Bulletin of Networking, Computing, Systems, and Software – www.bncss.org, ISSN 2186-5140
Volume 9, Number 1, pages 1–6, January 2020

Preliminary version: Attempt of modeling of connected Industorial Control System's communication aiming information security risk extraction

Satoshi Agatsuma
Institute of Information Security
Yokohama，Japan
mgs185501@iisec.ac.jp

***Abstract*—In order to secure Cyber-Physical System (CPS), it is necessary to analyze security of Information Technology (IT) and safety of Operational Technology (OT) in an integrated manner.**

There are many Industry Control System (ICS) protocols and their information security capabilities varies. To secure ICS communication, we need to know vulnerabilities of each protocol. To extract such vulnerabilities, we need a model that can be referred as a practically ideal communication model.

This is an interim report of my master's thesis that will propose a communication model of ICS that can be used for risk assessment.

Keywords—Cyber-Physical System (CPS), Industrial Control System (ICS), Perdue Model, Risk assessment, Hazard, Incident, Safety, OSI 7 Layer Model, Petri Net, Coloured Petri Net, Programable Logic Controller (PLC), Safety Instrumented System (SIS)

I. Introduction

A Cyber-Physical System (CPS), also known as Society5.0 in Japan, is aiming to solve many social problems.

It consists of many sensors in Physical systems which collect a wide variety and huge volume of data. Data is forwarded to Cyber systems and analyzed by AI or other mechanisms, and then results of which will be provided to Physical systems to solve many issues we are facing.

Now industry-government-academia is strongly promoting it.

A connected industry control system (ICS) is one of CPSs and is the fusion of control systems and information systems.

As a result of networking, connected ICSs are exposed to many emerging cyber threats. Traditionally, operational technology (OT) engineers have been focusing on safety. But now, they need to understand such emerging threats from connected world and fight against them. On the other hand, information technology (IT) engineers, who have been building connected world, must take responsibility for outcomes that are created by information security breaches, along with OT engineers.

The purpose of this research is to build a communication model of CPSs that will be able to be used as a reference model to evaluate risks in ICSs communication mechanisms.

II. An attack against an ICS and problems we recogniezed

A. TRITON, attacking Safety Instrumented System (SIS)

In 2017, a cyber attack occurred against petrochemical plant in Saudi Arabia. In this incident, the plant was tripped two times until the malware called TRITON［1］ was discovered. It is said that Engineering Workstations (EWS) of SIS were used for the island hopping of the attacker, and the malware modified application memory of SIS controllers in the plant.

B. Problems we recognized

In this case, it is reported that operators of the plant did not think of a possibility of a cyber attack at all at the first trip of the plant. Eventually, they treated the incident as a system failure, so that the malware was still alive in the system, which led to the second outage of the process.

This incident seemed to reveal the fact that operators did not recognize that cyber attacks might lead to a physical phenomenon.

At the same time, the incident gets us to re-acknowledge the fact that distance and walls between targeted systems and malicious parties do not mean anything for them, as is indicated by Stuxnet.

III. Overview of ICS network

In this paper, I have selected an ICS as a target of my modeling attempt.

Fig.1 is a simplified figure of ICS Purdue model.[2]

Traditionally, proprietary network technologies have been used in ICSs, but now general networking technologies such as Ethernet, TCP/IP have been being used in order to build connected ICSs.

I understood that this was one of the reasons of exposure of ICSs to outside of factories.

