OVE Aktuell – Informationstechnik „IoT Security“
GIT – Gesellschaft für Informations- und Kommunikationstechnik
Juli 2020

Sehr geehrte Damen und Herren!

Nachfolgend erhalten Sie den Newsletter OVE Aktuell, diesmal mit dem **Schwerpunkt „IoT Security“**. Zu unserer „alten Normalität“ zurückkehrend, machen wir Sie an dieser Stelle gerne wieder auf künftige **Veranstaltungen des OVE** aufmerksam. Zum jetzigen Zeitpunkt sollte der Durchführung der Veranstaltungen nichts im Wege stehen, selbstverständlichen behalten wir mögliche COVID-19-bedingte Maßnahmen im Auge. Etwaige Änderungen sowie weitere Informationen zu unserem Ausbildungsangebot finden Sie auf unserer Website.

01.-03.09.2020: Sicherheit und Arbeitsabläufe in der Elektrotechnik, ONLINE-Seminar

15.-16.09.2020: Geräte / Betriebsmittel, wiederkehrende Prüfung und Überprüfung nach Reparatur ÖVE/Önorm 8701, ONLINE-Seminar

15.09.2020: Digital Grid, Workshop, Wien

17.09.2020: Planungsgrundsätze für die Errichtung von Trafostationen, Seminar, Wien

24.09.2020: Prüfungen von Niederspannungsanlagen; Seminar, Wien

28.-29.09.2020: E-Mobilität für Anwender, ONLINE-Seminar

IoT-Termine:

14.10.2020: IoT und Data Science, Wien, Seidler Consulting

04.11.2020: 4. IoT Fachkongress, Wien, Austrian Standards

05.11.2020: IoT Forum CE, Wien, SUCCUS

10.12.2020: Summit Industrie 4.0, Graz, Plattform Industrie 4.0

Weitere Neuigkeiten aus dem OVE finden Sie am Ende dieses Newsletters.

IoT Security

IoT Security als Basis von Industrie 4.0

Die derzeitige Krise hat uns dramatisch vor Augen geführt, wie abhängig wir von reibungslos funktionierenden grenzüberschreitenden Lieferketten sind. War in der aktuellen Situation der Ausfall von Fertigungs- und Transportkapazitäten aufgrund der Ausgangsbeschränkungen und Grenzschließungen der ausschlaggebende Faktor, könnte in Zukunft auch ein Zusammenbruch der digitalen Infrastruktur zu ähnlichen oder gar noch schlimmeren wirtschaftlichen Folgen führen. Es ist daher unumgänglich zu überlegen, wie wir die derzeitigen komplexen Produktionssysteme gegen Angriffe (und Störungen) verlässlich absichern können und wie wir verhindern können, dass durch einen Cyber-Angriff ganze Produktionsketten lahmgelegt werden.

IoT spielt in modernen Produktionssystemen eine zentrale Rolle, da mittels IoT Informationen über den Zustand der Produktionsanlagen, der Warenflüsse, bis hin zum Zustand des Transportgutes gesammelt und ausgetauscht werden. Da IoT alle Ebenen der Produktion durchdringt, sind die Sicherheitsanforderungen entsprechend breit gefächert. Auf der einen Seite müssen Produktionsanlagen physischen Schaden verhindern (Safety), während auf der anderen Seite auch die digitale Sicherheit gewährleistet sein muss (Security). Die Interessen der Operational Technologies (OT) und Information Technologies (IT) müssen in solchen Bereichen von Anfang an (sprich schon beim Design der Systeme) berücksichtigt werden. Zusätzlich ist eine laufende Überwachung der Systeme erforderlich, um allfällige Störungen oder Angriffe frühzeitig erkennen und entsprechende Gegenmaßnahmen einleiten zu können. Darüber hinaus ist auch das laufende Management der Anlagen ein wesentlicher Sicherheitsfaktor. Durch Integration der mittels IoT gesammelten Daten können digitale Zwillinge der Produktionsanlagen erstellt werden, die Vorhersagen und Analysen über den Lebenszyklus ermöglichen.

