Infrastructures IT destinées à la gestion des réseaux électriques

Autor(en): **Joye, Philippe / Buntschu, François / Sauvain, Hubert**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **101 (2010)**

Heft 4

PDF erstellt am: **08.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-856067

Infrastructures IT destinées à la gestion des réseaux électriques

Identification des risques et optimisation de la sécurité

Si les infrastructures IT facilitent le contrôle et la commande des réseaux électriques, les moyens de communication ouverts reliant les différents serveurs et calculateurs amoindrissent leur niveau de sécurité. Basée sur une méthodologie reconnue, une étude rigoureuse a été menée à la HES-SO de Fribourg afin de mettre en évidence les vulnérabilités et points faibles de ces infrastructures. Plusieurs directives et recommandations en vue d'optimiser la sécurité des réseaux électriques ont pu en être déduites.

Philippe Joye, François Buntschu, Hubert Sauvain

Les infrastructures IT (infrastructures de calcul et de communication) font partie intégrante des réseaux électriques. Elles contribuent à faciliter le contrôle et la commande de ceux-ci. Mais l'introduction de serveurs et autres calculateurs numériques reliés entre eux par des moyens de communication ouverts (Internet/TCP-IP) influence négativement le niveau de sécurité et la fiabilité des installations. Or, de par son caractère stratégique, un réseau électrique ne doit pas pouvoir être manipulé par des personnes non autorisées et malveillantes.

Sur la base des configurations usuelles des infrastructures IT des réseaux électriques et du miniréseau de test de la HES-SO Fribourg [1, 2], une analyse complète et rigoureuse de leur sécurité, basée sur une méthodologie reconnue, a mis en évidence quelques vulnérabilités et points faibles à corriger. A l'aide d'un exemple, cet article retrace cette démarche, et rappelle quelques principes de base à mettre en œuvre afin d'augmenter le niveau de sécurité et de fiabilité d'une telle infrastructure. L'exemple choisi présente un réseau restreint, mais équipé d'un système de surveillance WAMS (Wide Area Monitoring System).

Situation et problématique

L'infrastructure IT prend en charge la visualisation et par exemple la commande de flux d'énergie sur les lignes de transport [1]. Les techniques de mesure et de prédiction recourent à des calculateurs embarqués ou intégrés dans des PCs (Personal computers). Ces importantes capacités de calcul communiquent entre elles au moyen de systèmes de communication de données, spécifiés tant au niveau du support physique que du protocole de communication utilisé.

Situation actuelle

Le développement des capacités de calcul et des facilités de communication mises à disposition (fibres optiques, protocoles TCP/IP) laisse entrevoir d'intéressantes perspectives en termes d'efficacité et de performances. En effet, la précision des mesures (synchronisation temporelle par GPS) ainsi que la rapidité de transfert des valeurs mesurées et calculées (latence très faible) font tendre ces solutions vers l'optimal. Les opérateurs de réseaux électriques ont donc mis en place et adapté leurs infrastructures IT de façon à maximiser les capacités de transfert en intégrant de manière générale divers composants, tels que les éléments représentés schématiquement dans la **figure 1** et décrits ci-dessous.

En premier lieu, des dispositifs WAMS incluent des PMUs (Phasor Measurement Units) dont les antennes GPS sont chargées de la synchronisation temporelle. Ces systèmes sont disposés dans les postes à proximité immédiate des lignes dont on désire connaître les valeurs de courant, de tension et de phase (phaseurs).

Des capacités de transmission de données numériques supportant la couche de protocole TCP/IP sont intégrées, permettant ainsi de relier les différents PMUs vers le calculateur central hébergeant un logiciel de corrélation [3–5]. Ces liaisons sont en principe constituées de systèmes à haut débit synchrone (SHDSL ou Single-pair High-speed Digital Subscriber Line) pour les accès de proximité (< 5,4 km), puis convertis en signaux optiques pour la transmission à longue distance par fibre optique. Finalement, un serveur de calcul capable de concentrer les données transmises, est utilisé afin de calculer par exemple les charges correspondantes sur les différentes lignes à surveiller dans le contexte global du réseau à grande échelle. Ce serveur est disposé dans un centre de contrôle afin de pouvoir, à tout instant et en temps réel, être capable de visualiser, de sauvegarder et de contrôler les contraintes sur les lignes.

