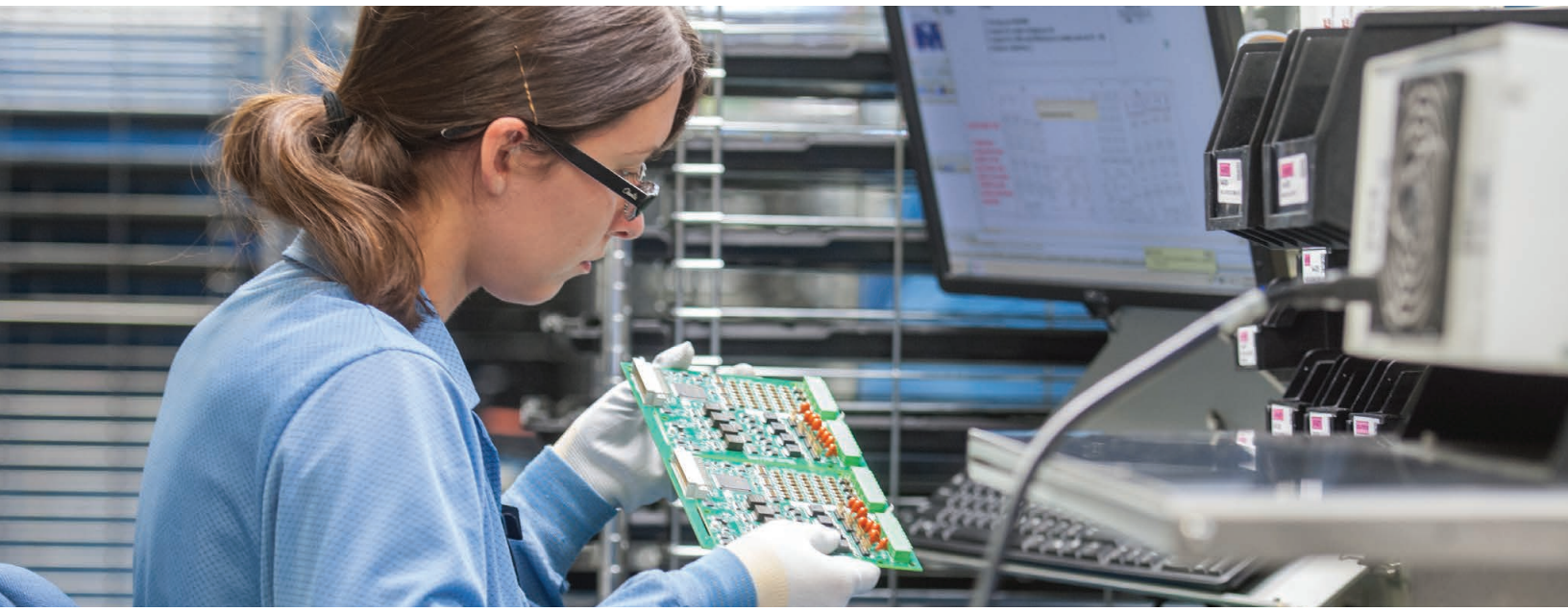
Sécuriser votre chaîne d'approvisionnement

Meilleures pratiques selon SEL



Élaboration de plans de gestion des risques liés à la cybersécurité de la chaîne d'approvisionnement

La gestion des risques liés à la chaîne d'approvisionnement est une composante essentielle d'un programme exhaustif de cybersécurité. L'interconnexion et la complexité des chaînes d'approvisionnement rendent l'évaluation systématique des risques plus importante que jamais, mais c'est un grand défi. Chez SEL, depuis plus de 30 ans, nous avons fait de la sécurité, notamment de la sécurité de la chaîne d'approvisionnement, une priorité absolue et selon nous, la gestion des risques liés à la chaîne d'approvisionnement est fondamentale pour garantir la qualité de nos produits. Nous espérons que le partage de nos connaissances et nos meilleures pratiques en la matière vous aideront à accélérer les efforts en vue de la cybersécurité et de la conformité à la norme CIP-013 du NERC. Le présent document décrit les processus suivis par SEL visant à garantir une chaîne d'approvisionnement sûre et fiable des produits à livrer aux clients du monde entier.

