CRYPTOGRAPHIC AUTHENTICATION-BASED MECHANISM FOR SECURING SECS/GEM COMMUNICATIONS FOR INDUSTRY 4.0 MANUFACTURING

SHAMS UL ARFEEN LAGHARI

UNIVERSITI SAINS MALAYSIA

2023

CRYPTOGRAPHIC AUTHENTICATION-BASED MECHANISM FOR SECURING SECS/GEM COMMUNICATIONS FOR INDUSTRY 4.0 MANUFACTURING

by

SHAMS UL ARFEEN LAGHARI

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

April 2023

ACKNOWLEDGEMENT

I would like to express my profound gratitude to everyone who helped in any way to the completion of this thesis. To begin, I would like to immensely thank our "Allah," who immersed me with His boon and blessings and bestowed me with the tenacity of purpose, good health during this Covid pandemic, sound mind, and conducive facilities to conduct and document this research work.

I would like to express my heartfelt appreciation to my Research Supervisor, Dr. Selvakumar Manickam; my Co-Supervisor, Dr. Shankar Karuppayah; and Field Supervisor, Dr. Shafiq ur Rahman. This study would have been implausible without their vehement cooperation, commitment, unconditional support, and guidance over the last three years.

I would like to give innumerable thanks to the lecturers and peer researchers at the National Advanced IPv6 Center, the librarians, and other Center administrative staff for their generous support during my PhD journey, without which I would not have been able to complete this research.

I needed more than academic help to complete my thesis. Indeed, I owe a debt of gratitude to a large number of individuals for listening to and, at times, tolerating me over the last three years. I am speechless in my thanks and admiration for their friendship and loyalty. I must appreciate Dr. Ayman Al-Ani, Dr. Ahmed Al-Ani, and Ashish Jaisan for their steadfast personal and professional support during my stay at the USM University.

Most significantly, none of this would have been possible without the support of my parents, brothers, sisters, and extended relatives. I really do not have the words to express my gratitude for your assistance in getting me to where I am today, Mrs.

Sadaf Shams - my life partner. I intend to express my deepest love to my sons, Muhammad Suhaib and Muhammad Zuhaib, for being brave and having the fortitude to take care of everyday affairs back at home in my absence. I love you all.

Finally, I would like to convey my indebtedness to the unknown soldier, who supported me in every thick and thin. May the Almighty Allah abundantly bless you all. I dedicate my efforts to each and every one of you.

Shams Ul Arfeen Laghari, *Penang Malaysia, 2023*.

TABLE OF CONTENTS

ACKNOWLEDGEMENT ..... **ii**

TABLE OF CONTENTS ..... **iv**

LIST OF TABLES ..... **x**

LIST OF FIGURES ..... **xii**

LIST OF ABBREVIATIONS ..... **xv**

LIST OF APPENDICES ..... **xvii**

ABSTRAK ..... **xviii**

ABSTRACT ..... **xx**

CHAPTER 1 INTRODUCTION **1**

1.1 Overview 1

1.2 Background 3

1.2.1 Industrial Networks Communication Protocols 4

1.2.2 Cybersecurity Threats 5

1.3 Research Problem 8

1.4 Research Objectives 10

1.5 Research Scope and Limitations 11

1.6 Research Contribution 12

1.7 Research Steps 13

1.8 Thesis Organization 16

CHAPTER 2 LITERATURE REVIEW **17**

2.1 Background 17

2.2 SEMI Equipment Communication Standards 20

2.2.1 SEMI Equipment Communication Standard: Part 1 (SECS-I) 22

2.2.2 SEMI Equipment Communication Standard: Part 2 (SECS-II) 23

2.2.3 High-Speed SECS Message Services (HSMS) 27

2.2.3(a) HSMS Message Types 29
2.2.3(b) HSMS State Model 30
2.2.3(c) HSMS Communication Processes 31
2.2.1(c)(i) Connection Establishment Process 31
2.2.1(c)(ii) Connection Management Process 32
2.2.1(c)(iii) Connection Termination (Tear-Down) Process 33
2.2.4 Generic Equipment Model (GEM) 33
2.2.5 Message Encoding and Packaging 34
2.2.6 SECS/GEM Alarms and Data Collections 36
2.3 Cyber-attacks on SECS/GEM 37
2.3.1 Lack of Authentication Mechanism 38
2.3.2 Denial of Service (DoS) Attack Issues 38
2.3.3 Replay Attack Issues 41
2.3.4 False Data Injection Attack Issue (FDIA) 42
2.4 Rule-Based System 43
2.5 Cryptographic Hash Functions 44
2.6 Industrial M2M Communication Protocols 51
2.6.1 Message Queuing Telemetry Transport (MQTT) 51
2.6.2 Open Platform Communications – Unified Architecture (OPC UA) 52
2.6.3 Constrained Application Protocol (CoAP) 53
2.6.4 Data Distribution Service (DDS) 53
2.6.5 SECS/GEM 54
2.7 Related Work 56
2.7.1 Authentication Mechanisms for M2M Communications 56
2.7.1(a) Digital Signature-Based Systems 56

2.7.1(b) Authentication Mechanisms – Issues and Limitations 60

2.7.2 SECS/GEM Security Mechanisms 61

2.7.2(a) SECS/GEMsec Mechanism 62

2.7.2(b) Secured SECS/GEM 67

2.8 Discussion 70

2.8.1 SECS/GEMsec – Issues and Limitations 70

2.8.2 Secured SECS/GEM – Issues and Limitations 72

2.8.3 Critical Review 74

2.9 Requirements for New Security Mechanism 75

2.9.1 Resilience Against Cyber-Attacks 76

2.9.2 Lightweight 76

2.9.3 Multi-Featured Solution 76

2.9.4 Customization and Compatibility 77

2.10 Chapter Summary 77

CHAPTER 3 RESEARCH METHODOLOGY 79

3.1 Methodology of the Proposed SECS/GEM Security Mechanism (SGSM) ... 80

3.1.1 Assumptions 80

3.1.2 Threat Model 81

3.1.3 Design Goal 82

3.2 Proposed SECS/GEM Security Mechanism (SGSM) 84

3.2.1 ACB Generation and Initialization (Stage 1) 87

3.2.1(a) Authentication Code Block (ACB) – The Message Structure 88

3.2.1(b) The combined functionality of Mode, Algorithm, and Secret-key ID 91

3.2.1(c) Replay Prevention Mode (RPM) 94

3.2.2 Authentication and Message Integrity (Stage 2) 95

3.2.2(a) Placement of ACB in HSMS Message 96

3.2.2(b) Hashing-Based Mechanism 98

3.2.3 Prevention of Cyber-Attacks (Stage 3) 101

3.3 The Workflow of the Proposed SGSM Mechanism 105

3.4 Testbed Design and Performance Evaluation 110

3.4.1 Evaluation Matrices 110

3.4.2 Processing Time 110

3.4.2(a) Processing Time for Generating Request Message at the Sender 111

3.4.2(b) Processing Time for Verifying Response Message at the Receiver 112

3.4.3 ACB Control Message Overhead 112

3.4.4 Cyber-Attack Prevention Success Rate 113

3.5 Chapter Summary 114

CHAPTER 4 DESIGN AND IMPLEMENTATION OF THE PROPOSED SECS/GEM SECURITY MECHANISM (SGSM) 115

4.1 Prerequisites for SGSM Implementation 115

4.1.1 Programming Language 116

4.1.2 Packet Capturing 117

4.1.2(a) Scapy – A Packet Manipulation Tool 117

4.1.2(b) Wireshark – A Packet Analyzer 119

4.1.3 Testbed Environment Setup 120

4.2 Packet Crafting using Scapy 122

4.3 SGSM Implementation Details 126

4.3.1 ACB Generation and Initialization (at the Sender) 127

4.3.2 Timestamp Generation 128

4.3.3 Computing Hash Using HMAC Algorithms 129

4.4 Processing SGSM Messages (at the Receiver) 130

4.4.1 ACB Verification 131

4.4.2 Hash Verification at the Receiver 133

4.4.3 Timestamp Verification at the Receiver 134

4.5 SGSM implementation Scenarios 136

4.5.1 Normal Scenario 136

4.5.2 Attack Scenario 139

4.6 Chapter Summary 139

CHAPTER 5 RESULTS AND DISCUSSION 141

5.1 Normal Scenario Experiment 142

5.1.1 Processing Time 143

5.1.1(a) Calculating the Processing Time of SGSM with Different HMAC Algorithms 144

