Anlagenbeobachtung mit der Data Capture Unit im Bahnumfeld

System monitoring with the Data Capture Unit in the rail environment

Martin Bakala

Im Zeitalter der Digitalisierung sind Kritische Infrastrukturen und deren Anlagen ein mögliches und interessantes Angriffsziel. Für eine effektive Erkennung und Abwehr von Cyber-Bedrohungen ergibt sich die Notwendigkeit, aus den IT/OT-Netzwerken gezielte Informationen für weiterverarbeitende Systeme zu extrahieren. Durch die nachgelagerte Analyse lassen sich Anomalien im Datenverkehr erkennen und Rückschlüsse auf mögliche Angriffe ziehen. Der Datenabgriff muss dabei rückwirkungsfrei sein und kann mit einer Data Capture Unit (DCU) der Firma Siemens realisiert werden. Dieser Beitrag zeigt eine Möglichkeit für die Umsetzung eines rückwirkungsfreien Datenabgriffs mittels einer DCU. Dabei wird kurz die Funktionalität der DCU beschrieben, um anschließend die in Zusammenarbeit mit der DB Netz AG durchgeführten Erprobungen zu beleuchten.

1 Motivation

Bereits in den 1990er Jahren hat die Vernetzung in Anlagen der Leit- und Sicherungstechnik (LST) mittels Standardkomponenten und auf Basis von TCP/IP stark zugenommen. Somit findet man heute schon großflächig vernetze Strukturen vor. Dadurch sind gemäß der Einschätzung von Sicherheitsbehörden interne und externe Bedrohungen hinsichtlich der IT-Sicherheit zu betrachten [1]. An dieser Stelle sei auf den Lagebericht des BSI (Bundesamt für Sicherheit in der Informationstechnik) verwiesen, in dem die Lage der IT-Sicherheit in Deutschland als angespannt bis kritisch bezeichnet wird [1]. Seitens des Gesetzgebers wurden auf Grundlage des EU-Rechts (NIS-Directive) mit dem IT-Sicherheitsgesetz Rahmenbedingungen geschaffen [2], damit bei Errichtung und Betrieb einer Kritischen Infrastruktur Mindeststandards für einen Risikomanagementprozess eingehalten werden. Eine wichtige Rolle im Rahmen des Risikomanagements kommt hierbei der Anlagenbeobachtung zu und ist ein wesentlicher Bestandteil der Angriffserkennung. Die technischen und organisatorischen Maßnahmen zur Identifizierung einer Bedrohung und die nachgelagerten Beseitigungsmaßnahmen sind die Hauptfunktionen eines Security Operations Center (SOC), das die Bestandteile Incident Management System (IMS) und Security Information and Event Management (SIEM) beinhalten kann. Typische Bausteine für die Erfassung von beispielsweise Log-Daten sind das Intrusion Detection System (IDS) und Intrusion Prevention System (IPS). Die zuletzt aufgezählten Bausteine unterscheiden sich zwar in ihrem Aufbau und in deren Funktionsumfang, aber sie haben eins gemeinsam: Sie müssen für eine Analyse mit Kommunikationsdaten aus den jeweiligen Netzwerken versorgt werden. Hierbei hat die Rückwirkungsfreiheit bei der Datenextraktion eine essenzielle Bedeutung. Dabei muss sichergestellt werden, dass ein unbefugter

In the age of digitalisation, critical infrastructures and systems are becoming a target of interest for potential attacks. In order to be able to effectively detect and defend against cyber threats, it must be possible to extract targeted information from IT/OT networks for processing in other systems. Any anomalies in the data traffic can be identified by a downstream analysis, thus allowing any potential attacks to be picked up. This data must be tapped without having an impact on the system, something that can be achieved using a Siemens data capture unit (DCU). This article describes one data tapping solution using a DCU that does not cause any interference in the network. It examines the functionality of the DCU before then shedding light on the tests that have been carried out in conjunction with DB Netz AG.