Mesures prises pour diminuer les risques

Les infrastructures de production, transport et distribution d'énergie électrique sont des éléments vitaux et stratégiques pour les consommateurs. A ce titre, l'approvisionnement en énergie électrique doit être garanti et ces infrastructures doivent disposer d'une fiabilité et d'une sécurité sans faille. A partir du moment

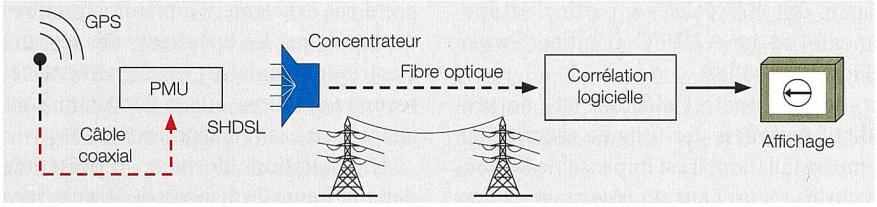


Figure 1 Infrastructure IT en exploitation dans un réseau de distribution.

où les calculateurs et autres composants de l'infrastructure IT communiquent, un certain nombre de portes sont ouvertes et un risque pour la sécurité et la fiabilité apparaît. Ces risques peuvent se révéler de plusieurs natures et vont de la simple négligence d'un employé à des attaques ciblées et destructives portées par des organisations criminelles.

De manière générale, les opérateurs ont répondu à ces menaces en établissant des mesures visant à limiter au maximum les connexions de données vers les réseaux extérieurs publics (par exemple Internet), en installant une redondance systématique des calculateurs et des lignes de communication physiques, et finalement en instaurant une responsabilisation des employés couplée à une organisation très bien structurée.

Malgré ces dispositions, le risque inhérent à la présence de PCs, de systèmes d'exploitation publics (Windows, Linux, etc.), de protocoles ouverts (HTTP, TCP, IP) et d'applications développées sur mesure ne pourra pas être réduit à zéro. Des risques subsistent, par exemple, en cas de présence de programmes malveillants (cheval de Troie, virus, logiciel espion) sur les machines, importés lors des installations, copies de fichiers ou lecture de messagerie électronique, ou lors de la communication via le réseau internet, même infime, mais qui reste cependant indispensable pour les mises à jour des systèmes d'exploitation ou même des logiciels anti-virus.

Une étude sur un miniréseau pour améliorer la sécurité

Afin de mieux appréhender cette problématique et d'être capable de quantifier plus précisément la fiabilité et la sécurité de ces infrastructures, une analyse et une série de tests de sécurité sur l'installation expérimentale du miniréseau de la HES-SO de Fribourg ont été effectués. Cette installation est plus complète que celle présentée dans la **figure 1**. Elle comprend également, comme le montre la **figure 2**, de la rétroaction sur des dispositifs tels que des transformateurs déphaseurs ou une ligne de transport à courant continu (HVDC). Les transformateurs déphaseurs ont été réalisés à partir d'équipements de type UPFC (Unified Power Flow Controller).

Vu le caractère aléatoire et non prédictif des effets des tests de sécurité sur une installation, il est impensable de pouvoir les réaliser sur un réseau en exploitation. Certes, le miniréseau ne correspond pas exactement aux infrastructures déployées par les opérateurs des réseaux électriques, mais les enseignements et recommandations qui en découlent, sont adaptés au cas réel d'utilisation.

