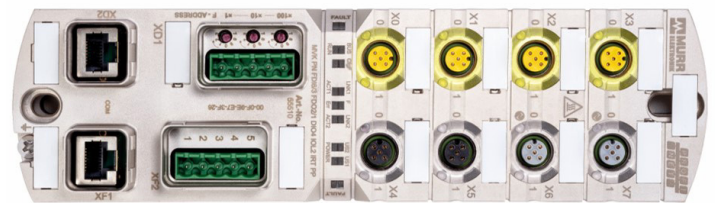


KOMPETENZZENTRUM CyberProtect

EIN QUICK-CHECK DES KOMPETENZZENTRUMS CyberProtect



SICHERHEITSANALYSE PLASMA

KONTAKT



Fraunhofer IOSB

Anne Borcharding
anne.borcharding@iosb.fraunhofer.de

Christian Haas
christian.haas@iosb.fraunhofer.de

IN ZUSAMMENARBEIT MIT



Murrelektronik GmbH

Jörg Hinze
joerg.hinze@murrelektronik.de

Ausgangssituation und Problem

Durch die steigende Vernetzung in industriellen Netzwerken wird auch die Vermischung zwischen Feldbus- und IT-Kommunikation zunehmen. Mit der Öffnung der industriellen Netze werden einem Angreifer zudem neue Möglichkeiten für den Zugriff und die Manipulation des Netzes gegeben. Dies führt zu neuen Anforderungen, die an industrielle, eingebettete Systeme gestellt werden. Unter anderem wird eine hohe Stabilität, Netzwerkperformance und IT-Sicherheit gefordert. Im Rahmen dieses Quick-Checks soll ein Feldbus-E/A-Modul auf seine Stabilität und IT-Sicherheit untersucht werden. Dabei wird ein Fokus auf die angebotene Webanwendung gelegt. Es werden automatisierte Verwundbarkeitsscanner eingesetzt, die durch eine umfassende manuelle Analyse ergänzt werden. Durch diese Untersuchung wird so auch erreicht, dass die Performanz der Verwundbarkeitsscanner

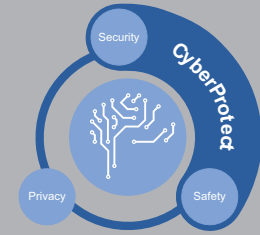
an einem Feldbus-Modul evaluiert werden kann.

Lösungsansatz

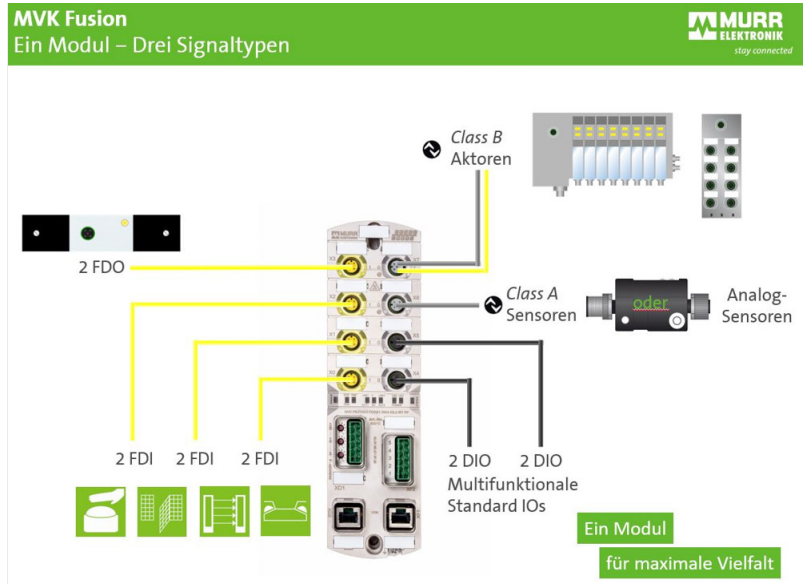
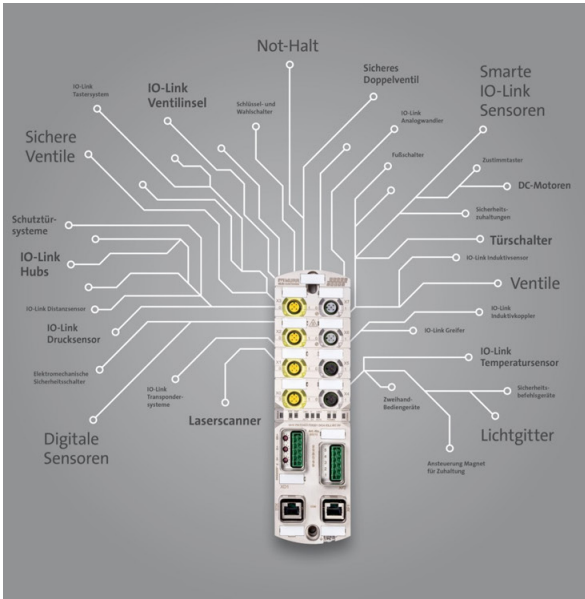
Die Durchführung des Quick-Checks wird in mehrere Phasen aufgeteilt. Diese haben zum einen das Ziel, den Stand der IT-Sicherheit des Feldbus-E/A-Moduls zu analysieren. Zum anderen dienen sie dazu, verschiedene Verwundbarkeitsscanner anhand einer weiteren Automatisierungskomponente zu evaluieren. Die erste Phase des Quick-Checks dient dazu, mit einem sogenannten Portscanner geöffnete Ports des zu untersuchenden Geräts aufzudecken.