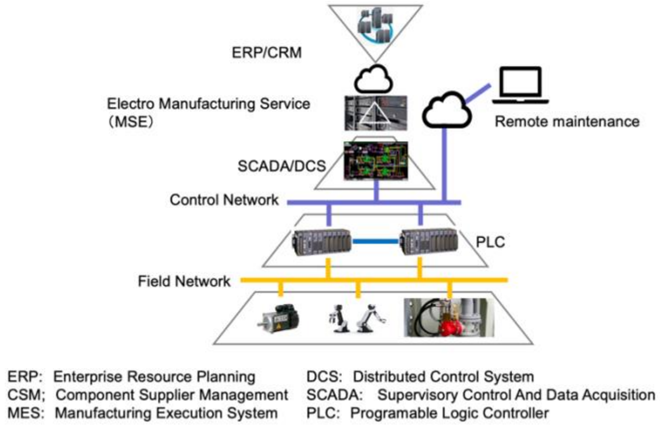
ERP/CRM
Electro Manufacturing Service
（MSE）
Remote maintenance
SCADA/DCS
Control Network
PLC
Field Network
ERP: Enterprise Resource Planning
CSM; Component Supplier Management
MES: Manufacturing Execution System
DCS: Distributed Control System
SCADA: Supervisory Control And Data Acquisition
PLC: Programable Logic Controller

Fig. 1 Simplified architecture of an ICS network

IV. Definition of Accidents, Hazards, incidents and causes of occurrence

A. Causes of Hazards

I followed the definition of causes of hazards described in 『SEC BOOKS 組込みシステムの安全性向上の勧め』[3]. In the brochure, two causes of occurrence of hazard are defined.

Random fault

Faults caused by faults of component parts and/or subsystems occurring in random manner by various ways of deterioration, which include hardware deterioration, random fault, human errors in simple procedures.

Fault by deterministic mechanism

Faults caused by deterministic mechanisms that have direct relations with design process, manufacturing, operation and documentation, which include software bugs, mistakes of safety analysis and/or safety management and design flaws.

B. Newly introduced cause of occurrence of hazard by connecting

I summarized that the cyber attack caused by intervention of the outsider, as is described in II, happened in a following way: malicious 3rd party intentionally generated a hazard or a couple of hazards. Such a hazard or hazards satisfied conditions of malfunctioning of processes and led to the trips of the plant.

According to observations thus far, I have reached the conclusion that the 3rd cause of hazard, “malicious intent,” should be introduced , in addition to the two causes described in IV. A.

C. Hazard occurred by malicious intent

To do harm to a targeted ICS, a malicious party should try to penetrate into an ICS via the Internet. Once they get into the system, they will manipulate messages between controllers and controlled processes in order to get targeted machines to perform unintended behavior.

In short, breaking Confidentiality, Integrity and Availability (CIA) of data in motion or data at rest will lead to harmful physical conditions or hazards.

It is difficult to make a direct physical effect on ICSs from outside of a plant. Although it is possible to make interference on Wi-Fi signal used by hand-held HMI devices with a jamming equipment, such an attack method has a high risk for attackers because they need to be close to target systems.

D. Threats against ICSs by breachs of message’s CIA

In ICSs, attacks against control messages that lead to hazards are as follows:

(1) Changing values of parameters
(2) Changing timing of a processes
(3) Changing order of processes
(4) Increasing/decreasing of the number of processes
(5) Issuing false alarms
(6) Interrupting alarms

By (1) through (4), control processes could be put into unappropriated range of tolerance. By (5), false alarms mislead operators to misjudgments and get them to do unexpected operations. In case important messages were interrupted, (6), SIS action could be sabotaged, which might support other campaigns.

V. effects of existing incident response

Countermeasures against traditional hazards and accidents have been established. In the process of establishing countermeasures, risk assessments such as FTA/ETA, FMEA, HAZOP are performed to extract potential risks in ICSs. But we need to understand that cyber attacks have not been considered as causes of hazards and accidents until now.

Recovering from hazardous physical phenomenon will not solve the root cause of incidents in case of cyber attacks, even though those countermeasures are effective on the surface against such phenomenon caused by cyber attacks.

Just treating visible phenomenon will lead to another attacks as is described in I.*B*.

That is why we need another risk assessment method or procedures to hamper cyber attacks. If we could extract risks on information security in ICSs and map such risks and outcomes, we could make use of existing countermeasures. And I believe it is safe to say that we could think of a possible list of cyber attacks that could be causes of visible physical phenomenon.

In this paper, I will propose a communication model of ICSs which can be used to extract risks that leads to security information breaches which result in physical outcomes.

