Cyber Security Enhancement on MHPS Digital Analytics Platform for Power Plants

Hiroyasu ISHIGAKI
Mitsubishi Hitachi Power Systems (Japan)

Kazuyuki Misawa
Mitsubishi Hitachi Power Systems (Japan)

Abstract:

Today's increasingly digitized power plants benefit from improved access to advanced analytics and fleet-wide data correlations. However it brings us cyber security threats and concerns as well, we need to cope with those to utilize advanced data analytics platform. This paper describes the approach to this challenge taken by Mitsubishi Hitachi Power Systems (MHPS) that led to today's MHPS-TOMONI Analytics Platform.

This problem could be summarized as two parts, cloud and edge systems. This paper shows MHPS-TOMONI platform overview, new and old cyber security concerns, general solutions to them and actual solutions provided by MHPS on MHPS-TOMONI Analytics Platform.

Unfortunately there is no silver bullet for those cyber security concerns, so we have to take a lot of steady works to resolve it. We need to evaluate and asses own asset, plan necessary and sufficient actions and prioritize these actions, then begin.

I. Overview of MHPS Digital Power Plant Initiative (MHPS-TOMONI)

The Digital Power Plant is an all-encompassing "big picture" concept that became commonly discussed about 10 years ago. Strategic thinkers across the power industry have increasingly been talking about the Digital Power Plant -- promoting its promise, current status and prospects for its full implementation. It has been a multi-year journey to today's Digital

Power Plant, and each step along the way has been enabled by what at the time were the latest advancements in digital and communications technologies, and always driven by evolving needs of power plant owners and operators. MHPS began the journey to the Digital Power Plant over 20 years ago, with major milestones including the heavily instrumented verification combined cycle power plant at the Takasago Machinery Works in Japan, commissioned in 1997 and dispatching into the Kansai Electric grid, and the implementation of Remote Monitoring and Diagnostics Centers (RMC) in 1999 and 2001. More recently, many data-driven digital solutions have been applied to improve the reliability, flexibility and performance of power plants around the World.

At MHPS the result of leveraging those steadily advancing digital and communications technologies is called MHPS-TOMONI. TOMONI means "Together" in Japanese and signifies heavy involvement with power plant owners and operators in a collaborative manner to most effectively unleash the potential of power plant digitalization. It combines digital technology with extensive equipment designer and equipment user collaboration and comprehensive total plant design, operation and maintenance experience. The MHPS-TOMONI concept continues to provide new opportunities for flexible operation, performance improvement, and optimized power plant O&M, with the ultimate objective of maximizing total plant reliability and productivity.

MHPS-TOMONI is going to provide Monitoring, O&M Support, Advanced O&M and Autonomous Operation with customer real/historical plant data. It has various applications and services to realize the Digital Power Plant with OSISoft PI system as core system running on Microsoft Azure cloud and edge based systems.