1 Motivation

Networking in signalling and control (S&C) systems using standard components and based on TCP/IP protocols was already on a steep growth curve as early as in the 1990s. This is precisely why there are so many large networked structures around today. The safety authorities take the view that these pose both internal and external threats to IT safety [1]. At this juncture, we should mention the BSI's (Federal German Office for Information Security) status report, which describes the status of IT security in Germany as "strained to critical" [1]. From a legislator's perspective, EU law (in the shape of the NIS – Network and Information Security Directive) was the starting point when drawing up the underlying principles of the German IT Security Act [2] in order to ensure that minimum standards for risk management processes are observed when creating and operating critical infrastructures. System monitoring has an important role to play in risk management and is a key component in identifying attacks. Technical and organisational measures aimed at identifying threats and further actions to avert any such threats are the main functions of a Security Operations Centre (SOC), which may include aspects such as incident management systems (IMS) and security information and event management (SIEM). Typical modules for recording items such as log data include intrusion detection systems (IDS) and intrusion prevention systems (IPS). Each of these modules may have a different structure and functional scope, but they do have one thing in common: they all need to be supplied with communication data from the relevant networks before they can perform any analyses. This is where their ability not to interfere with the data during the extraction process takes on a critical importance. It must be possible to guarantee that the unauthorised access to and intelligent corruption of data is not possible during data tapping, thus ruling out any impact on the

Zugriff sowie eine intelligente Verfälschung der Daten über den Abgriffsweg nicht möglich sein können und somit Rückwirkungen auf die sicherheitstechnischen Funktionen ausgeschlossen sind. Durch den aktuellen Stand des IT-Sicherheitsgesetzes sind Betreiber einer Kritischen Infrastruktur verpflichtet, ein System für die Angriffserkennung einzusetzen [3]. Als Termin bis zur verbindlichen Umsetzung ist der 1. Mai 2023 vorgegeben. Die Siemens Mobility GmbH unterstützt im Rahmen der Anlagenbeobachtung den Kunden dabei, eine Lösung für die Erfassung von spezifischen Anlageninformationen zu etablieren, was für Anlagen der Bauform Siemens sowohl im Bestand als auch für zukünftige Anlagen gilt. Speziell bei der Angriffserkennung liegt der Fokus auf der Protokollierung und Auswertung von Sicherheitsvorfällen sowie Cyber-Angriffen. In diesem Kontext wurden Pilotprojekte vereinbart, um die Möglichkeiten einer Datenausleitung unmittelbar über die DCU von Siemens bzw. mittelbar über das mit der DCU verknüpfte Siemens Diagnosesystem DB (Sidis DB) in Richtung des SOC der DB Netz AG zu erproben.

2 Funktionsprinzip

Die DCU realisiert einen passiven Netzwerkabgriff, indem eine bestehende Netzwerkverbindung aufgetrennt und mittels der Capture Access Ports (CAP A/CAP B) die Konnektivität wieder hergestellt wird. Die DCU leitet die gewonnenen Daten an ein weiterverarbeitendes System weiter. Das Ausleiten der Daten erfolgt auf Ethernet-Basis und ist protokollunabhängig. Die in Bild 1 dargestellte DCU kann ausschließlich für kupferbasierte Verbindungen (10 Mbit/s oder 100 Mbit/s) ein rückwirkungsfreies Ausleiten der Daten gewährleisten [4]. Anhand der vier CAP können direkt über die DCU Daten von vier physisch getrennten Netzwerken gleichzeitig ausgeleitet werden. Abhängig von dem gewählten Betriebsmodus kann die DCU in eine Datenleitung zwischengeschaltet werden (TAP-Mode) oder den Datenverkehr eines Endteilnehmers abgreifen (Gateway-Mode). Die ausgeleiteten Daten stehen dann mit Zeitstempel im PCAPNG-Format (Packet Capture Next Generation) zur Verfügung und können mit einem geeignetem Analyse-Tool verarbeitet werden.

