Cyber-Sicherheit in der Smart City der Zukunft

Für den Schutz sensibler Daten und Systeme in der Smart-City-Leitstelle stattete IHSE das Übertragungssystem mit Multi-Sicherheitsfunktionen aus.

Forscher tüfteln an nachhaltigem Mobilitätskonzept zur Entlastung des innerstädtischen Verkehrs in Friedrichshafen

Das Forschungs- und Entwicklungsprojekt ALFRIED (Automatisiertes und vernetztes Fahren in der Logistik am Testfeld Friedrichshafen) erarbeitet intelligente Technologie für die Steuerung und Überwachung des innerstädtischen Verkehrs. Sowohl die Fahrgäste als auch die Netzbetreiber sollen von einem ungehinderten, sicheren, lärm- und emissionsreduzierten Verkehr profitieren. Bei dem vom Bundesministerium für Digitales und Verkehr geförderten Projekt greifen modernste Technologien wie künstliche Intelligenz, Datenanalytik, Passagiermanagement, Netzwerküberwachung und automatisiertes Routing zahnradartig ineinander.

Von entscheidender Bedeutung für das autonome Fahren der Zukunft sind zentrale Leitstellen, die sämtliche Verkehrsdaten sammeln, validieren und die relevanten Informationen den Verkehrsteilnehmern bzw. ihren autonomen Systemen in Echtzeit zur Verfügung stellen und entsprechende Handlungsempfehlungen geben.

Die Smart-City-Leitstelle: Für die Steuerung und den Zugriff auf mehrere Computer kommt ein IHSE KVM-System zum Einsatz.

© IHSE

KVM IN DER SMART-CITY-LEITSTELLE

Die dafür errichtete Smart-City-Leitstelle ist ein offenes Demonstrationszentrum, das den Realbetrieb so simuliert, dass verschiedene Konzepte entwickelt und getestet werden können. Für die Steuerung und den Zugriff auf mehrere Computer kommt ein IHSE KVM-System zum Einsatz. KVM steht für „Keyboard, Video, Mouse". Die KVM-Technologie ermöglicht es, mehrere Computer oder Server von einer zentralen Konsole aus in Echtzeit zu bedienen.

Neben der zentralen Überwachung ermöglicht das KVM-System ein flexibles Arbeitsumfeld, bei dem die Bediener zwischen verschiedenen Computern und Anwendungen nahtlos wechseln und diese gemeinschaftlich nutzen können, ohne die räumliche Trennung in den Arbeitsabläufen wahrzunehmen.

Um optimale Handlungsempfehlungen für die Routenplanung zu treffen, verarbeitet das KVM-System sowohl öffentlich zugängliche Informationen als auch sensible Daten mit speziellen Sicherheitsanforderungen.

SCHUTZ VOR CYBER-ANGRIFFEN

Gerade in Zeiten von Cyberangriffen ist der Schutz vor Datendiebstahl von zentraler Bedeutung für Smart-City-Leitstellen. Ein Angriff könnte dramatische Folgen auf die gesamte Infrastruktur haben: Verkehrschaos, Ausfall oder Einschränkungen bei den Notfalldiensten. Daher muss diese Pionier-Leitstelle zukünftige Sicherheitsanforderungen erfüllen, die von aktuellen kommerziellen Leitstellenkonzepten noch nicht berücksichtigt werden.

Für den Schutz sensibler Daten und Systeme in der Leitstelle stattete IHSE das Übertragungssystem mit Multi-Level-Sicherheitsfunktionen aus. Das KVM-Setup verhindert unbefugten Zugriff durch die Unterbringung der sensiblen Geräte und Computer in einem gesicherten Serverraum. Die Verbindung zu den Arbeitsplätzen läuft über eine proprietär verschlüsselte und abhörsichere Datenübertragung nach militärischen Standards (NIAP PP4.0 und EAL4+), die auch den KRITIS-Kriterien für kritische Infrastruktur entsprechen. Die Bediener müssen sich zudem an ihren Konsolen authentifizieren und unterliegen einer Zugriffskontrolle, die genau festlegt, welche Nutzer zu welchen Bereichen Zugang erhalten.

Indem nur notwendige Signale übertragen werden, lässt sich der Hardwarezugriff weiter einschränken: Die Beschränkung von USB-Anschlüssen auf Tastatur- und Mausbefehle verhindert etwa den Datendiebstahl per USB-Stick oder das Einspeisen von Schadsoftware. Der zentrale Matrixswitch (die eigentliche Schaltzentrale) ist physisch vom IP-Netz getrennt, wodurch potenzielle Hackerangriffe über IP von vornherein ausgeschlossen sind. Im unwahrscheinlichen Falle eines Systemausfalls erlaubt die eingesetzte Redundanzfunktion zudem den nahtlosen Wechsel zu Backup-Computern und -Systemen. ■