Mobile Working auch in Ex-Zonen

Smarte mobile Endgeräte für digitale Workflows im explosionsgeschützten Bereich


© Pepperl+Fuchs

Mobile Devices wie Smartphones, Tablets und Smart Glasses erleichtern und beschleunigen Wartung und Support in Prozessanlagen signifikant und bieten den Mitarbeitern darüber hinaus mehr Sicherheit – insbesondere in explosionsgeschützten Bereichen.

In vielen Anlagen der Chemieindustrie sind notwendige, strenge Sicherheitsformalien zu beachten. Wo immer mit Gasen oder entzündlichen Flüssigkeiten gearbeitet wird, herrscht Explosionsgefahr, genauso bei Prozessen mit einer hohen Staubentwicklung. In diesen explosionsgefährdeten Bereichen werden mobile Endgeräte immer wichtiger für die digitale Produktion und die Wartung der Anlagen. In weitläufigen Anlagen können die Wege zwischen den digitalisierten Bereichen und der analogen Welt der Ex-Zonen viel Zeit in Anspruch nehmen. Das verzögert nicht nur Arbeitsabläufe, sondern auch den Transfer und die Verfügbarkeit dringend benötigter Informationen, was einen Risikofaktor darstellen kann.

Voller Durchblick in rauen Umgebungen

Für diese Anforderungen gibt es mobile, explosionsgeschützte Gesamtlösungen wie die explosionsgeschützten Smart Glasses Visor-Ex 01 für den industriellen Einsatz in den Ex-Zonen ATEX Zone 1 und 2. Mit dieser Brille können mobile Servicetechniker auch im Ex-Bereich weitere Vorteile der Digitalisierung nutzen, indem sie freihändig arbeiten können. Die Datenerfassung und Datenanalyse in Echtzeit erleichtern den Arbeitsablauf. In schwierigen Einsätzen können sie sich über die Smart Glasses z.B. Checklisten und Anleitungen einblenden oder einen fachkundigen Remote Support per Video zuschalten. Dieser kann das gleiche sehen wie der Mobile Worker und unter die Arme greifen, als wäre er vor Ort.


© Pepperl+Fuchs

> *In der Chemieindustrie sind mobile Geräte mehr als bloße Kommunikations-Tools.*
>
> Christian Uhl, Pepperl+Fuchs

Zur Kommunikation sind vier Mikrofone mit Spracherkennung und Rauschunterdrückung für Umgebungen mit einem hohen Lärmpegel verbaut. Je nach Notwendigkeit kann der Träger das System entweder freihändig über die Spracherkennungsfunktion der Mikrofone bedienen oder über das Touchpad an der Seite der Smart Glasses sowie das Touch-Display des zugehörigen Smartphones Smart-Ex 02.

In Kombination mit dem eigensicheren Smartphone als Recheneinheit mit LTE-Konnektivität und einer Akku-Einheit zur Stromversorgung bilden die Smart Glasses ein intelligentes Kombipaket, das Bewegungsfreiheit auch in widrigen Umgebungen gewährleistet. Mithilfe der Kombination aus Kameras und Bildverarbeitung lassen sich QR-Codes auslesen, um via Smartphone Zugang zu den Sensordaten aus der Anlage zu erhalten. Der integrierte Laser-Aimer zeigt dem Träger genau, worauf die Kamera gerade gerichtet ist; Stabilisatoren wirken einem Verwackeln entgegen.

Smartphone oder Tablet?

Wenn größere Mengen an Text, etwa in Formularen, erfasst werden müssen, sind Tablets die komfortablere Wahl gegenüber Smartphones, die wiederum durch ihre kompakte Form in anderen Anwendungen punkten. Bei der Wahl des Betriebssystems ist die Kompatibilität zu den eigenen Systemen und Plattformen ein zentraler Entscheidungsfaktor. Auch die LTE- und 4G-Konnektivität ist gerade auf weitläufigen Geländen und in abgelegenen Einsatzorten von Vorteil, um von einem WLAN unabhängig zu sein. Ausschlaggebend für die Wahl des konkreten Anbieters sind außerdem die IT-Sicherheit, ein schneller Support vor Ort sowie die Möglichkeit, die Konfiguration ebenso wie Software-Updates auch over-the-air durchzuführen.

> *Fernwartung schließt besonders in Zeiten von wachsender Komplexität und von Fachkräftemangel entstehende Lücken beim Personal vor Ort.*

Mit dem Samsung-Tablet TabActive3 als leistungsfähiges und anerkanntes Basisgerät und Android als Betriebssystem sind bei Tab-Ex die Themen Updates, Konfiguration und OEM-Support durch Samsung zuverlässig und benutzerfreundlich abgedeckt. Für eine kompromisslose IT-Sicherheit sorgt Samsung Knox. Nicht zuletzt eröffnet die Tab-Ex-Serie durch die Unterstützung von Augmented Reality (AR) sowie Barcode-Scans eine Vielzahl von weiteren Anwendungsmöglichkeiten.