3 Sicherheitsaspekte

Für die DCU existiert ein Nachweis der Rückwirkungsfreiheit gemäß EN 50129 und darauf aufbauend Genehmigungen bzw. Betreiberfreigaben. Der rückwirkungsfreie Übergang wird dadurch realisiert, dass an dem Eingang der PHY-Module die Sendeleitung auf Massepotenzial gelegt wird und auf der Ausgangsseite physisch keine Verbindung vorhanden ist. Es sind lediglich die Empfangsleitungen verbunden, sodass nur in Richtung des offenen Netzwerks gesendet werden kann (Bild 2).
Des Weiteren bietet die spezielle Architektur eine hohe Verfügbarkeit und Ausfallschutz der aktiven Netzwerkverbindung, sodass die DCU vor externen Einflüssen geschützt ist. Sollte es zu einem Spannungseinbruch über die Capture-Ports kommen, so sind zusätzlich zu der externen Seite des Übertragers Schmelzsicherungen integriert. Bei einem Isolationsverlust des Übertragers der CAP trennen somit die Schmelzsicherungen bei Überlast die Schnittstelle vom internen Potenzial. Durch einen Ausfall der DCU werden somit die angeschlossenen Teilnehmer nicht beeinflusst. Der angewendete Entwicklungsprozess der DCU basiert auf EN 5012X und bettet ebenfalls Aspekte der IT-Sicherheit mit ein. Der resultierende Prozess ist im Zusammenspiel mit der Bewertung von Kritikalität und Schutzbedarf relevanter Assets nach IEC

safety functions. As it stands, the IT Security Act requires operators of critical infrastructures to use a system to detect attacks [3]. This must be implemented by May 1, 2023 as a mandatory requirement. Siemens Mobility GmbH is keen to support its customers with their system monitoring efforts by providing a solution with the ability to detect specific system information. This covers both legacy and future Siemens-designed systems. The solution will focus on recording and assessing any security incidents and cyber-attacks with an emphasis on detecting attacks. Against this background, pilot projects have been agreed to explore the possibilities of data extraction to the DB Netz AG SOC directly using a Siemens DCU and / or indirectly via the Siemens diagnostic system linked to a DCU, DB (Sidis DB).

2 The operating principle

The DCU uses passive connections to tap into a network by isolating an existing network connection and restoring connectivity by means of capture access ports (CAP A/CAP B). The DCU then sends the tapped data to the processing system. The data is tapped via the Ethernet and it is not protocol-dependent. The DCU shown in fig. 1 is able to guarantee data tapping without any interference solely for copper-based connections (10 Mbit/s or 100 Mbit/s) [4]. Data from four physically separate networks can be tapped simultaneously by a DCU using all four CAPs. The DCU can either be connected to a data bus (TAP mode) or the data traffic from an end user can be tapped (Gateway mode), depending on the selected operating mode. The extracted data is then available in the PCAPNG (Packet Capture Next Generation) format and it can be processed using a suitable analysis tool.

3 The safety aspects

The DCU has been proven not to cause any interference as defined in EN 50129 and in any licenses or operator authorisations based on this standard. Interference-free transfer is possible, because the send line is connected to the ground at the input to the PHY module and there is no physical connection on the output side. Only

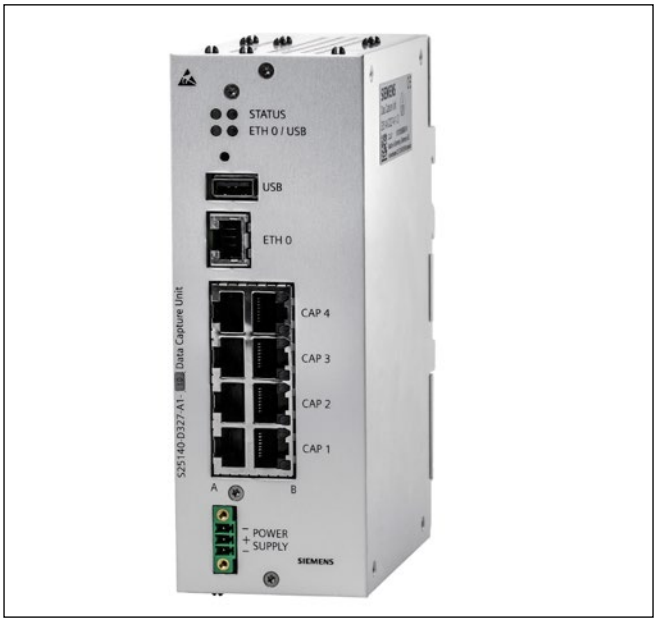

Bild 1: Frontseite der Data Capture Unit mit CAP 1-4
Fig. 1: The front of a data capture unit with CAP 1-4

