Albert-Ludwigs-Universität Freiburg
Technische Fakultät
Studiengang Embedded Systems Engineering

Proposal für eine Bachelorarbeit zum Thema:

Entwicklung eines automatisierten Datensammlers mit einer geeigneten MQTT-Lösung zur sicheren Datenübertragung für elektrische Stellantriebe

Betreuer:

Professor Marco Zimmerling, Albert-Ludwigs-Universität Freiburg
Dipl.-Ing. Dirk Kraemer, AUMA Riester GmbH & Co. KG
Ralf Geiger, AUMA Riester GmbH & Co. KG

Eingereicht von:

Dominic Rueb
E-Mail: domi.rueb@gmx.net
Matrikelnummer: 4742303

Datum: 23.05.2022

1 Einleitung

Die Automatisierung spielt in der heutigen Industrie eine große Rolle, weil dadurch Arbeitsschritte erleichtert werden können und eine höhere Effizienz und Zuverlässigkeit erreicht wird. Ein großer Teil der Industrieautomation beschäftigt sich mit der automatisierten Datensammlung, um z.B. Maschinen und Prozesse zu überwachen und zu kontrollieren. So können beispielsweise Betriebszustände von Maschinen über eine Internetverbindung von verschiedensten Standorten aus kontrolliert werden. Dies ermöglicht unter anderem eine erleichterte Kontrolle und eine schnelle Fehlerdetektion.

Oftmals sind die bereits existierenden Maschinen in der Industrie noch nicht mit einer direkten Internetverbindung ausgestattet, weshalb hierzu ein Zwischenmedium benötigt wird. Dieses empfängt und sammelt die Daten der Maschinen und stellt diese mithilfe einer gesicherten Internetverbindung in einer Cloud zur Verfügung. Die Vernetzung der industriellen Maschinen mithilfe des Internets wird auch als Industrial-Internet-Of-Things (IIoT)[2] bezeichnet. Für diese Machine-to-Machine Kommunikation wird aufgrund seiner Flexibilität, Schlankheit und Effizienz sehr häufig das Nachrichtenprotokoll MQTT verwendet. Neben der Effizienz ist jedoch oftmals die Sicherheit und die Verlässlichkeit der Datenübermittlung eine weitere sehr wichtige Anforderung, die ein Nachrichtenprotokoll insbesondere in der Indutrie erfüllen muss.

2 Zielsetzung

2.1 Problemdefinition

Mit dem Fortschreiten der Digitalisierung der heutigen Industrie in Richtung Industrie 4.0 oder Smart Manufactoring nimmt die Automatisierung und die Datenübermittlung eine immer wichtigere Rolle ein. Aktuell müssen die Betriebs- und Prozessdaten der AUMA Stellantriebe durch manuelle Arbeitsschritte eingesammelt werden. Dieses Problem bzw. diese Arbeitsschritte sollen im Hinblick auf die Industrie 4.0 automatisiert werden, wobei die Datenübermittlung eine wichtige Rolle spielt.

Essentiell bei der Datenübermittlung ist das verwendete Nachrichtenprotokoll. Das sehr häufig verwendete Netzwerkprotokoll MQTT basiert auf einer Publish-Subscribe-Architektur und ist für seine Flexbilität und seinen sehr einfachen und schlanken

Aufbau zur Datenübermittlung bekannt. Aufgrund des Publish-Subscribe-Prinzips mit einem Message-Broker werden die Kommunikationspartner voneinander entkoppelt. Dies erweitert zwar einerseits die Flexibilität, aber gleichzeitig lässt sich die Frage stellen, wie sicher und wie verlässlich diese Datenübermittlung dann noch ist. Wie kann beispielsweise sichergestellt werden, dass nicht ein unerwünschtes Gerät Daten an den Broker veröffentlicht und somit das Ergebnis manipuliert? Oder wie lässt sich sicherstellen, dass die Datenübermittlung auch bei vielen Sendern verlässlich funktioniert und alle Datenpackete garantiert ankommen?

2.2 Die Ziele

In dieser Bachelorarbeit soll ein automatisierter Datensammler entwickelt- und auf dessen Grundlage eine geeignete MQTT-Lösung insbesondere bezüglich dessen Cyber-Security zur sicheren Datenübertragung analysiert- und realisiert werden. Der automatisierte Datensammler soll anhand der Produktanforderungen der AUMA entwickelt werden.

