il y a peu d'ouvrages contrôlés, des mesures alternatives adéquates peuvent être mises en œuvre.



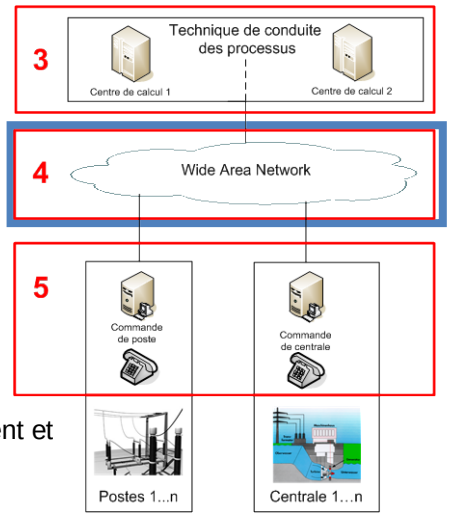
7.5. Technique de télécommunication et infrastructure

7.5.1. Directive quantifiée

(1) L'END au niveau technique de télécommunication et infrastructure ne doit pas dépasser 50 MWh par évènement.

7.5.2. Recommandation

(1) Toutes les centrales et tous les postes des niveaux de réseau 1 à 4 doivent être reliés physiquement de manière redondante par des tracés de télécommunication séparés. Le processus ICT (SCADA) doit être séparé au moins logiquement et



encore mieux physiquement de l'ICT bureautique[3] et des ICT [4] commerciaux. Il ne doit y avoir que des interfaces contrôlées (p. ex. par des pare-feu) entre les différentes utilisations ICT. Les accès au réseau informatique doivent être pourvus de mesures de sécurité correspondant à l'état actuel de la technique (p. ex. authentification et cryptage).

(2) Une communication vocale sécurisée conforme au niveau (réseau téléphonique des entreprises électriques, téléphone rouge, radiocommunication à usage professionnel) doit être disponible. Toutes les voies de communication doivent disposer d'un autocontrôle approprié (Watch Dog) de manière à ce qu'une interruption soit immédiatement identifiée et réparée.

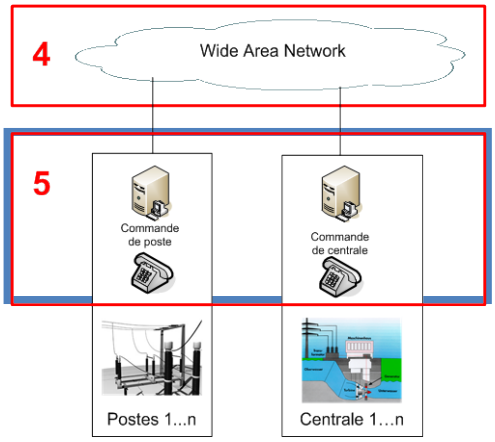
7.6. Contrôle-commande des postes et centrales

7.6.1. Directive quantifiée

(1) L'END au niveau contrôle-commande des postes électriques et centrales des niveaux de réseau 1 à 4 ne doit pas dépasser 50 MWh par évènement.

7.6.2. Recommandation

(1) Une commande manuelle des champs sur site doit être possible. Pour des installations complexes, un poste de commande sur site dans l'ouvrage est conseillé. Le délai d'intervention du service de piquet est à définir pour chaque poste ou centrale selon une directive quantifiée. Les réseaux informatiques internes et les accès externes (p. ex. piquet ou fournisseurs) doivent être pourvus de mesures de sécurité correspondant à l'état actuel de la technique (p. ex. authentification et cryptage). Du matériel de rechange pour tous les composants critiques doit être disponible.



[3] Par exemple SAP ou MS Office

[4] Par exemple vente de bande passante à des fournisseurs de télécommunication ou FTTH

8. Autre bibliographie

(1) Les documents suivants peuvent constituer une aide à la mise en œuvre de la présente recommandation de la branche pour les entreprises d'approvisionnement en électricité.

Titre	Auteur/éditeur	Date	Lien/fichier
Procédure de sécurité IT – Code de bonnes pratiques pour la gestion de la sécurité de l'information	ISO/IEC 27002	2008	http://de.wikipedia.org/wiki/ISO/IEC_27002
Security for Information Systems and Intranets in Electric Power Systems (Sécurité des systèmes d'information et de l'Intranet des réseaux d'électricité) Brochure Technique N°317	Cigré	Avril 2007	http://www.cigre.org/
Viking Project	EU financed Framework 7 Collaborative STREP Project (7e programme-cadre européen - projet collaboratif STREP –)	Nov. 2008 à oct. 2011	http://www.vikingproject.eu
Analyse des dangers pour l'AEP de l'AE	Office fédéral pour l'approvisionnement économique du pays OFAE	Mai 2010	http://www.bwl.adadm.ch/themen/00050/index.html?lan=de
Critical infrastructure protection for the smart grid (Protection des infrastructures critiques pour le smart grid)	Accenture	2010	http://www.accenture.com/us-en/Pages/insight-critical-infrastructure-protection-smart-grid.aspx
Reliability Standards for the Bulk Electric Systems of North America (Normes de fiabilité pour les réseaux de transport et de distribution d'électricité d'Amérique du Nord)	NERC - North American Electric Reliability Corporation	2008 - 2011	http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf
Meeting NERC CIP requirements with Cooper Power Systems IED Integration and Automation Solutions (Satisfaire les exigences NERC CIP avec Cooper Power Systems IED: solutions d'intégration et d'automatisation)	Cooper Power Systems	Mars 2009	http://compliance.npcc.org/Documents/TFE%20Library/Cooper%20Power%20Systems%20-%20IED%20Intergration%20-%20Meeting%20NERC%20CIP%20requirements.pdf
ITIL Service Design	ITIL, Information Technology Infrastructure Library (Bibliothèque pour l'infrastructure des technologies de l'information)	2007	http://de.wikipedia.org/wiki/ITIL_V3_Service_Design

Tableau 2: Documents d'aide pour la mise en œuvre de la recommandation de la branche

(2) Dans le cadre de stratégie suisse de cyber défense, un groupe d'experts dirigé par la Confédération va établir une stratégie globale de la Confédération contre les menaces. Elle est d'importance capitale pour l'approvisionnement en électricité en raison des conséquences primaires et secondaires drastiques d'une défaillance de grande ampleur. Il s'agit là avant tout d'un concept qui décrit comment les exploitants (étatiques et privés) peuvent s'armer contre des attaques cybernétiques.

(3) La norme ISO 27002 contient de précieuses indications sur les domaines qu'il pourrait s'agir de protéger et de tester:

- Domaine ISO 27002 9 – Sécurité physique et environnementale, objectifs ISO 27002 9.1 et 9.2
- Domaine ISO 27002 10 – Gestion de l'exploitation et des télécommunications, objectifs ISO 27002 10.1, 10.5, 10.6 et 10.10
- Domaine ISO 27002 11 – Contrôle d'accès, objectifs ISO 27002 11.1, 11.2 et 11.6
- Domaine ISO 27002 12 – Acquisition, développement et maintenance des systèmes d'information: objectifs ISO 27002 12.2 et 12.5
- Domaine ISO 27002 13 – Gestion des incidents liées à la sécurité de l'information: objectifs ISO 27002 13.1.