5.1.1(a)(i) Sending Message (at the Host) 145

5.1.1(a)(ii) Receive Message (at the Equipment) 148

5.1.1(b) Processing Time of SGSM vs. SECS/GEMsec vs. Secured SECS/GEM 151

5.1.1(b)(i) Sending Messages 152

5.1.1(b)(ii) Receiving Messages 154

5.1.1(c) Total Processing Time 156

5.1.2 Control Overhead 159

5.1.2(a) SECS/GEMsec Control Overhead 159

5.1.2(b) Secured SECS/GEM – Control Overhead 161

5.1.2(c) SGSM – Control Overhead 162

5.1.2(d) Control Overhead: SGSM vs. SECS/GEMsec vs. Secured SECS/GEM 164

5.2 Attack Scenario Experiments 165

5.2.1 SGSM (SHA256) Security Analysis 166

5.2.1(a) DoS Attack Prevention 166

5.2.1(b) FDIA Detection and Prevention 169
5.2.1(c) Replay Attack-Detection and Prevention 170
5.2.2 Summary of Attack Analysis 172
5.3 Discussion 173
5.3.1 Attainment of Authentication and Integrity 174
5.3.2 Lightweight 175
5.3.3 Multi-Featured and Versatility 177
5.3.4 Attainment of Customizability 178
5.3.5 Cyber-Attack Detection and Prevention 179
5.4 Chapter Summary 180
CHAPTER 6 CONCLUSION AND FUTURE WORK 182
6.1 Conclusion 182
6.2 Impact and Significance of the Proposed Research 185
6.3 Research Limitations and Future Works 186
REFERENCES 188
APPENDICES
LIST OF PUBLICATIONS

LIST OF TABLES

Page

Table 1.1 Research Scope and Limitations 11

Table 2.1 SEMI's SECS/GEM Communication Standards 21

Table 2.2 Description of HSMS Header Fields 28

Table 2.3 The Purpose and Values of the SType Header Field 29

Table 2.4 The SECS/GEM's Data Packaging Density 36

Table 2.5 Comparison of the Protocols and Main Features 55

Table 2.6 Summary of Related Works on Securing SECS/GEM 75

Table 4.1 Testbed Specifications 122

Table 5.1 Processing Time (in Milliseconds) of SGSM with Different HMAC Algorithms (at the Sender) 147

Table 5.2 Processing Time (in Milliseconds) of SGSM with Different HMAC Algorithms (at the Receiver) 149

Table 5.3 Total Processing Time Overhead 157

Table 5.4 SECS/GEMsec Control Overhead with RSA key size = 2048-bits . 160

Table 5.5 SECS/GEMsec Control Overhead with RSA key size = 4096-bits . 161

Table 5.6 Secured SECS/GEM - Anticipated Control Overhead with Different-Sized Payloads 162

Table 5.7 SGSM Control Overhead (key=256 bits) 163

Table 5.8 Summary of Control Overhead 164

Table 5.9 DoS Attack Prevention Analysis 169

Table 5.10 FDIA Attack Analysis 170

Table 5.11 Replay Attack Analysis 172

Table 5.12 Summarized Results of Cyber-attacks 173

Table 5.13 Summary of the Performance Comparison 180

LIST OF FIGURES

Page

Figure 1.1 Industry Sectors with the Most Cyber-incidents Globally in 2020.....6

Figure 1.2 Research Steps 15

Figure 2.1 A Simplified and Generalized Industrial Shop-floor Network 19

Figure 2.2 SECS/GEM Capabilities 22

Figure 2.3 Scenario to Illustrate the Exchange of S1F13/S1F14 Message Pair ..24

Figure 2.4 S1F13 Message Structure and Data Packaging.....25

Figure 2.5 S1F14 Replay Message From Equipment.....26

Figure 2.6 S1F14 Response Message Captured in Wireshark.....26

Figure 2.7 HSMS Message Structure 28

Figure 2.8 HSMS Connection States.....30

Figure 2.9 Equipment/Host Configuration Scenario 31

Figure 2.10 SECS/GEM's Connection Establishment, Control, and Data Message Processes 32

Figure 2.11 SECS-II Format Code-Byte 35

Figure 2.12 List Datatype with 500 Data Items 36

Figure 2.13 Scenario of Capturing, Intercepting & Attacking SECS/GEM Communications 40

Figure 2.14 Common Cryptographic Hashing Algorithms 46

Figure 2.15 Sending and Receiving Messages Using SECS/GEMsec Mechanism 64

Figure 2.16 SECS/GEMsec Architecture 66

Figure 2.17 Workflow of Secured SECS/GEM Security Mechanism.....68

Figure 3.1 The Placement of SGSM in the Layer-Architecture of SECS/GEM 85

Figure 3.2 The Architecture of the SECS/GEM Security Mechanism (SGSM) 86
Figure 3.3 Host and Equipment Configurations Using SGSM 88
Figure 3.4 ACB Message Structure 89
Figure 3.5 Authentication and Encryption Mode Activation 94
Figure 3.6 The Piggybacked ACB with SECS/GEM Message 98
Figure 3.7 Rule-Based Controls for Verifying HSMS Messages 102
Figure 3.8 SGSM Mechanism with Configurable Options 105
Figure 3.9 SGSM Workflow (Authentication) 109
Figure 4.1 Running Scapy on the Attack Machine 118
Figure 4.2 Packet Capturing using Wireshark 119
Figure 4.3 Testbed Environment: Attack Scenario 121
Figure 4.4 Packet Capturing using Scapy 123
Figure 4.5 Capturing HSMS Packets using Scapy 124
Figure 4.6 Captured Linktest.res Control Message 124
Figure 4.7 Crafting and Transmitting Attack Packets using Scapy 125
Figure 4.8 Attack Packet Captured and Dissected using Wireshark 126
Figure 4.9 High-Level Overview of SGSM Processes 127
Figure 4.10 ACB Generation, Timestamp Generation, and Computing HMAC Value at the Sender 130
Figure 4.11 Rule-Based Code for Verifying Message at the Receiver 131
Figure 4.12 Flowchart of ACB Verification at the Receiver 132
Figure 4.13 Pseudocode for HMAC Verification 133
Figure 4.14 HMAC Verification Steps 134
Figure 4.15 Pseudocode of Timestamp Verification at the Receiver 135
Figure 4.16 Timestamp Steps Performed at the Receiver 136
Figure 4.17 Testbed Environment: Normal Scenario 138

Figure 5.1 Evaluation Strategy 142

Figure 5.2 SGSM Processing Time at the Sender 148

Figure 5.3 SGSM's Processing Time (at the Receiver) 151

Figure 5.4 Processing Time: SGSM(SHA256) vs. Secured SECS/GEM vs. SECS/GEMsec 153

Figure 5.5 Processing Time: SGSM(SHA512) vs. Secured SECS/GEM vs. SECS/GEMsec (at the Sender) 154

Figure 5.6 Processing Time: SGSM(SHA256) vs. Secured SECS/GEM vs. SECS/GEMsec (at the Receiver) 155

Figure 5.7 Processing Time: SGSM(SHA512) vs. Secured SECS/GEM vs. SECS/GEMsec (at the Receiver) 156