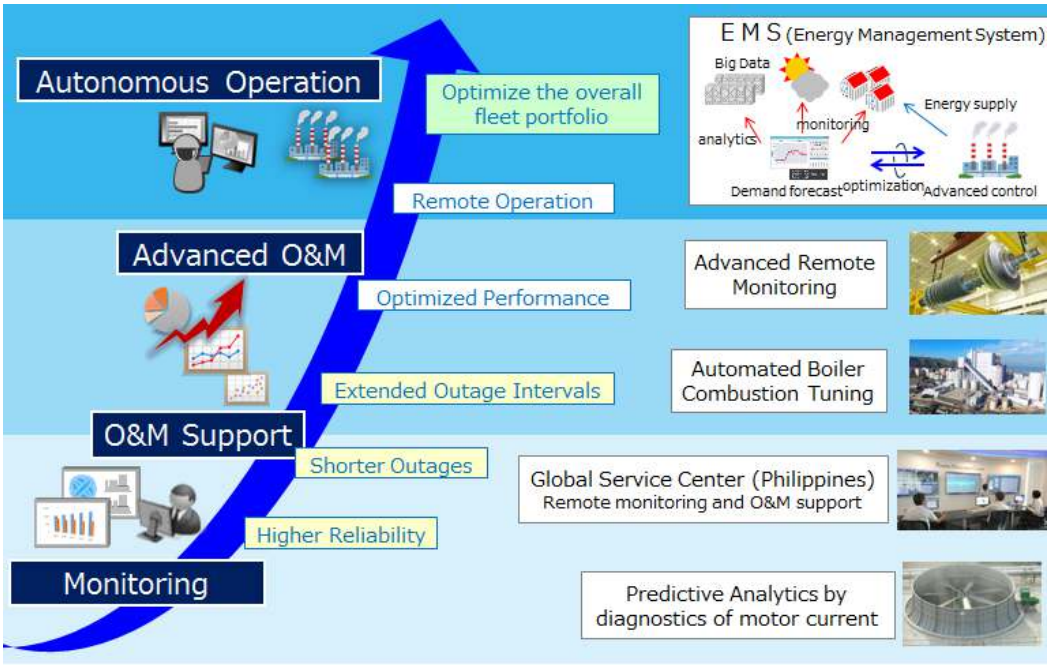

Figure 1: MHPS-TOMONI Roadmap

The figure 2 shows examples of those services. 24/7 Remote monitoring service by plant expert operators in multiple centres, Predictive analysis application, AI enhanced boiler optimal tuning tool, Plant performance analysis, KPI analyst web application. Those applications are designed for gas turbine combined cycle as well as coal fired conventional plants.

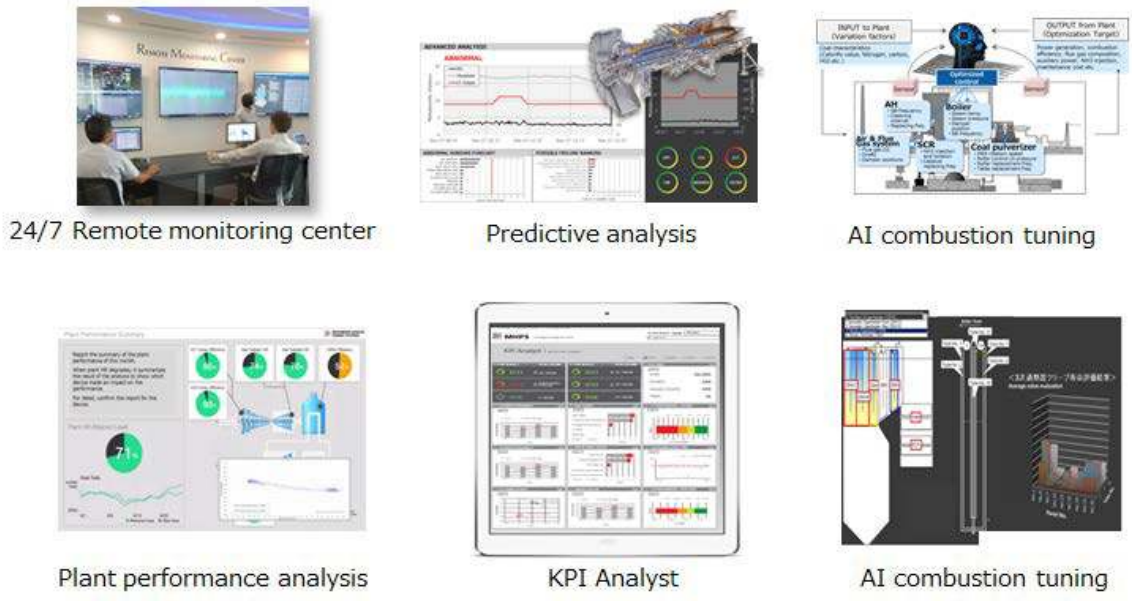

Figure 2: MHPS-TOMONI Services

MHPS-TOMONI platform is constructed on Microsoft Azure cloud. It is built as IaaS with Microsoft authentication system (Azure Active Directory), online management system and other advanced tools. At the core of the system, OSISoft PI system is configured as data historian and analysis platform. The platform is connected with power plants with simple HTTPS connection on Internet or PI interface on IP-VPN, Internet-VPN connection for larger size data collection. MHPS-TOMONI users use the system through remote client applications running on the cloud or standard web applications.