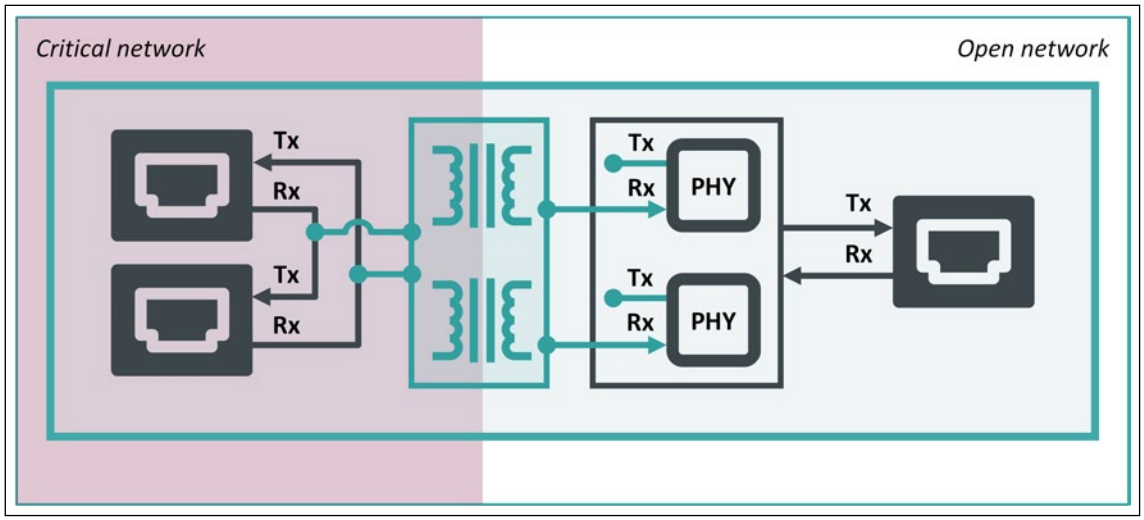

Bild 2: Darstellung des rückwirkungsfreien Übergangs an einem CAP
Fig. 2: A diagram showing the interference-free transfer at a CAP

62443-4-1 zertifiziert. Die derzeit aktuelle Version der DCU erfüllt die Normenanforderungen entsprechend 62443-4-2 mit dem Ziel der Erreichung eines SL-C 3, was durch ein TÜV Süd Zertifikat bestätigt und in Kürze verfügbar ist.

4 Pilotprojekte und Anwendungsfälle

Für die oben genannte Pilotierung wurden verschiedene typische Anlagenkonfigurationen ausgewählt, um optimale Abgriffspunkte für die Anlagenbeobachtung zu identifizieren. Im ersten Schritt wurden drei Erprobungsszenarien für die Pilotprojekte festgelegt. Diese Konfigurationen sind:

- Vernetzung Betriebszentrale (BZ) zu Unterzentrale (UZ) (DCU Steuerbezirk)
- Netzwerk in der UZ, speziell RBC / ESTW
- Netzwerk in Zugbildungsanlagen.

Da die DCU bereits in Kombination mit Sidis DB in UZ eingesetzt wird, konnten hier bestehende Abgriffspunkte für den zu untersuchenden Zweck verwendet werden. Die Weiterleitung der gewonnenen Daten wurde über die Diagnosekomponente Siemens Diagnose Data Storage (Sidis DS) selbst realisiert. Für die Durchführung der Pilotprojekte erfolgte im ersten Schritt eine Erprobungsfreigabe durch die DB Netz AG.

4.1 Pilotprojekt Hannover (Steuerbezirk)

Auf Wunsch des Betreibers wurde als Pilotanlage für den Anwendungsfall DCU im Steuerbezirk ein DCU-Aufbau im Steuerbezirk 11 in der BZ Hannover realisiert. Enge Abstimmungen für die genannte Anschaltung erfolgten zwischen

- SOC und LST in der BZ
- SOC, LST und PT2-Planer des Herstellers
- SOC und Fachgebietsbetreuung Leittechnik
- SOC und Fachteam Hersteller.