VI. Selecting risk assessment method

As atomic manipulations on information, I selected 3 of them:

(1) Message insertion
(2) Message blocking
(3) Message eavesdropping

I considered that the Man-In-The-Middle (MITM) attack consists of a combination of above three methods.

I chose Petri Net, in this paper, to describe messaging between two entities. And as a visual aid to express information flow, I also used OSI 7-layer model.

A. Expression by layering modelof OSI

To express a perspective view of message flow, I used a simplified model of OSI 7-layer model as follows, Fig.2:

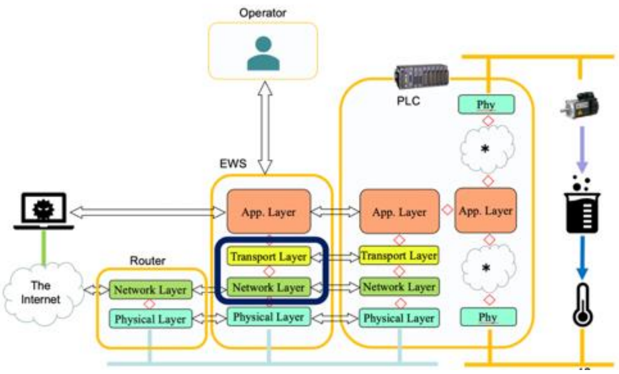

Fig. 2 Layering model of ICS communications

Communication protocol is a conversation between two entities, so it is a lateral movement of messages. Usually protocol analysis is done within a certain layer, but I tried to focus on a vertical movement of messages between two layers.

B. Expression by objects

I started my analysis from an application's message exchange between a client and a server, such as command/response. First, I used an object diagram for this purpose.

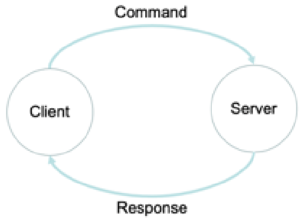

Fig. 3 Message exchange between a Client and a Server

Virtually, messages are exchanged between two entities, but actually these messages are delivered by lower layer as a vehicle.

In general, [N] layer uses [N-1] layer as a service, and [N] layer does not recognize the mechanism of [N-1] layer's service. In other words, an upper layer is a service user of its lower layer, and a lower layer is a service provider of the upper layer. Therefore, offering a service to its upper layer, a lower layer must satisfy its protocol specifications. I thought it could be said that [N-1] layer's protocol specifications were necessary conditions for [N] layer to exchange messages between the two entities.

As is described above, each layer's protocol specifications could be recognized as a constrains between a controller and a controlled process in its upper layer. I considered that implementing appropriate conditions in each layer's protocol would increase the robustness of communication against information security breach attempts.

I started from writing an object model between a [N] layer and a [N-1] layer. Fig.4 is an object diagram that I tried to express interactions between a [N] layer and a [N-1] layer.

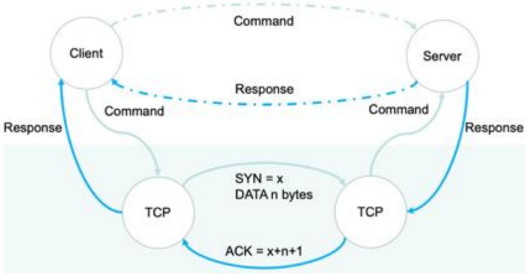

Fig. 4 Relations between Application layer and Transport Layer

C. Introducing Petri Net

Fig.5 is a diagram to show application message exchange between two entities of application layer in Petri Net notation.

Please take notice that the Place C has one token as an initial marking.

When the "Set" transition fires, the number of tokens in the Place C will become two, then the "Send command" transition will be fireable. When the "Set command" transition fires, there will be a token in the Place S and the "Receive response" transition will be fireable. After the "Receive response" transition fires, the Place C will have a token, and markings of this net will become its initial marking. It is equivalent to one round of command/response sequence of a protocol.

