Biogastechnologie verringert den CO_2-Fußabdruck

Grünes Gas. Mit Biogastechnik können natürliche Prozesse umweltschonend genutzt werden

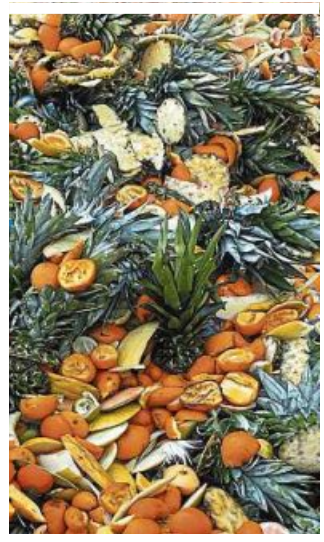

SHUTTERSTOCK/CLAUDIA HARMS-WARLIES

In der Biogasanlage wird Biomasse zu CO_2-neutralem Biogas vergoren. Wird es zu Biomethan veredelt, kann es direkt ins Gasnetz eingespeist werden

Biomethan ist eine wichtige Energiequelle, die aus einer Vielzahl von festen oder flüssigen Abfällen gewonnen werden kann – aus Biomasse – wie zum Beispiel Biomüll, Gülle, Ernterückstände, Abfällen der Futter- und Lebensmittelindustrie oder auch Klärschlamm. Biogas entsteht in Biogasanlagen durch die Vergärung von Biomasse. Dieses kann in Blockheizkraftwerken zu Strom und Wärme umgewandelt oder aber zu Biomethan veredelt und direkt ins Gasnetz eingespeist werden. Biomethan ist ein umweltfreundliches Gas, besitzt die gleichen Qualitäten wie fossiles Gas und kann dadurch in selber und vielfältiger Weise eingesetzt werden: zur Wärmeerzeugung, als Rohstoff oder Prozessenergie in der Industrie, zur Stromerzeugung, zur Kühlung und als Kraftstoff im Verkehrssektor.

Ausbau stockt

Das Erneuerbaren-Ausbau-Gesetz (EAG) sieht vor, dass bis 2030 zumindest fünf TWh erneuerbarer Gase pro Jahr ins Netz eingespeist werden sollen. Aus heutiger Sicht erscheint dies mangels verlässlicher Rahmenbedingungen hochgesteckt – es würde das 40-fache der aktuellen Biomethan-Einspeisung bedeuten – obwohl das eigentliche österreichische Biomethan-Potenzial auf Basis biogener Abfälle bei 40 TWh liegt. Fakt ist, dass die Planung momentan zu wenig ambitioniert ist: Um die Erzeugung von Grünen Gasen wie Biomethan und auch von grünem Wasserstoff hochzufahren, bedarf es – genauso wie für Photovoltaik, Wind - oder Wasserkraft – einer der Ökostromförderung vergleichbaren Regelung, die Rechtssicherheit für Investoren bietet und entsprechende Rahmenbedingungen liefert.


PRIVAT

Aus Mist entsteht Bioenergie und organischer Dünger

Saubere Energie

Biomethan ist speicherbar, witterungsunabhängig, verringert den Import von fossilem Gas und ist ein gutes Beispiel für die Prinzipien der Kreislaufwirtschaft und wertvollen Ressourcennutzung.

Die österreichische Biogasfirma Botres Global GmbH widmet sich dieser ausgereiften technologischen Energiegewinnung. Der erfolgreiche Anbieter hochmoderner anaerober Vergärungstechnologie errichtete zahlreiche Abfall- und Reststoff-Biogasanlagen in Europa und der Türkei. Zu ihren Kunden zählen einige der größten Abfallwirtschafts- und Infrastrukturunternehmen. Mit ihrem hocheffizienten Bioabfallbehandlungssystem (Bio Scraper) kann Botres Global nahezu alle Arten von organischen Abfällen für Biogasanlagen aufbereiten. In Österreich übernahmen sie kürzlich ihre erste Biogasanlage in Wildon/Stmk. „Wir freuen uns über die tolle Partnerschaft mit dem weiteren Gesellschafter“, so Markus Grasmug, Geschäftsführer Botres. Die Umstellung der Anlage von reiner Stromerzeugung auf die Aufbereitung und Einspeisung von 300 m3/h Biomethan ins Gasnetz ist geplant, Genehmigungen liegen bereits vor. Botres wird künftig sein Know-how im Bereich Bioabfälle und Reststoffe einbringen. „Die Zeit ist reif für Grünes Gas in österreichischen Leitungen, um eine nachhaltige Zukunft für uns alle zu schaffen“, betont Stefan Kromus, Geschäftsführer von Botres Global.

gruenes-gas.at
botres.com

Cybersecurity im Bahnwesen

Sicherheit. Forschungsprojekt umfasst Methoden zur Erkennung von Cyberangriffen auf Eisenbahninfrastruktur

Hackerangriffe werden für Unternehmen zunehmend zum Problem - auch wenn man oft gar nichts davon in den Medien mitbekommt. Denn in den meisten Fällen kommen die Cyberangriffe auf Firmen nicht ans mediale Tageslicht. Immerhin wird befürchtet, zusätzlich zum bereits erlittenen Schaden negative Schlagzeilen zu produzieren. Nicht selten wird als geringstes Übel schlicht Lösegeld gezahlt, um das Tagesgeschäft rasch wieder aufnehmen zu können. Dabei kann jede Branche von Cyberangriffen betroffen sein - auch das Bahnwesen. Verbrecher, die sich in das Schienennetz einhacken, Züge zum Stoppen bringen und den Bahnverkehr lahmlegen, um so Geld zu erpressen - ist nur ein Horrorszenario.

