Produkte = Produits

Objekttyp: **Group**

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

Band (Jahr): **112 (2021)**

Heft 7-8

PDF erstellt am: **25.05.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Hauptsitz der HFTM in Grenchen.

Komplettanbieter im Elektrobereich

Rund 450 Studierende und Weiterbildungsinteressierte setzen jährlich auf eine technische Ausbildung an der HFTM in Grenchen oder Biel, mitunter in den Bereichen Elektro-, Energie- und Gebäudetechnik. Die modular aufgebauten Kurse bieten eine effiziente und professionelle Prüfungsvorbereitung für Berufsprüfungen wie z. B.: Elektroprojektleiter/-in Installation und Sicherheit, Elektroprojektleiter/-in Planung (beide nach neuster PO2020) oder die Praxisprüfung zur Fachkundigkeit. **Studienstart: Oktober 2021**

Höhere Fachschule Technik Mittelland, 2540 Grenchen
Tel. 032 654 12 00, www.hftm.ch

TPI-Serie – 30, 65 und 125 W.

Kompakte AC/DC-Schaltnetzteile

TPI 30, TPI 65 und TPI 125 sind drei Serien von AC/DC-Schaltnetzteilen in offener Bauform zwischen 30 und 125 W mit verstärktem Isolationssystem bis 3000 V AC. Bei der TPI-Linie steht die Bereitstellung kostengünstiger und platzsparender Netzteile für die Industrie im Vordergrund. Als Erweiterung der bestehenden TPI-Reihe bieten diese neuen Serien eine Spitzenleistungsfunktion, mit der sie bis zu 10 s lang bis zu 130 % der Nennleistung liefern können. Der Wirkungsgrad beträgt bis zu 93 %.

Traco Electronic AG, 6340 Baar
Tel. 043 311 45 11, www.tracopower.com

Türsprechen für hindernisfreie Bauten.

Aussensprechstellen mit Zustandsanzeigen

Die Baunorm SIA 500 «Hindernisfreie Bauten» verlangt von Türsprechanlagen, dass die Zustände an der Aussensprechstelle nach dem 2-Sinne-Prinzip, also akustisch und optisch, signalisiert werden. Eine TC:Bus-Türsprechanlage erfüllt diese Anforderungen. Die Aussensprechstellen «ATS» und «VTS» sind mit LED-Anzeigen für die Unterstützung von Hörbeeinträchtigten ausgerüstet. Diese integrierten LEDs signalisieren die Zustände «Türruf», «Sprechen» und «Türe öffnen».

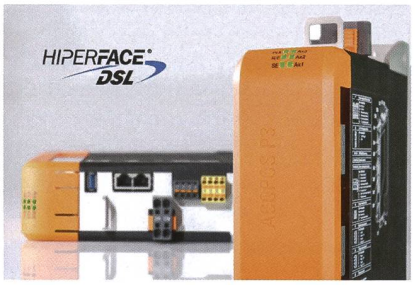
René Koch AG, 8804 Au/Wädenswil
Tel. 044 782 60 00, www.kochag.ch

Ein hochmodernes und flexibles HMI.

Skalierbare Multikomponenten-Software

Camille Bauer Metrawatt führt zum Datenmanagement die SmartCollect SC² als HMI/Scada-Software ein. Im Gegensatz zu einigen anderen Scada-Tools in dieser Kategorie basiert die SC² auf einer neuen Plattform mit einer webbasierten grafischen 2D/3D-Benutzeroberfläche. Dabei überzeugt die Einfachheit, Funktionalität, Flexibilität, aber auch das Preis-Leistungsverhältnis. Die Systemarchitektur ist offen für jegliche Messdaten, visualisiert diese und kann bei Bedarf in übergeordnete Systeme kommunizieren.

Camille Bauer Metrawatt AG, 5610 Wohlen
Tel. 056 618 21 11, www.camillebauer.com



Für Motoren mit Hiperface-DSL-Encoder.

Der passende Antrieb für jede Applikation

Die Sicherheitsfunktionen des B&R-Servoverstärkers Acopos P3 sind nun auch für Motoren mit sicherem Hiperface-DSL-Encoder verfügbar. Maschinenbauer haben damit eine grössere Motorenauswahl bei der Umsetzung von sicheren Antriebsapplikationen.

Neben EnDat 2.2 Safety hat sich Hiperface DSL Safety als Industriestandard für die sichere Datenübertragung zwischen Motoren und Servoreglern etabliert. Wie EnDat 2.2 ist HDSL-Safety kompatibel mit allen B&R-Sicherheitsfunktionen.

B&R Industrial Automation, AT-5142 Eggelsberg
Tel. +43 7748 6586-0, www.br-automation.com

Schalten ohne Kontamination.

Berührungslose Schalter

Die Covid-19-Pandemie hat einer Technologie Vorschub geleistet, die zuvor nur aus Spezialapplikationen bekannt war: berührungslose Taster. Das klingt im ersten Moment verwirrend. Wir sind uns gewohnt, auf Taster zu drücken. Wir hören oder spüren zumeist ein sattes Klacken und wissen sogleich: Aha, meine Eingabe wurde angenommen. Taktiles Feedback nennen wir das beim Hubtaster.

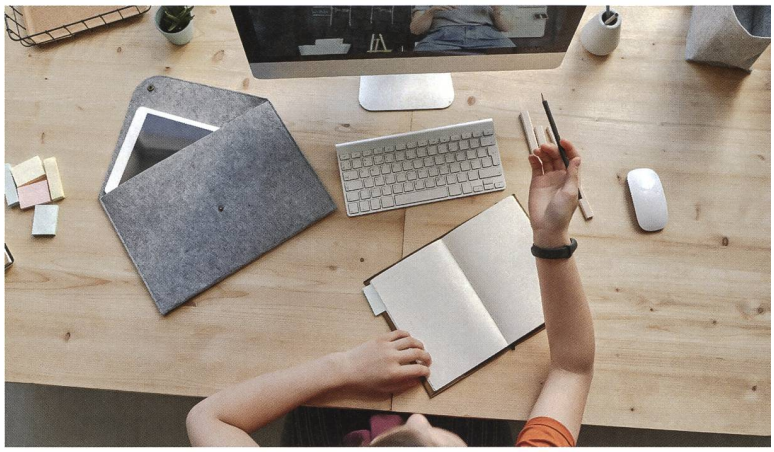
Die Funktionsweise solcher Taster wird nun in einem White Paper beschrieben: www.schurter.com/de/data/download/5257927

Schurter AG, 6002 Luzern
Tel. 041 369 31 11, schurter.com

Sicheres Arbeiten im Homeoffice

Die Coronakrise hat nicht nur die Homeoffice-Verbreitung beflügelt, sondern auch die Cyberkriminalität. Gerade im Hinblick auf häufigeres Arbeiten zu Hause lohnt es sich, Massnahmen zum Schutz der Geschäftsdaten zu ergreifen.