In diesem Newsletter wollen wir die Sicherheitsanforderungen an IoT im Produktionsumfeld und mögliche Lösungskonzepte näher betrachten. Im ersten Artikel beleuchtet Christos Thomos (Infineon Technologies Austria) die Anforderungen an industrielle IoT-Systeme (IIoT) und stellt Ergebnisse aus dem nationalen IoT Security-Leitprojekt IoT4CPS vor. Im zweiten Beitrag berichten Paul Smith und David Allison (beide: AIT) wie Digital Twins zur Absicherung von IIoT-Systemen genutzt werden können und welche offenen Fragestellungen noch bestehen. Welche Aspekte bei der Absicherung von IIoT-Systemen betrachtet werden müssen, erläutern Heribert Vallant, Katharina Hofer-Schmitz und Christian Derler (Joanneum Research) im dritten und letzten Beitrag.

Wir hoffen, dass diese Themen bei Ihnen, werte Leserinnen und Leser, auf Interesse stoßen und wünschen Ihnen eine spannende Lektüre dieses Newsletters. Diskussionsbeiträge, Terminhinweise, Kommentare und Anregungen an informationstechnik@ove.at sind wie immer herzlich willkommen!

Dr. Mario Drobics
OVE Informationstechnik
Arbeitsgruppenleiter „IoT Security"
Head of Competence Unit Cooperative Digital Technologies
AIT Austrian Institute of Technology
Kontakt: mario.drobics@ait.ac.at

Secure IoT für Industrie 4.0

Die industrielle Produktion entwickelt sich seit ihrer Einführung ständig weiter. Aktuell beginnt mit der so genannten Industrie 4.0 die 4. Phase, welche geprägt ist von der Konvergenz von OT/IT und durch steigende Digitalisierung von Fertigung und Produkten neue Wertschöpfungsketten, Geschäftsmodelle und Einnahmequellen schafft. Die Hauptziele umfassen einen höheren Automatisierungsgrad für Produktionsprozesse mit zunehmend intelligenten und integrierten Lieferketten, Produktivitätsoptimierung über den Betrieb hinweg und vorausschauende Wartung durch ein Überwachungs-, Diagnose- und Präskription-System, um die Fertigung an die Kundenbedürfnisse anzupassen.

Die wichtigsten Komponenten, die die Entwicklung von Industrie 4. 0 prägen, sind Technologien, wie das industrielle Internet of Things (IoT), basierend auf vernetzten intelligenten Sensoren, Aktoren, Industriegeräten und IT-Systemen, kollaborativen Cyber-Physical-Produktions-Systemen mit stark verflochtenen digitalen und physischen Komponenten, Big/Smart-Data-Analysen, die auf Konzepten wie dem Digital Twin und der On-Demand-Verfügbarkeit von Computing-Ressourcen auf Basis von Edge/Fog- und Cloud-Diensten aufbauen. Der Einsatz solcher Technologien und Systeme im Produktionsprozess führt zum Konzept der Smart Factory, das sich auf die technologische Entwicklung von isolierten (security-through-obscurity) industriellen Embedded-Systemen hin zu einer ICT-basierten Integration vernetzter Objekte bezieht, die intelligente Netzwerke autonomer cyber-physikalischer Systeme bilden. Diese Systeme sind in der Lage, physische Prozesse in digitale Daten umzuwandeln, die verarbeitet und analysiert und dann zurückgespeist werden können, um digitale Aktionen wieder in die physische Domäne zu bringen.