SEL

CIP-013-1 du NERC, « Cybersécurité — gestion des risques liés à la chaîne d'approvisionnement »

Objectif

« Atténuer les risques liés à la cybersécurité pour assurer un fonctionnement fiable du réseau de production-transport d'électricité (BES) en mettant en œuvre des contrôles de sécurité au niveau de la gestion des risques liés à la chaîne d'approvisionnement des systèmes cybernétiques du BES. »

Date d'entrée en vigueur

1er juillet 2020

Résumé des exigences

- Évaluation des risques liés aux produits ou aux prestations de fournisseur (R1.1)
- Notification des incidents identifiés par le fournisseur (R1.2.1)
- Coordination de la réponse aux incidents (R1.2.2)
- Notification par le fournisseur lorsque l'accès à distance/sur site n'est pas nécessaire (R1.2.3)
- Divulgation par les fournisseurs des vulnérabilités connues (R1.2.4)
- Vérification de l'intégrité et de l'authenticité du logiciel (R1.2.5)
- Coordination des contrôles d'accès à distance (R1.2.6)

Comment SEL garantit une chaîne d'approvisionnement sûre et fiable

La chaîne d'approvisionnement de SEL est globale et complexe. Pour évaluer les risques pour notre chaîne d'approvisionnement, nous adoptons une approche globale en cinq parties.

Partie 1 : Établir des réseaux d'approvisionnement de confiance

Système d'évaluation des fournisseurs

Chez SEL, nous utilisons un système d'évaluation des fournisseurs qui évalue chaque fournisseur en fonction du prix, de la qualité, des caractéristiques, de l'innovation, de la livraison et de la prestation. Pour arriver à cette notation, nous évaluons les risques liés aux fournisseurs suivants :

- Sites de production
- Délais de livraison du matériel
- Santé financière
- Méthodes de réapprovisionnement
- Type de technologie
- Respect des délais de livraison

Conférence annuelle des fournisseurs

Chaque année, nous organisons une conférence destinée aux fournisseurs qui nous livrent des éléments constitutifs, des équipements et des prestations. Au cours de cet évènement, plus de 200 entreprises se rendent à notre siège social de Pullman, Washington où nous partageons nos besoins techniques et nos objectifs stratégiques pour l'année à venir et identifions des moyens de collaborer pour assurer un approvisionnement continu en pièces de qualité.

Audits sur place

Nous établissons des relations avec nos fournisseurs en menant des audits continus sur place pour vérifier que leurs processus de qualité et de sécurité répondent à nos exigences.

Approche organisationnelle de la sélection et de la surveillance de fournisseur

Chez SEL, la gestion des risques liés à la chaîne d'approvisionnement repose sur une collaboration transversale. Le processus commence par la sélection des fournisseurs, ce qui constitue un effort d'équipe entre nos groupes de développement de produit, de qualité et d'achat. De même, différentes équipes interviennent lors de la sélection des composants, de la surveillance continue des fournisseurs et des pièces, ainsi que des audits des fournisseurs sur place. Selon cette approche, la gestion des risques devient une responsabilité collective.

Confidentialité

Nous ne partageons pas nos nomenclatures (BOM). Nous fournissons des prévisions par numéro de pièce, sans rapport avec le produit. Pour éviter de divulguer des informations sur les produits et les pièces d'autres fournisseurs, nous n'envoyons jamais de schémas de conception.

Fournisseurs de nos fournisseurs

Il ne suffit pas de connaître nos fournisseurs de premier rang. Nous demandons à nos fournisseurs d'identifier leurs fournisseurs de premier rang ainsi que les principaux risques, les stratégies d'atténuation et les méthodes de réapprovisionnement.

Préférence pour les fournisseurs nationaux

Dans la mesure du possible, nous nous approvisionnons en matériaux aux États-Unis.

Qualification du fournisseur de services de transport et d'expédition

Pour garantir la livraison sécurisée de nos produits à nos clients, nous appliquons les mêmes processus de qualification des fournisseurs à nos fournisseurs de services de transport et d'expédition.

