

**Bewertung der
Einsatzmöglichkeiten
moderner, durch
IT-Angriffe nicht
manipulierbarer
Leittechniksysteme zur
Ausführung von Sicher-
heits-, Sicherungs- und
Schutzfunktionen in
kerntechnischen Anlagen
und Einrichtungen**

**Bewertung der
Einsatzmöglichkeiten
moderner, durch
IT-Angriffe nicht
manipulierbarer
Leittechniksysteme zur
Ausführung von Sicher-
heits-, Sicherungs- und
Schutzfunktionen in
kerntechnischen Anlagen
und Einrichtungen**

Kurzfassung

Robert Arians
Laura Kleinert
Oliver Rest
Alexander Schug
Birthe Ulrich

Juni 2025

Anmerkung:

Das diesem Bericht zugrunde liegende Eigenforschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit (BMUKN) unter dem Förderkennzeichen 4722R01570 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei der GRS.

Der Bericht gibt die Auffassung und Meinung der GRS wieder und muss nicht mit der Meinung des BMUKN übereinstimmen.

Deskriptoren

Cyberangriffe, ICS, Industrielle Steuerungssysteme, IT-Angriffe, IT-Angriffsvektoren, IT-Sicherheitsvorfälle, kerntechnische Anlagen, Leittechnik, nichtmanipulierbare Leittechnik

Inhaltsverzeichnis

1	Einleitung	1
2	Verfügbare Leitechniksysteme mit verringerter Angriffsoberfläche für IT-Angriffe	3
2.1	ProSafe-SLS.....	3
2.2	Hardline	4
2.3	Tricon	6
2.4	Teleperm XS Compact.....	7
3	IT-Angriffsvektoren unter Verwendung der schwieriger manipulierbaren Leitechniksysteme	9
4	Zusammenfassung	13

1 **Einleitung**

In den letzten Jahren hat die Zahl der IT-Angriffe auf industrielle Steuerungssysteme stark zugenommen. In vielen Fällen wurde die bei diesen Angriffen verwendete Schadsoftware für Angriffe auf industrielle Steuerungssysteme entwickelt. Dabei wurde sowohl Software zur Manipulation von betrieblichen Leittechniksystemen als auch speziell für die Manipulation von Leittechniksystemen für Sicherheits-, Sicherungs- und Schutzfunktionen entwickelte Schadsoftware eingesetzt. Generell lässt sich sagen, dass es keinen umfassenden Schutz von kerntechnischen Anlagen gegen IT-Angriffe auf dort eingesetzte rechnerbasierte oder programmierbare Systeme und Komponenten gibt.

Im Rahmen dieses Vorhabens wurde daher der mögliche Einsatz moderner Leittechniksysteme untersucht, die möglicherweise weniger anfällig für IT-Angriffe sind als typische rechnerbasierte oder programmierbare Leittechniksysteme. Dazu wurde in einem ersten Schritt eine Evaluierung relevanter IT-Angriffsvektoren auf rechnerbasierte oder programmierbare Leittechniksysteme durchgeführt. In einem zweiten Schritt wurden verfügbare leittechnische Systeme und Komponenten untersucht, wobei der Fokus auf leittechnischen Systemen und Komponenten lag, die nicht bzw. weniger anfällig für IT-Angriffe sind, wie beispielsweise fest verdrahtete und nicht programmierbare Systeme. Im dritten Arbeitsschritt wurde eine vergleichende Analyse der nicht bzw. schwieriger manipulierbaren Leittechniksysteme und Komponenten mit typischen rechnerbasierten oder programmierbaren Leittechniksystemen und Komponenten durchgeführt, um eventuelle Vor- und Nachteile der jeweiligen Systeme aufzuzeigen. Im letzten Arbeitsschritt wurde analysiert, inwieweit die identifizierten IT-Angriffsvektoren durch den Einsatz von gegen IT-Angriffe weniger anfälligen Leittechniksystemen geschlossen oder eingeschränkt werden können.

Dieser Bericht stellt eine Kurzfassung der Ergebnisse des Vorhabens dar, wobei insbesondere auf die schwieriger manipulierbaren Leittechniksysteme und die IT-Angriffsvektoren unter Verwendung dieser Systeme eingegangen wird. Die kompletten Ergebnisse des Vorhabens sind detailliert in dem Bericht GRS-A-4174 dargestellt.