Disruptive Lieferkettenkonfigurationen, basierend auf diesen Fortschritten, können Herstellern einen enormen Wettbewerbsvorteil verschaffen, indem sie neue Wachstumschancen und Rentabilität durch ein vertikal integriertes, fortschrittliches Fertigungsgerüst mit selbstkonfigurierenden, selbstüberwachenden und selbstheilenden Eigenschaften ermöglichen. Gleichzeitig gibt es jedoch viele Herausforderungen, die berücksichtigt werden müssen, wenn industrielle Technologien und Geräte einer IT-Welt ausgesetzt werden, die voll von Malware und Cyberangriffen ist. Trotz der rasanten Weiterentwicklung von High-Performance-Computing, hochwertigen Sensoren, Kommunikationsnetzen, Künstlicher Intelligenz, autonomer Robotik und IKT wollen die meisten Industriehersteller die Kontrolle über ihre Daten behalten, um Zuverlässigkeit, Sicherheit und Datenschutz gewährleisten zu können. Diese Bedenken bleiben für den industriellen Bereich bisher aber noch unbeantwortet. Der Grund dafür ist, dass das industrielle IoT und der OT-Bereich immer noch auf einem Ökosystem voll alter, proprietärer Technologien und einer Vielzahl von Gerätetypen basieren, die jeweils mit verschiedenen Funktionalitäten in eine Vielzahl von Endmärkten übergehen, mit verschiedenen Betriebssystemen sowie Funkfrequenzen arbeiten und verschiedene Protokolle mit unterschiedlichen Rechenleistungen und Speicherkapazitäten verwenden. Dies erfordert andere Strategien als in modernen IT-Umgebungen, die sicherlich auf Homogenität angewiesen sind, da es wenig Vielfalt in Gerätetypen, Funktionen und Betriebssystemen und viele gemeinsame, etablierte Standards, Protokolle, Sprachen und Plattformen gibt, die Interoperabilität fördern. Gleichzeitig erfordert ein industrielles IoT eine durchgehende, sichere und zuverlässige Verbindung, sowohl kabelgebunden als auch drahtlos, um den neuen Anwendungserfordernissen gerecht werden zu können. Kommunikation in einer dezentralen Architektur ist sicher, wenn sie sich von den Edge-Geräten bis zum Cloud-Netzwerk erstreckt, um eine vollständige, durchgängige und zuverlässige Verbindung zu gewährleisten. Dazu gehören sowohl die im CPPS gespeicherten Daten als auch die im Netz befindlichen. Die Daten im Transit sind anfälliger für Cyber-Angriffe, da das Sicherheitsniveau an jedem Routing-Punkt des Netzes überwacht werden muss. Dies steht im Einklang mit der Tatsache, dass CPPS-Systeme anfällig für Cyber-Sicherheitsangriffe sind, da sich der Austausch zwischen der physischen und der Cyber-Welt auf einem gehobenen Niveau befindet.

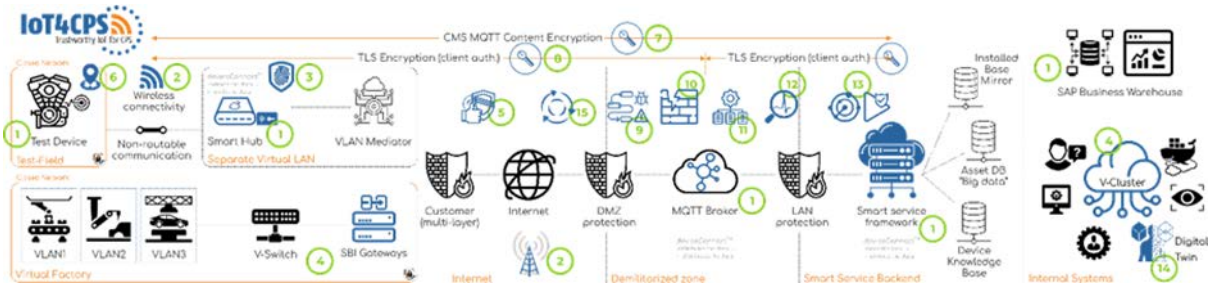
In diesem neuen Rahmen können industrielle IoT-Systeme noch nicht die kryptografische Agilität bieten, die in vielen industriellen Sicherheitsanwendungen erforderlich ist. Diese Anwendungsfälle könnten Herausforderungen beinhalten, wie:

- Sicherheitsmaßnahmen im industriellen Umfeld, die häufig verwendete Architekturen ausschließen könnten
- Ressourcenbeschränkungen von Kommunikationskanälen (Low-Power-WAN-Protokolle erlauben es Geräten, Energie zu sparen, aber dies bedeutet zusätzliche Sicherheitsprobleme) und von Geräten (z. B. geringe/verlustige Bandbreite, geringe Rechenressourcen usw.)
- Gruppen-Schlüssel-Verhandlungen für Multicast-Kommunikation mit geringem Risiko für Kompromittierung, wenn der Schlüssel abgefangen wird
- hohe Mobilität von Geräten, die Anpassungen erfordern, um die Kryptokosten aufgrund der Netzwerkdynamik zu reduzieren, und häufige Konfigurationen mit Test- und Debugging-Bedürfnissen
- kontinuierliche Software-/Firmware-Updates, die zusätzliche Schwachstellen schaffen könnten
- Integritäts- und Authentizitätsprüfungen und die Überprüfung des Verhaltens von Geräten und Systemen
- Protokollübersetzungen, die zusätzliche End-to-End-Sicherheitsmaßnahmen und Unterstützung bei der Produktlebenszyklusverwaltung erfordern

Der Schlüssel zur Lösung dieser Herausforderungen in einem industriellen Umfeld besteht darin, industrielle IoT-Geräte und deren Netzwerk durchgängig zu sichern. Das heißt: während der Designphase durch zusätzliche Sicherheit bei der Hardware- und Anwendungsentwicklung, während der Bereitstellungs-Phase bei der Aktivierung der Geräte und Systeme und während des Lebenszyklus dieser Geräte durch Nutzung sicherer Plattformen und Dienste, um das Ökosystem, das Netzwerk, die Daten und die Geräte bis zum Funktionsende zu schützen.