Im Anschluss werden verschiedene protokollübergreifende Verwundbarkeitsscanner eingesetzt. Diese überprüfen, ob das zu überprüfende Gerät bekannte Schwachstellen aufweist. In der nächsten Phase werden dann spezialisierte Web-Verwundbarkeitsscanner eingesetzt, die die angebotene Webanwendung auf Schwachstellen unter-

SICHERHEITSANALYSE PLASMA



EIN QUICK-CHECK DES KOMPETENZZENTRUMS CyberProtect



suchen. Die Ergebnisse der verschiedenen Verwundbarkeitsscanner werden manuell ausgewertet und gegebenenfalls durch Proof-of-Concept-Implementierungen bestätigt.

In der letzten Phase werden die Ergebnisse in einem Abschlussbericht zusammengefasst und in einer Abschlusspräsentation diskutiert.

Nutzen

Der Nutzen des Quick-Checks lässt sich in zwei Bereiche aufteilen. Zunächst zeigt die Untersuchung den aktuellen Zustand der IT-Sicherheit des untersuchten Feldbus-E/A-Moduls auf. Die Ergebnisse des Quick-Checks können nun verwendet werden, um das Modul weiterzuentwickeln und so die IT-Sicherheit zu verbessern. Ebenso können die Untersuchungen dazu dienen, die IT-Sicherheit bei Neuentwicklungen von Beginn an einzubeziehen.

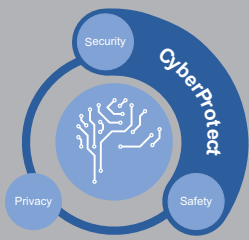
Der zweite Bereich umfasst die Evaluation

der verschiedenen Verwundbarkeitsscanner bei der Untersuchung eines Feldbus-Moduls. Diese Ergebnisse und die dabei gesammelten Erfahrungen werden in das IT-Sicherheitslabor am Fraunhofer IOSB einfließen. So werden die Ergebnisse dieses Quick-Checks auch in weiteren Untersuchungen und Analysen verwendet und können diese effizienter und effektiver machen.

Projektergebnisse

Die Ergebnisse dieses Quick-Checks umfassen einen umfangreichen Abschlussbericht, der das Vorgehen und die Ergebnisse der Analyse darstellt, sowie eine Abschlusspräsentation mit einer ausführlichen Diskussion der Analyseergebnisse. Die Analyse legt einen Fokus auf die automatisierte und manuelle Untersuchung der angebotenen Webanwendung. Dafür wurden verschiedene protokollübergreifende Verwundbarkeitsscanner sowie Web-Verwundbarkeitsscanner eingesetzt. Die Erfahrungen und

die Ergebnisse der Analyse können nun in die Optimierung der Entwicklungsprozesse sowie in zukünftige Entwicklungsprojekte einfließen, um die IT-Sicherheit von Feldbus-Modulen nachhaltig zu verbessern.



KOMPETENZZENTRUM CyberProtect

EIN QUICK-CHECK DES KOMPETENZZENTRUMS CyberProtect



FZI Forschungszentrum Informatik



Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung



Fraunhofer-Institut für Produktions-
technik und Automatisierung

Gefördert durch:



Baden-Württemberg

MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND WOHNUNGSBAU

Ministerium für Wirtschaft, Arbeit und
Wohnungsbau

Ansprechpartner

Dr.-Ing. Arne Rönnau

Telefon 0721 9654-228

roennau@fzi.de

Dr.-Ing. Erik Krempel

Telefon 0721 6091-292

erik.krempel@iosb.fraunhofer.de

Dipl.-Wi.-Ing. Ramez Awad

Telefon 0711 970-1844

ramez.awad@ipa.fraunhofer.de

ÜBER DAS KOMPETENZZENTRUM CyberProtect

Das durch das Ministerium für Wirtschaft, Arbeit und Wohnungsbau Baden-Württemberg geförderte Projekt CyberProtect verfolgt im Sinne der Stärkung von Firmen in Baden-Württemberg das Ziel der besseren Absicherung von komplexen Softwaresystemen. Dabei werden alle drei Bereiche von Sicherheit (Security, Safety und Privacy) betrachtet, der Fokus liegt hierbei auf dem Teilgebiet der Security. Im Rahmen des Projektes werden hierfür Methoden entwickelt, um das Verhalten bzw. die Entscheidungen von komplexen Softwaresystemen z.B. von KI-Systemen sichtbar zu machen und somit Aussagen über den Sicherheitszustand der Systeme zu ermöglichen. Über ein weitreichendes Angebot wie Quick-Checks, Schulungen und Open Lab Days werden Firmen in das Projekt einbezogen, um ihnen die Möglichkeit zu bieten, ihre komplexe Software auf Sicherheit untersuchen und ggf. verbessern zu lassen.

Bereit für Ihre Anwendung

Quick-Checks sind ein kostenloses, individuelles Angebot hinsichtlich Sicherheit in der Produktion für Firmen aus Baden-Württemberg. In diesen Quick-Checks werden mit ausgewählten Unternehmen die Themen Safety, Security und Privacy bearbeitet. Die Ergebnisse aller Quick-Checks werden als Steckbriefe im Webauftritt des Kompetenzzentrums CyberProtect (www.cyberprotect-bw.de) veröffentlicht.