Figure 5.8 SGSM: Control Overhead vs. Message Size 165

Figure 5.9 Launching DoS Attack on SGSM 167

Figure 5.10 SGSM Detected and Prevented DoS Attack (at the Equipment) 168

Figure 5.11 Wireshark Capture of Injected DoS Attack Message 168

Figure 5.12 SGSM: Replay Attack Detection and Prevention 171

Figure 5.13 Comparison of Processing Time Overhead 177

LIST OF ABBREVIATIONS

ASCII	American Standard Code For Information Interchange
CoAP	Constrained Application Protocol
DDS	Data Distribution Service
DTLS	Datagram Transport Layer Security
EEF	Engineering Employers Federation
FDIA	False Data Injection Attack
GEM	Generic Equipment Model
HMAC	Hash-Based Message Authentication Code
HSMS	High-Speed SECS Message Services
HTTP	Hyper Text Transfer Protocol
IBM	International Business Machines
IT	Information Technology
M2M	Machine-to-Machine
MD5	Message Digest 5
MQTT	Message Queuing Telemetry Transport
NIST	National Institute of Standards and Technology
OPC UA	Open Platform Communications – Unified Architecture
OSI	Open Systems Interconnection
OT	Operational Technology
PLC	Programmable Logical Controller
PPChanged	Process Program Changed
REST	REpresentational State Transfer
RFC	Request for Comments
SECS	Semiconductor Equipment Communication Standard

SECS-I	SEMI Equipment Communications Standard, Part 1
SECS-II	SEMI Equipment Communications Standard, Part 2
SEMI	Semiconductor Equipment and Material International
SGSM	Secured SECS/GEM
SHA	Secure Hash Algorithm
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TSMC	Taiwan Semiconductor Manufacturing Company
UDP	User Datagram Protocol
WFH	Work From Home

LIST OF APPENDICES

Appendix A Processing Time

Appendix B Python-Based Attack Script

MEKANISMA BERASASKAN PENGESAHAN KRIPTOGRAFIK UNTUK MELINDUNGI KOMUNIKASI SECS/GEM BAGI PEMBUATAN INDUSTRI 4.0

ABSTRAK

Industri 4.0 merupakan satu kuasa pemandu yang sedang membuat perubahan besar terutamanya dalam sektor pembuatan yang melibatkan pendigitalan komponen integral yang tersaling-hubung dalam proses pengeluaran. Dengan integrasi teknologi robotik, pembelajaran mesin, kecerdasan buatan, data raya, pengkomputeran awan, Internet of Things (IoT), dan penambahbaikan proses automasi, kesalinghubungan terbuka ini menyebabkan sistem perindustrian semakin terdedah kepada serangan siber. Standard Komunikasi Perkakasan Semikonduktor/ Model Perkakasan Generik (SECS/GEM) merupakan protokol komunikasi Mesin-ke-Mesin (M2M) legasi yang digunakan secara meluas dalam industri semikonduktor serta industri lain yang berkaitan. Protokol ini direkabentuk untuk digunakan dalam persekitaran kilang yang boleh dipercayai, terkawal serta diregulasikan, dan terasing dari rangkaian luar. Industri 4.0 yang telah merevolusikan industri pembuatan dan ketersambungan perkakasan ke rangkaian Internet telah menyebabkan perhatian diberikan semula kepada SECS/GEM kerana protokol ini tidak mempunyai sebarang perlindungan terhadap serangan siber. Tesis ini mencadangkan Mekanisma Sekuriti SECS/GEM (SGSM) yang menawarkan komponen pengesahan, integriti, dan perlindungan terhadap serangan siber. Mekanisma yang dicadangkan telah dibandingkan dengan piawai SECS/GEM, Secured SECS/GEM, dan SECS/GEMsec dari segi masa pemprosesan, overhed kawalan, dan daya tahan terhadap serangan siber. SGSM telah menunjukkan keputusan yang sangat memberangsangkan, sekaligus menunjukkan ia

dapat memastikan peranti SECS/GEM dapat berkomunikasi hanya dengan perkakasan industri yang sah sahaja, dengan integriti mesej dikekalkan, mesej yang dipalsukan dibuang, serta dapat mengelakkan serangan seperti serangan Penafian Perkhidmatan (DoS) , serangan main semula, dan serangan injeksi data palsu (FDIA) dilakukan terhadap komunikasi SECS/GEM. Berdasarkan hasil dan ciri-ciri yang disokong oleh SGSM (iaitu, berdaya tahan terhadap serangan siber, kaya dengan ciri, ringan, dan boleh disesuaikan), dapat kita disimpulkan bahawa SGSM adalah mekanisma keselamatan yang paling sesuai pada masa sekarang untuk membolehkan komunikasi SECS/GEM dalam persekitaran Industri 4.0.

CRYPTOGRAPHIC AUTHENTICATION-BASED MECHANISM FOR SECURING SECS/GEM COMMUNICATIONS FOR INDUSTRY 4.0 MANUFACTURING

ABSTRACT

Industry 4.0 as a driving force is making huge strides, particularly in the manufacturing sector, where all integral components involved in the production processes are getting digitally interconnected. Fused with improved automation and robotics, machine learning, artificial intelligence, big data, cloud computing, and the Internet of Things (IoT), this open network interconnectivity makes industrial systems increasingly vulnerable to cyber-attacks. Semiconductor Equipment Communication Standard/Generic Equipment Model (SECS/GEM) is a legacy Machine-to-Machine (M2M) communication protocol used profoundly in the semiconductor and other manufacturing industries. It is mainly designed to be utilized in a trusted, controlled, and regulated factory environment separated from external networks. Industry 4.0 has revolutionized the manufacturing industry and has brought SECS/GEM back to the limelight, as it lacks security safeguards to protect against cyber-attacks. This thesis proposes SECS/GEM Security Mechanism (SGSM) that offers authentication, integrity, and protection against cyber-attacks. The proposed mechanism is compared with the standard SECS/GEM, Secured SECS/GEM, and SECS/GEMsec mechanisms in terms of processing time, control overhead, and resilience against cyber-attacks. The SGSM exhibited promising results, indicating that it effectively enabled SECS/GEM devices to only communicate with authorized industrial equipment, maintained message integrity, discarded forged messages, and prevented attacks such as Denial-of-Service (DoS)

attacks, Replay attacks, and False-Data-Injection-Attack (FDIA) attacks launched on SECS/GEM communications. Based on the results and features supported by SGSM (i.e., resilient against cyber-attacks, feature-rich, lightweight, and customizable), it is concluded that the SGSM is the best option among currently available security mechanisms such as Secured SECS/GEM and SECS/GEMsec for securing SECS/GEM communication in an industrial 4.0 environment.

CHAPTER 1
INTRODUCTION

This chapter, divided into nine sections, discusses the research topic and the critical aspects of the SEMI Equipment Communication Standard / Generic Equipment Model (SECS/GEM) communication standard. Section 1.1 presents a general overview of Industry 4.0 and underlines the importance of Machine-to-Machine (M2M) communication protocols in Industrial Networks. Section 1.2 presents trends of cyber-attacks in industrial networks and highlights the significance of an effective and efficient security mechanism that protects SECS/GEM devices against cyber-attacks such as DoS attacks, False-Data-Injection-Attacks, and replay attacks. The problem statement, research objectives, and scope of the thesis are presented in sections 1.3, 1.4, and 1.5, respectively. Section 1.6 discusses the contribution of this study, which is to propose a security mechanism to authenticate SECS/GEM devices and prevent cyber-attacks such as Denial-of-Service (DoS) attacks, impersonation attacks, replay attacks, and False-Data-Injection Attacks. Section 1.7 illustrates the roadmap and discusses the steps for securing SECS/GEM communications in Industry 4.0 ecosystem. Section 1.8 presents the organization of this thesis.