2 Verfügbare Leitechniksysteme mit verringerter Angriffs- oberfläche für IT-Angriffe

Im Rahmen des Vorhabens wurde nach Leitechniksystemen recherchiert, die im Vergleich zu typischen rechnerbasierten oder programmierbaren Systemen eine möglichst verringerte Angriffsfläche für IT-Angriffe aufweisen. Dabei wurde ausschließlich nach Systemen recherchiert, die aktuell erhältlich sind und die das Potenzial bieten, durch IT-Angriffe nicht oder zumindest schwieriger manipulierbar zu sein als typische rechnerbasierte Systeme. Folgende vier Systeme, die anschließend kurz beschrieben werden, wurden bei der Recherche ausgewählt:

- ProSafe-SLS
- Hardline
- Tricon
- Teleperm XS Compact

2.1 ProSafe-SLS

Das Leitechniksystem ProSafe-SLS wurde von Yokogawa, einem japanischen Hersteller von Test- und Messgeräten sowie Automatisierungssystemen, bereits im Jahr 1958 entwickelt, damals noch unter dem Namen MagLog. Im Jahr 1997 erfolgte die Umstellung auf den Namen ProSafe-SLS. Des Weiteren erfolgte eine Weiterentwicklung der Technologie und die Aufrüstung hin zu modernen Komponenten und Fertigungsmethoden.

Das ProSafe-SLS-System bietet laut Hersteller die Möglichkeit, in sicherheitskritischen Bereichen eingesetzt zu werden. Der Aufbau der sicherheitskritischen Logik ist festverdrahtet, also ohne rechnerbasierte oder programmierbare Baugruppen. Bei dem ProSafe-SLS-System werden die logischen Funktionen mittels Magnetkernen verarbeitet, womit diverse logische Funktionen realisierbar sind. Das System arbeitet dabei (wie das im Reaktorschutzsystem deutscher Kernkraftwerke verwendete EDM-System) mit dynamischen Signalen in Form von Impulsfolgen. Diese Impulsfolgen werden über die Magnetkerne des ProSafe-SLS-Systems geschaltet. Alle Schaltkreise werden somit im Normalbetrieb kontinuierlich dynamisch betrieben. Diese dynamische Arbeitsweise bietet

den Vorteil, dass Fehler selbstmeldend sind, da das Auftreten von Fehlern zur Unterbrechung der Impulsfolge führt.

Durch den modularen Aufbau des ProSafe-SLS-Systems ist es möglich, ein Design für verschiedene Anwendungen zu entwickeln. Ein Einsatz einzelner Module ist ebenso denkbar wie der Aufbau ganzer Leittechnikssysteme. Dabei ist die Anzahl der Ein- und Ausgänge laut Hersteller unbegrenzt erweiterbar und der Aufbau von Leittechnikssystemen mit mehreren Redundanzen ist möglich. Die Module zur Ausführung nicht sicherheitskritischer Funktionen sowie Computerschnittstellen beispielsweise zur Anbindung des ProSafe-SLS-Systems an andere Systeme sind mikroprozessorbasiert realisiert. Die Ein- und Ausgangssignale zum ProSafe-SLS-System sind dabei galvanisch vom Logikteil getrennt. Die Kommunikationsfunktionen, die Aufzeichnung von Ereignissen sowie die Remote-Eingangs- und Ausgangsfunktionen werden vom ProSafe-COM-System übernommen. Der Aufbau des ProSafe-SLS-Systems erfolgt in Baugruppenträgern in Standard 19“-Racks in Standard-Leittechniksschränken.