Figure 3 shows this MHPS-TOMONI system architecture.

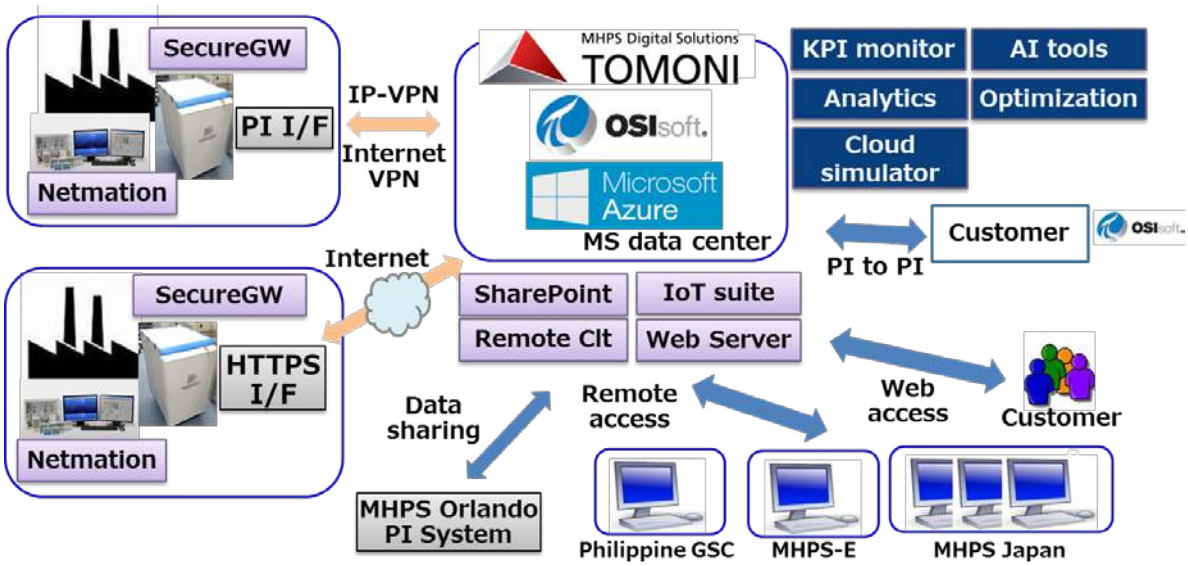

Figure 3: MHPS-TOMONI system overview

II. New and old tasks for digital power plant cyber security

1. Security risks to utilize advanced digital services

Though a lot of users understand necessity and benefit of those digital services described in the previous chapter, many of them feel vaguely insecure about those systems. It makes them to hesitate to start utilizing those services.

- Could anyone steal our precious plant data on Internet? - data breach
- Isn't it risky to connect our power plant to outside? - cracking, penetration, plant shutdown

However, in many cases, they do not know clearly what risk is and where those risk exist. In this chapter we find what kind of actual risks are there to utilize those digital services.

2. Concerns of using cloud services

On those power plant digital services, main data source is power plant operational data. Those are very important for power plant owners to compete in their business domain, operation pattern, power generation efficiency etc. Storing those important data on cloud service, in other words, on Internet might lead to data breach risk of company's precious intellectual property.

Indeed there are expected risks on cloud services as follows.

- Malicious hacker could penetrate to the cloud to steal those data
- Operators inside the cloud data centre steal those data using USB stick

However those are considered as risks not only on cloud services. Those have been residing in on premise systems as well. There is data breach risk caused by malicious access or internal incident using USB sticks. This means we have to cope with those security risks regardless we use cloud services or on premise system.