Dafür sollen verwandte Forschungsfragen und -artikel zu den Themen 'Kommunikation in der Industrieautomation', 'MQTT' und 'Cyber-Security' analysiert werden, um die Forschungs-Frage zu beantworten, inwieweit das Nachrichtenprotokoll MQTT unter Berücksichtigung der industriellen Cyber-Security Anforderungen in der heutigen Industrie zur Datenübermittlung geeignet ist.

Die analysierte MQTT-Lösung soll dabei folgende Anforderungen erfüllen:

- Sie soll eine zuverlässige Datenübertragung sicherstellen, sodass alle Datenpackete auch von sehr vielen Publishern ankommen.
- Die Datenübertragung soll sicher sein gemäß der industriellen Cyber-Security Standards, wie beispielsweise die Normenreihe für Cybersecurity in der Industrieautomatisierung IEC 62443 diese festlegt.

Das Ziel dieser Bachelorarbeit ist es, mithilfe geeigneter Untersuchungen eine für die Industrie geeignete Lösung für die Datenübermittlung mittels MQTT zu finden und diese auf dem entwickelten automatisierten Datensammler anzuwenden.

3 Ausgangslage und Forschungsstand

3.1 Die AUMA Riester GmbH

Die AUMA Riester GmbH & Co. KG ist ein industrielles Großunternehmen und ein Hersteller von elektrischen Stellantrieben und Armaturengetrieben. Momentan können die Betriebs- und Prozessdaten der elektrischen Stellantriebe über eine manuell aufgebaute Bluetooth-Verbindung mithilfe eines Endgerätes von der AUMA Steuerung abgerufen und gespeichert werden. In einem zusätzlichen manuellen Schritt können diese Daten an die AUMA Cloud übermittelt werden.

Diese manuellen Schritte sollen durch die Entwicklung eines automatisierten Datensammlers ersetzt werden, sodass die Daten in der AUMA Cloud verfügbar sind. Jedoch ist für diese Übermittlung in die Cloud eine Absicherung der Kommunikation notwendig. Insbesondere im Hinblick auf den industriellen Einsatz gibt es Herausforderungen und Chancen in der Absicherung des Industrial Internet of Things [6]. Weil in der Industrie die Sicherheitsanforderungen oftmals andere sind, als im Verbraucher IoT, wird ein geeignetes Netzwerkprotokoll benötigt, das für die Datenübermittlung genügend Sicherheit bietet.

3.2 Das Nachrichtenprotokoll MQTT

Message-Queuing-Telemetry-Transport (MQTT) ist ein Nachrichtenprotokoll für Netzwerke mit geringer Bandbreite und für IoT-Geräte mit extrem hoher Latenzzeit, weshalb es ideal ist für die Machine-to-Machine-Kommunikation (M2M) [3]. MQTT ist ein sehr einfach aufgebautes und leichtgewichtiges Protokoll und wurde für Geräte mit geringer Rechenleistung entwickelt. Dies führt jedoch im Gegenzug zu Sicherheitsproblemen. Grundsätzlich kommunizieren im Standard-MQTT-Protkoll Publisher und Subscriber mit dem Broker ohne Verschlüsselung, ohne Authentifizierung und auch ohne Autorisierung [1]. Somit könnten Angreifer die Daten nicht nur mitlesen, sondern sie könnten die Daten auch manipulieren. Jedoch hängt die Sicherheit von MQTT fast ausschließlich von dem Broker bzw. von der Implementierung ab. Deshalb kann die Sicherheit durch Konfiguration des Brokers bzw. durch Erweiterung der Implementierung erheblich optimiert werden.

Mit Erweiterungen von MQTT wie beispielsweise 'Secure MQTT' [7] oder dem

Authorisierungs-Mechanismus für MQTT [5] gibt es bereits Forschungsartikel bzw. Lösungen, die die Sicherheit von MQTT optimieren. Z.B. kann die Kommunikation mit SSL/TLS verschlüsselt werden und die Authentifizierung von Publishern und Subscribern mit Benutzernamen und Passwort umgesetzt werden. Auch zur Anwendbarkeit der Normenreihe für Cybersecurity IEC 62443 in der Industrie 4.0 bzw. IIoT gibt es bereits Forschungsartikel wie beispielsweise [4], welche untersucht werden sollen.

4 Geplante Untersuchungen

Nach der Realisierung einer geeigneten MQTT-Lösung zur sicheren Datenübermittlung unter Berücksichtigung der Cyber-Security Standards sollen folgende Untersuchungen durchgeführt werden, um die MQTT-Lösung entsprechend zu analysieren und zu erproben.