Real-Time Beobachtung

Nun haben ForscherInnen der Fachhochschule St. Pölten im Projekt „Resilient Rail – Resiliente Sensorinfrastruktur im Bahnwesen“ die Resilienz von Systemen im Bahnsektor untersucht und entwickelten Methoden, um Cyberangriffe rechtzeitig zu erkennen. „Resilient Rail – Resiliente Sensorinfrastruktur im Bahnwesen“ ist ein Kooperationsprojekt der Fachhochschule St. Pölten und Frauscher Sensortechnik. „Die Real-Time Beobachtung von durchgeführten Angriffen auf unser System erlaubte uns neue Sichtweisen auf den Aspekt Cybersecurity zu gewinnen. Nur durch das unmittelbare Erkennen und Analysieren von Bedrohungen können wir effektive Schutzmechanismen entwickeln und unsere digitalen Ressourcen vor immer raffinierteren Angriffen bewahren“, sagt Stefan Raschhofer, Projektleiter bei Frauscher Sensortechnik.

Angriffe rasch erkennen

„Da moderne Achszähler zum Teil auf klassischen IT-Systemen und -Netzwerken beruhen, können wir bekannte IT-Sicherheitsschutzmechanismen anwenden, um die Resilienz zu verbessern. Netzwerkangriffe spielen auch in anderen Bereichen kritischer Infrastrukturen eine wichtige Rolle. Unser Hauptziel bestand daher darin, spezielle Mechanismen zur Erkennung von Angriffen zu entwickeln“ betonte Henri Ruotsalainen, Forscher am Institut für IT Sicherheitsforschung an der FH St. Pölten.

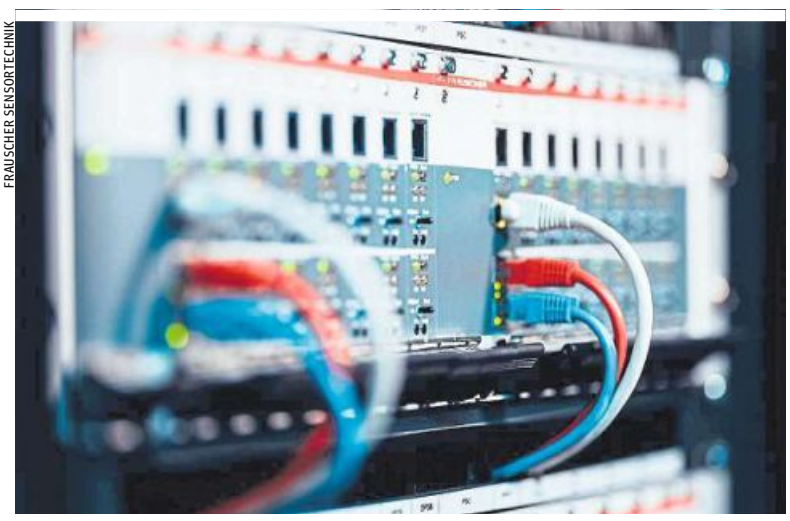
Abgeblockt

Resilienz bezeichnet hier die Fähigkeit eines Systems trotz Störungen den Betrieb aufrechtzuerhalten. Resiliente Systeme blocken Angriffe nicht einfach ab, sondern sie funktionieren auch während eines erfolgreichen Angriffs noch. Ein Projektziel war, die Zeit bis zur Erkennung und die Implementierung der Erkennungsalgorithmen im Echtzeitbetrieb zu verbessern. Dazu führt Resilient Rail resiliente Systeme für im Bahnsektor eingesetzte Sensortechnik ein.

Durch die Betrachtung über verschiedene Systemebenen hinweg, entwickelten die ForscherInnen Methoden, um verschiedene Kategorien von Angriffen effizient zu detektieren. Diese basieren oft auf klassischen Algorithmen des maschinellen Lernens sowie auf fortgeschritteneren Techniken des Deep Learning.

„Wir haben Methoden zur Erkennung von Angriffen entwickelt, die eine höhere Erkennungsgenauigkeit und eine schnellere Erkennungszeit bei kontinuierlichem Betrieb bieten“, freut sich Henri Ruotsalainen. Die Ergebnisse besitzen ebenso hohe Praxisrelevanz.


FRAUSCHER SENSORTECHNIK


FRAUSCHER SENSORTECHNIK

ForscherInnen untersuchten die Sicherheit von Achszählsensoren der Eisenbahninfrastruktur und entwickelten Methoden zur Erkennung von Angriffen

Gekennzeichneter Download (ID=WsXuUSf05h1xI8_-ceHmHg)