Neben den Erkenntnissen zur eigentlichen Datengewinnung wurden gemeinsam Grundlagen für die serienreife Anschaltung, Fachplanung, Abnahme und Instandhaltung erarbeitet. Diese gingen in den Erprobungsbericht und die bevorstehende Serienfreigabe ein. Der Abschluss der Erprobung erfolgte im Januar 2022; die Anlage wurde in den Regelbetrieb übernommen.

4.2 Pilotprojekt Erfurt (RBC)

Eine hohe Priorität sieht die DB Netz AG bei der Beobachtung von elektronischen Stellwerken (ESTW) und Radio Block Centern

the receiving lines are connected, which means that transmission is only possible in one direction: i.e. toward the open network (fig. 2). The special architecture also ensures high levels of availability and failure protection for the active network connection, which means that the DCU is protected against any external events. Fuses are also built into the external side of the transmitter to protect against a voltage dip via the capture ports. In other words, if the CAP transmitter loses its insulation, the fuses will isolate the interface from any internal potential in the event of overloading. This means that the connected users would not be affected, if the DCU were to fail. The DCU development process is based on EN 5012X and also incorporates aspects of IT security. The resulting process has been certified according to IEC 62443-4-1 based on an assessment of the criticality and security-related assets. The latest version of the DCU meets the standard requirements set out in 62443-4-2 with the aim of achieving SL-C 3, as confirmed by TÜV Süd certification, which will shortly be available.

4 Pilot projects and applications

A range of typical system configurations were chosen for the aforementioned pilot projects with a view to identifying optimum tapping points for system monitoring purposes. Three test scenarios were defined for the pilot projects in the initial phase. The configurations were as follows:

- networking between the operations management centre and the sub-centre (SC) (DCU control area)
- the network in the SC, specifically RBC / electronic interlockings
- the network in the train formation yards.

As the DCU is already being used alongside Siemens Diagnostics DB (Sidis DB) in SC, the existing tapping points could also be used for analysis purposes in these cases. The tapped data was transmitted using Siemens Diagnostics Data Storage (Sidis DS) components. A test release was granted by DB Netz AG in the initial phase in order to enable the pilot projects to go ahead.

4.1 The Hanover pilot project (control area)

A DCU set-up was installed in control area 11 in the Hanover operations centre as a pilot system for the DCU application at the operator's request. The interfaces between the following areas have been carefully defined:

- the SOC and S&C in the operations centre
- the SOC, S&C and the manufacturer's PT2 designers

(RBC). ESTW haben bereits eine hohe Verbreitung und sind im Fern- und Ballungsnetz ein essenzieller Bestandteil. RBC spielen im Zielbild der DB Netz AG eine entscheidende Rolle. Daher war es naheliegend, für die Erprobung eine Zielanlage auszuwählen, die dem Zielbild schon sehr nahekommt (ESTW mit RBC und Anlage ausgeprägt als Level 2 ohne Signale (L2oS)). Die Datenausleitung erfolgt in diesem Projekt für die RBC Erfurt Knoten und Erfurt Neubaustrecke (NBS). Weitere Abgriffspunkte befinden sich in der UZ Erfurt NBS, speziell Schnittstellen innerhalb der UZ-Leittechnik sowie zwischen Leittechnik und Stellwerk. Wichtige Bausteine für die Instandhaltung in den genannten Anlagen sind Sidis RBC (Diagnoseeinrichtung für die RBC-Zentralen) und Sidis IL (Diagnoseeinrichtung für ESTW). Grundlage der Datenaufbereitung für die Diagnose ist der Abgriff von internen und Umsystem-Schnittstellen der betroffenen Techniken. Die Speicherung der Daten der bereits verbauten DCU erfolgt auf Datenspeicher der Sidis DS (lokale Festplatte oder NAS). Sidis DS sorgt auch für die Weiterleitung der aufgezeichneten Rohdaten im PCAPNG-Format an die Schnittstellenpartner des SOC (Bild 3).
Die IDS überwachen den Netzwerkverkehr und können in Echtzeit alarmieren. Die Alarme und Log-Daten werden in SIEM gespeichert und im SOC kontinuierlich Analysen unterzogen. Da es sich bei den überwachten Netzwerken um hochgradig stabile Kommunikation handelt, können Angriffe mit hoher Präzision erkannt werden – wobei ein solcher „Angriff" auch ein bislang unbekannter Wartungs-Laptop sein kann. Die Auswahl weiterer ggf. erforderlicher Abgriffspunkte sowie der Austausch zur Analyse der aufgezeichneten Daten ist ein wichtiger Aspekt der immer noch laufenden Erprobungstätigkeit. Ziel ist der Abschluss bis Mitte 2023.