1.1 Overview

One of the most significant developments in the history of mankind that has influenced the most human life is the industrial revolution(Sari et al., 2020). The advent of mechanical equipment powered by thermal and kinetic energy revolutionized industrial processes at the culmination of the 18th century and was vocally referred to as the first industrial revolution. This echoed mass production, which was achieved with the emergence of electrical technology during the mid of

19th century, thus, recognized as the second industrial revolution. The industries took flight with the invention of the Programmable Logical Controller (PLC) in late 1960, which revolutionized industrial automation and was referred to as the third industrial revolution (Masset et al., 2018; Oztemel & Gursev, 2020). Technological advances have progressed so exponentially over the last few decades that we have entered the fourth industrial revolution, dubbed Industry 4.0 (Aheleroff et al., 2020). As the turning point of this technological revolution, cyber-physical structures have been praised so that the physical world can be completely incorporated into the virtual world. Additive Manufacturing, Internet of Things (IoT), Machine Learning, Big-Data Analytics, 5G Networks, Cloud Computing, and Autonomous Robots are the main developments of this modern technological age, which bring revolutionary changes in the economy, industry, society, and individuals (Galli, 2018). Industry 4.0 is moving towards modernizing the production process and increasing industrial productivity with its emphasis on advanced robotics and automation, new forms of machine-to-machine interaction, real-time data collection, machine learning, and enhanced connectivity (Azaiez et al., 2019). The growing population has growing demands for customized products in the shortest possible time at the cost of large-scale production.

Industrial equipment/machines usually generate a massive amount of data (Masset et al., 2018; Oztemel & Gursev, 2020), and this generated data can be highly useful for improving various aspects of the production processes, such as throughput, maintenance, performance, and other key-performance-indicators. The Machine-to-Machine (M2M) communication protocols play a critical role in the shop floor, allowing manufacturing equipment/machines to be integrated with wired or wireless network adaptors to communicate and exchange information without human

intervention. M2M communication refers to the interaction as well as data exchange between two or more interconnected machines without human intervention (Amodu & Othman, 2018). This encompasses almost everything, including smartphones, laptops, tablets, factory equipment, robots, and automatic sensors. These devices are enabled to react and adjust their internal processes based on external feedback (Yang et al., 2019). Based on effective M2M communications and interactions, machines and factory equipment provide information on patterns in usage (or misuse) and signal events to act immediately. Machines can be interconnected to produce operational performance statistics, predictive diagnostic data, inactivity analysis, and a host of related monitoring and control information. Thus, a bird's-eye view of the shop floor can be visualized, and timely preemptive decisions with simple cost-savings advantages may be made. M2M can transform the conventional linear supply chain into a feedback loop that continuously flows through dynamic business alliances that produce, distribute, and service the objects (Esfahani et al., 2019). Human intermediaries will, in many cases, be entirely eliminated from the equation. With specified and managed parameters, equipment assets can make key decisions themselves, thus providing the stakeholders with maximum cost-effectiveness.

1.2 Background

While emerging technology is bringing operational hardware online, the separation line between operational technology (OT) and information technology (IT) is becoming increasingly blurred. IT deals with digital information and data flow, whereas OT is focused on the operation of physical processes and the machinery required to carry them out. Industry 4.0, smart manufacturing, and industrial internet-of-things (IIoT) are all terms that refer to the intersection of IT and

OT in order to monitor physical processes within an industry setting and use data to make predictive, corrective, and adaptive decisions in order to reduce operational costs (Tay et al., 2021). Although the separation line between OT and IT is disappearing, the emphasis is still on protecting OT assets (Laghari et al., 2021). The protection of IT assets is usually ignored altogether (especially the cybersecurity aspects). Many believe that manufacturing is a closed environment and is thus immune to cyber-attacks; however, this is a complete misconception (Lezzi et al., 2018).

1.2.1 Industrial Networks Communication Protocols

A number of industrial and IIoT protocols for M2M communication are available such as SECS/GEM, Modbus, Message Queuing Telemetry Transport (MQTT), Open Platform Communications – Unified Architecture (OPC UA), Constrained Application Protocol (CoAP), Data Distribution Service (DDS), and many more. Cybersecurity was not a primary consideration throughout the development of many of these protocols since they were designed mainly for use only in closed, air-gapped, and trusted industrial networks (Asghar et al., 2019). Industry 4.0 as a driving force requires interconnectivity with industrial networks to access real-time equipment/machine data whenever and wherever needed. The security of these protocols against cyber-attacks must, therefore, be assured.

SECS/GEM is an industry-standard protocol that has been widely used in virtually every semiconductor industry for several years, including surface mount technology, electronics assembly devices, photovoltaic, and solar cell manufacturing (Ewe et al., 2020). SECS/GEM provides various capabilities that enable the rapid transformation of traditional factories into smart ones via M2M communication, automation, and real-time data acquisition for monitoring, control, and analytics. It

cannot be denied that the SECS/GEM interface is becoming an increasingly important requirement for newly built industrial equipment (Cimetrix, 2020). Nevertheless, it is also a bitter truth that SECS/GEM is absolutely devoid of security features and hence absolutely vulnerable when utilized in an Industry 4.0 environment without the required safeguards and security measures. This is because once cybercriminals breach an industrial network's frontline defenses (such as firewalls), they gain easy access to SECS/GEM machines and can do anything they want, including injecting malicious content and launching a denial-of-service (DoS) attack. Thus, the purpose of this study is to secure SECS/GEM operations by authenticating the communicating entities, preventing alterations to the message in transit, and strong defense against cyber-attacks.

1.2.2 Cybersecurity Threats

Figure 1.1 depicts the number of reported cyber-incidents globally in 2020, with the manufacturing sector suffering from 67 incidents and expected to grow significantly (Johnson, 2021). Cybercriminals are well aware of the existence of sensitive IT and networking assets within industrial networks. Due to stakeholders' failure to address cybersecurity concerns, cybercriminals find it very easy to penetrate such networks. (Mullet et al., 2021).

The worldwide outbreak of the coronavirus pandemic in 2019 was shortly afterwards pronounced as a pandemic by the world health organization (WHO), resulting in strict lockdowns, requiring governments to suspend operations in most sectors, including the manufacturing industry. The manufacturers were left with no alternative but to allow employees to carry out their responsibilities remotely, i.e., work from home (WFH), to ensure their health and safety while ensuring the continued operation of their businesses. Although working from home and remotely

accessing critical infrastructure allowed business continuity, it also expanded the threat landscape. Today, manufacturers face an increased risk of cyber-attacks by cybercriminals looking to take advantage of these uncertain times.

Awareness of the effects of Industry 4.0 and the increase in cybercrime gradually increased in 2017 and 2018. However, many companies in the industry remained unaware of the dangers. By 2019, Manufacturing had risen to become the eighth-most targeted industry by cyber attackers (Miller, 2021). The issue became particularly acute in 2020 when many businesses were compelled to rely nearly completely on remote workers owing to pandemic limitations. The cyber-criminals were aware of the WFH situation, hence intensified attacks, which resulted in Manufacturing jumping from the eighth to the second most targeted industry by cyber attackers, trailing only finance and insurance, implying a 300% increase in a single year (Kazu & Thomas, 2021).