Das ProSafe-SLS-System ist gemäß diversen international gültigen Normen, insbesondere IEC-Normen, qualifiziert. Hinsichtlich funktionaler Sicherheit für Sicherheitssysteme wurde die IEC 61508 berücksichtigt, nach welcher das ProSafe-SLS-System SIL 4 zertifiziert ist. Die Qualifizierung des Systems erfolgte laut Hersteller ausschließlich nach Industrienormen, eine Qualifizierung nach kerntechnischem Regelwerk ist nicht geplant. Nichtsdestotrotz wird das ProSafe-SLS-System weltweit in ca. 20 kerntechnischen Anlagen (vor allem im Vereinigten Königreich) bis hin zum Reaktorschutz eingesetzt. Das ProSafe-SLS-System kann laut Hersteller in diversen Anlagensystemen zum Einsatz kommen, wie z. B. dem Reaktorschutz, dem Abfallmanagement, dem Kesselschutz oder der Brennstoffhandhabung. Ein Ausschluss bestimmter Systeme, in denen kein Einsatz möglich wäre, erfolgt vom Hersteller nicht.

2.2 Hardline

Das Leittechniksystem Hardline wurde von Rolls Royce in Frankreich entwickelt und wird mittlerweile von Framatome vertrieben. Bei dem Hardline-System handelt es sich um ein nicht programmierbares, festverdrahtetes Leittechniksystem, welches laut Hersteller speziell zum Betreiben von Sicherheitsleittechnik in kerntechnischen Anlagen entwickelt wurde. Auf dem Markt erhältlich ist das Hardline-System seit Ende des Jahres 2021.

Der Aufbau der sicherheitskritischen Logik ist festverdrahtet, also ohne rechnerbasierte oder programmierbare Baugruppen. Die Ausführung der logischen Funktionen in den sicherheitstechnisch wichtigen Anwendungen erfolgt mittels nicht programmierbarer, diskreter Bauelemente. Mit den nicht programmierbaren, festverdrahteten Modulen sind diverse Anwendungen und logische Funktionen realisierbar. Die Module zur Ausführung sicherheitstechnisch wichtiger Funktionen sind mit Funktionen zur Selbstüberwachung und automatischen Diagnose ausgestattet und werden während des Betriebs kontinuierlich überprüft, wodurch Hardwarefehler laut Hersteller in den meisten Fällen erkannt werden können.

Durch den modularen Aufbau des Hardline-Systems besteht zum einen die Möglichkeit, einzelne Module in bereits bestehenden Leittechniksystemen zu ersetzen, zum anderen können auch komplett neue Leittechniksysteme aufgebaut werden. Dabei besteht die Möglichkeit eines Aufbaus von Systemen mit bis zu vier Redundanzen. Die Größe des Leittechniksystems ist dabei auf etwa 200 Module je Redundanz (ca. 1.500 Ein- und Ausgangssignale) begrenzt. Die Module zur Ausführung nicht sicherheitstechnisch wichtiger Funktionen sowie Module zur Kommunikation sind programmierbar ausgeführt. Die Isolation und Trennung zwischen den Modulen zur Ausführung sicherheitstechnisch wichtiger Funktionen (festverdrahtet) und den programmierbaren Modulen wird beim Hardline-System mit nicht programmierbaren, elektronischen Komponenten realisiert. Zwischen den Modulen zur Ausführung von Funktionen mit sicherheitstechnischer Bedeutung und den programmierbaren Modulen ist nur eine Ein-Wege-Kommunikation hin zu den programmierbaren Modulen erlaubt, um sicherzustellen, dass etwaige Fehler in den programmierbaren Modulen nicht auf die Module zur Ausführung sicherheitstechnisch wichtiger Funktionen übertragen werden können. Der Aufbau des Hardline-Systems erfolgt in Baugruppenträgern in Standard 19“-Racks in Standard-Leittechnik-schränken.

Die Entwicklung und Qualifizierung des Hardline-Systems erfolgte laut Hersteller nach diversen international gültigen Normen und Anforderungen, wobei auch nukleare Regelwerke berücksichtigt wurden. Dabei wurden diverse Anforderungen der IAEA sowie diverse IEC-Normen berücksichtigt. Laut Hersteller ist das Hardline-System für den Einsatz in Systemen qualifiziert, die Funktionen der Kategorie A nach DIN EN 61226 (bzw. Class 1E in den USA) ausführen, also Funktionen der höchsten Sicherheitskategorie (z. B. Reaktorschutz). Das Hardline-System wird beispielsweise in einem Kernkraftwerk in China als Diverse Protection System eingesetzt, zudem ist ein Einsatz im EPR 2 und

in SMR in Diskussion. Das Hardline-System kann laut Hersteller in diversen Anlagensystemen zum Einsatz kommen, wie z. B. dem Reaktorschutzsystem, der Prioritätslogik, der Notstromdieselgeneratorsteuerung oder dem Post-Accident-Monitoring-System. Ein Ausschluss bestimmter Systeme, in denen kein Einsatz möglich wäre, erfolgt vom Hersteller nicht, allerdings ist das Hardline-System laut Hersteller eher zum Aufbau kleinerer Systeme mit begrenztem Funktionsumfang und nicht für z. B. den Reaktorschutz eines Leistungsreaktors konzipiert.