Kleine und mittlere Unternehmen gehen oft fälschlicherweise davon aus, keine lohnenden Ziele für Cyberkriminelle zu sein. Leider irren sie sich, wie eine aktuelle Studie der GFS-Zürich zeigt: Ein Viertel aller KMU in der Schweiz ist schon mindestens einmal Opfer eines Angriffs mit schwerwiegenden Folgen geworden. Mit der Verbreitung von Homeoffice hat die Zahl der Cyberangriffe weiter zugenommen. Die Infrastruktur zu Hause ist oft schlechter geschützt als jene im Büro. Deshalb ist es für Cyberkriminelle einfacher, an geschäftliche Daten zu kommen oder Dokumente mittels Ransomware zu verschlüsseln und Lösegeld zu erpressen. Gelingt es den Angreifern, Geschäfts-Notebooks zu verseuchen, stellt das auch eine Gefahr für die Infrastruktur in der Firma dar. Sobald die Mitarbeitenden im Büro sind, tragen sie die Malware direkt ins Firmennetz und erleichtern den Cyberkriminellen den Angriff auf die Büroinfrastruktur.



Homeoffice ist interessant für Cyberangriffe, weil die Infrastruktur zu Hause oft schlechter geschützt ist.

Welche Sicherheitsvorkehrungen sind zu treffen, wenn Mitarbeitende von unterwegs oder zu Hause arbeiten können?

Halten Sie Computer aktuell
Halten Sie private und geschäftliche Computer stets auf dem aktuellen Stand, indem Sie automatische Updates aktivieren. Das ist die Grundregel für IT-Sicherheit überhaupt. Das gilt insbesondere für Betriebssystem, Virenschutz und Webbrowser wie Chrome und Firefox.

Arbeiten Sie mit einem normalen Benutzerkonto
Verwenden Sie für die tägliche Nutzung ein normales Benutzerkonto, und nicht eines mit Administratorenrechten. Dieses sollte nur für die Systemverwaltung genutzt werden, beispielsweise für die Installation von Software. Ein normales Benutzerkonto sorgt für eine zusätzliche Hürde, weil bei einer Cyberattacke der Angreifer zuerst versuchen muss, Administratorenrechte zu erlangen.

Nutzen Sie sichere Cloud-Dienste
Für Kommunikation und Datenaustausch zwischen verschiedenen Standorten – dazu gehört auch das Homeoffice – sind Cloud-Dienste ideal. Wählen Sie einen Anbieter, der die Daten in der Cloud mit zusätzlichen Schutzmassnahmen vor Verlust schützt. Mit Microsoft 365 z. B. können Dokumente nach einem Ransomware-Befall in einer früheren Version wiederhergestellt werden oder man kann zusätzlichen Schutz vor Phishing-Mails und verseuchten Anhängen beziehen.

Speichern Sie geschäftliche Daten nicht lokal auf dem privaten Computer
Vertrauliche Firmeninformationen auf dem privaten PC sind ein gefundenes Fressen für Cyberkriminelle. Nutzen Sie den Cloud-Speicher des Unternehmens, wenn Sie geschäftliche Dokumente auf dem privaten PC bearbeiten. So sorgen Sie für besseren Schutz, etwa im Falle eines Ransomware-Angriffs.

Schützen Sie den Zugang zu Ihren Daten doppelt
Die Zwei-Faktor-Authentifizierung (2FA) hilft Ihnen, Ihre Daten besser zu schützen. Neben dem Passwort benötigen Sie zusätzlich einen per SMS oder App erhaltenen Code, um sich anzumelden. Wenn Sie von zu Hause aus auf das Firmennetzwerk zugreifen wollen, sollten Sie die Verbindung mit einem Virtual Private Network (VPN) absichern und so für Angreifer unlesbar machen. Beim VPN-Zugang empfiehlt sich aus Sicherheitsgründen immer eine 2FA.

Bereiten Sie den Fernzugriff ins Homeoffice für den Support vor
Wenn Mitarbeitende einen Homeoffice-Tag einlegen, kann der IT-Support bei einem Problem nicht einfach mal schnell vorbeischauen. Planen Sie den Fernzugriff, bevor etwas passiert. Für einfache Fälle reicht unter Umständen die Bildschirmfreigabe (Screen Sharing) in einer Microsoft-Teams-Besprechung. Wenn der Supporter selbst aktiv werden muss, können Sie Fernwartungssoftware wie z. B. TeamViewer installieren.

Führen Sie regelmässige IT-Sicherheitsaudits durch
Besonders Änderungen in der IT-Landschaft – wie das aktuelle Beispiel der Homeoffice-Verbreitung durch Corona – schaffen neue Rahmenbedingungen oder Arbeitsweisen. Dadurch entstehen neue Schwachstellen in der IT. Um diese aufzudecken, sollten regelmässige IT-Sicherheitsaudits durchgeführt werden, also eine Prüfung der eigenen Infrastruktur.

ANDREAS HEER, SWISSCOM (SCHWEIZ) AG

Swisscom (Schweiz) AG, KMU, Postfach, 3050 Bern

Wie steht es um die IT-Sicherheit in Ihrem KMU?

Finden Sie es heraus: swisscom.ch/security-check

Bild: Pexels

Le télétravail en toute sécurité

Si la crise du coronavirus a donné un coup d'accélérateur au télétravail, la cybercriminalité n'est pas en reste. Des mesures de protection des données commerciales sont particulièrement judicieuses lorsque l'on travaille plus fréquemment à domicile.