Bisher gab es verschiedene Allzwecklösungen (z. B. TLS, DTLS, IKEv2/IPSec, HIP, PANA, Kerberos, etc.), die an IoT-spezifische Sicherheitsprotokolle angepasst sind (z. B. ACE-OAuth, HIPDEX, OSCORE, ACME), Protokolle, die den Ressourcenverbrauch reduzieren (basierend auf ECC, z. B. X25519, ChaCha, DietHIP) und Protokolle, die gegen DoS resistent sind. Außerdem wurden verschiedene bestehende Standards und Best-Practice-Richtlinien, wie die NIST SP 800-Serie oder die ISO/IEC 270xx-Serie, aufgestellt, um Leitlinien für die Schaffung einer sicheren Kommunikation für eine End-to-End-Verbindung anzubieten. Diese bestehenden Standards und Leitlinien sollen in verschiedenen Bereichen der CPPS-Umgebung angewendet werden, um die sichere Vernetzung von Produktionssystemen und Produktionsanlagen in der Lieferkette und gleichzeitig die Zuverlässigkeit, Integrität und Verfügbarkeit der Daten (CIA) zu gewährleisten. Sichere Messaging-Protokolle wie Message Queuing Telemetry Transport (MQTT) oder Constrained Application Protocol (CoAP) werden verwendet, um Netzwerk- und Applikationsschicht-Sicherheit während des Datenaustausches zu garantieren.

In diesem Zusammenhang hat das von der FFG geförderte Forschungsprogramm IoT4CPS in den letzten zweieinhalb Jahren erfolgreich innovative Komponenten realisiert, die die Entwicklung, Produktion und Wartung sicherer IoT-basierter Anwendungen für vernetztes und automatisiertes Fahren sowie intelligente Produktion unterstützen. Die bereitgestellte Design-Framework-Bibliothek für zuverlässige IoT-Tools und -Lösungen umfasst konzeptionelle Richtlinien, wiederverwendbare Architekturmuster, Methoden und Tools, die den gesamten IoT-Lebenszyklus (Entwicklung, Produktion, Betrieb) in einem ganzheitlichen Ansatz abdecken, während sie als eine Reihe von Technologiebausteinen fungiert, um vertrauenswürdige industrielle IoT-Anwendungen zu entwickeln. Die folgende Grafik stellt eine Hauptarchitektur mit diesen Bausteinen dar.



IoT4CPS arbeitet bereits daran, die Anwendbarkeit dieser innovativen und zuverlässigen Komponenten im Labor- und Großindustrie-Demonstrator zu demonstrieren. Die Ergebnisse werden in den Projektdokumentationen und Whitepapers veröffentlicht, die auf der Projektwebsite https://iot4cps.at/zur Verfügung stehen.

Christos Thomos, PhD
Engineer R&D, Infineon Technologies Austria

Digital Twins für ein sicheres Industrial IoT

Industrie- und Produktionsumgebungen enthalten oft viele heterogene Systeme. In den letzten Jahren wurden diese Systeme digitalisiert, um Vorgänge zu ermöglichen, die von analogen Systemen nicht ausgeführt werden können. Heute wird dieses Phänomen das Industrial Internet of Things (IoT) oder Industrie 4.0 genannt. Diese modernen cyber-physischen Systeme – bei denen die operative Technologie (OT) auf die physische Maschinerie trifft – sind Ziele für hochentwickelte Bedrohungsakteure, die einen physischen Prozess stören wollen, um großen Schaden bei den Opfern zu verursachen.

