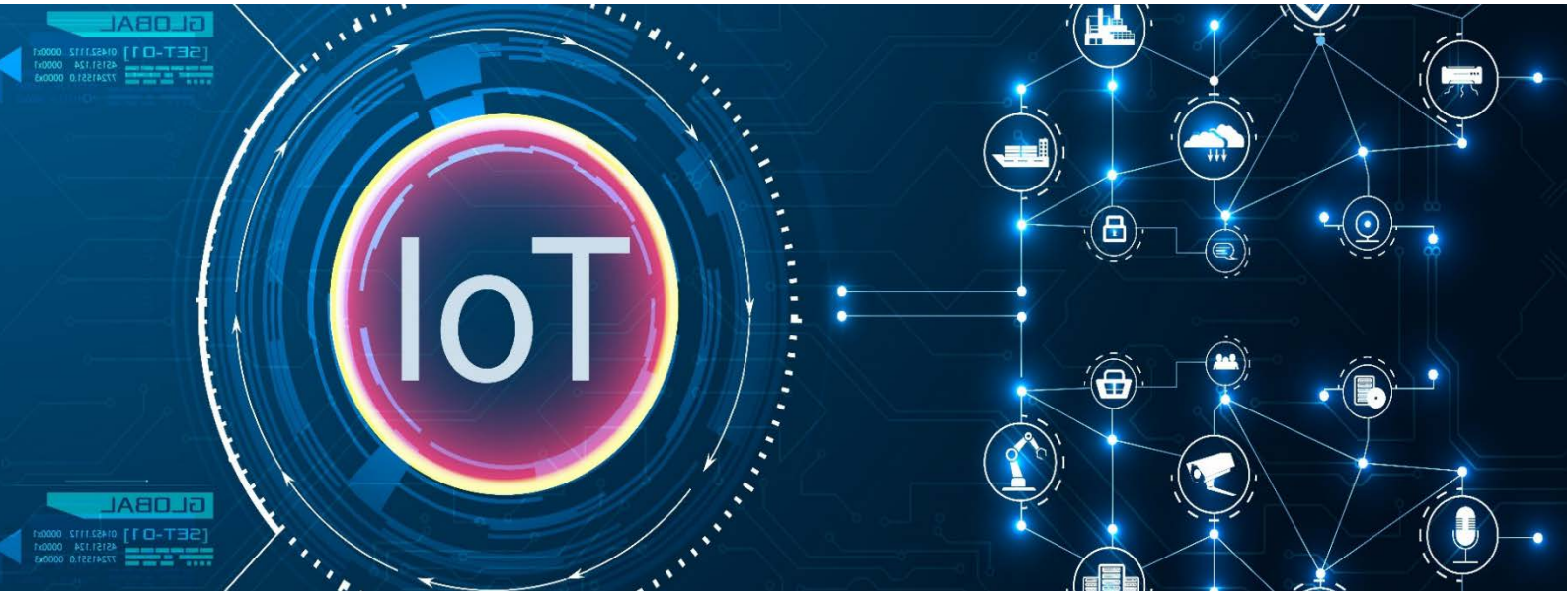

OVE AKTUELL

Schwerpunkt Informationstechnik

IoT Security

Sehr geehrte LeserInnen,

nachfolgend erhalten Sie den Newsletter **OVE Aktuell** mit dem Schwerpunkt **„IoT Security“**.

Ein kurzer Gesamtüberblick:

1. OVE Academy Seminare/Veranstaltungen

Digital Grid – Digitalisierung des Stromnetzes

Möglichkeiten zum Monitoring und zur Steuerung von Netzkomponenten im Niederspannungsverteilnetz und grundlegende Kenntnisse zu Kommunikationstechnik

Termin
Di., 19.01.2021, 09:00 – 16:00 Uhr

Systematische Absicherung industrieller Automatisierungssysteme mit der IEC 62443

Automatisierungssysteme sind immer häufiger Teil von modernen Industrieanlagen – und die Gefahr IT-basierter Angriffe auf diese Anlagen wird zu einem immer wichtigeren Aspekt bei der Planung und beim Betrieb solcher Systeme.