Partie 2 : Garantir l'intégrité et la disponibilité de composant

Processus de qualification de composant

Pour garantir l'intégrité de nos produits, nous vérifions les performances des composants achetés par rapport aux spécifications des produits des fournisseurs. Dans la mesure du possible, nous achetons les composants directement auprès du fabricant ou des distributeurs officiels. Dans les cas où les composants doivent provenir de distributeurs indépendants, nous utilisons plusieurs méthodes de détection des produits contrefaits, notamment des tests fonctionnels et des inspections microscopiques, par rayons X, par fluorescence X et par décapsulation.

Tests continus

Tout au long du processus de fabrication, nous effectuons de manière régulière le test de nos produits. Si des variations de performance sont constatées, nous nous efforçons de comprendre la cause profonde de la divergence.

Réduire au minimum l'incidence des perturbations

Nous collaborons avec nos fournisseurs pour nous assurer d'avoir un stock suffisant de pièces spécialisées et à risque. Dans la mesure du possible, nous nous assurons que les composants critiques peuvent provenir d'au moins deux fournisseurs approuvés.

Partie 3 : Vérifier la sécurité du logiciel et du micrologiciel

Code source

Nous ne partageons pas le code source ou les schémas. Nous développons la plupart des logiciels en interne, qui fournissent un avantage en matière de contrôle de la qualité ainsi que la possibilité d'apporter des améliorations rapides. Si nous utilisons des composants tiers dans notre micrologiciel, nous acquérons le code source. L'accès au code n'est donné qu'aux ingénieurs R&D de SEL travaillant sur ces projets.

Tests internes

Nous disposons d'un processus robuste comprenant des évaluations par des pairs développeurs, ainsi que des tests positifs et négatifs. Nous utilisons également des outils automatisés pour inspecter le code afin d'identifier les questions potentielles que les développeurs peuvent avoir manqués. Tous les tests sont effectués sur place chez SEL par des employés de SEL.

Signatures numériques SEL et hachages de micrologiciel

Un logiciel signé numériquement vous permet d'être sûr que les fichiers du logiciel et du micrologiciel sont authentiques (produits par SEL) et qu'ils n'ont pas été modifiés ou altérés. Les utilisateurs de Microsoft Windows peuvent rechercher et vérifier les signatures numériques des produits logiciels SEL à l'aide de l'Explorateur Windows. Les produits matériels SEL vérifient de manière transparente l'intégrité des fichiers du micrologiciel lors du processus de mise à niveau du micrologiciel à l'aide des données supplémentaires intégrées au micrologiciel. En cas de non-concordance, le dispositif SEL rejette le fichier du micrologiciel et interrompt le processus de mise à niveau. SEL fournit des hachages du micrologiciel comme outil supplémentaire pour vérifier l'intégrité des fichiers du micrologiciel SEL.

Partie 4 : Protéger les opérations et contrôler l'accès

Sécurité physique et cybersécurité SEL

Notre infrastructure interne de sécurité physique et informatique est à plusieurs niveaux et conforme aux normes internationalement reconnues. Cela garantit que tous les dispositifs et toutes les prestations SEL sont fournis en toute sécurité et que toutes les données confiées à SEL sont protégées. Nous nous mettons également au défi d'aller au-delà des normes pour accroître la cybersécurité. À titre d'exemple, nous avons mis en place une mise en réseau défini par logiciel dans notre opération de fabrication pour éliminer plusieurs vulnérabilités courantes en matière de sécurité du réseau.

Notre système de gestion de la qualité est certifié conforme à la norme ISO 9001 et nos processus de fabrication sont conformes à la norme de fabrication IPC-A-610 Classe 3 pour les produits nécessitant une grande fiabilité, tels que ceux utilisés dans les systèmes de survie et les systèmes aérospatiaux.

Tous les employés de SEL sont soumis à un processus exhaustif de vérification des antécédents, notamment des antécédents criminels, avant d'être embauchés. L'accès aux bâtiments SEL et aux espaces sensibles qui s'y trouvent est protégé par des contrôles d'accès configurables, la vidéosurveillance et d'autres systèmes de surveillance. Les équipements SEL et les systèmes d'information sont protégés contre les menaces physiques et environnementales. Les systèmes de sécurité SEL sont surveillés et pris en charge 24 h/24 et 7 j/7 par les employés SEL de notre centre d'opérations de sécurité. Nos équipes analysent tout un éventail de menaces publiques et privées et d'autres flux de renseignements pour détecter les menaces potentielles.