Cyber-physische Systeme, insbesondere in der Fertigungsindustrie, sind datenreiche Umgebungen. Prozessdaten können mit IT-Software gesammelt werden, die auf OT-Hardware ausgeführt wird. Diese neuen Technologien haben die Schaffung des Digital Twins ermöglicht: ein virtuelles Modell eines realen Gebildes, das Echtzeit- und historische Daten verwendet, um Berechnungen im virtuellen Raum durchzuführen. Digital Twins können automatisch Analysen durchführen und bei Bedarf mit dem physischen Prozess interagieren. Da Digital Twins jedoch noch in den Kinderschuhen stecken, gibt es in diesem Bereich ein deutliches Defizit an Forschung im Bereich der Cyber Security. Das betrifft vor allem die Forschung zur Sicherheit von Infrastrukturen für den Betrieb digitaler Zwillinge sowie auch die Forschung zur Nutzung digitaler Zwillinge für Cyber-Sicherheitsanwendungen.

Der Digital Twin kann auch selbst als Vorteil bei der Sicherung eines cyber-physischen Systems dienen. Durch die Implementierung und Kombination verschiedener Modellierungstechniken kann ein vollständiges Bild des Systems in der realen Welt geschaffen werden.

Zu Beginn muss festgestellt werden, ob das System normal funktioniert. In einigen Fällen kann dies durch die Überwachung von Prozessvariablen und deren Vergleich mit vordefinierten Schwellenwerten erfolgen. Dynamischere und komplexere Systeme erfordern jedoch anspruchsvollere Modelle. Ein solches Modell – ein künstliches neuronales Netz (KNN) – kann auch diese Aufgabe erfüllen. Wenn ein KNN Prozessvariablen unter normalen Betriebsbedingungen genau vorhersagen kann, kann es verwendet werden, um die anormalen Bedingungen zu identifizieren, wenn die Vorhersagen des Modells ungenau werden.

Sobald die anormalen Bedingungen identifiziert wurden, ist es entscheidend, die Problemquelle zu finden. Die Unterscheidung zwischen Fehler und Cyber-Angriff ist nicht leicht, aber KNNs können auch in dieser Hinsicht helfen. Die Ausführung verschiedener Formen von Cyber-Angriffen, wie DoS-Flooding und ARP-Spoofing, gegen einen Digital Twin oder ein reales System und die Aufzeichnung der Digital Twin-Ergebnisse können einen gekennzeichneten Datensatz erschaffen. Auf diese Weise kann ein Modell erstellt werden, das die Symptome abnormaler Operationen in Kategorien bekannter Cyber-Angriffe klassifiziert und gleichzeitig Vertrauen für diese Klassifizierungen bietet.

Durch die Kombination der oben genannten KNNs ist es möglich, das spezifische Subsystem hervorzuheben, das von den Bedrohungsakteuren in der Tötungskette ins Visier genommen wird. Das kann dazu beitragen, die digitale Forensik und die Reaktionsteams für Zwischenfälle anzuleiten und die Reaktionszeit auf einen cyber-bezogenen Zwischenfall zu verkürzen.

An der Gewährleistung, dass ein cyber-physisches System vor Cyberattacken sicher ist, sind mehrere Akteure beteiligt, wie z. B. das Personal in der Leitwarte, das Personal in einem Security Operations Centre (SOC) und sogar Dritthersteller von Ausrüstung. Daher ist ein Rahmen für die gemeinsame Nutzung digitaler Twin Models und ihrer Daten wichtig, um die Zusammenarbeit zwischen diesen Beteiligten zu fördern. Dies kann das Bewusstsein des SOC erhöhen, indem es ermöglicht, sich auf die Bereiche der Anlage zu konzentrieren, die abnormales Verhalten produzieren. Infolgedessen können das SOC und das Betriebspersonal in einem frühen Stadium eines Vorfalls Entscheidungen treffen.

Das AIT wird diese Forschung fortsetzen, um herauszufinden, wie Digital Twins bei der Gestaltung von Sicherheitslösungen für industrielle Steuerungssysteme der nächsten Generation helfen können.

Dr. Paul Smith
Senior Scientist, AIT Austrian Institute of Technology
David Allison
Junior Scientist, AIT Austrian Institute of Technology

IoT in der Produktion sicher im Griff

Industrial IoT (IIoT) ist ein wesentliches Element im Zusammenhang mit Industrie 4.0. Das Ziel ist dabei, die Betriebszeiten der Maschinen bei unterschiedlichsten Losgrößen entlang des gesamten Produktentstehungsprozesses bestmöglich auszunutzen, um die optimale Produktivität unter Berücksichtigung des Instandhaltungsaufwands zu erreichen.