Termin
19.01.-20.01.2021, 09:00 – 16:00 Uhr

OVE E 8101 und OVE-Richtlinie R 12-2

Detaillierter Einblick zu den anerkannten Regeln der Technik OVE E 8101 und OVE R 12-2 und den bei der Errichtung von Niederspannungsanlagen zu beachtenden wesentlichen Änderungen

Termin
Mi., 20.01.2021, 09:00 – 16:00 Uhr

Notbeleuchtungsanlagen

In diesem Seminar erläutern wir Ihnen die Erfordernisse für die Errichtung, den Betrieb und die Prüfung von Not- und Sicherheitsbeleuchtungen.

Termin
Do., 21.01.2021, 09:00 – 16:00 Uhr

2. Vorwort

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

Resiliente IoT Systeme

Während unsere Gesellschaft und Wirtschaft gerade ihre Resilienz gegenüber einer globalen Pandemie unter Beweis stellen müssen, wollen wir in diesem Newsletter die Resilienz von IoT-Lösungen näher betrachten. Dieses Thema gewinnt mit der zunehmenden Verbreitung von IoT in komplexen Steuer- und Regelsystemen immer mehr an Bedeutung.

Denn, was aber passiert, wenn plötzlich ein Hardware-Defekt auftritt? Was, wenn die Funkverbindung unterbrochen wird, oder ein Angreifer die Steuersoftware manipuliert? Gerade in Cyber-Physikalischen Systemen, also Systemen, die mit der realen Welt interagieren, kommt neben einem Cyber Security- auch ein reales physisches Schadensrisiko hinzu.

Um sicherzustellen, dass die IoT-Geräte verlässlich vertrauensvolle Daten erfassen bzw. Steuerungskommandos verlässlich umsetzen, sind daher umfangreiche Maßnahmen auf allen Systemebenen notwendig. Resilienz beschreibt dabei die Fähigkeit eines Systems, sich veränderten Rahmenbedingungen anzupassen. Dies geht über den klassischen Robustheitsbegriff hinaus, in dem das System nicht nur Veränderungen bzw. Störungen standhält, sondern sich aktiv den neuen Rahmenbedingungen anpasst.

Eine solche Anpassung kann auf unterschiedliche Arten erfolgen. Eine Möglichkeit ist, dass benötigte Funktionalitäten über alternative Komponenten abgedeckt werden. So kann beispielsweise ein Fahrzeug, dessen Radarsensor ausfällt, auf den optischen Sensor zurückgreifen. Dafür muss aber möglicherweise die Geschwindigkeit reduziert werden. Ein anderes Beispiel wäre der Ausfall der zentralen Steuereinheit im Fahrzeug. Moderne Fahrzeugarchitekturen nutzen hier redundante Systemkomponenten im Sinne eines robusten System-Designs. Neu ist, dass die zweite Steuereinheit im Normalbetrieb die Entertainment-Funktionen übernimmt. Kommt es dann zum Ausfall der Fahrzeugsteuerung, kann die zweite Steuereinheit in Echtzeit diese Funktionen übernehmen. Somit wird ein hohes Maß an Verfügbarkeit und Robustheit mit minimalem Overhead erzielt.

Um ein hohes Maß an Resilienz zu erreichen ist es notwendig, dies bereits im System-Design zu berücksichtigen. Durch entsprechende flexible Architekturen und Prozesse wird die Grundlage für eine hohe Verfügbarkeit und Verlässlichkeit des Gesamtsystems erreicht. Darüber hinaus ist aber eine laufende Beobachtung des Systemverhaltens unabdingbar, um Veränderungen rechtzeitig erkennen und geeignete Maßnahmen initiieren zu können. Da die Systemumgebungen oft nicht im Vorhinein klar definiert sind, ist hier ein hohes Maß an Adaptivität und Flexibilität erforderlich.

In diesem Newsletter wollen wir uns dem Thema Resilienz von unterschiedlichen Richtungen nähern. Im ersten Beitrag werden die „Anforderungen und Potentiale resilienter IoT-Systeme" näher betrachtet. Der zweite Beitrag widmet sich speziell der Frage, ob „Sensoren in IoT-Systemen" ein Einfallstor für Cyber-Angriffe oder auch die Möglichkeit zur Absicherung bieten. Im dritten (englischsprachigen) Beitrag werden schließlich spezielle Methoden der „Runtime Verification" vorgestellt, die einen sicheren Betrieb von IoT-Systemen gewährleisten können.