Besoin de connaître

La culture de sécurité SEL est ancrée dans les concepts de moindre privilège, de besoin de connaître et de défense en profondeur. Nous compartimentons les projets et limitons l'accès à l'information en interne à ceux ayant le besoin de connaître.

Protection des informations client

Nous protégeons les informations client dans nos systèmes commerciaux et pendant les activités d'assistance. Cela inclut la sécurisation des informations client dans les produits renvoyés pour réparation. Lorsque nous identifions un incident affectant les informations client, nous en informons nos clients et offrons une assistance complète pour la réponse à l'incident.

Accès à distance

Lorsque l'accès à distance est nécessaire pour le soutien technique, nous utilisons un système de suivi et de notification pour documenter et coordonner le contrôle de cet accès.

Partie 5 : Surveiller les vulnérabilités en matière de qualité et de sécurité

Déterminer la cause profonde

Une garantie décennale fournit une incentive à nos clients à nous retourner les produits en cas de défaillance. Nous pouvons ensuite examiner ces produits et trouver les causes profondes des défauts, ce qui nous permet d'identifier les problèmes concernant notre processus de conception ou nos fournisseurs et d'améliorer la conception de nos produits. Nous offrons une garantie décennale sans frais sur tous les produits.

Suivi des produits au niveau composant

Nous gardons un enregistrement détaillé de chaque produit que nous fabriquons et des composants qui y sont intégrés afin de savoir où nos produits sont installés et de pouvoir informer les clients des questions potentielles en ce qui concerne la qualité ou la sécurité.

Bulletins de service

Lorsque nous identifions un problème potentiel concernant un produit, nous rassemblons une équipe multidisciplinaire d'experts en conception de produits pour analyser le problème. Si cela présente un risque pour les clients, nous informons les clients concernés par un bulletin de service. Les bulletins de service comprennent une explication du problème identifié ainsi que la cause profonde, l'incidence, le taux de défaut observé, les produits affectés par client, les actions correctives et les solutions de maintenance recommandées. Un bulletin de service permet au client de prendre une décision éclairée sur la façon de résoudre le problème. Nous distribuons des bulletins de service aux clients directement et par le biais de notre force de vente.

Vulnérabilités en matière de sécurité

Un bulletin de service qui se rapporte à une vulnérabilité en matière de sécurité des produits concernés est classé comme « vulnérabilité en matière de sécurité ». Notre équipe élabore des suggestions de mesures correctives pour toute vulnérabilité en matière de sécurité du produit avant la divulgation et les inclut dans le bulletin de service associé.

Implication de l'industrie

Nous participons à diverses initiatives et activités d'élaboration de normes dirigées par le gouvernement afin de pouvoir être informé des meilleures pratiques actuelles des autres acteurs de l'industrie, contribuer aux meilleures pratiques de l'industrie et rester à l'écoute des exigences changeantes imposées à nos clients. De même, nous contribuons et utilisons des documents d'orientation, tels que le cadre de cybersécurité de NIST, pour améliorer nos propres processus et contrôles et pour aider à façonner les meilleures pratiques convenues de l'industrie.

Engagement continu de SEL

Chez SEL, notre politique de qualité est la suivante : « comprendre, créer et simplifier ». Cela représente notre quête incessante dans le but de comprendre les opportunités et les défis, de créer des solutions innovantes et de garantir que ces solutions sont simples, robustes et sécurisées. Les cadres de SEL incluent la gestion des risques liés à la sécurité dans le cadre de leurs activités quotidiennes. Ils restent informés des menaces émergentes liées à la chaîne d'approvisionnement et aux opérations de SEL et procèdent aux adaptations nécessaires.

SEL SCHWEITZER ENGINEERING LABORATORIES

Vers une énergie électrique plus sûre, plus fiable et plus économique
+1.509.332.1890 | info@selinc.com | selinc.com

20211130

WORLDWIDE 10 years WARRANTY