Les petites et moyennes entreprises pensent souvent ne pas constituer des cibles intéressantes pour les cybercriminels. Il s'agit malheureusement d'une idée reçue, comme le montre une étude de GFS-Zürich : un quart des PME en Suisse ont déjà été victimes d'une attaque lourde de conséquences. Le nombre de cyberattaques a encore augmenté avec la prévalence du télétravail. Bien souvent, l'infrastructure à la maison est moins bien protégée que celle du bureau. Il est donc plus facile pour les cybercriminels d'accéder à des données commerciales ou de chiffrer des documents au moyen d'un rançongiciel pour réclamer de l'argent. Et si ces acteurs parviennent à s'immiscer dans un ordinateur professionnel, l'infrastructure de l'entreprise est en danger : de retour au bureau, l'appareil permet à des logiciels malveillants d'accéder au réseau interne, facilitant la tâche des cybercriminels.

Le télétravail est intéressant pour les cybercriminels, car l'infrastructure domestique est souvent moins bien protégée.

Quelles mesures de sécurité faut-il prendre lorsque les collaborateurs travaillent en déplacement ou à domicile ?

Maintenez vos logiciels et antivirus à jour
Assurez-vous que vos ordinateurs privés et professionnels soient toujours à jour en activant les mises à jour automatiques : c'est la règle d'or de la sécurité informatique. Ce point vaut particulièrement pour les systèmes d'exploitation, antivirus et navigateurs comme Chrome et Firefox.

Travaillez à partir d'un compte utilisateur normal
Utilisez un compte utilisateur normal au quotidien au lieu d'un compte disposant de droits d'administrateur. Ce dernier ne doit être utilisé que pour des tâches de gestion du système telles que l'installation de logiciels. Un compte normal constitue un obstacle supplémentaire en cas de cyberattaque, car le cybercriminel doit d'abord essayer d'obtenir des droits d'administrateur.

Quel est le niveau de sécurité informatique de votre PME ?

Découvrez-le sur swisscom.ch/security-check

Utilisez des services cloud sécurisés
Les services cloud conviennent parfaitement à la communication et à l'échange de données entre plusieurs sites, télétravail inclus. Optez pour un fournisseur qui protège les données dans le cloud contre la perte au moyen de mesures supplémentaires. Microsoft 365 permet notamment de restaurer une version antérieure des documents en cas d'attaque de rançongiciel, ou encore de mettre en place des protections complémentaires contre l'hameçonnage et les pièces jointes infectées.

Ne sauvegardez aucune donnée professionnelle sur votre PC privé
Les informations confidentielles sur un appareil personnel constituent une véritable aubaine pour les cybercriminels. Utilisez le cloud de l'entreprise pour traiter des documents professionnels sur votre ordinateur privé : vous bénéficierez d'une protection accrue en cas d'attaque de rançongiciel.

Protégez doublement l'accès à vos données
L'authentification à deux facteurs (2FA) vous aide à mieux protéger vos données. Outre un mot de passe, l'identification nécessite un code reçu par SMS ou via une appli. Pour accéder au réseau de l'entreprise depuis chez vous, nous vous conseillons de sécuriser la connexion au moyen d'un Virtual Private Network (VPN) afin qu'un attaquant ne puisse consulter vos données. Une authentification 2FA est toujours recommandée dans le cadre d'un accès VPN.

Préparez l'accès à distance pour l'assistance technique
Quand un collaborateur est en télétravail, l'assistance informatique ne peut pas jeter un rapide coup d'œil à son ordinateur en cas de problème. Préparez vos accès à distance avant tout incident. Dans des cas simples, il suffit d'utiliser la fonction de partage d'écran dans une conversation Microsoft Teams. Si des actions sont nécessaires, vous pouvez installer des logiciels de télémaintenance comme TeamViewer.

Réalisez des audits de sécurité informatique à intervalles réguliers
Les transformations du paysage informatique – à l'instar du télétravail pour cause de coronavirus – fixent un nouveau cadre ou d'autres méthodes de travail, avec à la clé de nouvelles vulnérabilités informatiques. Pour les identifier, il convient de réaliser régulièrement des audits de sécurité informatique, c'est-à-dire un examen de votre infrastructure.

ANDREAS HEER, SWISSCOM (SUISSE) SA

Swisscom (Suisse) SA, PME, case postale, 3050 Berne

Figure : Pexels

electro suisse VSE AES

Power-Quality-Fachkraft

Zertifikatslehrgang VSE

Ab 30. August 2021, bei Eniwa in Buchs/AG
und ibW in Maienfeld

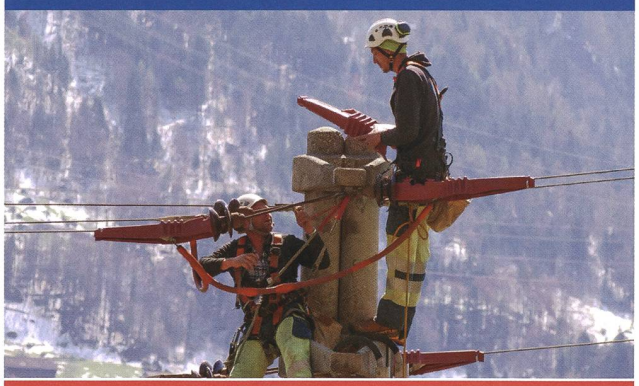
Infos und Anmeldung:
strom.ch/power-quality-fachkraft

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

VSE AES

SIGMAFORM

Ihr Spezialist für Vogel- und Kleintierschutz



Isolationssysteme zum Schutz von Masten, Freileitungsanlagen und Unterwerken

Sigmaform (Schweiz) AG
Langackerstrasse 25
CH-6330 Cham / ZG

Tel. +41 (0) 44 727 30 50
Fax +41 (0) 44 727 30 60

Seit 1981 erfolgreich am CH-Markt

info@sigmaform.ch
www.sigmaform.ch

Transparenz ist auch Teil der Energiestrategie

Die Energiestrategie 2050 gibt vor, dass «die Messdaten des betroffenen Endverbrauchers, Erzeugers oder Speicherbetreibers, namentlich die Lastgangwerte, für diesen verständlich dargestellt werden» müssen. Dies lässt sich am besten mit einem Kundenportal umsetzen, wo Lastgangdaten jederzeit abrufbar sind. Für die Erfüllung dieser Vorgabe bieten wir seit über sechs Jahren ein Kundenportal für Endkunden an. Währenddessen hat sich das Aussehen des Kundenportals immer wieder verändert und neue Funktionen sind hinzugekommen.

