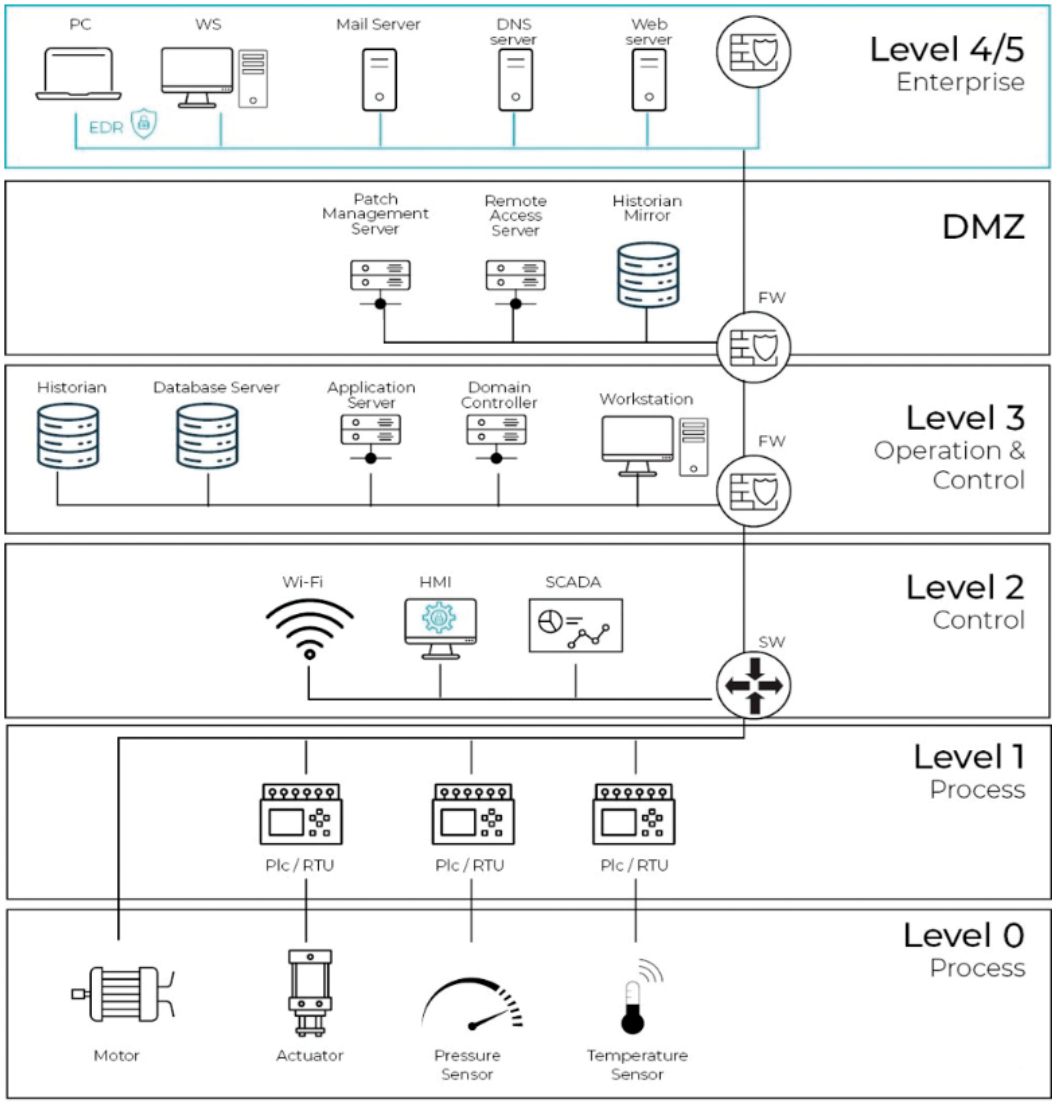
# Risiko durch ungeschütztes industrielles Wireless-IoT

***Otorio erläutert die Gefahr durch den direkten Pfad zu Level 0***




In den vergangenen Monaten hat Otorio zusammen mit Forschern eines weltweit führenden Cybersicherheitsanbieters umfassende Untersuchungen zu industriellen drahtlosen IoT-Geräten durchgeführt. Hierzu zählen z. B. industrielle Mobilfunk-Gateways/Router und WLAN-Access-Points. Diese Untersuchungen führten zur Entdeckung zahlreicher Probleme bei der Implementierung dieser Geräte. Im Rahmen der Studie sind 38 Schwachstellen bei vier führenden Anbietern ans Tageslicht gekommen. Einige davon wurden im Rahmen eines verantwortungsvollen Offenlegungsprozesses behandelt. Die Anzahl der betroffenen Anbieter macht diese Entdeckung zu einem weit verbreiteten Problem.