Wir wünschen Ihnen, werte Leserinnen und Leser, eine spannende Lektüre dieses Newsletters sowie alles Gute und ein hohes Maß an Resilienz für das kommende Jahr! Diskussionsbeiträge, Terminhinweise, Kommentare und Anregungen an informationstechnik@ove.at sind wie immer herzlich willkommen.

3. Zunehmende Vernetzung

Mag. Kevin Mallinger
Business Development Manager
SBA Research

Anforderungen und Potentiale resilienter IoT-Systeme

Industrie 4.0, Internet of Things (IoT) und Cyber-Physikalische Systeme (CPS) sind nur einige der aktuellen Schlagworte der fortschreitenden Digitalisierung. Systeme, die zuvor lokal abgegrenzte Funktionalität hatten, werden nun Teil eines heterogenen, vielschichtigen und globalen Netzwerks. IoT-Komponenten wie Sensoren, Aggregatoren, Kommunikationskanäle, externe Versorgungseinrichtungen oder Entscheidungsauslöser werden zudem häufig in Legacy-Systeme und -Prozesse integriert. Durch diese zunehmende Vernetzung werden individuelle Systeme (stand alone-Systeme) zu einem hypervernetzen Verbundsystem (system-of-systems), dessen Folgen für die Gesellschaft meist nicht weiter hinterfragt werden.

Es ist jedoch mit einer Reihe an Folgewirkungen und Risiken bei solch hochkomplexen Systemen zu rechnen:

- emergentes Verhalten mit unerwarteten Folgen
- mangelndes Verständnis der Systemzusammenhänge und damit einhergehend Kontrollverlust
- größere (digitale) Angriffsfläche, die zusätzlich kaskadenartige Verbreitung von Störungen ermöglicht
- „single points of failures“ und Verlust an Diversität durch Monopolisierung sowie Zentralisierung
- unklare rechtliche Verantwortlichkeiten

Dass dies keine theoretischen Risiken sind, zeigte sich bei der jüngsten Störung des US-Amazon Cloud-Dienstes AWS im November 2020, der einen Ausfall von unzähligen IoT-Geräten nach sich zog. Ohne Cloud saugen Staubsaugerroboter nicht mehr, Mietautos sind weder sperr- noch startbar und, wahrscheinlich noch das geringste Übel von allen, Entertainment-Systeme funktionieren nicht mehr. Abseits dieses Debakels ist auch der Fall einer Heimautomatisierungslösung, deren cloud-basierte Infrastruktur vom Hersteller aus internen, strategischen Gründen abgedreht wurde, bekannt. Den Nutzer/innen blieb funktionsloser Elektroschrott.

Das ordentliche Zusammenspiel der einzelnen Komponenten ist ein komplexes, vielschichtiges Problem und kann nur durch integrierte Betrachtung aller Systemebenen – also die Menschen, Prozesse und Technologien inkludierend – bewerkstelligt werden. In komplexen Systemen, wie dies in der IoT-Landschaft der Fall ist, lassen sich viele systemische Risiken dennoch, wie das folgende Beispiel zeigt, nicht vorhersagen. Mirai, ein Botnet aus IoT-Geräten, legte im Jahr 2016 nicht nur einzelne Internet-Services lahm, sondern auch das dynamische DNS-Service DynDNS, wodurch eine wesentlich höhere Anzahl an Services nicht mehr erreichbar war. Ein solches Botnet kann durch konzertierte Lastschwankungen aber auch das Stromnetz destabilisieren und flächendeckende Blackouts verursachen. Die Ausnahmesituation der Corona-Pandemie führte zu einem geringerem Gesamtverbrauch, ein Zustand, der solche Angriffe nur noch einfacher macht. Um die Gesamtheit dieser Problemlagen zu adressieren, muss die Gestaltung resilienter IoT-Systeme in den Vordergrund gerückt werden. Resilienz meint dabei die Fähigkeit eines Systems, auf Störungen reagieren zu können, wichtige Systemeigenschaften wiederherzustellen und eine fortlaufende Entwicklung voranzutreiben.