Die Cyber-Bedrohungslandschaft im Zusammenhang mit IoT ist vielfältig, entwickelt sich rasant weiter und hat enorme Auswirkungen auf die Sicherheit in den Produktionsanlagen sowie auf den Schutz des Firmen Know-hows.

Eine große Herausforderung für die Definition von wirkungsvollen Sicherheitsmaßnahmen im IoT-Umfeld ist die hohe Komplexität. Sie ergibt sich aus der Vielfalt der Anwendungsbereiche für IoT und stellt abgesehen von den einzelnen Applikationen auch vielfältige Schnittstellen und Features der IoT-Komponenten bereit. Eine weitere Problematik im industriellen Umfeld ist jedoch auch die OT-Thematik (Operational Technology) mit einer Vielzahl an Legacy-Systemen.

Daher ist es stets wichtig zu wissen, was abgesichert werden muss und welche spezifischen Sicherheitsmaßnahmen sich dafür anbieten. Die Identifikation der abzusichernden Assets in einem

komplexen System kann durch eine theoretische Modellierung des Sicherheitsstatus bewerkstelligt werden. Ein solcher Modellierungsansatz ist die so genannte Bedrohungsmodellierung, mit dem Ziel, potenzielle Bedrohungen und Schwachstellen basierend auf der Architektur des jeweiligen IT/OT-Systems zu identifizieren. Die Bedrohungsmodellierung kann bei bestehenden Produktionsumgebungen angewendet werden, ist aber auch besonders nützlich, wenn sie während der Entwurfsphase durchexerziert wird und bereits in einer frühen Phase die Sicherheitsprobleme und die wahrscheinlichsten Angriffsmethoden aufzeigt. Ein einmal so erstelltes Modell kann jederzeit mit den sich ständig ändernden Bedrohungen aktualisiert werden und damit die aktuelle Bedrohungslage abbilden. Neu in die Produktionsumgebung eingefügte Komponenten, wie z. B. IIoT-basierte Sensoren für die Instandhaltung, können einfach hinzumodelliert werden. Dadurch kann sofort festgestellt werden, inwieweit die neu hinzugefügten Komponenten die Bedrohungslage des gesamten Produktionssystems beeinflussen.

Ein weiterer Modellierungsansatz ist die so genannte „Formale Verifikation“. Dazu werden mathematische Ansätze zum Nachweis oder zur Widerlegung der Richtigkeit einer Software-/Hardwarekomponente in Bezug auf eine bestimmte formale Spezifikation und eine bestimmte Eigenschaft herangezogen. So kann eine formale Überprüfung angewendet werden, um beispielsweise die Protokollspezifika hinsichtlich Authentifizierung, Vertraulichkeit, Integrität oder Verschlüsselung oder aber auch die korrekte Bereitstellung der Daten und die Korrektheit von Algorithmen zu verifizieren.

Neben der Kommunikation und den Daten ist die Software das zentrale Element jedes IoT-Systems. Sie ermöglicht deren Funktionalität bzw. kann nützliche Mehrwertfunktionen bereitstellen. Um auch in der Softwareentwicklungsphase proaktiv gegen mögliche Schwachstellen im IoT-Umfeld vorgehen zu können, ist die Anwendung von Prinzipien des so genannten Secure Software Development Life Cycle unumgänglich. Dieser strukturierte Ansatz besteht aus verschiedenen Phasen und zielt darauf ab, sichere, effektive und effiziente Systeme gemäß ihrer Design-und Funktionsanforderungen bereitzustellen. So kann bereits in der Designphase der oben beschriebene Bedrohungsmodellierungsansatz angewendet werden, der wiederum auch nützliche Hinweise für ein effizientes Testen des Systems liefert, um die Behebung der zuvor identifizierten Bedrohungen zu verifizieren.

Neben der Applikationssoftware gibt es auch noch das Betriebssystem selbst, die Firmware, den Kommunikationstack sowie APIs zur Unterstützung der Interoperabilität, die abhängig vom Hersteller potentiell auch verschiedenartige Fehlerquellen aufweisen können. Um den Konsumenten hier einen Überblick bzw. eine Vergleichbarkeit von Komponenten hinsichtlich Cyber Security zu ermöglichen, hat die Europäische Kommission einen Verordnungsvorschlag mit dem Namen Cybersecurity Act vorgelegt, mit dem Ziel, eine einheitliche Zertifizierung von Cyber-Sicherheit auf europäischer Ebene zu gewährleisten. Zu diesem Zweck wurde die ENISA (European Union Agency for Cybersecurity) damit beauftragt, dieses so genannte Cybersecurity Certification Framework zu etablieren. Eurosmart ist das erste IoT-Zertifizierungsschema, das auf der Grundlage der Anforderungen des Cybersecurity Acts entwickelt wurde. Dabei wird mittels eines Security-Profils, welches die Sicherheitsanforderungen und Absicherungsmaßnahmen für ein IoT-Produkt im Konnex zu seiner Einsatzumgebung und den damit verbundenen Risiken definiert, eine Sicherheitszertifizierung durchgeführt.