2.3 Tricon

Das Leittechniksystem Tricon wurde von Triconex, einer Tochter von Schneider Electric, einem französischen Hersteller unter anderem von Steuerungs- und Sicherheitssystemen entwickelt und im Jahr 1986 erstmals eingesetzt. Mittlerweile wird das Tricon-System von Framatome vertrieben. Das System basiert auf einer dreifach redundanten, modularen Architektur (TMR-Architektur, triple modular redundant), bei welcher drei voneinander isolierte, parallel arbeitende Systeme verwendet werden.

Das Tricon-System kann laut Hersteller in sicherheitskritischen Bereichen eingesetzt werden. Von den Eingangsmodulen über die Hauptprozessoren bis zu den Ausgangsmodulen ist das System durchgängig mit einer dreifachen Architektur aufgebaut. Ein an einem Eingangsmodul anliegendes Signal wird in diesem in drei parallele, voneinander unabhängige Pfade aufgeteilt. Von jedem dieser Pfade wird das Eingangssignal ausgelesen und an den jeweiligen Hauptprozessor weitergeleitet. Das Signal wird von allen drei Hauptprozessoren verarbeitet und nach der Signalverarbeitung werden die Ergebnisse zur Ausgabebaugruppe weitergeleitet. Vor der Ausgabe des Signals erfolgt ein 2 v 3-Voting der Signale mit dem Ziel, auch bei auftretenden Einzelfehlern einen ununterbrochenen Betrieb zu gewährleisten. Die sicherheitskritische Logik wird im Rahmen des vom Nutzer erstellten Anwendungsprogramms in den Hauptprozessoren ausgeführt, dass Tricon-System ist somit rechnerbasiert. Durch den Einsatz der TMR-Architektur bietet das System eine gewisse Fehlertoleranz. Laut Hersteller sind Möglichkeiten zum digitalen Online-Monitoring und zur Selbstüberwachung und -diagnose implementiert.

Aufgrund des modularen Aufbaus des Tricon-Systems ist es möglich, das System von einfachen bis hin zu komplexen Anwendungen zu nutzen. Der Einsatz der dreifach redundanten, modularen Architektur ist in jeder Redundanz des gesamten Leittechniksystems vorgesehen. Soll ein Leittechniksystem mit mehreren Redundanzen aufgebaut

werden, besteht die Möglichkeit, mehrere Tricon-Systeme miteinander zu verbinden. Maximal können je Redundanz 118 Ein-/Ausgabemodule verwendet werden, was einer maximalen Anzahl von ca. 5000 Ein-/Ausgangssignalen je Redundanz entspricht. Mittels eines hardwarebasierten Schlüsselschalters lässt sich die Betriebsart des Tricon-Systems steuern, wobei für Veränderungen des Anwendungsprogramms eine bestimmte Schalterstellung erforderlich ist. Der Aufbau des Tricon-Systems erfolgt in 19“-Chassis, die in NEMA-Leittechnikschränken nach Industriestandard installiert werden können.

Das Tricon-System ist in den USA gemäß diversen kerntechnischen Richtlinien und Regelwerken (z. B. EPRI, IEEE) qualifiziert und von der U.S.NRC zur Verwendung in Class 1E-Systemen, also Systemen mit der höchsten sicherheitstechnischen Bedeutung, zugelassen. Für Europa und Deutschland liegen der GRS keine Informationen bezüglich einer kerntechnischen Qualifizierung vor, das System ist gemäß IEC 61508 für funktionale Sicherheit für Sicherheitssysteme SIL 3 zertifiziert. Das Tricon-System wird weltweit in mehr als 10.000 Systemen verschiedener Industriezweige eingesetzt, darunter auch in kerntechnischen Einrichtungen (z. B. als Reaktorschutzsystem). Das Tricon-System kann laut Hersteller in diversen Anlagensystemen zum Einsatz kommen, wie z. B. dem Reaktorschutz, in Brand- und Gasschutzsystemen, in der Brennersteuerung oder in Systemen zur Turbomaschinensteuerung. Ein Ausschluss bestimmter Systeme, in denen kein Einsatz möglich wäre, erfolgt vom Hersteller nicht.