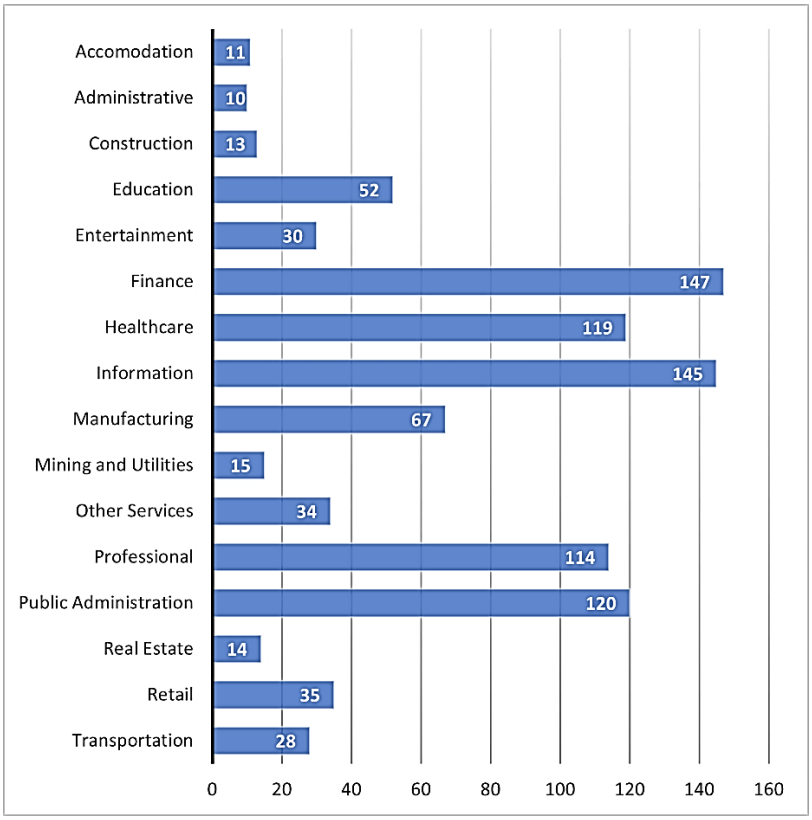

Figure 1.1 Industry Sectors with the Most Cyber-incidents Globally in 2020

Recent cyber-incidents have particularly reached a dangerous level in the manufacturing industry, making it a highly vulnerable and targeted sector (Gupta et al., 2018). According to a recent survey by the Engineering Employers Federation (EEF), 48 percent of manufacturers have been exposed to a cyber-incident at some point, half of which caused financial loss or adversely affected the market. Similarly, according to a study performed by Cyber Security Ventures, cybercrimes would cost companies across the world $10.5 trillion per year by 2025, representing a significant rise from the $3 trillion per year estimated in 2015 (Morgan, 2021). While manufacturing production has picked up rapidly in recent years, the Verizon data breach investigation report 2019 described 352 cyber-incidents, of which 87 (i.e., 24.7%) were among manufacturers. The Taiwan Semiconductor Manufacturing Company (TSMC) malware attack is the biggest security breach in the history of Taiwan. It exposed the cybersecurity vulnerabilities in manufacturing environments, as this sector embraces Industry 4.0 with increased automation and networked communication (Peng, 2018).

The criticality of cybersecurity issues in manufacturing has been recognized recently, and several studies have been carried out to recommend appropriate security mechanisms for Industry 4.0 and IIoT (Conti et al., 2019; Gupta et al., 2021; Oztemel & Gursev, 2020; Yu & Guo, 2019). Relying on devices participating in the IIoT network is crucial to the smooth functioning of the network because a single hacked node may become malevolent, bringing the whole system to a halt or causing catastrophes. Therefore, it is vital that the equipment and machinery interacting in the IIoT environment establish a reliable relationship and communicate only with

trusted and authorized devices. Various studies address cybersecurity issues in the industry and propose authentication mechanisms as a potential solution.

1.3 Research Problem

Within the landscape of Industry 4.0, cybersecurity plays a leading role in preventing the loss of companies' competitiveness (Corallo et al., 2020). However, the focus of security in the manufacturing and automation industry has been up until recently on securing organizational perimeters, i.e., preventing unauthorized access to the industrial network (Culot et al., 2019; Lezzi et al., 2018). It was formerly assumed that rigorous access regulations adapted to limit physical access to industrial equipment, computing infrastructure, and communication infrastructure would prevent attacks, which is a complete myth. In today's digital and interconnected world, attackers do not require physical access to initiate attacks; instead, attacks can be conducted remotely at any time. Recent studies suggest that the number of targeted cyber-attacks is rising, and the manufacturing industry is an attractive target (Gupta et al., 2021; Tuptuk & Hailes, 2018). The spike in cyber-attacks indicates that adapting features promised by Industry 4.0 without considering security makes the manufacturing industry one of the leading targeted and among the most vulnerable sectors.

The SECS/GEM is an industry protocol and has been in profound use for several years in almost all manufacturing industries (Ewe et al., 2020). The SECS/GEM protocol is widely deployed on manufacturing equipment in all major semiconductor industries (Shackelford, 2020). SECS/GEM-enabled industrial equipment and machines generate a massive amount of data (Ruiz-Sarmiento et al., 2020; Shackelford, 2020). The great precision with which this data is generated can

be extremely insightful and beneficial for optimizing several aspects of the manufacturing processes, including predictive maintenance, performance, throughput, and other key performance indicators. The Standard SECS/GEM implementations offer no security features by default to establish a network connection with other entities in the network (Al-Shareeda et al., 2022; Cimetrix, 2018). Authentication and encryption are the two primary methods that are proposed to secure SECS/GEM communications over the network. Existing authentication mechanisms rely on digital signatures, which have the drawback of requiring a significant amount of processing time. As a result, these mechanisms are not ideal for SECS/GEM since SECS/GEM is designed to provide near real-time insights into the production systems. On the other hand, the existing encryption mechanism only encrypts the payload and leaves the message header unencrypted. This is a problem because the header contains sensitive information, and leaving it unencrypted makes the communication vulnerable to attacks such as FDIA, DoS, and replay attacks. The potential damage caused by these attacks is significant and devastating in terms of business continuance, theft of confidential data, and reputational damage (Djenna et al., 2021). For secure communication, authentication and encryption are both equally important; however, the existing mechanisms only provide either authentication or encryption, but not both. In addition, the existing mechanisms have been hard-coded with predefined key sizes and algorithms, making it challenging to alter either the key size or the algorithms used. This reduces the adaptability and flexibility of these mechanisms to changing threats and requirements for security.

The SECS/GEM protocol uses the HSMS transport protocol, which has a well-defined message structure. Changing or adding new fields to the header of the HSMS message structure may cause instability and incompatibility issues with

existing software tools designed for analytics. This is because these tools are developed to read, interpret and process the messages based on a well-defined message structure. Changing the structure of the message can cause these tools to fail to interpret the message correctly.

Based on the drawbacks and issues highlighted above, there is a need for a proper security mechanism to protect SECS/GEM communication and prevent DoS attacks, FDIA attacks, and replay attacks. Therefore, the problem statement is summarized as follows:

1. Existing SECS/GEM security mechanisms are inflexible in design and do not permit adjusting the algorithm or key size based on the desired level of security.
2. The existing SECS/GEM security mechanisms either fail to maintain data integrity or fail to prevent unauthorized devices from communicating and disrupting SECS/GEM communications in the manufacturing industry.
3. The existing SECS/GEM security mechanisms are vulnerable to several cyber-attacks, including False-Data-Injection Attack (FDIA), Denial of Service (DoS) Attack, and Replay attack.

1.4 Research Objectives

This research aims to prevent various attacks, such as DoS attacks, replay attacks, and False-Data-Injection Attacks (FDIA), carried out on SECS/GEM in industrial networks. Additionally, this research addresses authentication issues in SECS/GEM communications and assures that equipment in the industrial network

communicates with only authorized devices. Following are the research objectives that have been established in order to attain the goals of this research study.

1. To propose a flexible security mechanism for SECS/GEM that piggybacks control information with each message exchanged while retaining the original message structure of the SECS/GEM protocol.
2. To propose a security mechanism that employs cryptographic hash algorithms for maintaining data integrity and authenticates SECS/GEM devices to prevent unauthorized devices from communicating and disrupting SECS/GEM communications in the manufacturing industry.
3. To propose a rule-based mechanism for preventing cyber-attacks such as DoS attacks, False-Data-Injection attacks, and replay attacks against manufacturing equipment communicating over SECS/GEM protocol.

1.5 Research Scope and Limitations

The scope of this thesis is limited to proposing a security mechanism for authenticating industrial devices communicating over SECS/GEM protocol and protecting these devices from cyber-attacks such as DoS attacks, False-Data-Injection-Attack, and replay attacks. Table 1.1 summarizes the overall research scope for the proposed security mechanism.