Effizienz steigern mit smarten Devices

Neben den Sicherheitsaspekten sind Kosteneinspar- und Effizienzsteigerungspotenziale, die smarte Devices mit sich bringen, nicht von der Hand zu weisen: In der Chemieindustrie sind mobile Geräte mehr als bloße Kommunikations-Tools. Sie unterstützen Mitarbeiter in der Anlage dabei, Daten zu erfassen, auszuwerten und vor allem schnell und zuverlässig auf Herausforderungen zu reagieren. Ausfallzeiten werden dank vorausschauender Planung von Wartungsvorgängen minimiert. Techniker werden durch die Nutzung von Echtzeitdaten auf Basis von Sensoren direkt alarmiert, wenn eine Störung zustande kommt.

Mobile Devices für Fernwartungsnutzung bieten Mitarbeitern Echtzeitzugang zu allen notwendigen Informationen. Mobile Worker können direkt Kontakt zum Experten aus dem Remote Support aufnehmen, der Unterstützung bietet oder Anweisungen gibt, während die relevanten Informationen per Smart Glasses in Echtzeit in das Sichtfeld des Mobile Workers eingeblendet werden. So werden nicht nur Inspektions- und Ausfallzeiten verkürzt, in vielen Fällen entfallen auch die Reiseaufwände für Support-Experten. Die Fernwartung schließt besonders in Zeiten von wachsender Komplexität und von Fachkräftemangel entstehende Lücken beim Personal vor Ort. Techniker im Feld haben so jederzeit Zugang zu allen notwendigen Informationen und Experten können ortsunabhängig bei speziellen Problemstellungen oder Fragen unterstützen.

Sicherheit geht immer vor

Anbieter wie die Pepperl+Fuchs Marke Ecom Instruments schneiden ihre eigensicheren Mobile Devices auf die Bedürfnisse des modernen Servicetechnikers zu: Mobile Endgeräte müssen den Mitarbeiter bei seiner täglichen Arbeit unterstützen und gleichzeitig den hohen Anforderungen der Industrie standhalten. Die Sicherheit des Alleinarbeiters steht dabei stets an erster Stelle. Dies setzt die Erfüllung unterschiedlicher Standards und die Einsatzfähigkeit in diversen Infrastrukturen voraus. Deshalb entsprechen die weltweit einsetzbaren Geräte den höchsten Sicherheitsstandards und enthalten Funktionen zur schnellen Notfallalarmierung.

Christian Uhl, Head of Communication, Global Marketing, Pepperl+Fuchs, Mannheim

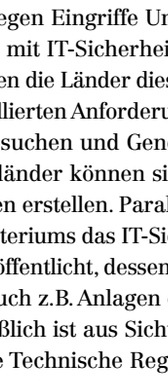
■ www.pepperl-fuchs.com


© Pepperl+Fuchs

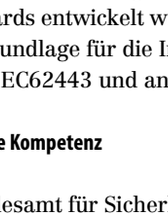
Mit dem Android-Betriebssystem arbeitet das eigensichere Smartphone sehr schnell, sicher und effizient und die Benutzeroberfläche ist intuitiv bedienbar. Das 5-Zoll-Display ist durch das stoß- und kratzfeste Gorilla-Glas extrem widerstandsfähig und lässt sich einwandfrei auch mit Handschuhen bedienen.

KOLUMNE: PROZESSINDUSTRIE

Cybersecurity erfordert mehr Taten, nicht mehr Regulierung


© Rene Neijts

Rene Neijts, Dow, Mitglied des Vorstands der NAMUR


© Bayer

Felix Hanisch, Bayer, Vorstandsvorsitzender der NAMUR

Kürzlich erläuterte der ehemalige NATO-General Koen Gijsbers anhand einer Reihe von Beispielen, dass Cyberangriffe ein etabliertes Mittel in Konflikten zwischen Nationen sind. Während im Zusammenhang mit dem aktuellen russisch-ukrainischen Krieg eine deutliche Zunahme von Cyber-Attacken erwartet, diese jedoch bislang nicht beobachtet wurde, steht fest: Das nächste große Cyber-Ereignis wird kommen. Weiterhin bleiben der „gelangweilte Teenager" oder der professionelle Cyberkriminelle eine ständige Bedrohung auch für jedes Unternehmen der Prozessindustrie.