Aus Kosten- und Effizienzgründen sollte dieser Prozess bereits in der Design-Phase beginnen. Der Fokus liegt dabei nicht auf der Vermeidung von einzelnen, spezifischen Vorfällen oder Angriffen, sondern im Aufbau adaptiver Kapazitäten. Dies kann sowohl durch die Beachtung von Modularität (Microservices, Cloud-Auslagerung etc.), Entkoppelung (Container-Lösungen, Rechte-Management etc.) als auch die Bereitstellung von horizontaler und vertikaler Diversität und Redundanz (mit automatischer Konsensbildung, Virtualisierung von Prozessen und Daten, N-varianten Systeme usw.) begünstigt werden. Darüber hinaus muss das Verhalten

solcher Systeme jederzeit beobachtbar bleiben, weshalb automatisierte Monitoring-Systeme (Gesundheitschecks, Legacy Code-Analysen, Prüfsummen etc.) sowie Resilienzmetriken ebenfalls vorab einzurichten sind.

Diese architektonischen Prinzipien ermöglichen es, (1) Abweichungen vom gewünschten Systemverhalten zu erkennen und (2) entsprechende Gegenmaßnahmen ergreifen zu können, um den Funktionsverlust von Ressourcen, Applikationen und Services so gering wie möglich zu halten. Autonome Rekonfigurationsmechanismen können Angriffe abwehren oder deren Schaden begrenzen, Ressourcen verteilen und Lücken schließen. Dabei können ganze Systembereiche abgekapselt (z. B. dynamische Isolierung, Terminierung von Prozessen), Angreifer in die Irre geführt (z. B. Honeypots) oder zusätzliche Ressourcen akquiriert werden (z. B. Autoscaling).

Zeitgleich zur Reaktion vorgestellter Probleme wird der Prozess zur Wiederherstellung der ursprünglichen Funktionalität gestartet. Dabei werden verlorene Aufgaben neu zugeteilt (z. B. Änderung der Prozess- und Speicherstrukturen), angegriffene Bereiche repariert (z. B. automatische Laufzeit-Fehlerbehebung) und sichere Prozessabschnitte neu gestartet (z. B. Checkpointing). In einem kontinuierlichen (Resilienz-)Verbesserungsprozess werden dann die als kritisch erkannten Systemteile und deren Abhängigkeiten evaluiert, das Risikopotenzial neu eingestuft und notwendige architektonische Veränderungen vorgenommen.

Die Implementierung dieses zyklischen Prozesses scheitert oft an den zusätzlichen Aufwänden zu Projektstart beziehungsweise in der Wartung. Schon eine mittelfristige Betrachtung zeigt aber, dass mit vergleichsweise geringen Investitionen sehr hohe mittel- und langfristige Kosten, die aus komplexen Wartungsarbeiten, Datenverlusten, Privacy-Problemen oder gar kompletten Ausfällen resultieren, vermieden werden können. Darüber hinaus ermöglichen modulare und multifunktionale Systeme auch eine agilere Weiterentwicklung und das Wachstum der Infrastruktur auf höherem Qualitätsniveau. Das führt zu weniger Stress bei Mitarbeiter/innen und höherer Zufriedenheit der Kund/innen, was ebenfalls ökonomische Vorteile verspricht. Es gilt also auch wie in so vielen anderen Bereichen: Vorsorge ist besser (und günstiger) als Nachsorge.

Weitere Autoren
Dipl.-Ing. Dr. techn. Johanna Ullrich
Head of Networks and Critical Infrastructures Security Research Group
SBA Research

Dipl.-Ing. Dr. techn. Alexander Schatten
Senior Scientist
TU Wien

4. Sensoren in IoT-Systemen

© DUK, Andrea Reischer

Dipl.-Ing. Albert Treytl
Department for Integrated Sensor Systems
Donau-Universität Krems

Einfallstor oder Möglichkeit zur Absicherung?

Mit dem Siegeszug des Internets der Dinge werden einfach zu vernetzende Geräte immer häufiger in den unterschiedlichsten Anwendungsbereichen eingesetzt. Dies wird verstärkt durch den Trend zur Digitalisierung, die maßgeblich von der Erfassung und Verarbeitung von Daten lebt – andererseits macht das IoT die Digitalisierung überhaupt erst möglich. Die einfache Möglichkeit des „Plug and Play" bei der Installation von IoT-Geräten führt jedoch oft zu einer Vernachlässigung des Sicherheitsgedankens, sei es aus Bequemlichkeit oder Unwissen. Die Philosophie vieler Hersteller, ihre IoT-Geräte mit einer zumeist firmeneigenen Cloud zu verbinden, resultiert überdies leicht in der Entstehung von parallelen und schlecht nachvollziehbaren Netzwerkstrukturen, die sich einer Absicherung oftmals entziehen und damit ein Ziel für Cyber-Angriffe werden können.