Table 1.1 Research Scope and Limitations

Item	Scope of Research
Environment	TCP/IP Network
Security Mode	Authentication and Integrity

Key Storage	Securely stored locally, no key distribution mechanism employed
Attack Types	DoS, Replay Attack, False-Data-Injection-Attack (FDIA)
OSI Target Layer	Application Layer, Transport Layer
Evaluation Metrics	Processing Time, Protocol Control Overhead, Attack Prevention Success Rate

Although the DoS attacks can be accomplished by flooding the target with traffic beyond the receiver's processing capacity, rendering it inaccessible; however, this type of DoS attack is beyond the scope of this study. Instead, this study is limited to sending the receiver control commands, which force the victim to terminate the connection.

This study focuses solely on the authentication and integrity features and prevention of cyber-attacks of the proposed mechanism. The mechanism supports other security features, such as confidentiality, but they are not covered in this study.

1.6 Research Contribution

Although the standard SECS/GEM protocol is widely regarded as the backbone of the manufacturing industry and has been widely used for several years, it lacks any security features and is therefore unsuitable with Industry 4.0-compliant industrial networks. Although a few attempts have been made to address security issues with SECS/GEM, the existing security mechanisms are either vulnerable to cyber-attacks or require an excessively long processing time, neither of which is acceptable in a production environment. The proposed security mechanism is unique in that it protects SECS/GEM communications against cyber-attacks and is flexible, customizable, and lightweight. Upon completion of this research, the following contributions will be the most significant:

- The proposed mechanism is highly flexible and configurable, allowing the selection of different HMAC algorithms with different key sizes.
- The proposed mechanism is customizable, meaning that it provides different modes to operate in (e.g., authentication, confidentiality, both authentication, and confidentiality), depending on the requirements.
- The proposed security mechanism attains message integrity and ascertains that the communication over SECS/GEM protocol only takes place amongst the authorized devices in the manufacturing industry.
- The proposed rule-based security mechanism aims to prevent cyber-attacks (i.e., DoS, FDIA, and Replay Attacks) carried out on SECS/GEM communications in the industrial network.

1.7 Research Steps

In order to achieve the intended objectives of this study, the research is divided into five distinct phases, as depicted in Figure 1.2. The specifics of each of these stages are discussed in further detail below.

Step 1: Problem Identification. This stage covers the SECS/GEM communication protocol in general and delves deeper into the underlying SEMI communication standards to highlight the SECS/GEM protocol's strengths and weaknesses. Security threats to SECS/GEM communications are also identified at this stage.

Step 2: Literature Review. This stage addresses existing authentication and security solutions against cyber-attacks for various industrial communication protocols. Hence, this stage provides deeper insight into the limitations of present solutions, the research problem, the scope, and the requisite knowledge to describe the proposed solution.

Step 3: Research Methodology. This phase describes the proposed mechanism for authenticating and preventing cyber-attacks against SECS/GEM communications. The proposed mechanism must be highly configurable and capable of operating in a variety of modes, depending on the level of security desired in any given situation. Hence, a control structure is required to convey additional information to the receiver. Thus, this phase discusses the intricacies of the control structure, fields, options, and permissible operations.

Step 4: Implementation. This stage explains the specifics of how the proposed mechanism will be implemented, the programming language as well as the steps that will be taken to put the proposed mechanism into action. Additionally, this phase discusses software tools for monitoring network traffic and capturing and manipulating packets. The tools discussed will be used in conjunction with the development of the proposed mechanism. Additionally, a testbed will be developed to examine the functioning and efficacy of the proposed mechanism. The proposed mechanism is executed, and its performance is evaluated in a variety of configuration modes. Moreover, several attack scenarios will be developed to assess the proposed mechanism's resilience to DoS, replay, and FDIA Attacks.

Step 5: Evaluation and conclusion. This step evaluates the efficiency of the proposed mechanism in terms of processing time, control overhead, and resilience to

cyber-attacks using various scenarios. Additionally, this stage evaluates the capacity of the proposed mechanism to prevent unauthorized devices from establishing communication links with legit industry equipment. The proposed mechanism is validated by comparing its accuracy and usefulness to those of other existing mechanisms.

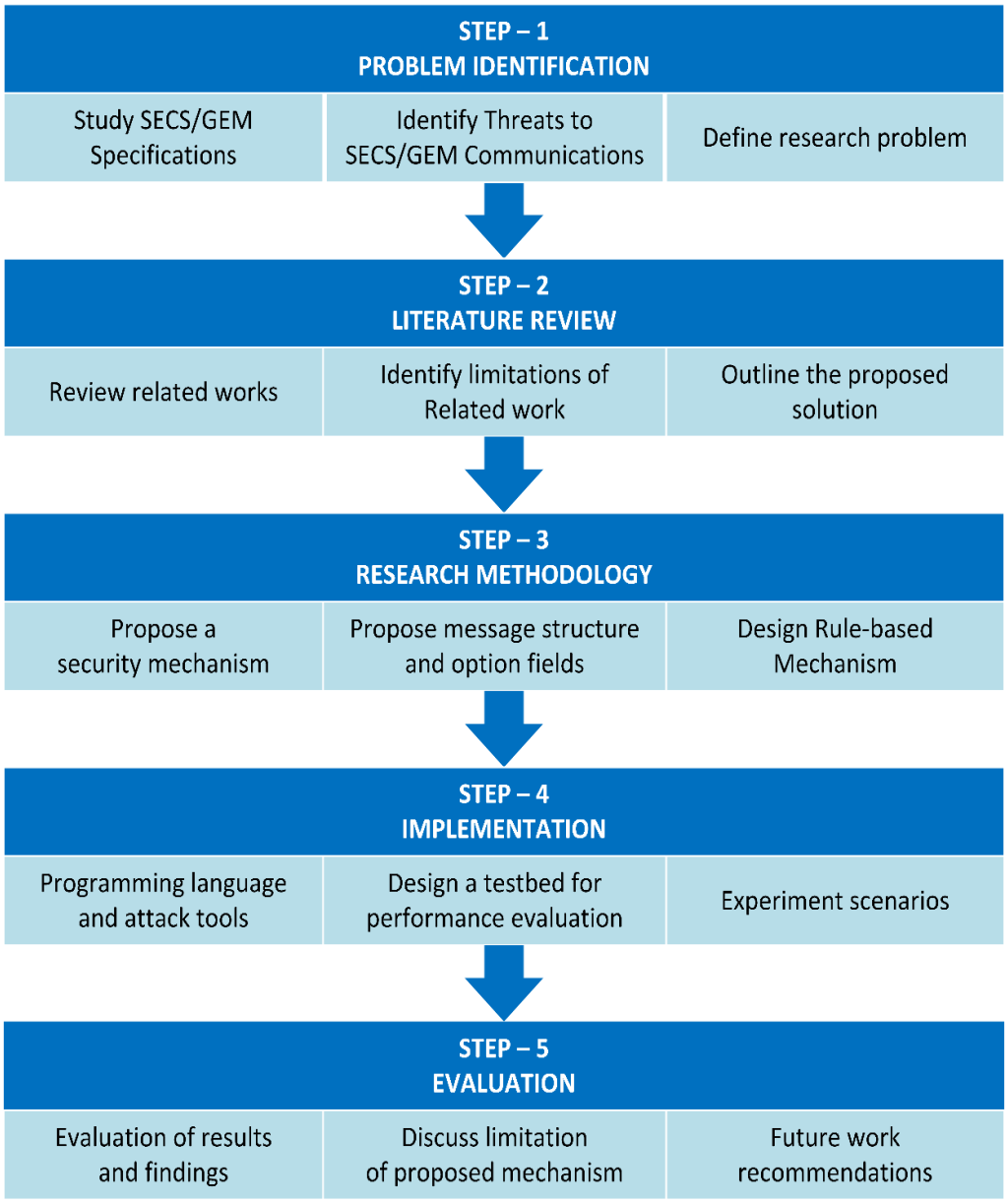

Figure 1.2 Research Steps

1.8 Thesis Organization

This thesis is organized into six chapters, with this chapter being an introduction to this entire thesis. The remaining chapters are arranged as follows.