Ansprechendes Look & Feel mit einfacher Anwendung

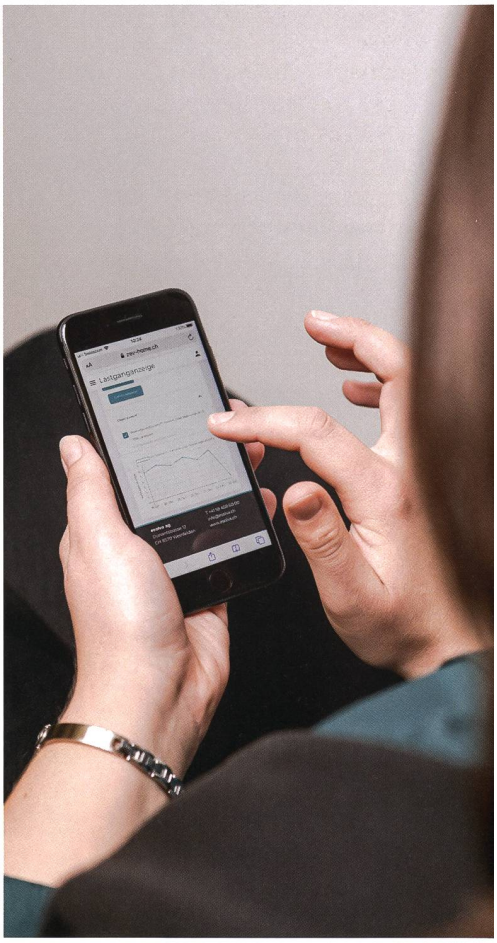
Eines ist klar: Ein modernes Erscheinungsbild erhöht die Benutzung des Kundenportals. Die Kunden loggen sich öfter in ein Portal ein, welches intuitiv, einfach zu bedienen und dem Stand der Technik angepasst ist. Diesen Punkten wurde besondere Aufmerksamkeit geschenkt, unabhängig vom Endgerät. Ob mit dem Tablet, Handy oder dem klassischen Desktop: Das Portal kommt immer übersichtlich und modern daher. Ausserdem war es uns wichtig, dass das Kundenportal direkt und problemlos in das Verrechnungssystem IS-E integriert ist. Wechselprozesse werden direkt als vorgefertigte Aktivitäten dem Sachbearbeiter zur Bestätigung bereitgestellt. Dies spart Zeit und reduziert Fehler.

Die Übersicht ist gewährleistet: Auch bei mehreren Liegenschaften

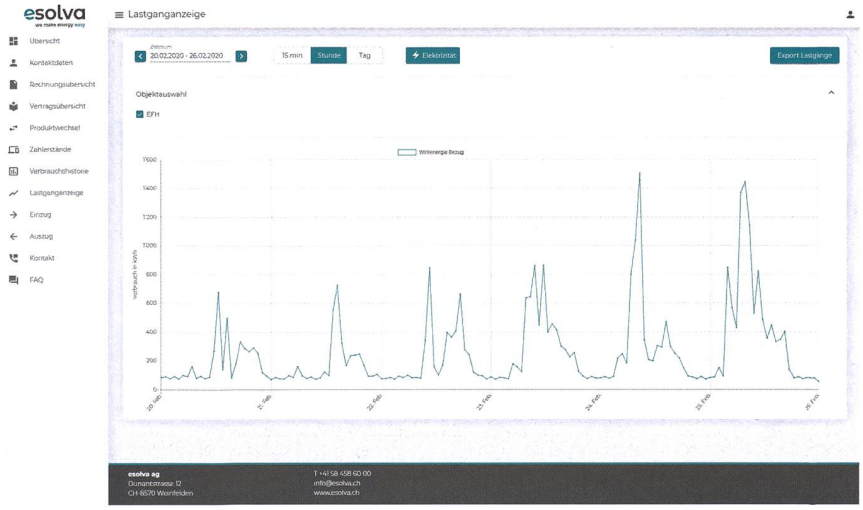
Alle Module, sei es die Vertragsübersicht, die Übersicht über die Verbrauchshistorie oder auch die Lastganganzeige, sind nach Liegenschaftsobjekt sortiert gelistet. Das ist vor allem für Verwalter praktisch, die so all ihre Objekte direkt miteinander vergleichen können. Auch PV-Anlagenbetreiber haben daraus den Vorteil, dass sie genau nachvollziehen können, welche Verträge mit dem EVU wegen der Stromlieferung und welche wegen des Stromkonsums geschlossen wurden. Grossverbraucher können den Verbrauch und die Verträge – auch für Liegenschaften, die ausserhalb des Netzgebietes beliefert werden – überprüfen.

Lastgangvisualisierung an die aktuellen Marktbedürfnisse angepasst

Die Vorgabe der «verständlichen Darstellung» ist zentral bei der Lastgangvisualisierung. Durch verschiedene Summierungen (von Viertelstundenwerten bis hin zu ganzen Wochen) und die individuelle Einstellung des Betrachtungsintervalls erfüllt die Visualisierung die Ansprüche jeder Gruppe: vom Laien bis zum Ingenieur. Als Neuerungen können jetzt auch mehrere Zähler einer Liegenschaft gleichzeitig dargestellt werden. Der Hauptgrund für diese Neuerung ist, dass so spezielle Zähler – z. B. von Batterien oder Ladestationen von Elektroautos – in die Darstellung integriert werden können, wenn sie vom EVU ausgelesen werden. Das EVU hat somit die Möglichkeit, seinen Kunden eine Gesamtübersicht über all ihre Strominfrastruktur zu bieten.



Zufriedene Kundin nutzt das Kundenportal oft.



Lastgangvisualisierung einfach, übersichtlich und aktuell dargestellt.