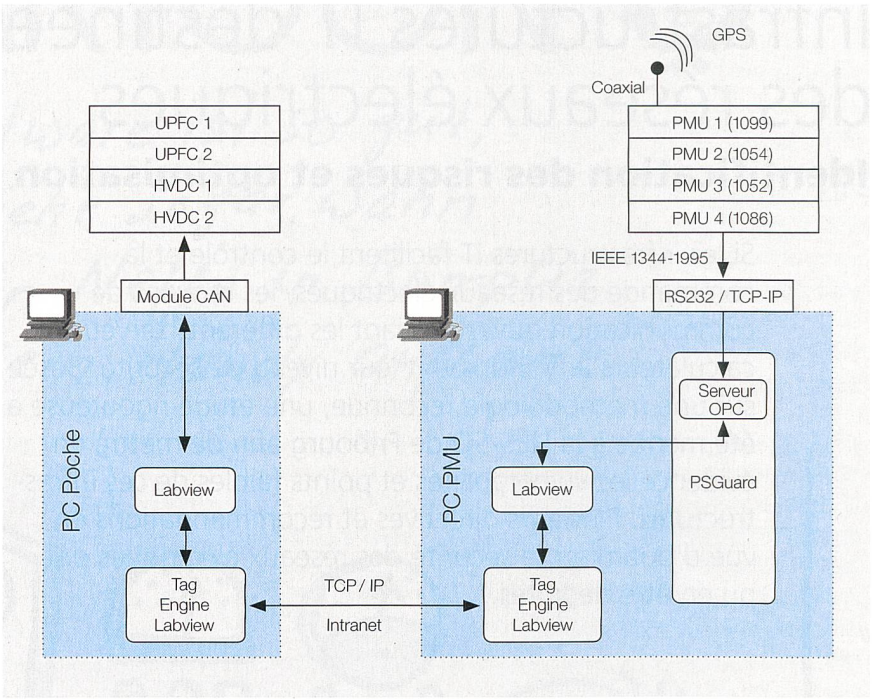


Figure 2 Structure IT du réseau de simulation (miniréseau).

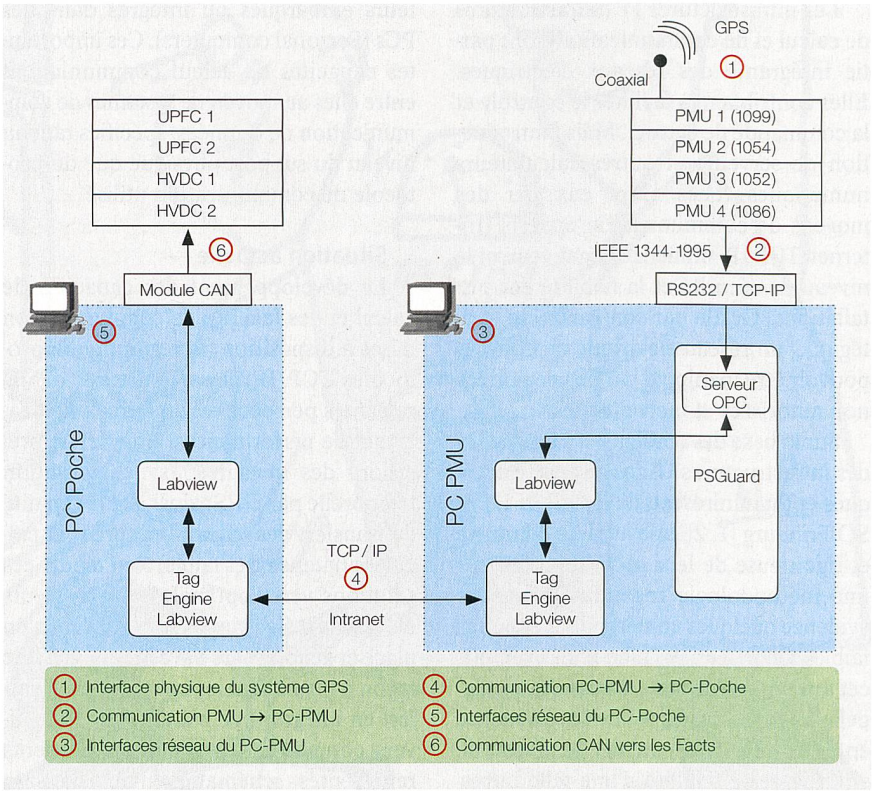


Figure 3 Points sensibles de l'infrastructure IT.