2.4 Teleperm XS Compact

Das Teleperm XS Compact-System wurde speziell zum Betreiben von Sicherheitsleittechnik in Kernkraftwerken von der Firma Framatome entwickelt, wobei die wichtigsten Funktionsprinzipien im Jahr 2017 fertig gestellt wurden. Das Teleperm XS Compact-System basiert auf der FPGA-Technologie (FPGA - Field Programmable Gate Array) und ist vollständig kompatibel mit dem ebenfalls von Framatome entwickelten, rechnerbasierten Leittechniksystem Teleperm XS.

Das Leittechniksystem Teleperm XS Compact bietet laut Hersteller die Möglichkeit, in sicherheitskritischen Anwendungen eingesetzt zu werden. Der Aufbau der sicherheitskritischen Logik erfolgt auf Basis von FPGAs, in welche mittels der Hardwarebeschreibungssprache VHDL (Very High Speed Integrated Circuit Hardware Description Language) beschriebene leittechnische Funktionen geladen werden. VHDL ist keine Programmiersprache, sondern eine textbasierte Beschreibung digitaler Systeme. Über

die Simulation der in VHDL beschriebenen Funktionen findet die Datenverarbeitung statt, indem Eingangsvariablen von der simulierten Hardware verarbeitet werden. Eine einmal in die FPGAs geladene Logik bleibt dabei während der gesamten Lebensdauer des Teleperm XS Compact-Systems veränderbar. Das Teleperm XS Compact-System ist mit einer permanent laufenden Selbstüberwachung sowie der Möglichkeit zur Durchführung von Selbsttests ausgestattet, die laut Hersteller sowohl ein fehlerhaftes Verhalten der Hardware als auch Fehler in den mittels VHDL beschriebenen leittechnischen Funktionen auf den FPGAs erkennen können.

Durch den modularen Aufbau des Teleperm XS Compact-Systems ist es möglich, sowohl kleine und dezentrale Leittechnikssysteme als auch größere Leittechnikssysteme aufzubauen, wobei Systeme mit bis zu vier Redundanzen realisiert werden können. Eine Automatisierungseinheit des Teleperm XS Compact-Systems besteht aus maximal 71 Ein-/Ausgabemodulen und kann damit maximal 142 Eingangssignale und 284 Ausgangssignale verarbeiten. Die Verbindung mehrerer Automatisierungseinheiten in einer Redundanz des Teleperm XS Compact-Systems ist möglich, wobei der GRS die maximale Anzahl an Automatisierungseinheiten je Redundanz nicht bekannt ist. Die Systemteile des Teleperm XS Compact-Systems, die sicherheitstechnisch wichtige Funktionen ausführen, sind laut Hersteller durch eine schaltbare Datendiode von den Systemteilen, die nicht sicherheitstechnisch wichtige Funktionen ausführen, getrennt. Der Aufbau des Teleperm XS Compact-Systems erfolgt in Baugruppenträgern in Standard 19“-Racks in Standard-Leittechniksschränken.

Bei der Qualifizierung des Teleperm XS Compact-Systems wurden laut Hersteller diverse Regelwerke, insbesondere auch IEC-Regelwerke spezifisch für leittechnische Systeme zum Einsatz in Kernkraftwerken, berücksichtigt. Die Komponenten zur Realisierung von sicherheitstechnisch wichtigen Funktionen sind hinsichtlich eines Einsatzes in der höchsten Sicherheitskategorie (Kategorie A nach DIN 61226) qualifiziert. Nach Informationen der GRS ist ein Einsatz des Teleperm XS Compact-Systems in diversen Kernkraftwerken in Osteuropa geplant, zudem ist ein Einsatz im EPR 2 und in SMR in Diskussion. Das Teleperm XS Compact-System kann laut Hersteller in diversen Anlagensystemen zum Einsatz kommen, wie z. B. dem Reaktorschutzsystem, dem Neutronenflussmesssystem, der Notstromdieselgeneratorsteuerung oder der Prioritätslogik. Ein Ausschluss bestimmter Systeme, in denen kein Einsatz möglich wäre, erfolgt vom Hersteller nicht.