Was bei einer smarten Bewässerungsanlage im privaten Bereich unangenehm sein kann, wird bei der Wasserzufuhr in einem industriellen Prozess oder bei IoT-Sensoren zur Überwachung von Industrieanlagen unter Umständen problematisch. Die Absicherung von Sensoren ist daher essentiell, damit die Datenbasis korrekt ist. Besonderes Augenmerk muss auf die stark limitierten Ressourcen der Sensoren und der verbindenden (Sensor-)Netzwerke gelegt werden. Verfügbarkeit, Integrität und Authentifizierung sind hierbei wesentliche Sicherheitsziele.

Während es heute in vielen Bereichen bereits entsprechende Hardware-Beschleunigung für zuverlässige Kryptographie wie etwa AES (Advanced Encyption Standard) gibt, die auch für IoT-Geräte nutzbar wäre, bestehen hier doch einige prinzipielle Probleme, die sich aus der Art der Sensordaten und den Rahmenbedingungen der Anwendung ergeben: Sensordaten sind zumeist kleine Daten von einigen Bit bzw. wenigen Bytes Länge. Dem gegenüber stehen bei klassischen Verschlüsselungsmethoden Blockgrößen von 16 oder mehr Bytes, um Integritätsprüfungen zu implementieren. Auf den ersten Blick ist das vielleicht keine große Diskrepanz, für einige Low-Power Long-Range-Funknetze wie LoRa oder Sigfox, die eine beliebte Basis für IoT-Installationen bilden, stellt eine 16 Byte lange Prüfsumme aber bereits einen erheblichen Aufwand dar, der die Übertragung eines zweiten Datenpakets und damit eine zusätzliche Belastung des Netzwerks bedeuten kann. Zusätzlich darf der Energieaufwand nicht unterschätzt werden, da viele IoT-Anwendungen darauf ausgelegt sind, dass Geräte mit Batterien bzw. Energy Harvesting für Zeiträume von bis zu einigen Jahren betrieben werden müssen. Digitale und analoge Wasserzeichen, die wir im Rahmen der Projekte IoT4CPS und ARES erforschen, bieten hier eine ressourcenschonende Möglichkeit, Integritätsprüfung innerhalb des Signalrauschens der Messwerte oder in Seitenkanälen wie dem Interpaket Delay des Netzwerks zu kodieren, ohne zusätzliche Security-Daten versenden zu müssen. Man kann sogar so weit gehen, das Wasserzeichen in Hardware zu erzeugen und dem eigentlichen analogen Sensorwert noch vor der Analog-Digitalwandlung zu überlagern und damit bereits die eigentlichen Sensordaten zu sichern.

Während die direkte Absicherung von Sensoren und IoT-Geräten natürlich Priorität hat, muss jedoch akzeptiert werden, dass die IoT-Philosophie der klassischen Sichtweise entgegensteht, Sicherheit durch geschlossene Systeme erzielen zu können. IoT-Geräte bieten oft aus Kosten- und Ressourcengründen keine starke Security an, und Plug and Play ermöglicht auch die Präsenz von „Babbling Idiots" oder anderen nicht

legitimierten Sensoren, ebenso wie die Einschleppung von Schadsoftware über Geräte von Wartungsfirmen oder Zulieferern.

Auch hier können Sensoren dazu dienen, Angriffe zu detektieren und entsprechende Gegenmaßnahmen zu treffen. Das Prinzip von klassischen Intrusion Detection-Systemen, die den Netzwerkverkehr in einem IT-Netzwerk analysieren und atypische Muster erkennen, kann auch auf die erfassten Sensordaten angewendet werden: Soll eine industrielle Anlage durch eine Manipulation eines Füllstandsensors angegriffen werden, kann dieser Angriff durch Vergleich mit dem Zufluss- und Abflusssensor erkannt werden, selbst wenn die Attacke durch eine schleichende Wertänderung verschleiert wurde. Ein entsprechendes Modell des industriellen Prozesses ist dafür jedoch Voraussetzung. Ähnlich können Metadaten wie Stromverbrauch oder On-Air-Time von Sensoren verwendet werden, um möglichen Missbrauch oder die Vorbereitung eines Angriffes zu detektieren. In diesem Zusammenhang beschäftigen sich andere Arbeiten auch mit der Analyse von Schwankungen der Feldstärke des Funksignals, um zu sehen, ob ein Angreifer einen Sensorknoten dupliziert hat und für seinen Angriff verwendet.