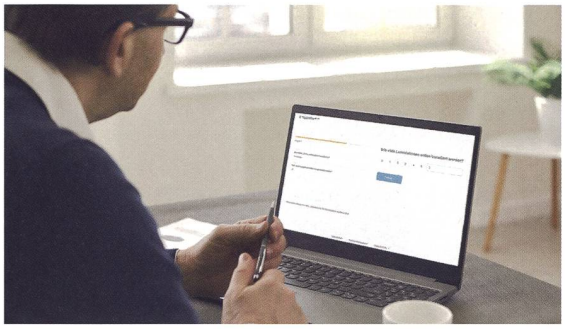
Klingt das spannend für dein EVU? Dann freuen wir uns über deine Kontaktaufnahme.

esolva ag
Dunantstrasse 12, 8570 Weinfelden
sales@esolva.ch
www.esolva.ch/angebot/kundenportal

In zwei Minuten zum E-Mobilitäts-System – Eturnity launcht Konfigurator

Nur zwei Minuten, und Sie kennen alle Komponenten und bei Bedarf den Preis Ihres gewünschten E-Mobilitäts-Systems. Das klingt fast zu einfach. Doch das Greentech-Start-up Eturnity hat genau solch einen bequemen Konfigurator umgesetzt.

Sektorenkopplung war in den SaaS-Lösungen des Greentech-Start-ups Eturnity schon immer zentral. Die Vertriebs-Software für Akquise, Beratung, Planung und Verkauf war seit Markteinführung 2015 auf alles, von PV, ZEV, Heizung und Fernwärme, bis zu E-Mobilität, ausgerichtet. Der E-Mobilitäts-Konfigurator stellt nun ein neues Glied im Eturnity-Portfolio dar.



Intuitive Eingabe des Ortes und der Anzahl Ladestationen.

Garantie: Dynamische Fragen in zwei Minuten ausgefüllt

Der neue Konfigurator führt dabei seine Nutzerinnen und Nutzer durch einen kurzen Fragebogen, der dynamisch aufgebaut ist, je nach Ausgangssituation. Im Anschluss erhalten Interessierte alle Infos zu den benötigten Komponenten, bei Bedarf auch als PDF mit Preisangabe.

Der grösste Vorteil ist laut Eturnity-CEO Matthias Wiget, dass die Firmen, die den Konfigurator einsetzen, selbst entscheiden, wie viele und welche Fragen gestellt werden sollen – ohne Programmieraufwand. Damit schafft Eturnity es, kostengünstig hoch-individualisierte Konfiguratoren anzubieten. Wie auch beim Solar- und Heizungsrechner der Eturnity AG wird das Thema Sektorenkopplung beim neuen Konfigurator berücksichtigt, denn das Interesse an einer PV-Anlage beispielsweise lässt sich mit abfragen.

Mehr dazu unter: www.eturnity.ch

Cyberangriffe in Schaltanlagennetzwerken erkennen

Wie die Sicherheit von Schaltanlagen verbessert werden kann

Um die Cybersicherheit von digitalen Schaltanlagen sicherzustellen, sind Überlegungen auf mehreren Ebenen erforderlich. Mit Verschlüsselungsverfahren können zwar Geräte authentifiziert werden, allerdings verhindern diese Massnahmen nicht alle Angriffe. Firewalls und «Air Gaps» lassen sich mit vorhandenen Remote-Access-Tunneln oder durch Wartungscomputer, die direkt an die IEDs oder den Anlagenbus angeschlossen sind, umgehen. Deshalb erfordert es Massnahmen für das Erkennen von Angriffen, die schnelle Reaktionszeiten sicherstellen und die Folgen auf ein Minimum reduzieren.

Das Intrusion Detection System StationGuard wurde speziell für den Einsatz in Schaltanlagen entwickelt.

Intrusion Detection Systeme für Schaltanlagen

Daher empfehlen die meisten Sicherheits-Frameworks die Verwendung eines «Intrusion Detection Systems» (IDS) – einem Einbruchserkennungssystem, ein bekannter Begriff in der klassischen IT –, um Bedrohungen und bösartige Aktivitäten im Netzwerk zu erkennen. Diese IDS werden heute immer häufiger im Bereich der Stromversorgung eingesetzt.
IDS aus der klassischen IT sind für den Einsatz in einer Anlagenumgebung nicht geeignet. Während sich die klassische IT-Sicherheit mit Hochleistungsservern und deren unzähligen simultanen Verbindungen beschäftigt, befasst sich die IT-Sicherheit in Schaltstationen mit Geräten, die begrenzte Ressourcen aufweisen, proprietären Betriebssystemen, Echtzeit-Anforderungen und speziellen Redundanzprotokollen.

Lernbasierte Systeme

Um ihre Systeme in die Lage zu versetzen, unbekannte Angriffe zu erkennen, verwenden viele Anbieter eine «Lernphase» bei ihren Lösungen. Diese Systeme beobachten die Häufigkeit und den Zeitpunkt bestimmter Protokollmarker. Damit soll das übliche Verhalten des Systems erlernt werden. Nach der Lernphase wird immer dann ein Alarm ausgelöst, wenn einer der Marker deutlich ausserhalb des erwarteten Bereichs liegt. Dies hat zur Folge, dass Fehlalarme für alle Ereignisse ausgelöst werden, die während der Lernzeit nicht aufgetreten sind. Dabei handelt es sich beispielsweise um Schutzereignisse, Schalt- oder Automatisierungsaktionen oder die routinemässige Instandhaltung und Prüfung. Ein weiteres Problem ist, dass die Alarmmeldungen in Form von technischen Protokolldetails ausgedrückt werden, weil diese IDS die Vorgänge in der Anlage nicht kennen. Somit können Alarme nur von einem Ingenieur geprüft werden, der mit den Einzelheiten des IEC-61850-Protokolls und mit der IT-Netzwerksicherheit vertraut ist. Deshalb tritt bei jeder Anlage eine Vielzahl von Fehlalarmen auf, die eine Überprüfung durch hochqualifiziertes Personal erfordern. Dies führt nicht selten dazu, dass Alarme ignoriert oder verworfen werden, ohne dass die notwendige Prüfung erfolgt, und das IDS schliesslich abgeschaltet wird.