4.3 Pilotprojekt Zugbildungsanlage

Relevante Rangierbahnhöfe und Bereitstellungsanlagen zählen auch zur Kritischen Infrastruktur. Für das Umfeld Zugbildungsanlagen wurden bereits Laborerprobungen durchgeführt. Die dafür erforderlichen Schritte erfolgten in enger Kooperation zwischen Betreiber und Hersteller. Dabei bestand ein wichtiger Teil der Kooperation in der Aufbereitung der relevanten Datenflüsse

- the SOC and the control technology technical team
- the SOC and the manufacturer's technical team

In addition to establishing the details of the actual data extraction process, the connection, planning, acceptance and maintenance for production maturity were also defined. This information was then recorded in the test report and the forthcoming production release. The test phase was completed in January 2022; the system was then transferred to standard operations.

4.2 The Erfurt pilot project (RBC)

DB Netz AG has assigned high priority to monitoring electronic interlockings and radio block centres (RBC). Electronic interlockings are in widespread use and are key components in long-distance and urban networks. RBCs have an important role to play in DB Netz AG's target vision. This explains why it was an obvious choice to trial a target system that closely resembles the target vision (an electronic interlocking with an RBC and a system described as Level 2 without signals (L2wS)). In this project, data was tapped for the RBC Erfurt nodes and Erfurt high-speed line (HSL). Additional tapping points are located in the Erfurt HSL sub-centre, with specific interfaces within the sub-centre control system and between the control system and the interlocking. Sidis RBC (a diagnostics device for RBC units) and Sidis IL (a diagnostics device for electronic interlockings) are important modules for carrying out maintenance in the specified systems. The preparation of the data for diagnostic purposes is based on tapping the internal and peripheral system interfaces for the relevant technologies. The data from the legacy installed DCU is stored in data memories in the Sidis DS system (local hard drive or NAS). Sidis DS is also responsible for transmitting the recorded raw data to the SOC interface partners in the PCAPNG format (fig. 3).
The IDS monitor the network traffic and can raise the alarm in real time. Alarms and log data are saved in the SIEM and analyses are carried out continuously in the SOC. As the monitored networks experience high-level stable communication, attacks can be detected with a high degree of accuracy. A previously unknown maintenance laptop may even constitute an "attack" of this nature. Select-