Diese Zertifizierungen bieten für die sichere Einbindung zukünftiger Komponenten in die Produktionsumgebung eine wertvolle Grundlage. Um einen sicheren Einsatz der IoT-Komponenten zu ermöglichen, müssen diese Zertifizierungen aber immer im Zusammenhang mit den bereits im Einsatz befindlichen Komponenten betrachtet und durch eine laufend zu erweiternde Bedrohungsmodellierung, gekoppelt mit zyklischen (teilautomatisierten) Penetrationstests, abgesichert werden.

Dipl.-Ing. Heribert Vallant
Dipl.-Ing. Dr. Katharina Hofer-Schmitz
Dipl.-Ing. Christian Derler
alle: JOANNEUM RESEARCH, DIGITAL – Institut für Informations- und Kommunikationstechnologien, Kompetenzgruppe Cyber Security and Defence

Aktuelles aus dem OVE

Karl-Heinz Mayer in CENELEC-Verwaltungsrat gewählt
Die CENELEC-Generalversammlung am 18. Juni hat ein äußerst erfreuliches Wahlergebnis aus österreichischer Sicht gebracht: Karl-Heinz Mayer (Eaton Industries Austria) wurde in den Verwaltungsrat der europäischen Normungsorganisation gewählt.

Unfälle vermeiden: Sicher durch die Gewittersaison
In den Sommermonaten schlägt in Österreich durchschnittlich zwischen 100.000 und 250.000 Mal ein Blitz am Boden ein. ALDIS-Blitzexperte Dr. Gerhard Diendorfer hat Tipps, wie man sicher durch die Gewittersaison kommt.

OVE-Jahresbericht 2019 mit dem Schwerpunkt Energiewende
Der OVE-Jahresbericht 2019 mit dem Schwerpunktthema Energiewende ist da! Sie können den Jahresbericht online durchblättern, herunterladen oder in gedruckter Version anfordern.

Kostenfreie Normen für OVE Young Engineers
OVE Standardization bietet den OVE Young Engineers einen neuen Service: Zur Unterstützung von Studienarbeiten können sie die zutreffenden OVE-Normen und OVE-Richtlinien kostenfrei anfordern.

Wege aus der Krise: Bekenntnis zu Energiewende und Innovation
Kluge Konjunkturprogramme können Österreichs Wirtschaft aus der Krise führen. Die Umsetzung der Energiewende, aber auch die Stärkung des Innovationsstandortes Österreich bieten zahlreiche Möglichkeiten für zukunftweisende Investitionen. Im Rahmen eines Pressegesprächs hat der OVE seine Forderungen an die Regierung vorgestellt.

Krisensichere Berufe: Girls! TECH UP gibt Einblick in Welt der Technik
Die jüngsten Krisen beweisen einmal mehr, wie wichtig innovative Technik ist. Welche beruflichen Möglichkeiten die Welt der Technik Mädchen und jungen Frauen bietet, zeigt heuer bereits zum fünften Mal der Erlebnistag Girls! TECH UP.

"Klima wenden": Einreichfrist für Videowettbewerb verlängert
Aufgrund der aktuellen Situation wird die Einreichfrist für den Videowettbewerb von ScienceClip.at verlängert. Noch bis 13. November 2020 können Schülerinnen und Schüler ihr Video einreichen.

Mit freundlichen Grüßen
Ihr OVE Österreichischer Verband für Elektrotechnik

Hinweis: *Nicht immer werden in diesem Newsletter weibliche Formen explizit angeführt. Es wird jedoch ausdrücklich darauf hingewiesen, dass sich alle personenbezogenen Formulierungen grundsätzlich gleichermaßen auf Frauen und Männer beziehen.*

Impressum:
OVE Österreichischer Verband für Elektrotechnik
Krenngasse 37
8010 Graz