Der StationGuard-Ansatz

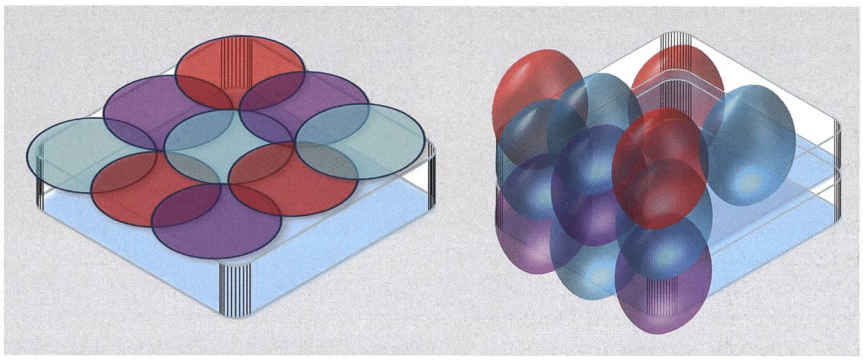
Für IEC-61850-Anlagen wird das gesamte Stationsautomatisierungssystem mit allen Geräten, den Datenmodellen und den Kommunikationsmustern in einem standardisierten Format, der SCL (System Configuration Language), beschrieben. SCD-Dateien (System Configuration Description) enthalten in der Regel auch Informationen über primäre Betriebsmittel. Für eine stetig wachsende Anzahl von Anlagen ist sogar schon das Prinzipschaltbild in der SCD enthalten.
Mit diesen Informationen lässt sich ein anderer Ansatz für die Erkennung von Angriffen verwenden: Das Monitoring-System kann ein vollständiges Systemmodell des Stationsautomatisierungssystems sowie der Schaltanlage erstellen und jedes einzelne Paket im Netzwerk mit dem Live-Systemmodell vergleichen. Auch die in den kommunizierten Nachrichten (Goose, MMS, SV) enthaltenen Variablen lassen sich anhand der aus dem Systemmodell abgeleiteten Erwartungen bewerten. Dieser Prozess ist ohne Lernphase und allein durch die Konfiguration des IDS mit der SCL möglich. Im neuen funktionalen Sicherheitsüberwachungssystem StationGuard wird genau dieser Ansatz umgesetzt. Damit wird nicht nur der Aufwand in der Installationsphase deutlich reduziert, sondern auch die Anzahl der Fehlalarme während dem Betrieb des Systems minimiert.
Durch die Darstellung der erkannten Ereignisse in der Sprache der Schutz- und Leittechniker bietet StationGuard zusätzlich den Vorteil, dass Schutz- und Leittechniker sowie IT-Security-Verantwortliche bei der Suche nach der Alarmursache und deren Behebung optimal zusammenarbeiten können.

Weitere Informationen:
Omicron Electronics GmbH
Oberes Ried 1, 6833 Klaus, Österreich
www.omicronenergy.com/stationguard
Tel. +43 59495 4444

WiFi-Planung, aber wie?

Um zeitgemässe Kommunikationslösungen End-to-End anzubieten, werden heute mehrheitlich WiFi-Access-Points (WAPs) benötigt. Es stellt sich jedoch die Frage, wo solche Geräte positioniert werden müssen, damit eine gute Signalabdeckung ohne Störungen möglich ist. Je nach Qualitätsanspruch eines Kunden wird bereits bei der Planung viel Wert darauf gelegt, ein System höchster Effizienz auszulegen. Ist dabei noch ein entsprechendes Netzwerkmanagement und eine Heatmap vorhanden, können Störungen und ein reibungsloser Betrieb jederzeit gewährleistet werden. Dies verhindert viel Ärger und nachträgliche Kosten.

Bereits bei der Planung sollte darauf geachtet werden, wie gross die Immobilie ist, welche verbauten Materialien und Frequenzbänder eingesetzt werden. Holz und Glas sind zum Beispiel durchgängiger für WiFi-Signale, Steinwände und Beton schirmen gut ab, und Metall ist sehr schlecht durchdringbar. Je genauer die Bausubstanz bekannt ist, desto besser stimmt die Planung mit der Installation überein. Weiter ist zu beachten, dass das 2,4-GHz-Frequenzband weniger abgeschwächt wird als das 5-GHz-Frequenzband.



Zweidimensionale (links) versus dreidimensionale Planung.

Die Grobplanung: Diese Art ist sicher die einfachste, schnellste, aber auch die ungenaueste Möglichkeit einer WiFi-Planung. Man kann zum Beispiel pro Schulzimmer einen Access Point vorsehen oder ein Bürogebäude in Zellen unterteilen und diese entsprechend ausrüsten. Dazu braucht es keine spezielle Software. Dies mag für den Heimbereich genügen, ist aber für eine professionelle Umgebung nicht zu empfehlen, da mögliche Störungen nicht vorher erkannt werden.

Die virtuelle Planung: Bei dieser Variante bezieht man Daten des Gebäudes mit ein, also die Baumaterialien und ihr Abschirm- und Reflexionsverhalten. Dies ist vor allem wichtig, wenn man nicht nur zweidimensional, sondern dreidimensional planen muss, was in Bürogebäuden oft der Fall ist. Damit erreicht man eine mittlere Effizienz.

Die effektive Planung: Die genauste Variante erfordert eine Ausmessung vor Ort. Damit erreicht man, dass nicht Plandaten in die Berechnung einfliessen, sondern die effektiven Werte der Bausubstanz. Mit dieser Methode erreicht man die höchste Effizienz.

Zellplanung und WiFi-Betriebsarten
Um Störungen zu minimieren, sollte jeder Access Point keine Frequenzüberlagerung mit seinen Nachbarn haben. Bei einer zweidimensionalen Planung ist dies schon eine Herausforderung, bei einer dreidimensionalen Planung, welche die Realität abbildet, noch um einiges aufwendiger.

Maximaler Datendurchsatz oder einfach nur Flächenabdeckung?
Je nach Ansatz kann die Datenrate maximiert werden oder es kann auch nur sichergestellt werden, dass ein WiFi-Signal flächendeckend vorhanden ist. Je nach Technologiewahl werden Restriktionen in Kauf genommen.

So liefert ein Multikanal Ansatz einen höheren Datendurchsatz, und die maximale Anzahl der Geräte skaliert mit der Anzahl der Access Points. Es gibt ein Roaming, und beim Übergang ist mit längeren Unterbrüchen zu rechnen. Es kann zu Interferenzen kommen, und die Kanalplanung ist schwierig, weshalb eine Begehung vor Ort empfohlen wird.

Ein Einzelkanal-WiFi-Netzwerk zeigt kaum Störungen vom eigenen Kanal, und es gibt keine Unterbrechungen. Die Platzierung ist weniger kritisch, und durch weitere Access Points sind Erweiterungen zu einem späteren Zeitpunkt einfach. Die Bandbreite ist aber geringer, da man ein einheitliches Funkfeld erstellt, und darin auch weniger Geräte pro Access Point möglich sind.