Sensoren und IoT sind das Tor zur Digitalisierung, das entsprechend gesichert werden muss. Sie bieten aber ebenso neue Möglichkeiten zur Absicherung von (industriellen) IoT-Systemen, die effizient genutzt werden können.

Referenzierte Projekte:
IoT4CPS – IKT der Zukunft Leitprojekt des BMVIT, www.iot4cps.at
ARES – Forschungsprojekt im FTI-Call der NÖ Forschungsförderungsgesellschaft, www.donau-uni.ac.at/diss

Co-Autor:
Univ.Prof. Dr. Thilo Sauter
Donau-Universität Krems und TU Wien

5. Rigorous Engineering and Safe Operation of IoT

Dr. Dejan Ničković
Senior Scientist
Center for Digital Safety & Security
AIT Austrian Institute of Technology

Runtime Verification

From Industry 4.0 and smart manufacturing to remote healthcare – rapidly proliferating Internet-of-Thing (IoT) applications are becoming pervasive in every aspect of our daily lives. IoT applications consist of physical entities that are interconnected with sensors, actuators, software and other technologies that interact with the physical environment, while processing and exchanging data with other devices over the Internet. IoT applications are evolving to be tremendously complex systems that can operate in sophisticated and unpredictable environments.

Many IoT applications are safety-critical and faults can have catastrophic consequences involving significant material damage or even loss of human lives. Therefore, verification and validation (V&V) for IoT is essential to achieve high standards with respect to safety requirements. Due to its complexity, exhaustive verification of IoT applications at the design time is virtually impossible and must be complemented with techniques applied during the operation of the system.

Runtime verification (RV), also known as runtime monitoring and illustrated in Figure 1, is an alternative approach for ensuring the safe operation of complex systems that cannot be statically verified. RV is a light-weight verification technique that combines formal specifications with the evaluation of individual system behaviors. When applied to an IoT system under operation, RV provides a reliable, rigorous and systematic way of finding property violations in real time and possibly taking a corrective action.

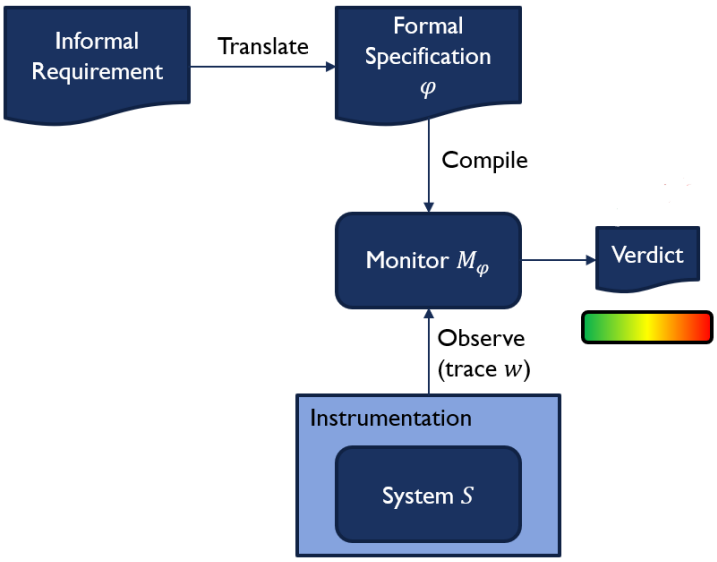

Fig. 1. Runtime verification architecture

RV can also be applied during the (model-based) design of IoT where behaviors correspond to simulation traces. In this context, monitoring can be viewed as part of the simulation-based V&V process, which gives up the complete coverage associated with verification, but still uses a rigorous mathematical specification language to classify behaviors.

In the past years, we worked on various aspects of RV applied to IoT and cyber-physical systems (CPS): (1) formal specification languages for RV, (2) RV algorithms and tools, and (3) additional analysis methods that use RV as basic technology.