## Ergebnisse

Die wichtigsten Ergebnisse der Untersuchung sind:

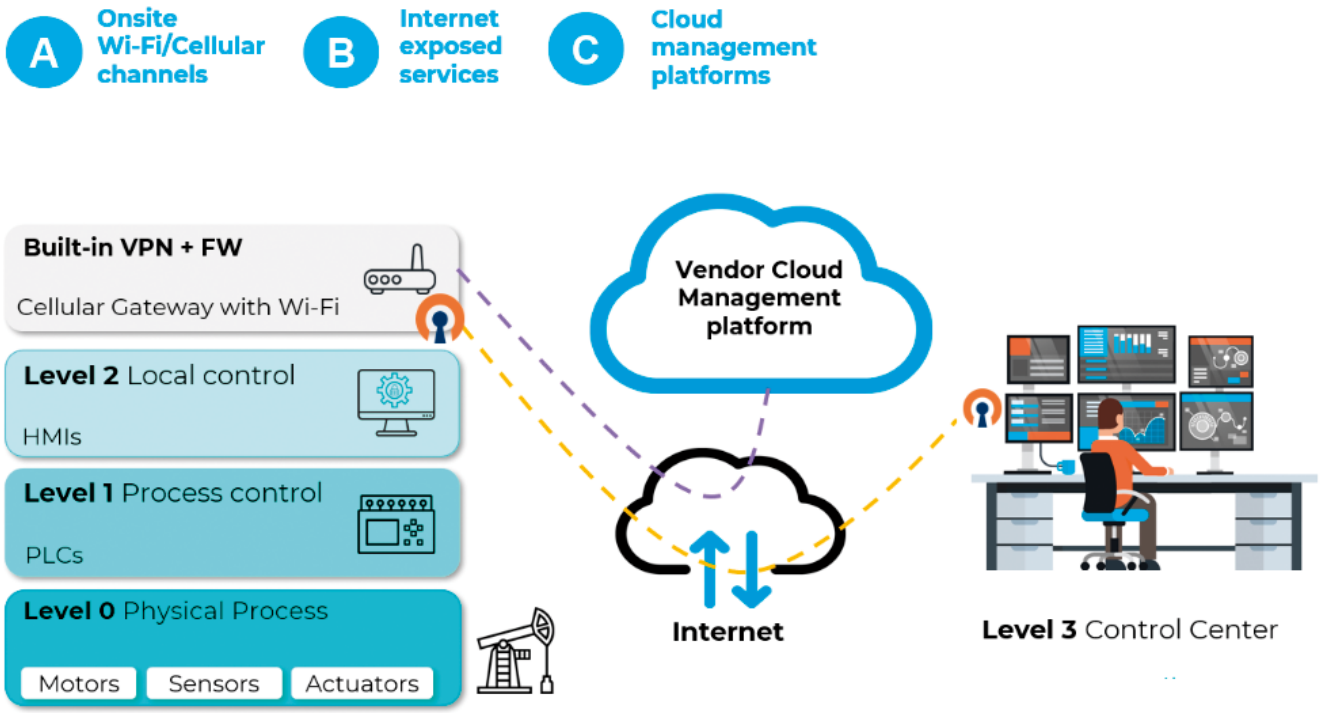
1. Wireless-IIoT-Infrastrukturen und ihre Cloud-Plattformen bieten in ihrem derzeitigen Zustand eine kritische Angriffsfläche für entfernte Industriestandorte.
2. Bei vier führenden Anbietern, die untersucht wurden, sind kritische Probleme aufgetaucht, einige befinden sich noch im Offenlegungsprozess.
3. Wireless IIoT, wie es üblicherweise zum Einsatz kommt, ist ein erhebliches Risiko für OT-Umgebungen, da es eine direkte Verbindung sowohl zum Internet als auch zum internen OT-Netzwerk herstellt. Dadurch entsteht ein einziger Fehlerpunkt und ein potenzieller Angriffspfad, der alle Sicherheitsebenen gemäß dem Purdue-Modell umgehen kann.
4. Angreifer können kostenlose Plattformen wie WiGLE einsetzen, um hochwertige, anfällige Ziele zu lokalisieren, ihren physischen Standort zu bestimmen und sie von der Nähe aus auszunutzen. Dies stellt ein kritisches Risiko für OT-Netzwerke und kritische Infrastrukturen dar – mit gefährlichen potenziellen Auswirkungen.