L'installation de test, représentée dans la **figure 2**, dispose de 4 antennes GPS connectées à 4 PMUs différents à l'aide de câbles coaxiaux. Les PMUs sont tous reliés à travers des liaisons RS-232 au calculateur central (PC-PMU) qui inclut PSGuard, un produit logiciel permettant d'afficher en temps réel l'état de tension, courant et phaseur d'un point du réseau de distribution électrique. Ce dernier communique avec le

deuxième calculateur (PC-Poche) au travers d'un Intranet (TCP-IP). Les commandes destinées aux composants de type Facts (Flexible Alternative Current Transmission System) passent par un bus de terrain de type CAN (Controller Area Network).

Approche et méthodologies

Les tests de fiabilité et de sécurité ont été réalisés sur la base de la méthodologie OSSTMM (Open Source Security Testing Methodology Manual) [6] développée par l'Isecom (Institute for Security and Open Methodologies) [7].

L'OSSTMM fournit une méthodologie précise et détaillée afin de réaliser des tests de sécurité sur une infrastructure. Cette méthodologie procure une mesure (valeur) relative du niveau de sécurité global et révèle les failles et vulnérabilités avérées et contrôlées. La table résultante, nommée RAV (Risk Assessment Value) n'est pas à utiliser de manière absolue, mais de manière relative en comparant les valeurs intermédiaires au fur et à mesure des modifications et améliorations apportées à l'infrastructure.

Les tests de validation ont été menés en suivant les étapes suivantes :

- Analyse détaillée de l'infrastructure IT du miniréseau.
- Identification des délimitations de l'infrastructure (« scope »).
- Définition des vecteurs de test susceptibles de révéler des vulnérabilités (« vectors »).
- Identification et contrôle des vulnérabilités détectées.
- Classification de ces dernières en tenant compte de leur portée et de leur incidence sur la sécurité globale du système.
- Définition de la valeur RAV et report des vulnérabilités constatées.

Des cinq canaux de tests principaux décrits dans la méthodologie, seul le canal de données, correspondant aux réseaux de transmission de données entre machines et autres dispositifs, a été retenu, les autres canaux ne correspondant pas au contexte de cette étude.

L'analyse globale et détaillée des composants désignés dans la **figure 3** a mis en évidence un premier problème général de structure. En effet, les composants (GPS, câble coaxial, PMU, RS-232, PC-PMU, Intranet, PC-Poche, CAN bus) sont disposés en série. Ceci signifie que la défaillance d'un seul d'entre eux conduit à la défaillance de l'ensemble. La fiabilité du système est donc plus petite que celle du composant le plus faible. La redondance appliquée dans les infrastructures des distributeurs est la seule solution possible et permet d'améliorer la fiabilité, mais évidemment elle double le coût des infrastructures.

L'analyse effectuée a permis d'identifier clairement les points sensibles de l'infrastructure à tester. Ils sont énumérés dans la **figure 3**.

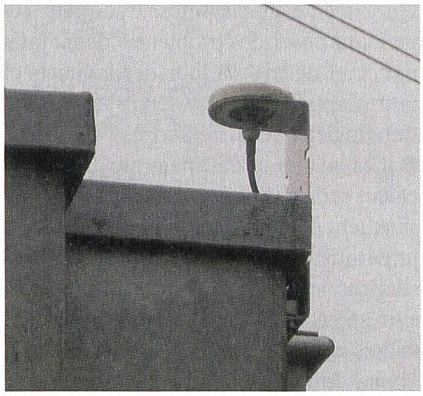
Résultats

Au total, sur l'équipement de test, 42 vulnérabilités et 30 points faibles ont été détectés. 80 % d'entre eux ont été exploités (vérifiés) avec des conséquences plus ou moins graves sur la fiabilité de l'infrastructure.

