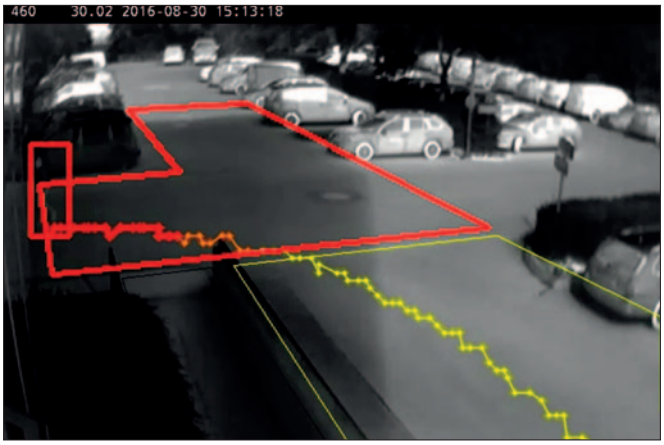
Mustererkennung

Systeme, die durch Mustererkennung Bildinhalte und Ereignisse bewerten können, ersparen langwierige Routinearbeit und helfen, den Datenschutz aufrechtzuerhalten.

Die Videoüberwachung etwa zum Schutz von Botschaften, Ämtern oder kritischer Infrastruktur ist mit herkömmlichen Methoden ermüdend und fehleranfällig. Ein Großteil der Alarme sind Fehlalarme, beispielsweise durch Tiere, Äste von Bäumen, die sich im Wind bewegen, oder unbeteiligte Personen ausgelöst. Die *PKE-Holding AG* hat in Zusammenarbeit mit Forschern des Software-Competence-Centers Hagenberg *(SCCH, www.scch.at)* im Rahmen eines KIRAS-Projektes eine Lösung auf Basis von Deep Learning und Mustererkennung entwickelt. SKIN steht für „Schutz der Außenhaut Kritischer INfrastruktur".



Das Überwachungssystem lernt Bewegungsmuster und Verhalten zu erkennen und den Gefährdungsgrad einzuschätzen.

Muster erkennen. Von Mitte 2014 bis 2018 arbeiteten drei Forscherinnen und Forscher an einem System der „Behavioral Analysis": Das automatische Überwachungssystem lernt laufend dazu, indem Bewegungen und Abläufe im Bildmaterial analysiert und mit bekannten Daten in Beziehung gesetzt werden, um verdächtige Muster von unverdächtigen Ereignissen unterscheiden zu können. Das System kann Fußgänger, Müllautos, Radfahrer oder das Plastiksackerl im Wind erkennen und als unverdächtig einordnen. Durch diese Lösung konnte die Fehlalarmrate pro eingesetztem Kamerasystem um rund 65 Prozent verringert werden. Das Videomaterial, das durch die Überwachungskameras erstellt wird, erfährt zugleich eine Kategorisierung, die eine leichtere Auffindung von Ereignissen ermöglicht.

„Aus unserer Sicht war SKIN ein rundum erfolgreiches Projekt", sagt Privatdozent Dr. Bernhard A. Moser, *SCCH*-Forschungsdirektor. „Es konnte auch ein wissenschaftliches Paper veröffentlicht werden – ein wesentlicher Aspekt für das Kompetenzzentrum. Unsere Mitarbeiterinnen und Mitarbeiter können Erfahrung mit dieser Art von Daten und verfeinerte Methoden mitnehmen. Diese fließen nun zum Beispiel in das Leitprojekt Connecting Austria ein, das die ideale Verbindung von energieeffizientem und automatisiertem Güterverkehr von der Autobahn in die Stadt untersucht, oder Projekten wie RAILEye – KI und der tote Winkel in Schienenfahrzeugen."

Forschungszentrum. Die *SCCH Hagenberg* ist ein unabhängiges Software-Forschungszentrum. Im Mittelpunkt stehen Data & Software Science. Die Kooperation mit Partnern aus der Wissenschaft, insbesondere mit dem Gründungspartner *JKU* sowie mit zahlreichen namhaften Unternehmen aus Wirtschaft und Industrie, macht das *SCCH* zu einem Paradebeispiel für eine funktionierende Ausrichtung entlang der „Innovation Chain" Bildung, Forschung und Wirtschaft.

Das S*CCH* hat seine Schwerpunkte sowohl in Software für die Produktion, als auch in den Daten, die durch die lernenden Systeme eine immer größere Rolle spielen. Ohne diese Kombination von Data & Software Science sind Industrie 4.0 und künstliche Intelligenz nicht denkbar.