Mit Softwareunterstützung kann bei den Messungen oder Berechnungen eines WiFi-Netzwerk eine Heatmap erstellt werden, welche die Signalstärken im Abdeckungsbereich bereits bei der Planung grafisch darstellt.

Mit den WiFi Access Points erweitert BKS das Produkte- und Serviceangebot an Endkunden, Installateure und Bauherren im Netzwerkbereich und bietet somit auch kabellose End-zu-End-Lösungen aus einer Hand an.

BKS DIGITAL CONNECTIVITY SOLUTIONS

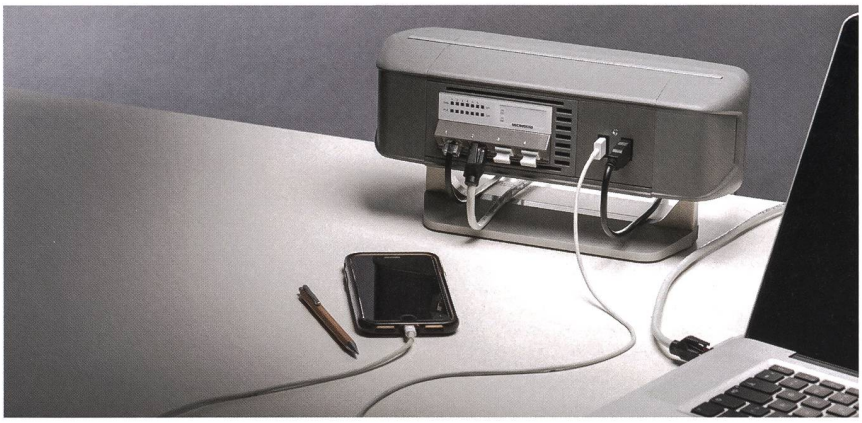
BKS Kabel-Service AG
Fabrikstrasse 8
4552 Derendingen

Tel. 032 681 54 54
info@bks.ch
www.bks.ch

Glasfaser bis an den Arbeitsplatz

Das Fiber to the Desk (FTTD) Konzept der Diamond SA führt die Glasfaser bis an den Arbeitsplatz. Dank der einfachen Handhabung ist es sowohl für Fachleute als auch für Anwender optimal ausgelegt.

Der DiaDesk vereint wichtige Schnittstellen in einem attraktiven Gerät. So sind Switch, Steckdosen und USB Power Adapter stets bequem am Arbeitsplatz verfügbar. Sowohl Einzelbüros als auch Arbeitsplatzinseln können unkompliziert erschlossen werden. Der robuste DiaLink-Steckverbinder kann mit seiner Zugkappe mit einer Zugkraft von bis zu 300 N direkt in Rohre eingezogen werden, ohne dabei beschädigt oder verunreinigt zu werden. Anschliessend reicht ein einfaches Einstecken in die Steckdose; ganz ohne Hilfe von Spleiss- oder anderen Spezialgeräten oder Werkzeugen. In Netzwerkinstallation sind Patchpanel, Anschlussdosen und Verbinder wichtige Bestandteile von Glasfasernetzen, denn sie helfen, die Effizienz und Qualität aufrechtzuerhalten.
Für zuverlässige und effiziente Datenübertragungen werden aktive Komponenten eingesetzt, welche Daten im Glasfasernetz übertragen. Diamond SA bietet hierfür verschiedene Qualitätslösungen an, um optimale und leistungsstarke Standards erfüllen zu können. Auf diese Weise kann ein zuverlässiger und effizienter Datentransfer sowie eine wartungsarme Struktur gewährleistet werden.



Fiber to the Desk bietet ultraschnelle Datenraten bis zum Pult.

www.diamond.ch/ukv

Cyber Security

Online Schulung für Mitarbeitende aller Stufen

Wir bieten drei Schulungsmodule zur Sensibilisierung Ihrer Mitarbeitenden an. Besondere Vorkenntnisse sind nicht erforderlich. Als Auftraggeber werden Sie über Ausbildungsstand und Testresultate informiert. Zeitaufwand pro Modul 30 bis 50 Minuten.

- Modul «Grundlagen»
- Modul «Sicheres Verhalten»
- Modul «Social Engineering»

Weitere Informationen:
strom.ch/cyber

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

BULLETIN SEV/VSE | BULLETIN SEV/AES

112. Jahrgang | **112e année**
ISSN 1660-6728
Erscheint 10-mal pro Jahr | **Paraît 10 fois par an**

Herausgeber | Éditeurs
Electrosuisse und Verband Schweizerischer Elektrizitätsunternehmen (VSE)
Electrosuisse et Association des entreprises électriques suisses (AES)

Verlag | Éditions
Marcel Stöckli, Leitung/**Direction**, Tel. 058 595 12 50, marcel.stoeckli@electrosuisse.ch
Electrosuisse, Luppmenstrasse 1, 8320 Fehraltorf, www.bulletin.ch

Redaktion Electrosuisse | Rédaction Electrosuisse
Informations-, Kommunikations- und Energietechnik
Techniques de l'information, de la communication et de l'énergie
Radomír Novotný (No), El.-Ing. HTL, BA, MA, Chefredaktor/**Rédacteur en chef**,
Tel. 058 595 12 66
Cynthia Hengsberger (CHe), **Dr ès sc./dipl. en électronique-physique**,
Redaktorin/**Rédactrice**, Tel. 058 595 12 59
Schweizerisches Elektrotechnisches Komitee / **Comité Electrotechnique Suisse (CES)**,
Tel. 058 595 12 69
Luppmenstrasse 1, 8320 Fehraltorf, bulletin@electrosuisse.ch

Redaktion VSE/AES | Rédaction VSE/AES
Elektrizitätswirtschaft, Energiepolitik/**Économie électrique, politique énergétique**
Ralph Möll (Mr), lic. phil., Chefredaktor/**Rédacteur en chef**, Tel. 062 825 25 21
Valérie Bourdin (VB), lic. phil., Redaktorin/**Rédactrice**, Tel. 021 310 30 23
Hintere Bahnhofstrasse 10, 5000 Aarau, bulletin@strom.ch