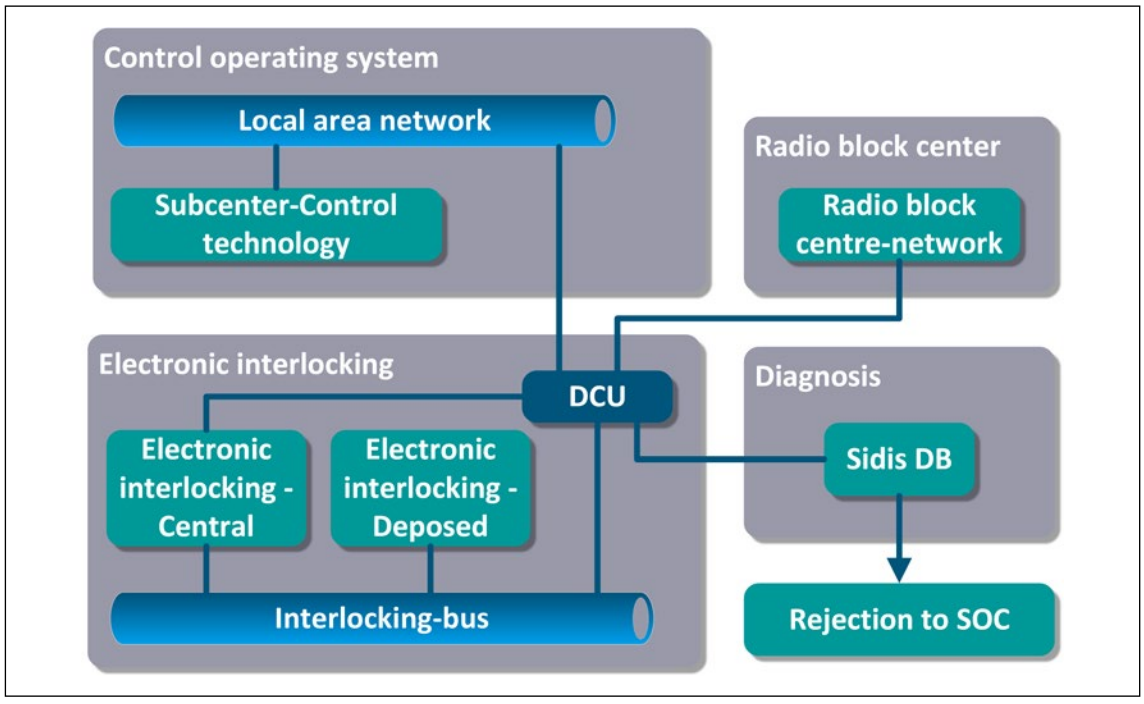

Bild 3: Datenausleitung über Sidis DS mittels DCU im Pilotprojekt Erfurt
Fig. 3: Data extraction via Sidis DS using a DCU in the Erfurt pilot project

sowie Austausch erforderlicher Protokollinformationen und -eigenschaften.

5 Zusammenfassung und Ausblick

Dank einer intensiven, vertrauensvollen und offenen Zusammenarbeit konnten bereits wichtige Schritte auf dem Weg zu einer umfassenden Anlagenbeobachtung genommen werden. Im Zuge der Diskussionen mit verschiedenen beteiligten Gewerken und Verantwortlichen ergaben sich wichtige Erkenntnisse für einen zukünftigen Roll-out, d. h. es wurden Grundlagen für die zukünftige Planung, Abwicklung, Abnahme und den Betrieb geschaffen. Somit konnte ein wesentlicher Meilenstein bzgl. der gesetzlichen Forderung des Einsatzes von Systemen zur Angriffserkennung im Integritätsbereich I für ESTW und RBC-Anlagen der Bauform Siemens erreicht werden. Für den Betreiber besteht damit die Möglichkeit einer kontinuierlichen Lagebewertung und -meldung derselben an die Aufsichtsbehörde. ■

ing additional tapping points that may be necessary and changing them to analyse the recorded data are key aspects of the ongoing testing activities. The aim is to complete the tests by mid-2023.

4.3 The train formation yard pilot project

Relevant marshalling yards and preparation systems are also regarded as critical infrastructure. Laboratory tests have already been carried out for train formation yard system environments. The necessary steps were carried out in close collaboration between the operator and the manufacturer. A large part of this cooperation has been concerned with preparing the relevant data flows and exchanging the required protocol information and properties.

5 Summary and outlook

Thanks to the intensive, open and trust-based collaboration, it has already been possible to make significant progress toward obtaining a comprehensive system monitoring service. Discussions with various trades and managers in the relevant fields have also led to important findings with regard to future rollouts, i.e. the foundations for future planning, processing, acceptance, and operation have been laid. This was therefore an important milestone toward meeting the statutory requirement to use systems to detect attacks in integrity area I for Siemens-designed electronic interlockings and RBC systems. This will enable operators to continuously assess the situation and report to the supervisory authorities accordingly. ■

LITERATUR | LITERATURE

[1] „Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)", [Online] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html. [Zugriff am 13.07.2022 um 9:37]
[2] „Gesetz zur Umsetzung der NIS-Richtlinie", [Online] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-Richtlinie/nis-richtlinie_node.html. [Zugriff am 15.08.2022 um 11:15]
[3] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Die Lage der IT-Sicherheit in Deutschland 2021", Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2021
[4] „Siemens Mobility, Sichere Konnektivität", [Online] https://www.mobility.siemens.com/global/de/portfolio/schiene/bahnautomatisierung/sichere-konnektivitaet.html. [Zugriff am 17.08.2022 um 14:10]

AUTOR | AUTHOR

Martin Bakala
Netzwerkingenieur / *Network Engineer*
Siemens Mobility GmbH
Anschrift / *Address*: Ackerstraße 22, D-38126 Braunschweig
E-Mail: martin.bakala@siemens.com