3 IT-Angriffsvektoren unter Verwendung der schwieriger manipulierbaren Leittechniksysteme

Im Rahmen des Vorhabens wurden relevante IT-Angriffsvektoren auf rechnerbasierte oder programmierbare Leittechniksysteme ermittelt. Dabei wurden Erkenntnisse aus anderen Vorhaben genutzt, relevante IT-Sicherheitsvorfälle und Schwachstellen betrachtet sowie die MITRE ATT&CK Matrix für industrielle Steuerungssysteme ausgewertet. Anschließend wurde analysiert, inwieweit die ermittelten IT-Angriffsvektoren durch den Einsatz der Leittechniksysteme ProSafe-SLS, Hardline, Tricon und Teleperm XS Compact, die das Potenzial bieten, durch IT-Angriffe nicht oder zumindest schwieriger manipulierbar zu sein als typische rechnerbasierte Systeme, geschlossen oder eingeschränkt werden können. Die Ergebnisse dieser Analyse werden nachfolgend kurz zusammengefasst.

Hinsichtlich des ProSafe-SLS-Systems hat die Analyse ergeben, dass es beim Einsatz des ProSafe-SLS-Systems ohne das zur Kommunikation und Anbindung an andere Systeme genutzte ProSafe-COM-System zu einer signifikanten Reduzierung der Angriffsfläche für IT-Angriffe kommt. Dies ist damit zu begründen, dass das ProSafe-SLS-System aufgrund der Nutzung einer festverdrahteten Magnetkernlogik mit Ausnahme direkter physischer Manipulation durch IT-Angriffe nicht manipulierbar ist. Da das ProSafe-COM-System rechnerbasiert aufgebaut ist, sind für dieses nahezu alle ermittelten IT-Angriffsvektoren relevant. Aufgrund der Möglichkeit, dass über das ProSafe-COM-System nach manueller Freigabe durch einen Schlüsselschalter Zustandsänderungen im ProSafe-SLS-System herbeigeführt werden können, ist das ProSafe-SLS-System bei Nutzung des ProSafe-COM-Systems durch IT-Angriffe beeinflussbar. Allerdings kann keine direkte Manipulation der sicherheitsrelevanten Logik erfolgen. Über die Einführung und Berücksichtigung strenger Anforderungen bezüglich der Nutzung des Schlüsselschalters kann die Angriffsfläche des ProSafe-SLS-Systems für IT-Angriffe über das ProSafe-COM-System erheblich reduziert werden.

Hinsichtlich des Hardline-Systems hat die Analyse ergeben, dass es beim Einsatz des Hardline-Systems aufgrund dessen spezifischen Aufbaus zu einer signifikant reduzierten Angriffsfläche für IT-Angriffe kommt. Sämtliche sicherheitstechnisch relevanten Funktionen werden von festverdrahteten Komponenten ausgeführt, diese sind durch IT-Angriffe nicht direkt manipulierbar. Zudem verhindert die unidirektionale Kommunikation von den festverdrahteten Komponenten zur Ausführung der sicherheitstechnisch relevanten Funktionen hin zu den rechnerbasierten oder programmierbaren Komponenten

des Systems, die keine sicherheitstechnisch relevanten Funktionen ausführen, dass die Komponenten zur Ausführung der sicherheitstechnisch relevanten Funktionen über IT-Angriffe auf die rechnerbasierten oder programmierbaren Komponenten manipuliert werden können. Durch IT-Angriffe auf die rechnerbasierten oder programmierbaren Komponenten des Hardline-Systems, für welche der Großteil der ermittelten IT-Angriffsvektoren relevant ist, kann es möglicherweise zum Verlust von Anzeigen oder Informationsfehlanzeigen kommen, allerdings können die Sicherheitsfunktionen der festverdrahteten Komponenten nicht kompromittiert werden. Einzig durch direkte physische Manipulationen sind die Sicherheitsfunktionen des Hardline-Systems direkt manipulierbar.