4.1 Zuverlässigkeit

Zunächst soll die Zuverlässigkeit der MQTT-Lösung untersucht werden, indem entsprechende Versuche durchgeführt werden. Hierfür soll die Datenübermittlung mittels MQTT mit sehr vielen, parallel-verbundenen Stellantrieben bzw. Publishern getestet werden. Außerdem soll untersucht werden, ob alle Datenpackete zuverlässig in die Cloud gelangen, wenn sehr viele Daten gesendet werden bzw. die Datenrate sehr hoch ist. Weiterhin sollen Versuche mit Störquellen wie beispielsweise Maschinen oder Anlagen durchgeführt werden, um die Zuverlässigkeit der Datenübermittlung trotz Störquellen zu analysieren. Bezüglich der Zuverlässigkeit soll zuletzt auch die Reichweite der Verbindung und die Reaktion bei Verbindungsabbruch untersucht werden.

4.2 Sicherheit

Neben der Zuverlässigkeit der Datenübermittlung mithilfe der MQTT-Lösung soll auch dessen Sicherheit untersucht werden. Hierfür sollen verschiedene Angriffe simuliert werden. Zuerst soll untersucht werden, ob ein unerwünschtes Gerät 'mithören' kann bzw. die Daten von einem Angreifer ausgelesen werden können. Insbesondere soll getestet werden, ob ein unerwünschter Subscriber anonym Daten empfangen kann. Weiterhin soll untersucht werden, ob ein Angreifer die Daten in der Cloud

manipulieren kann. Dafür sollen falsche Daten von einem unerwünschten Gerät an den Broker publiziert werden, um zu testen ob dies anonym möglich ist.

5 Zeitplan und Meilensteine

April - 30. Juni 2022 *Praktische Entwicklung des Datensammlers*

im Rahmen der Hiwi Tätigkeit bei der AUMA inklusive Evaluation des geeigneten Mikrocontrollers und Programmierung anhand der AUMA Produktanforderungen.

01. Juli - 13. Juli *Literaturstudium*

Einarbeitung in die Thematik und in diverse Forschungsartikel und -fragen zu den Themen MQTT und Industrial-Cyber-Securiy.

14. Juli - 02. August *Evaluierung und Entwicklung*

einer geeigneten MQTT-Lösung mithilfe der zuvor untersuchten Forschungsartikel.

03. August - 17. August *Analyse und praktische Untersuchungen*

der MQTT-Lösung bezüglich der Zuverlässigkeit und der Sicherheit der Datenübertragung.

11. + 12. August *Festlegung der Gliederung*

der schriftlichen Bachelor-Thesis.

15. August - 28. September *Schriftliches Verfassen der Bachelor-Thesis*

29. September *Druck der Bachelor-Thesis*

30. September *Abgabe der Bachelor-Thesis*

Literaturverzeichnis

[1] Santiago Hernández Ramos, M Teresa Villalba und Raquel Lacuesta. "Mqtt security: A novel fuzzing approach". In: *Wireless Communications and Mobile Computing* 2018 (2018).

[2] Avish Karmakar u. a. "Industrial internet of things: a review". In: *2019 international conference on opto-electronics and applied optics (optronix)*. IEEE. 2019, S. 1–6.

[3] Elektronik Kompendium. *MQTT - Message Queue Telemetry Transport*. URL: https://www.elektronik-kompendium.de/sites/net/2204051.htm. 19.05.2022.

[4] Björn Leander, Aida Čaušević und Hans Hansson. "Applicability of the IEC 62443 standard in Industry 4.0/IIoT". In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. 2019, S. 1–8.

[5] Aimaschana Niruntasukrat u. a. "Authorization mechanism for MQTT-based Internet of Things". In: *2016 IEEE International Conference on Communications Workshops (ICC)*. 2016, S. 290–295. DOI: 10.1109/ICCW.2016.7503802.

[6] Martin Serror u. a. "Challenges and opportunities in securing the industrial internet of things". In: *IEEE Transactions on Industrial Informatics* 17.5 (2020), S. 2985–2996.

[7] Meena Singh u. a. "Secure MQTT for Internet of Things (IoT)". In: *2015 Fifth International Conference on Communication Systems and Network Technologies*. 2015, S. 746–751. DOI: 10.1109/CSNT.2015.16.