Then I focused on the token in the Place C, and realized that the token indicates a necessary condition that would enable the Place C to send a command to the Place S. So, I presumed that this initial marking of the net would indicate availability of a lower layer as a service provider to its upper layer in a layering model.

By the above argument, I understood that modeling interactions between a [N] layer and a [N-1] layer was required.

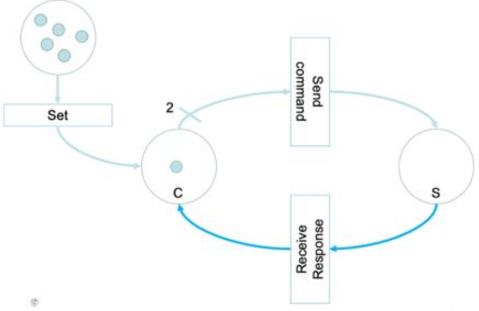

Fig. 5 P/T net diagram of a Ping-Pong protocol

D. Introducing extended Petri Net

I decided to introduce Coloured Petri Net (CPN) to get a perspective view of an ICS's communication model in this paper, because CPN has many extended features such as a hierarchical model. In CPN, tokens can be distinguishable and may have attributes, so I guessed that it would be easier to express conditions of interactions of protocols.

I guessed that it would require so many Places and Transitions

(P/T) to express every interaction between all layered protocols. Even though Petri Net had a strong capability of modeling, a model with huge number of P/T would not give us easy and high visibility.

E. Visualizing cyber attack steps

I examined two cyber attack scenarios: Case A and Case B.

In Case A, an attacker tries to access a Programable Logic Controller (PLC) from outside of a factory. In Case B, a malware infecting Engineering Workstation (EWS) for some reason. Case A and Case B are showen in Fig.6 and Fig.7 respectively.[4]

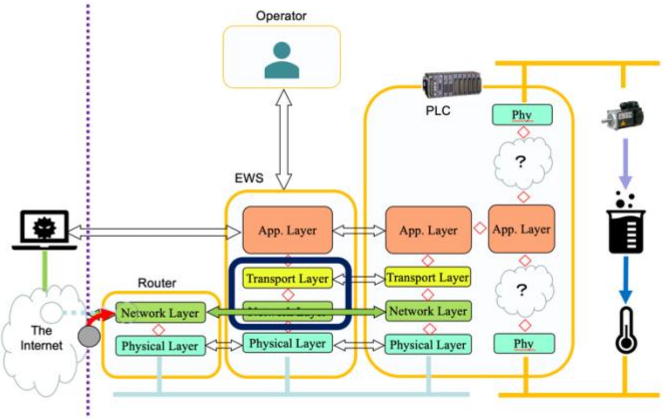

Fig. 6 Case A

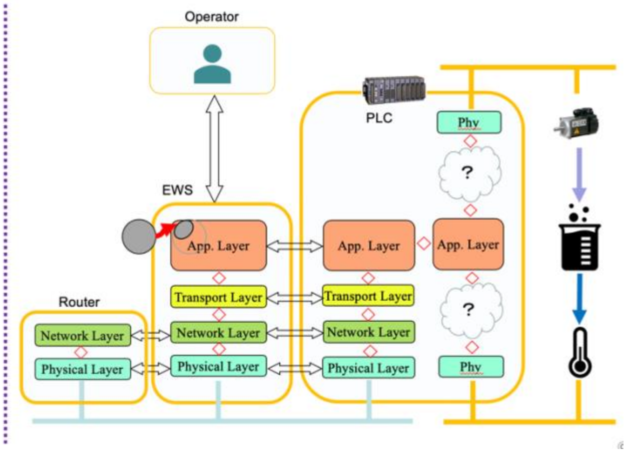

Fig. 7 Case B

F. Tokens in this model

I defined a set of coloured tokens of this model as is in Table 1.

Besides tokens of ICS's message and its header, each token is equivalent to an addressing information of a paired entities of each protocol. A pair of addressing information is given when a data unit is encapsulated and forwarded to lower layer along with other control information.