Hinsichtlich des Tricon-Systems hat die Analyse ergeben, dass es beim Einsatz des Tricon-Systems zu keiner signifikant reduzierten Angriffsfläche für IT-Angriffe kommt. Das Tricon-System ist ein programmierbares, rechnerbasiertes Leittechniksystem, welches über die auf einem beliebigen PC installierbare Tristation-Software nach Freigabe über einen Schlüsselschalter programmierbar und konfigurierbar ist. Generell ist ein Großteil der ermittelten IT-Angriffsvektoren für das Tricon-System relevant. Grundlegender Unterschied des Tricon-Systems zu typischen rechnerbasierten oder programmierbaren Leittechniksystemen ist der dreifach redundante Aufbau des Systems mit drei parallel arbeitenden Hauptprozessoren. Dieser Aufbau mit einem internen 2 v 3-Voting führt zu einer erhöhten Ausfallsicherheit des Tricon-Systems und außerdem zur Möglichkeit, dass IT-Angriffe früher erkannt werden können und somit deren Auswirkungen möglicherweise früher unterbunden und abgeschwächt werden können. Zur Verringerung der Angriffsfläche des Tricon-Systems für IT-Angriffe ist darauf zu achten, dass der PC mit der installierten Tristation-Software nicht dauerhaft mit dem System verbunden ist und dass über die Einführung und Berücksichtigung strenger Anforderungen bezüglich der Nutzung des Schlüsselschalters dieser nur dann zur Freigabe einer Veränderung der Programmierung gesetzt wird, wenn dies erforderlich ist.

Hinsichtlich des Teleperm XS Compact-Systems hat die Analyse ergeben, dass es beim Einsatz des Teleperm XS Compact-Systems ohne Service-Einheit, die zur Konfiguration sowie für Service-, Wartungs- und Diagnosearbeiten notwendig ist, sowie ohne optionales Gatewaymodul, welches zur Anbindung an externe Systeme verwendet wird, zu einer signifikant reduzierten Angriffsfläche für IT-Angriffe kommt. Aufgrund des Aufbaus der sicherheitstechnisch wichtigen Logik mittels FPGAs, die nach ihrer Konfiguration ohne Anschluss einer Service-Einheit und entsprechende Hardware-Freigabe durch einen Schlüsselschalter nicht mehr ohne weiteres veränderbar sind, ist das

Teleperm XS Compact-System ohne Service-Einheit und ohne Gatewaymodul durch IT-Angriffe nahezu nicht manipulierbar. Durch direkte physische Manipulationen ist das Teleperm XS Compact-System direkt manipulierbar. Allerdings ist zu beachten, dass das Teleperm XS Compact-System beispielsweise zur Erstkonfiguration, Diagnose, Wartung oder Rekonfiguration unabdingbar mit einer Service-Einheit verbunden werden muss, die durch einen Industrie-PC oder Service-Laptop realisiert wird. Unter Nutzung der Service-Einheit oder des optionalen Gatewaymoduls sind viele der ermittelten IT-Angriffsvektoren für das Teleperm XS Compact-System relevant. Über IT-Angriffe auf die Service-Einheit lassen sich beispielsweise auch Rückwirkungen auf die FPGAs erzielen, in denen die sicherheitstechnisch wichtige Logik implementiert ist. Über die Einführung und Berücksichtigung strenger Anforderungen bezüglich der Nutzung der Service-Einheit sowie der Nutzung des Schlüsselschalters zur Freigabe einer Konfiguration der FPGAs lässt sich die Angriffsfläche des Teleperm XS Compact-Systems für IT-Angriffe deutlich reduzieren.

4 Zusammenfassung

Im Rahmen des Vorhabens wurden relevante IT-Angriffsvektoren auf rechnerbasierte oder programmierbare Leittechniksysteme ermittelt. Dabei wurden Erkenntnisse aus anderen Vorhaben genutzt, relevante IT-Sicherheitsvorfälle und Schwachstellen betrachtet sowie die MITRE ATT&CK Matrix für industrielle Steuerungssysteme ausgewertet.