Titelbild | Couverture
Remo Inderbitzin

Anzeigenverkauf | Vente des annonces
Zürichsee Werbe AG, Marc Schättin, Laubisrütistrasse 44, 8712 Stäfa
Tel. 044 928 56 17, bulletin@fachmedien.ch

Auflagen (WEMF 2020) | Tirages (REMP 2020)

WEMF-SW-Auflagenbeglaubigung/**Certification des tirages par la REMP/FRP**	7176
Total verkaufte Auflage/**Total tirage vendu**	7176
Total Gratisauflage/**Total tirage gratuit**	0

Adressänderungen und Bestellungen | Changements d'adresse et commandes
Therese Girschweiler, Electrosuisse, Luppmenstrasse 1, 8320 Fehraltorf
Tel. 058 595 12 60, verband@electrosuisse.ch

Preise | Prix
Abonnement CHF 225.– (Ausland: zuzüglich Porto/**Etranger: plus frais de port**)
Einzelnummer CHF 25.– zuzüglich Porto/**Prix au numéro CHF 25.– plus frais de port**
Das Abonnement ist in den Mitgliedschaften von Electrosuisse und VSE enthalten.
L'abonnement est compris dans les affiliations à Electrosuisse et à l'AES.

Produktion | Production
Layout, Korrektorat/**Mise en page, correction:** Somedia Production AG,
Zwinglistrasse 6, 8750 Glarus, www.somedia-production.ch
Druck/**Impression**: AVD Goldach, Sulzstrasse 10-12, 9403 Goldach, www.avd.ch

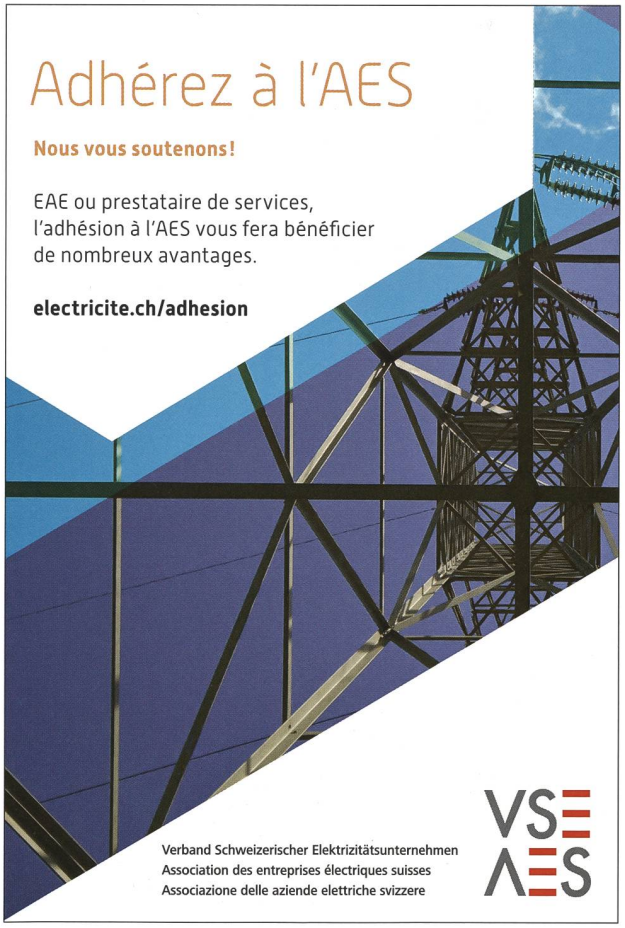
Nachdruck: Nur mit Zustimmung der Redaktion
Reproduction: Interdite sans accord préalable de la rédaction
Gedruckt auf chlorfrei gebleichtem Papier/**Impression sur papier blanchi sans chlore**

Die Fremdbeiträge im Fachteil geben die Meinung des jeweiligen Autors wieder. Sie muss sich nicht mit derjenigen der Redaktionen oder der Verbände VSE und Electrosuisse decken. Die Verbandsteile VSE und Electrosuisse geben die Meinung des jeweiligen Verbands wieder, welche nicht mit derjenigen des anderen Verbandes übereinstimmen muss.
Les articles dans la partie spécialisée reflètent l'avis de l'auteur et ne correspondent pas forcément à ceux des rédactions ou des associations AES et Electrosuisse. L'AES et Electrosuisse représentent l'avis de leur association qui n'est pas forcément celui de l'autre association.

Die in dieser Ausgabe des Bulletins SEV/VSE aufgeführten Adressdaten dürfen nicht für Werbezwecke verwendet werden.
Les adresses mentionnées dans cette édition du Bulletin SEV/AES ne peuvent être utilisées à des fins publicitaires.
I dati relativi ad indirizzi elencati in questo numero del Bulletin SEV/AES non possono essere utilizzati per scopi pubblicitari.

Offizielles Publikationsorgan von Electrosuisse und VSE
Organe officiel de publication d'Electrosuisse et de l'AES

Publikation 2021 FOKUSSIERT KOMPETENT TRANSPARENT
Publication 2021 CIBLÉ COMPÉTENT TRANSPARENT

Inserenten | Annonceurs

Arnold Engineering, 8152 Opfikon/Glattbrugg	19
Suva, 6002 Luzern	49
Universität Freiburg, 1700 Fribourg	72
Eturnity AG, 7000 Chur	75/97
Abacus Research AG, 9300 Wittenbach	19
Diamond SA, 6616 Losone	19/100
Robert Fuchs AG, 8834 Schindellegi	104
Swisscom (Schweiz) AG, 8901 Urdorf	34/93/94
Regionalwerke AG Baden	81
René Koch AG, 8804 Au-Wädenswil	81
Siemens Schweiz AG, 8047 Zürich	39
Sigmaform (Schweiz) AG, 6330 Cham	95
Hager AG, 6021 Emmenbrücke	65
BKS Kabel-Service AG, 4552 Derendingen	2/99
CTA Energy Systems AG, 3110 Münsingen	15
Omicron electronics GmbH, 6833 Klaus	15/98
Traco Electronic AG, 6340 Baar	39
InnoSolv AG, 9015 St. Gallen	25
VSAS Verband Schaltanlagen, 2503 Biel-Bienne	83
CFW EMV-Consulting AG, 9411 Reute AR	103
Brother (Schweiz) AG, 5405 Dättwil	30
Sysdex AG, 8600 Dübendorf	24
esolva ag, 7302 Landquart	96