SCHUTZ KRITISCHER INFRASTRUKTUR

IT-Sicherheit in der Industrie

Wie Unternehmen in puncto IT-Security aufrüsten können, erfuhren die Teilnehmer des *TÜV-AUSTRIA*-Expertentag-Livestreams im Mai 2020 (*www.tuv-akademie.at)*. Die Kernfrage war: Ist die IT-Security in der Industrie vernachlässigt worden? Die OT-Security (Operational Technology Security) regelt die Cyber-Sicherheit in industriellen Anlagen und ist in allen industriellen Sektoren zu finden, wie der Wasserversorgung, der Lebensmittelversorgung, der Energieversorgung oder in medizinischen Einrichtungen. Die Industrie ist mittlerweile Hauptangriffspunkt für Hacker: Es gibt eine Reihe von Angriffen, die gezielt und professionell ausgeführt werden. Grund dafür ist die wachsende Vernetzung der Industrie 4.0 sowie Systeme, die auf lange Lebenszeit ausgerichtet wurden, aber mit heutigen Anforderungen nicht mehr mithalten können. Die Folge sind eine breite Angriffsfläche für potenzielle Hacker. Laut Prof. Thomas Brandstetter vom Institut für Sicherheitsforschung der FH St. Pölten, sei die OT-Security umso wichtiger. Brandstetter appellierte an die Betreiber der Anlagen, die offenen Flanken der Systeme zu beseitigen und die Cyber-Sicherheit zu verstärken. Der regulatorische Druck dazu sei stärker geworden, die Regelwerke vielfältiger. Die NIS Verordnung zum Schutz kritischer Infrastruktur ist aktueller denn je, gut ausgebildetes OT-Personal wichtig für die Cyber-Resilienz des Unternehmens. Außerdem sollten Zugriffsbeschränkungen in den Netzwerken eingeführt und/oder erweitert werden, um vor Angriffen zu schützen.

FOTO: PKE HOLDING

Objekterkennung: Objekte werden erkannt und nur als Textobjekt DSGVO-konform gespeichert.

DSGVO-konforme Überwachung. *Swarm Analytics (www.swarm-analytics.com)* ein junges Unternehmen aus Innsbruck, forscht im Bereich Bildverarbeitung mittels künstlicher Intelligenz und bietet Lösungen für viele Anwendungsfälle: Fahrgaststromanalysen in öffentlichen Verkehrsmitteln, zuverlässig anonymisiert, Leitsysteme für Parkraumbewirtschaftung, detaillierte Verkehrsstromanalysen oder Anwendungen im Retail-Bereich können auf eine Weise aussagekräftig gemacht werden, die bisher nicht möglich war.

Die Swarm Perception Box P100 zum Beispiel wird direkt mit einer HD-Überwachungskamera verbunden und erzeugt in Echtzeit aus dem aufgenommenen Bildmaterial eine textliche Beschreibung, die für eine Vielzahl von Auswertungen wiederum der ideale Input ist, und zwar datensparend und DSGVO-konform. Da keine Bilder, sondern nur textliche Beschreibungen gespeichert werden, ist der Datenschutz zuverlässig gewährleistet.

Ergänzend zu *Swarm Perception Box P100* und *Swarm Outdoor Perception Box OP100* hat das Unternehmen mit dem *Swarm Control Center* ein Management-System für *Swarm Perception Boxes* entwickelt, das sich auf nicht invasive Weise mit bestehenden Systemen einfach verbinden lässt und so leicht in bestehende Management-Systeme und IT-Landschaften integriert werden kann.

Anwendungsfelder. Mit der *Swarm Perception Box* eröffnen sich weitere Anwendungsfelder: Neben den angesprochenen Smart-City-Anwendungen werden auch Lösungen denkbar, die beispielsweise in den Bereich datenschutzkonformer Liegenschaftsüberwachung gehen könnten.

Die Bilderkennungstechnologie von *Swarm Analytics* kann verwendet werden, um eine Pseudonymisierung von Personen durchzuführen, etwa im Sinne von bekannt oder unbekannt, ohne weitergehende Personenmerkmale zu speichern. Damit lassen sich DSGVO-konforme Whitelists erstellen und beispielsweise eine automatisierte bildgestützte Alarmanlage. Weiters bietet die Lösung auch die Grundlage, um bestimmte verdächtige Verhaltensweisen zu erkennen – etwa plötzliches Weglaufen auf einem Bahnsteig, das Abstellen und Stehenlassen von Gegenständen, oder längerer Aufenthalt an ungewöhnlichen Orten. *Michael Werzowa*

FOTO: SWARM ANALYTICS