Table 1 A set of tokens

{(1,	"ics_message")
(2,	"ics_hdr")
(3,	"proto")
(4,	"dst_port")
(5,	"src_port")
(6,	"dst_ip")
(7,	"src_ip")
(8,	"phy_hdr")
}	

G. Sets of tokens for each cases

Assume a malicious party (attacker) who wants to do harm to an ICS.

I added a * marking to tokens that the attacker's intentions were reflected. I used a word "contamination" hereafter when an attacker's intention was penetrated into data in motion or data at rest.

1) Case A

In case A, IP and above layer data unit could be crafted according to attacker's intention, so that IP datagrams could reach a targeted system from outside. Therefore, a set of tokens would be as follows:

Table 2 A set of tokens in Case A

{(1,	* "ics_message")
(2,	* "ics_hdr")
(3,	* "proto")
(4,	* "dst_port")
(5,	* "src_port")
(6,	* "dst_ip")
(7,	* "src_ip")
(8,	"phy_hdr")
}	

2) Case B

In Case B, a host of a malware is a legitimate workstation of a targeted system, and it is assumed that its OS itself is not affected by the malware, like trojan horses. In this case, a set of tokens would be as follows:

Table 3 A set of tokens in Case

{(1,	* "ics_message")
(2,	* "ics_hdr")
(3,	"proto")
(4,	"dst_port")
(5,	"src_port")
(6,	"dst_ip")
(7,	"src_ip")
(8,	"phy_hdr")
}	

H. How a set of tokens processed in a general host

I tried to describe how a set of tokens were processed in a general host, such as Windows workstation, in a CPN manner, Fig.8.

Generally speaking, an IP datagram will be accepted when its destination IP address owns IP address of a received host or the broadcast address.

Therefore, IP datagrams will be accepted either Case A or Case B.

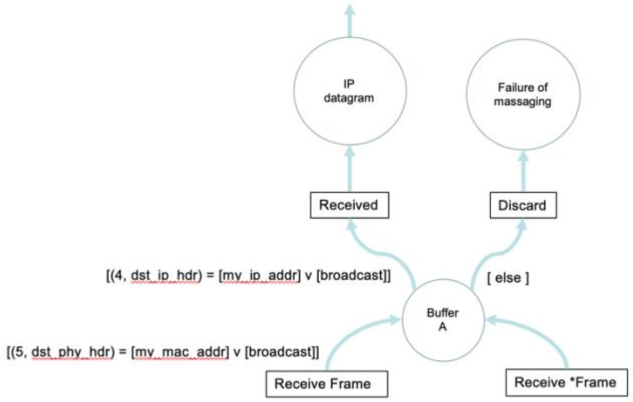
IP
datagram
Failure of
massaging
Received
Discard
[(4, dst_ip_hdr) = [my_ip_addr] v [broadcast]]
[else]
Buffer
A
[(5, dst_phy_hdr) = [my_mac_addr] v [broadcast]]
Receive Frame
Receive *Frame

Fig. 8 Ordinary process of IP layer

I. Introducing a constraint at Network layer

A P/T net inside of a one-dot chain line is newly introduced as a constraint of Network layer, host-to-host, communication, Fig. 9. Theoretically, it is equivalent to an IP address filter like a firewall.

For instance, when a constraint restricts packets with a source address of subnets inside of a factory to be received, messages from outside of a factory will be discarded by this mechanism. This is equivalent to zoning that many best practices propose.

I examined how this constraint works for both Case A and Case B.

In Case A, contaminated tokens were 1 through 6. When a host with this constraint received the set of tokens, the constraint would test #5 token, then the set of tokens would be discarded because the colour of #5 does not belonge to any subnet inside. Therefore, such sets of tokens from outside would never be forwarded to its upper layer.

On the other hand, in Case B, contaminated tokens were only 1 and 2. Therefore when the constraint would test a set of tokens of Case B, contaminations of attacker would not be detected with this constraint, so that the set of tokens would be forwarded to its upper layer.