## Purdue-Modell

Jahrelang bot das Purdue-Modell den OT-Sicherheitsfachkräften eine Referenzarchitektur für die Segmentierung und damit den Schutz ihrer Netzwerke. Die Revolution der Industrie 4.0, die eine rasche Übernahme von IT-Technologien und deren Sicherheitsrisiken in OT-Umgebungen mit sich brachte, warf Fragen nach der Relevanz des Purdue-Modells in der heutigen Zeit auf.

Im Industrie 4.0 sind Cloud, 5G, Edge Computing und KI gängige Begriffe im OT-Lexikon. Einige der Enabler sind industrielle drahtlose IoT-Geräte, wie z. B. industrielle Mobilfunk-Gateways und industrielle WLAN-Access-Points. Industrielle drahtlose IoT-Geräte

*Autor:*
*Kay Ernst*
*Regional Sales Director DACH*
*OTORIO*
*www.otorio.com*




sind in verschiedenen OT-Einsatzbereichen üblich:

- Industrielle Mobilfunk-Gateways sind in Wasserversorgungsunternehmen sowie in der Öl- und Gasindustrie für die Fernüberwachung von verteilten Standorten zu finden.
- Industrielle WLAN-Access-Points bieten sichere drahtlose Lösungen für Plant-Floor-Systeme, SCADA-Automatisierung, Prozesssteuerungssysteme und WLAN-Infrastruktur für mobile Mitarbeiter.

## Cloud-Management und drahtlose Konnektivität

Anbieter von Industrial Wireless IoT-Lösungen offerieren in der Regel eine cloudbasierte Managementlösung, um Operationen aus der Ferne durchzuführen. Weitere Merkmale sind Edge-Computing-Fähigkeiten und Gateway-Funktionen für OT-Protokolle wie Modbus oder DNP3, die über serielle Verbindungen übertragen werden.

Die Kombination aus Cloud-Management und drahtloser Konnektivität erhöht die potenzielle Angriffsfläche erheblich. Außerdem stellen diese Geräte eine direkte Verbindung zu den unteren Ebenen des Purdue-Modells her (Ebene 2 bis Ebene 0), was sie in den Augen eines Angreifers zum idealen Einstiegspunkt in OT-Netzwerke macht.

## Empfehlungen

Industrielle drahtlose IoT-Geräte und ihre cloudbasierten Managementplattformen sind attraktive Ziele für Angreifer, die in industriellen Umgebungen Fuß fassen wollen. Dies liegt an den minimalen Anforderungen für die Ausnutzung und den potenziellen Auswirkungen.

Die Studie konzentrierte sich auf drei Angriffsvektoren, die alle einen externen Zugriff auf das interne Netzwerk erfordern:

1. Über die Cloud, was Masseninfektionen und die Umgehung von IP-Filterung, NAT und lokalen Firewall-Konfigurationen ermöglicht.
2. Direkt über das WAN, wodurch ungeschützte Schnittstellen für opportunistische und fortgeschrittene Angreifer äußerst anfällig werden.
3. Von einem nahegelegenen Standort aus ermöglicht die physische Nähe zu diesen Geräten eine einfache Ausnutzung von Angriffsszenarien.

Diese Vektoren verdeutlichen die Anfälligkeit dieser Geräte für externe Angriffe. Dies gilt ebenso für die Tatsache, dass die Geräte direkt mit dem internen Netzwerk verbunden sind und somit in gängigen Umgebungskonfigurationen als Single Point of Failure dienen
.

Die direkte Verbindung zu den unteren Purdue-Ebenen des Netzwerks – die Ebenen 0 bis 2 – bedeutet in der Regel eine vollständige Umgehung der üblichen Sicherheitsmaßnahmen gemäß dem Purdue-Modell. Dies ermöglicht den Zugang zu sensiblen Geräten im OT-Netzwerk, die in der Regel von vornherein anfällig sind.

## Praktische Erkundungsmethoden

Darüber hinaus hat die Studie praktische Erkundungsmethoden demonstriert, womit es gelang, eine beträchtliche Anzahl von Netzwerken aufzudecken, die für verschiedene Angriffsvektoren anfällig sind. Dies verdeutlicht die zusätzlichen Bedrohungen durch Wireless IIoT für industrielle und kritische Umgebungen.

## Wer schreibt:

Otorio entwickelt und vermarktet die nächste Generation von OT-Sicherheits- und digitalen Risikomanagementlösungen. Das Unternehmen kombiniert die Erfahrung führender staatlicher Cybersicherheitsexperten mit modernsten Technologien für das digitale Risikomanagement, um ein Höchstmaß an Schutz für kritische Infrastrukturen und die Fertigungsindustrie zu bieten. ◄