Zudem wurden im Rahmen des Vorhabens diverse Leittechniksysteme untersucht, die aktuell erhältlich sind und das Potenzial bieten, durch IT-Angriffe nicht oder zumindest schwieriger manipulierbar zu sein als typische rechnerbasierte Systeme. Vertieft betrachtet wurden die Leittechniksysteme ProSafe-SLS (festverdrahtet, Magnetkernlogik), Hardline (festverdrahtet, diskrete Bauelemente), Tricon (rechnerbasiert, dreifach modulare, redundante Architektur) und Teleperm XS Compact (programmierbar, FPGA-basiert). Für diese Systeme wurde ein Vergleich mit dem rechnerbasierten System Teleperm XS durchgeführt, um Vor- und Nachteile der betrachteten Systeme aufzuzeigen. Die vergleichende Betrachtung der Leittechniksysteme hat ergeben, dass hinsichtlich vieler der betrachteten Aspekte keine deutlichen Vor- oder Nachteile für einzelne Systeme ausgemacht werden konnten.

Hinsichtlich der Einsatzmöglichkeiten zeigen die vertieft betrachteten Leittechniksysteme ProSafe-SLS, Hardline, Tricon und Teleperm XS Compact keine grundsätzlichen Unterschiede im Vergleich zu einem rechnerbasierten Leittechniksystem. Prinzipiell können mit jedem dieser Systeme beliebige leittechnische Funktionen aufgebaut werden. Allerdings ist zu erwähnen, dass die festverdrahteten Systeme ProSafe-SLS und Hardline eher nicht für den Aufbau großer Leittechniksysteme wie z. B. den Reaktorschutz eines Leistungsreaktors gedacht sind. Zumindest beim Hardline-System ist die Anzahl der möglichen Ein- und Ausgangssignale geringer ist als bei den anderen Systemen. Zudem wird die Anzahl der Leittechnikbaugruppen bei den festverdrahteten Systemen deutlich höher sein als bei programmierbaren oder rechnerbasierten Systemen, was zu einer Erhöhung der Komplexität des Aufbaus, der Installation, des Betriebs und der Instandhaltung dieser Systeme führen kann.

Die Analyse, inwieweit die identifizierten IT-Angriffsvektoren durch den Einsatz der vertieft betrachteten Systeme geschlossen oder eingeschränkt werden können hat gezeigt, dass es für das ProSafe-SLS-System ohne Nutzung des ProSafe-COM-Systems, für das Hardline-System sowie für das Teleperm XS Compact-System ohne Nutzung einer Service-Einheit oder eines optionalen Gatewaymoduls zu einer signifikanten Reduzierung

der Angriffsoberfläche für IT-Angriffe im Vergleich zum Betrieb eines rechnerbasierten Leittechniksystems kommt. Von den vertieft betrachteten Systemen bietet einzig das Tricon-System keine signifikant reduzierte Angriffsoberfläche für IT-Angriffe, allerdings ergibt sich beim Tricon-System aufgrund seines Aufbaus eine erhöhte Ausfallsicherheit und die Möglichkeit, IT-Angriffe früher zu erkennen und deren Auswirkungen möglicherweise früher zu unterbinden und abzuschwächen.

Somit konnte durch das Vorhaben gezeigt werden, dass Leittechniksysteme am Markt verfügbar sind, die im Vergleich zu typischen rechnerbasierten Leittechniksystemen eine deutlich verringerte Angriffsoberfläche für IT-Angriffe aufweisen und mit denen prinzipiell beliebige leittechnische Funktionen abgebildet werden können, wobei die betrachteten festverdrahteten Leittechniksysteme (ProSafe-SLS, Hardline) Einschränkungen hinsichtlich der möglichen Größe der mit ihnen zu realisierenden Leittechniksysteme aufweisen.

**Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH**

Schwertnergasse 1
50667 Köln

Telefon +49 221 2068-0

Telefax +49 221 2068-888

Boltzmannstraße 14

85748 Garching b. München

Telefon +49 89 32004-0

Telefax +49 89 32004-300

Kurfürstendamm 200

10719 Berlin

Telefon +49 30 88589-0

Telefax +49 30 88589-111

Theodor-Heuss-Straße 4

38122 Braunschweig

Telefon +49 531 8012-0

Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-911727-85-3