To summarize, this constraint within Network layer was effective for Case A, but not for Case B. Now I realized that other constraint(s) within upper layers were required for Case B.

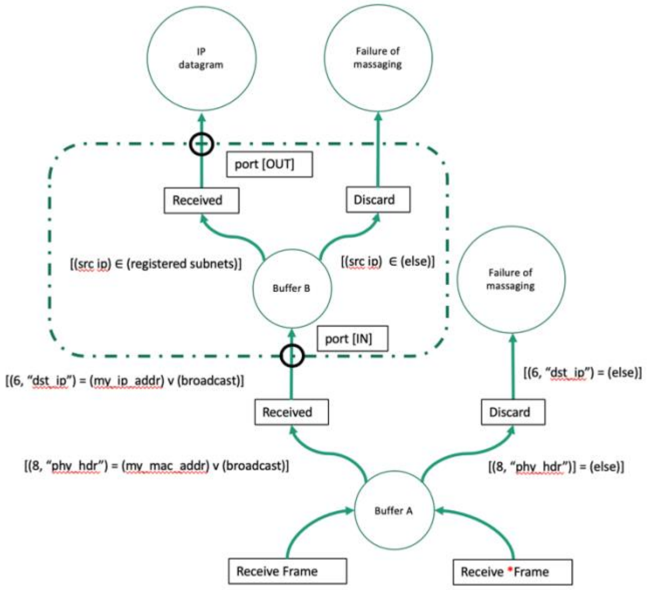

Fig. 9 Introducing a constraint in a Network layer

VII. Lessons learned

Modeling of ICS's communication along with layered architecture of protocol stack using Petri Net and its extensions is capable of identifying contaminated message elements. I understood that I could extract risks many ICS communication protocols might have by modeling those protocols and attack scenarios.

If contaminated communication elements could be identified, those elements could be selectively excluded by constraining mechanisms. At the moment, I assumed that most of contaminating mechanisms for ICSs could be offered by existing IT products or its modified ones, such as zoning by firewalls.

VIII. Future work

Up to Layer 4, TCP/IP protocol suite, I will try to model the protocols suite in more methodologically correct manners using Petri Net and its extensions.

Modbus/TCP, OPC/UA, CIP have many distinctive protocols in ICS communications, and most of them have unique specifications. That is why it is difficult to generalize them all in one model. Therefore, I will try to create a reference model along with best practices that many organizations are offering, such as NIST SP800-82.

When a proposed reference model is created, I would analyze known ICS communication protocols along the model and try to extract risks and potential weaknesses of each protocol. And then I would try to find out necessary constraints for them.

To prove a relevance of my reference model, I will analyze the same ICS accidents with other established risk assessment methods, and will try to compare the difference of the results of analysis.

It is OT engineers who can analyze risks on connected ICSs and presume outcomes by interfering in control processes. Therefore, I will propose an ICS communication model to make it easy for OT engineers with IT engineers to extract potential risks of connected ICSs and estimate losses of possible outcomes. This work will definitely contribute to the future connected society.

[1] FIREEYE， “Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure”， https://www．fireeye．com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton．html

[2] SANS， “Secure Architecture for Industrial Control Systems”， https://www．sans．org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327

[3] IPA， ”組込みシステムの安全性向上の勧め（機能安全編）”， https://www．ipa．go．jp/files/000005118．pdf

[4] Eric J． Byres， Matthew Franz， Darrin Miller， “The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems”， https://www．researchgate．net/publication/228952316_The_use_of_attack_trees_in_assessing_vulnerabilities_in_SCADA_systems

[5] Wolfgang Reisig， “Understanding Petri Nets: Modeling Techniques， Analysis Methods， Case Studies”， Springer， ISBN-10: 3662523078， ISBN-13: 978-3662523070

[6] Kurt Jensen， Lars M． Kristensen， “Coloured Petri Nets: Modelling and Validation of Concurrent Systems”， Springer， ISBN-10: 364242581X ISBN-13: 978-3642425813