Cependant, un certain nombre d'entre eux sont critiques car ils dépendent directement de la structure de l'installation. En voici la liste :

- Les antennes GPS sont très sensibles et sont faciles à perturber. Une très faible irradiation électromagnétique avec une puissance d'émission de –30 dBm (1 µW) à une distance de 30 m dirigée directement sur l'antenne GPS de réception, suffit à bloquer complètement les prises de mesure.
- La mise en œuvre de la suite de protocole TCP-IP des dispositifs PMU devrait être améliorée. Certaines suites de trames générées accidentellement lors des ouvertures des canaux TCP pour la communication entre le PMU et le calculateur, bloquent l'émission des données et nécessitent un redémarrage du PMU. Certes, cette vulnérabilité ne met pas la configuration de l'appareil en danger, mais, dans le cas où ce dernier jouerait un rôle actif (avec la boucle de contre-réaction), la fiabilité du système dans sa globalité serait diminuée.
- Les protocoles OPC (OLE for Process Control), et DCOM (Distributed Component Object Model), utilisés pour les communications entre les calculateurs ouvrent un nombre considérable de portes d'accès (ports TCP). La sécurité de ces accès devrait elle aussi être améliorée. Certains d'entre eux donnent un accès direct à l'application de calcul sans authentification formelle des requêtes.

Certes, il ne s'agit que d'une infrastructure de test et d'expérimentation. Même si la majorité des vulnérabilités et des points faibles peuvent facilement être corrigés sur les installations mises en exploitation, les points cités ci-dessus relèvent des technologies et des architectures mises en œuvre par les exploitants des



Figures : EIA-FR

Figure 4 Antenne GPS de synchronisation.

réseaux et peuvent se révéler très dangereuses.

Perspectives et contraintes

En conclusion, ce travail effectué en étroite collaboration avec Swisselectric Research, Swissgrid et Groupe E, à l'occasion d'un travail de diplôme à l'HES-SO [8], a permis d'avancer un certain nombre de recommandations et de directives :

- La vulnérabilité des antennes GPS, dont les conséquences sont importantes sur la fiabilité du système, oblige à porter une attention particulière à la protection physique de ces éléments. La **figure 4** montre le détail d'une antenne fixée sur le toit d'un poste. Cette installation doit être le moins visible possible et son accès physique contrôlé et limité aux personnes autorisées.
- Les accès réseaux aux calculateurs et aux PMUs doivent être limités par des listes (Access List) introduites dans les routeurs ou pare-feu (firewall). Cette mesure évitera des attaques ciblées sur les calculateurs où de nombreux ports sont ouverts par les applications (PSGuard et Labview) à partir d'autres machines introduites dans le réseau.
- Les canaux de communication de données utilisant le protocole TCP/IP devraient, afin de garantir une authentification minimale des sources, se baser sur des protocoles développés à cet effet tels que SSH (Secure Shell) ou SSL (Secure Sockets Layer).
- La visibilité externe des calculateurs et autres PMUs doit être réduite au minimum. Dans ce sens, ces machines ne doivent en aucun cas être référencées dans le serveur DNS (Domain Name System) ou les répertoires de type AD (Active Directory).
- Les connexions avec les réseaux extérieurs (internet) doivent être réduites

voire même inexistantes. Ceci peut cependant poser des problèmes de maintenance et de mise à jour des logiciels et autres applications (systèmes d'exploitation, logiciel de corrélation).

- Les machines destinées aux tâches de calcul et de prédiction doivent être exclusivement dédiées à ces applications. Il est impératif de désactiver tous les autres services annexes, tels que les messageries, serveurs FTP ou Telnet.
- Les systèmes d'exploitation (Windows, Unix, Linux) et logiciels (antivirus, Labview) doivent être mis à jour le plus souvent possible. Les patchs de sécurité doivent être installés avec la plus grande des précautions et avec une extrême rigueur.