Chapter Two provides a critical overview of the history and features of the SECS/GEM communication protocol in industrial networks. This chapter also goes through the fundamental concepts linked to this research, as well as the pertinent studies and limitations of each existing mechanism, which are discussed in detail in this chapter.

Chapter Three discusses the methodology of the proposed mechanism, sheds light on its salient features, and outlines its requirements.

Chapter Four provides the details of the implementation of the proposed mechanism. Additionally, it describes the thread model and the scenarios used to evaluate the proposed mechanism.

Chapter Five discusses the evaluation of the proposed mechanism and compares the results with other SECS/GEM implementations in terms of processing time, control overhead, and resilience against cyber-attacks.

Chapter Six summarizes the finding of this thesis and outlines its scope. The chapter also proposes some valuable suggestions and recommendations for future work.

CHAPTER 2
LITERATURE REVIEW

This chapter provides a thorough overview of the SECS/GEM standard and the core concepts underlying this study. It reviews related research on securing SECS/GEM communications in the industry 4.0 ecosystem. Additionally, it emphasizes the limitations of each approach, which serves as the impetus for this research.

Section 2.1 introduces the SEMI organization and provides a comprehensive overview of SEMI's SECS/GEM standards, including SECS-I, SECS-II, HSMS, and GEM, which are discussed in Section 2.2. Section 2.3 discusses common cyber-attacks carried out on industrial networks in general and sheds light on attacks carried out on SECS/GEM in particular. Section 2.4 introduces rule-based systems to prevent cyber-attacks. Section 2.5 presents the cryptographic hash functions and the secure hash standards. Section 2.7 covers the literature review and provides an in-depth discussion on several industrial M2M communication protocols used commonly. Section 2.8 covers related work, Section 2.8 provides a critical analysis of existing mechanisms, outlining their weaknesses and limitations. Section 2.9 discusses the requirements of the proposed mechanism, and Section 2.10 summarizes the chapter.

2.1 Background

Semiconductor Equipment and Materials International (SEMI), founded in the United States in 1970, is a global industry association with a worldwide membership of companies representing semiconductor-related industries. SEMI has 26 subcommittees that include, among factory others, the subcommittees for Automated

Test Equipment, Environment, Health and Safety, and Information and Control (Goh et al., 2017).

Automation in semiconductor manufacturing plays a vital role in day-to-day operations. The special focus is on boosting efficiency and productivity in the value-chain process by substituting human operators with automated machines in myriad situations, such as tasks that are recursive in nature, complex, prone to errors, dangerous and hazardous, and the like. The fab (also called a semiconductor fabrication plant or foundry) operations are categorized into three types, i.e., manual, semi-automated, and fully automated, based on the attention required by the operator (Moyne & Iskandar, 2017). Manual fab operations require an operator to run equipment, which makes it very astringent to find equipment operating without computer assistance in the modern semiconductor industries. The semi-automated fab operations have achieved cognizance in the modern factory installations (i.e., shop-floor), wherein processing tools and equipment are assisted, monitored, and controlled by computers for major activities, while operators carry out only tasks like material loading/unloading and other manual processes. The fully automated fab operations have eased processes in modern factory systems by installing systems that carry out automated processing without the involvement of the human operator. Figure 2.1 shows simplified equipment configurations in the production line within the industrial network.

Machine-to-Machine communication protocols are the cornerstone of industrial networks and are critical in achieving automation and higher productivity. As stated previously, M2M communication is a direct connection between devices through any communication channel, including wired and wireless. The M2M

communications protocols enable a network of smart systems to exchange, connect, and monitor data, allowing for efficient and intelligent decision-making without human involvement (Amodu & Othman, 2018). This encompasses almost everything, including smartphones, laptops, tablets, manufacturing equipment, robots, and autonomous sensors, and allows these devices to react to and adjust their internal operations in response to external feedback (Yang et al., 2019). Based on effective M2M communications and interactions, machines and factory equipment provide information on patterns in usage and signal events to act immediately. Manufacturing equipment may be networked together to provide operational performance statistics, predictive diagnostic data, inactivity analysis, and a variety of other monitoring and control data. Thus, managers may make preemptive decisions with apparent cost-cutting benefits.

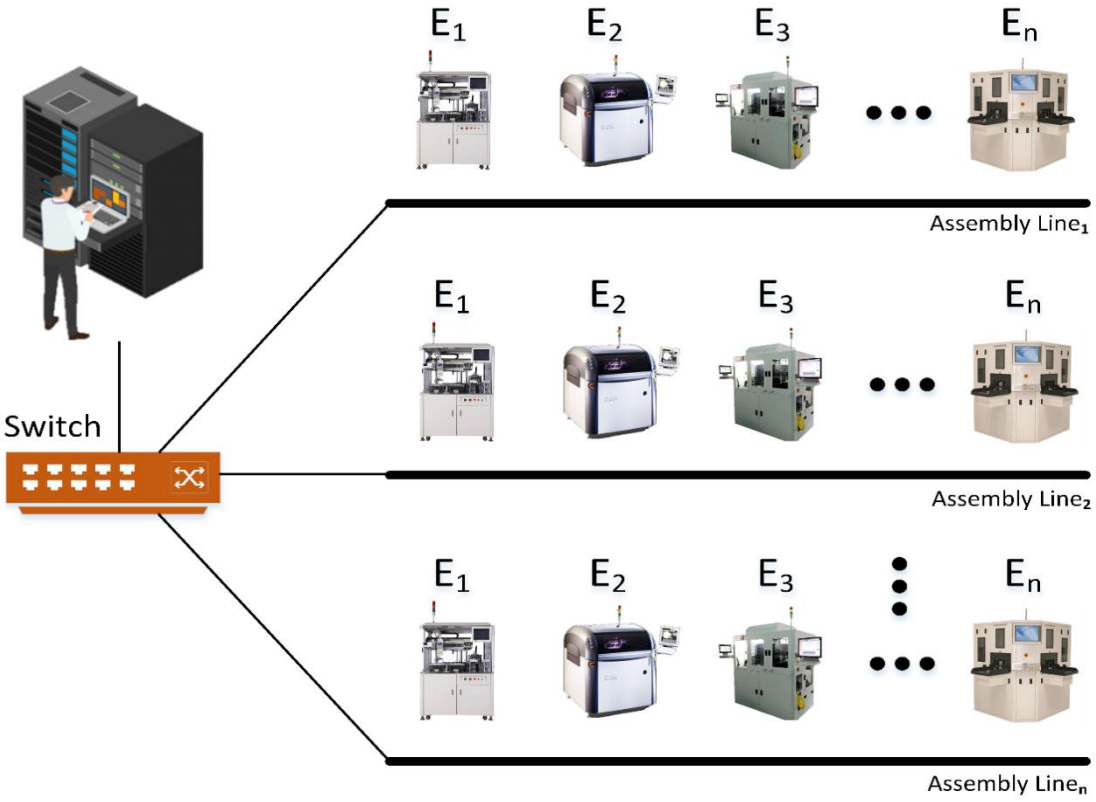

Figure 2.1 A Simplified and Generalized Industrial Shop-floor Network

M2M communication protocols can transform the conventional linear supply chain into a feedback loop that continuously flows through dynamic business alliances that produce, distribute, and service the objects. Human intermediaries will, in many cases, be entirely eliminated from the equation (Vashistha, 2021). With specified and managed parameters, equipment assets can make critical decisions themselves, thus providing the end-user with maximum cost-effectiveness.