We introduced Signal Temporal Logic (STL) [1], a specification language for expressing real-time temporal safety properties of IoT and CPS. STL allows to measure how far an observed signal is from satisfying or violating its specification. We developed methods for offline, online and real-time monitoring of STL specifications, using both qualitative and quantitative evaluation: (1) a translation from STL to monitors implemented on FPGA, (2) the rtamt[1] Python library for monitoring STL specifications, (3) that we integrated to the Robotic Operating System (ROS)[2] and MathWorks MATLAB/Simulink model-based development environments [2]. We finally used STL monitors to develop applications beyond RV for rigorous engineering of IoT and CPS. We developed search-based testing procedures that combine quantitative monitors with global optimization to efficiently find system failures [3]. We also devised methods for explaining and localizing faults in complex systems guided by STL specifications [4].

RV is a powerful and versatile technology that can be applied both during the design-time of a complex system as well as during its operation, facilitating the design-operation continuum. In addition to its ability to efficiently detect failures, RV can be used to develop other analysis procedures that support rigorous engineering of IoT.

[1] https://github.com/nickovic/rtamt
[2] https://github.com/nickovic/rtamt4ros

References:
[1] Oded Maler, Dejan Nickovic: Monitoring Temporal Properties of Continuous Signals. FORMATS/FTRTFT 2004: 152-166.
[2] Dejan Nickovic, Tomoya Yamaguchi: RTAMT: Online Robustness Monitors from STL. ATVA 2020: 564-571.
[3] Thomas Ferrère, Dejan Nickovic, Alexandre Donzé, Hisahiro Ito, James Kapinski: Interface-aware signal temporal logic. HSCC 2019: 57-66.
[4] Ezio Bartocci, Niveditha Manjunath, Leonardo Mariani, Cristinel Mateis, Dejan Nickovic: Automatic Failure Explanation in CPS Models. SEFM 2019: 69-86.

6. OVE News

„Klima wenden"-Videowettbewerb: Fünf Siegervideos ausgezeichnet

Mit einer Online-Preisverleihung ist der diesjährige Videowettbewerb der OVE-Initiative ScienceClip.at gemeinsam mit AIT Austrian Institute of Technology zu Ende gegangen. Auch Bundesministerin Margarete Schramböck gratulierte den Preisträgerinnen und Preisträgern in einer Videobotschaft.

Mehr

Covid-19-Maßnahmen: OVE durchgehend erreichbar

Der OVE unterstützt die Maßnahmen der Regierung gegen Covid-19. Wie bereits im Frühjahr bleiben aber alle Mitarbeiterinnen und Mitarbeiter wie gewohnt für Sie erreichbar.

Mehr

e&i aktuell: Universitätsrektor Harald Kainz im Interview

Diesmal im Interview für die e&i: Der Rektor der TU Graz und Präsident von TU Austria, Univ.-Prof. Dipl.-Ing. Dr. Harald Kainz. Er spricht unter anderem über zehn Jahre TU Austria, aktuelle Herausforderungen und das notwendige Beenden der Diskursvorherrschaft von COVID-19.

Mehr...

132. OVE-Generalversammlung erstmals online

Zum ersten Mal in der Verbandsgeschichte fand die Generalversammlung des OVE am 10. November 2020 online statt. Auf der Agenda standen Neuwahlen in Präsidium und Vorstand sowie ein Überblick über die jüngsten Verbandsaktivitäten. Das bestimmende Thema war hier die Energiewende.

Mehr

Wir bedanken uns für Ihre Aufmerksamkeit!

Bei Fragen, Wünschen oder Anmerkungen wenden Sie sich an informationstechnik@ove.at.

Aktuelle News aus der Welt der Elektrotechnischen Normung finden Sie bei **OVE Standardization**.

Normen, Richtlinien und Fachpublikationen können Sie in unserem **OVE-Shop** erwerben.

Wenn Sie Ihre elektrotechnischen Produkte zertifizieren lassen möchten, finden Sie hier den Kontakt zu **OVE Certification**.

OVE Österreichischer Verband für Elektrotechnik
OVE Informationstechnik, OVE Aktuell
Krenngasse 37 | 8010 Graz
T +43 316 873-7916
informationstechnik@ove.at | www.ove.at
ZVR 327279890