La méthodologie utilisée (OSSTMM) s'est montrée adaptée à cette étude, car très systématique. La liste des vulnérabilités et points faibles apparus à l'occasion de ce travail n'est pas exhaustive, car la sécurité absolue n'existe pas. Par contre, l'image régulièrement actualisée du niveau de sécurité atteint, permet de suivre son évolution dans le temps au gré des audits pratiqués. En effet, sans intervention et mise à jour régulière, la sécurité IT d'une installation globale se dégrade irrémédiablement en raison des progrès réalisés par les attaquants.

Références

[1] D. Westermann, H. Sauvain : Experience with Wide Area Monitoring and Facts Control in a Real Time Simulator. PowerTech, St Petersburg, Russia, 2005.
[2] M. Pellerin : Démonstrateur pour Facts. Conférence EPFL, Montpellier, 2002.
[3] Ch. Rehtanz, M. Larsson, M. Zima, J. Bertsch : System for Wide-Area Protection Control and Optimization based on Phasor Measurements. Power System and Communication Systems Infrastructure for the Future Conference, Beijing, China, 2002.
[4] ABB Product Description : Wide Area Measurement, Monitoring, Protection and Control. 2003.
[5] G. Glanzmann, G. Andersson : Coordinated Control Facts Devices based on Optimal Power Flow. North American Power Symposium (NAPS), Ames, USA, 2005.
[6] P. Herzog : OSSTMM 3.0. Institute for Security and open methodologies, avril 2008.
[7] www.isecom.org.
[8] A. Arrigoni, M. Restelli : Sécurité et fiabilité du système de gestion de distribution d'énergie électrique Suisse. Ecole d'ingénieurs et d'architectes de Fribourg, décembre 2008.

Informations sur les auteurs

Philippe Joye est professeur de systèmes d'information et de sécurité IT à l'Ecole d'ingénieurs et d'architectes de Fribourg (EIA-FR) depuis 1999. Ingénieur électricien ETS de l'EIA-FR avec spécialisation en énergie électrique, il a obtenu son diplôme d'ingénieur EPFL en électricité en 1989. Philippe Joye a ensuite développé les parties commande et régulation des installations de puissance pour Reliance AG, avant de bifurquer dans le monde des télécommunications et de leur sécurité pour l'entreprise Ascom.
EIA-FR, 1705 Fribourg, philippe.joye@hefr.ch

François Buntschu est ingénieur ETS en informatique. Il a obtenu son diplôme de l'EIA-FR en 1992 et est titulaire depuis 2009 d'un MAS en technologies de l'information et de la communication. Après plus de 10 ans d'expérience industrielle dans l'intégration et la sécurité des réseaux informatiques auprès d'entreprises nationales et internationales, il exerce actuellement une activité d'enseignant et de développement à l'EIA-FR.
EIA-FR, 1705 Fribourg, francois.buntschu@hefr.ch

Hubert Sauvain est ingénieur EPFL. Il enseigne les réseaux électriques à l'Ecole d'ingénieurs et d'architectes de Fribourg, HES-SO. Il est coordinateur du programme en économie des réseaux électriques à l'iimt (international institute of management in technology), Université de Fribourg. Il préside la société ETG d'Electrosuisse et est membre de différents conseils d'administration.
EIA-FR, 1705 Fribourg, hubert.sauvain@hefr.ch

Zusammenfassung **IT- Infrastrukturen zur Steuerung elektrischer Netze**

Risikoerfassung und Optimierung der Sicherheit

Zwar werden Überwachung und Steuerung elektrischer Netze durch IT-Infrastrukturen erleichtert, doch vermindern offene Kommunikationsmittel zwischen den einzelnen Servern und Computern deren Sicherheit. Aufgrund einer anerkannten Methodologie wurde an der HES-SO Freiburg eine rigorose Studie erstellt, um die Verletzlichkeit und die Schwächen solcher Infrastrukturen aufzuzeigen. Daraus konnten mehrere Richtlinien und Empfehlungen zur Optimierung der Sicherheit elektrischer Netze abgeleitet werden.