2.2 SEMI Equipment Communication Standards

SEMI deals in materials, services, and equipment required by the manufacturing industries. It unleashes various standards, including E4, E5, E30, and E37. SEMI Equipment Communications are centered on four primary standards, commonly referred to as SECS/GEM, and are summarized in Table 2.1. The SECS/GEM is an industry protocol and has been in profound use for decades in almost all manufacturing industries (Stoop et al., 2019). The SECS/GEM of SEMI is the jugular vein in the semiconductor industry, such as Intel, Samsung, TSMC, IBM, Qualcomm, Broadcom, Toshiba, and so on, proving as a communication protocol and control system for years (Weber et al., 2016).

The SECS/GEM communication protocol is feature-rich and offers two types of capability sets 1) The fundamental requirements and 2) the additional capabilities. All SECS/GEM-compliant equipment must support at least fundamental requirements, which are considered the minimum set of functionalities semiconductor equipment must support. The fundamental requirements include State models, Equipment processing states, host-initiated Scenarios, Event notification, Error messages, Online identification, Control (Operator Initiated), and documentation.

Table 2.1 SEMI's SECS/GEM Communication Standards

Year	SEMI Standard	Description
1978	**E4** SECS-I	**SEMI Equipment Communications Standard-I**: It is a communication protocol that helps establish communication between various equipment and a host on an RS-232 cable. This works at the physical layer.
1982	**E5** SECS-II	**SEMI Equipment Communications Standard-II**: It helps to exchange information between equipment and host as a series of streams and function messages in a defined format.
1992	**E30** GEM	**Generic Equipment Model**: It helps to define the usage of SECS-II messages and monitor the behavior of the equipment while exchanging messages with the host.
1994	**E37** HSMS	**High-Speed SECS Message Service**: It defines a communication protocol managing point-to-point communication between equipment and a host on TCP / IP.

In addition to the fundamental GEM requirements, the SECS/GEM specifies a myriad list of optional capabilities that can be implemented and supported by a GEM interface based on the complexity and requirements. The additional capabilities include the Establishment of Communication, Event Notification, Dynamic Event report configuration, variable data collection, trace data collection, status data collection, alarm management, remote control, equipment constants, process program management, material movement, equipment terminal services, clock, limit monitoring, spooling, and host initiated control (Sauter & Treytl, 2015). The complete list of fundamental and additional SECS/GEM capabilities is shown in Figure 2.2.

Fundamental GEM requirements (Basic)	Additional GEM capabilities (Advanced)
• State models • Equipment processing states • Host-initiated control • Event notification • Error messages • Documentation • Control (operator initiated)	• Establish communication • Dynamic event report configuration • Variable data collection • Trace data collection • Status data collection • Alarm management • Process program management • Remote control equipment constants • Material movement • Equipment terminal services • Clock • Limited Monitoring • Spooling • Control (Host-Initiated)

Figure 2.2 SECS/GEM Capabilities

2.2.1 SEMI Equipment Communication Standard: Part 1 (SECS-I)

The E4 standard, also known as SECS-I, defines the exchange of messages between semiconductor equipment and a host computer without requiring that the equipment and the host are aware of each other (Cimetrix, 2016). The SECS-I standard defines point-to-point communication by utilizing the RS-232 interface. SECS-I provides a slow transmission data rate over RS-232, whereas it is deficient in supporting TCP/IP-based local area networks. The communication is bidirectional, asynchronous, and half-duplex. Typically, communication takes place at a baud rate of between 9,600 and 19,200. SECS-I supports multi-block transfers using 256-byte blocks. The RS-232 communication protocol is inadequate for extended distances and provides only rudimentary noise immunity. Currently, the SECS-I protocol is

available only on legacy factory equipment and is not bundled with new machines. Thus, this research disregards SECS-I in favor of HSMS, a TCP/IP-based transport protocol for SECS/GEM.

2.2.2 SEMI Equipment Communication Standard: Part 2 (SECS-II)

The SEMI E5 standard, commonly termed as SECS-II, is a message content protocol that specifies a generic message layer to transmit any data structure supported by the specifications. It also describes a set of standard messages, with each specific message having an identity, purpose, and format. SECS-II reveals an interpretation of message types, data types, message structure, and message contents exchanged between intelligent factory equipment and the host. The message types are defined for various categories, covering a wide array of specific or general functions. The SECS-II messages are classified into various categories referred to as streams (e.g., Stream-1 deals with equipment status; Stream-7 covers specifications related to recipe management), whereas the functions are specific messages within a particular stream category (Jung et al., 2007). Both streams and functions are defined by combining a stream number and a function number, which are single-byte values ranging from 0 to 255. This combination of a stream and a function is expressed by the notation $Message = S_nF_m$, where $\boldsymbol{n}$ and $\boldsymbol{m}$ signify the numbers of a specific stream and a specific function, respectively, that have been allotted to execute a designated task. The odd-numbered function codes correspond to primary messages (request messages), while the even-numbered function codes correspond to secondary messages (reply messages). For example, a primary message S1F13 refers to Stream 1 and Function 13, which enables an entity to send an *Establish Communication Request* message to the intended host/equipment, and on receiving such a message, the device will reply with S1F14. The pair of primary and secondary messages (i.e.,

S1F13/S1F14) is called a transaction. Each transaction is identified with a unique transaction Id. The sender sets a special 4-byte integer value called SystemBytes, which pairs the primary message with its secondary message. Figure 2.3(a) depicts a host initiating a connection establishment request (i.e., S1F13/S1F14), while Figure 2.3(b) exhibits equipment initiating the same request.

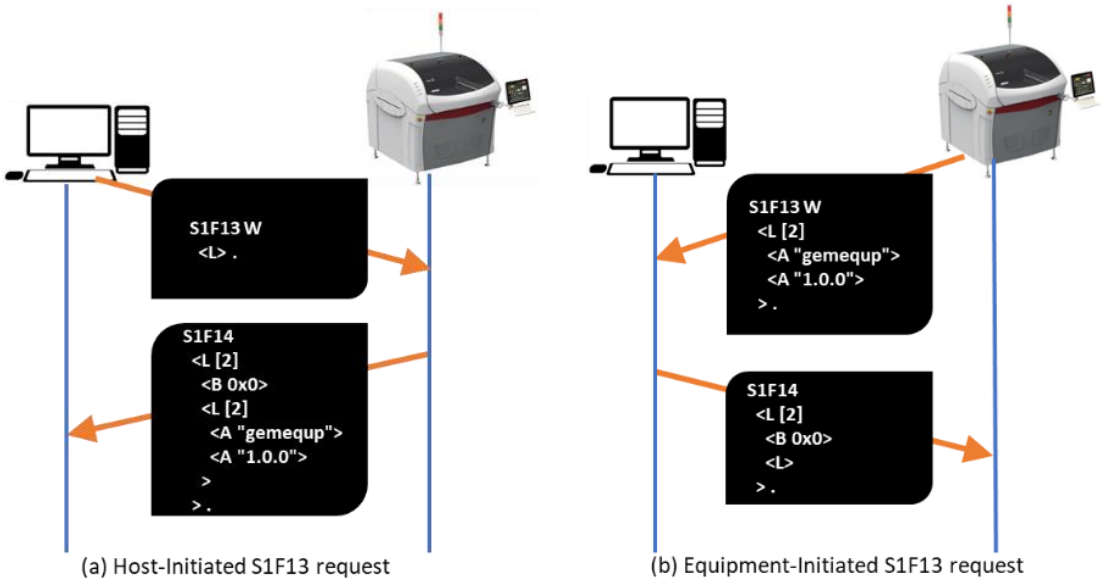

Figure 2.3 Scenario to Illustrate the Exchange of S1F13/S1F14 Message Pair

The simple S1F13 (connection establishment request) message from the host with an empty list is depicted in Figure 2.4. The W-bit in S1F13 message is turned ON, which signifies that the host computer is expecting a reply message from equipment. The message size is then computed based on the data passed from the SECS-II layer, and in this particular example, the data portion consists of an empty list; therefore, the payload size is just 2 bytes. The total message size is 16 bytes (i.e., four length bytes, ten header bytes, and two data bytes). It can be observed that the list data item has a Format Code and length bytes that are required to encode data.