Gesetze, Verordnungen, Dokumente

Dies beunruhigt auch die öffentlichen Regulierungsbehörden: infolgedessen sehen wir eine wachsende Zahl von Gesetzen, Verordnungen und zusätzlichen Dokumenten, die alle darauf abzielen, ein Problem zu lösen, an dessen Lösung die Prozessindustrie selbst ein großes Interesse hat. In Deutschland beispielsweise werden Anlagen, die unter die Seveso-Richtlinie der EU („Störfallbetriebe") fallen, durch das BImSchG und die entsprechende Störfallverordnung geregelt, die in den Zuständigkeitsbereich des Bundesministeriums für Umwelt fallen. Dessen Kommission für Anlagensicherheit hat einen Leitfaden „Maßnahmen gegen Eingriffe Unbefugter" herausgegeben, einschließlich eines Anhangs mit IT-Sicherheitsanforderungen. Im föderalen System Deutschlands müssen die Länder dies umsetzen, was NRW dazu veranlasst hat, einen sehr detaillierten Anforderungskatalog zu erstellen, der im Rahmen von Standortbesuchen und Genehmigungsverfahren herangezogen wird. Andere Bundesländer können sich daran orientieren oder eigene Listen und Anforderungen erstellen. Parallel dazu wurde unter Federführung des Bundesinnenministeriums das IT-Sicherheitsgesetz überarbeitet und 2021 als „ITSiG2.0" veröffentlicht, dessen Anwendungsbereich deutlich erweitert wurde und nun auch z.B. Anlagen einschließt, die unter die Störfallverordnung fallen. Schließlich ist aus Sicht des Arbeitsschutzes - anderes Bundesministerium - eine Technische Regel Betriebssicherheit für Cybersicherheit in Vorbereitung. Es ist unnötig zu erwähnen, dass auf internationaler Ebene bereits Standards entwickelt wurden, die gut akzeptiert sind und seit einiger Zeit die Grundlage für die Implementierung und Systementwicklung bilden, wie z.B. IEC62443 und andere.

Gebündelte Kompetenz

Erfreulicherweise bündeln das Bundesamt für Sicherheit in der Informationstechnik, der TÜV-Verband, Fachbehörden der Länder, die NAMUR und der VCI ihre Kompetenzen in einem Kompendium, das technische Hinweise und einen risikobasierten Ansatz zur Sicherung von Industrieanlagen bieten soll. Anstatt weitere Dokumente zu erstellen, möchten wir einen anderen Ansatz vorstellen, den eines der NAMUR-Mitgliedsunternehmen vor kurzem verfolgt hat: die Teilnahme an einer Table-Top-Übung in den USA namens Cyberstorm, die von der Cybersecurity and Infrastructure Security Agency unter der Leitung des Department of Homeland Security gesponsert wird. Die Planung und Durchführung dieser Übung findet seit 2006 alle zwei Jahre statt. Das für Cyberstorm ausgewählte Angriffsszenario unterscheidet sich von Übung zu Übung und baut auf den Erfahrungen aus früheren Cyberstorm-Übungen auf. Bei dem jüngsten Cyberstorm basierte der Angriff auf einer neuen, unentdeckten Version von Ransomware.

Repräsentative Unternehmen aus vielen verschiedenen kritischen US-Wirtschaftszweigen werden im Rahmen von Cyberstorm mit wichtigen Regierungsbehörden zusammengebracht, um ein simuliertes Angriffsszenario durchzuspielen. Eines der Primärziele dieser Übung ist es, zu verstehen, wie ein groß angelegter Cyberangriff auf zahlreiche Organisationen erfolgen könnte und wie diese durch einen solchen Angriff beeinträchtigt werden könnten. Die Übung ermöglicht es den Teilnehmern, ihre Reaktionsfähigkeit ohne die Folgen eines realen Ereignisses zu testen, und soll aufzeigen, wo Lücken und Schwachstellen in der operativen Sicherheit und in den Cyber-Reaktionsplänen der teilnehmenden Organisationen bestehen.

Zu dieser Übung gehört auch eine „simulierte" Social-Media-Umgebung, die die Kommunikation zwischen den teilnehmenden Organisationen/Unternehmen und an der Übung beteiligten Regierungsbehörden fördern und unterstützen soll, und natürlich eine anschließende Auswertung.

Unterm Strich bleibt: wir brauchen die richtige Balance aus rahmengebenden Vorschriften und praktischer Erfahrung und Austausch, möglichst in einer gesicherten Umgebung. Gerade bei Erfahrung und Austausch unterstützt NAMUR aktiv.

■ office@namur.de
■ www.namur.de