3. Concerns of connecting power plant to outside

Power plants in past were totally segregated from outside. Plant control system was not connected to any systems as Internet or even customer's information system.

The segregation of the plant control system was regarded as the most effective cyber security measure to take against intrusion or attack from outside so we did not need to consider any other countermeasures. Recently power plant control system is expected to connect with enterprise information system, and it has started connecting with cloud system or other power plant systems. The situation is getting more and more complex. On the other hand, cyber security measures of plant control system have not been changed significantly from the segregation era. We need to come up with "different cyber security counter measure" from past assuming there exists connection to outside as default.

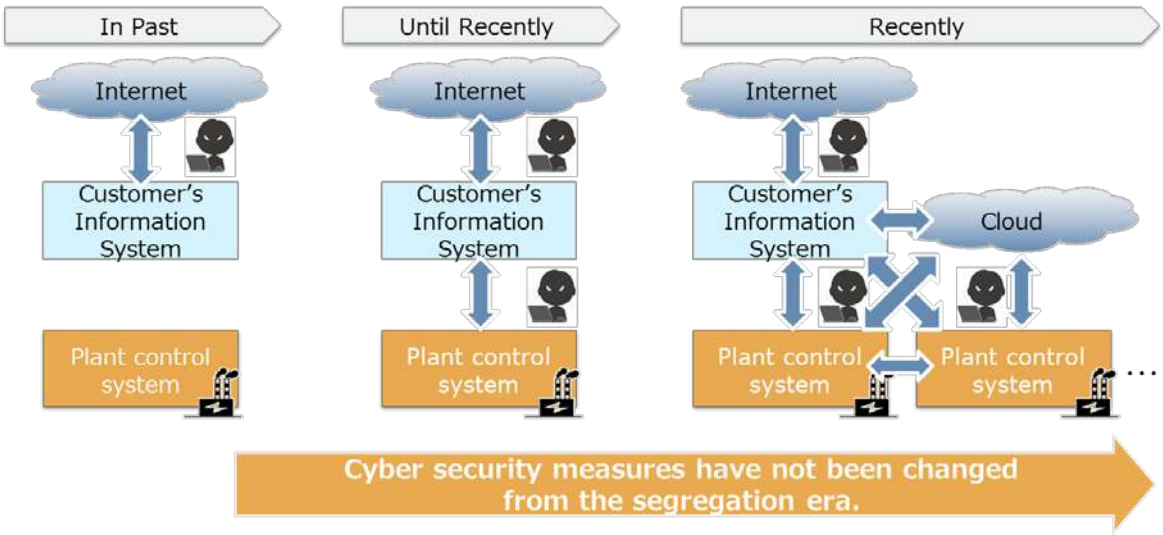

Figure 4: Changing environment between power station and outside

4. Cyber security risks on power plant control system

As described in the previous chapter there are growing concerns on utilizing advanced digital services. Meanwhile there have been known potential risks on power plant control system. This chapter shows real risks and problems happening in power plant.

It is often observed that adopted cyber security measures are not working effectively or those countermeasures are considered as difficult to take for plant control system. The below shows example of those security risks.

1) Inappropriate use of USB , unlocked cabinets

Since power plant control system was totally segregated from outside in past, operators and maintenance personnel were not required for high cyber security literacy.

As those mind set are still existing, inappropriate management for cyber security are often observed, such as use of personal USB device or unlocked control panel cabinet etc.

2) Sharing user ID, lack of proper ID lifecycle management

In central control room of power station, multiple PCs are usually shared by plant operators and those are displaying monitoring screens continuously. Those PCs are logged on with shared user ID. Sometimes those ID and password are written on paper on wall. Lifecycle management of user ID are hardly executed such as revoking a user ID of quit employee.

3) Difficulties of version up and applying security patches

Power plant control system is usually difficult to stop due to demand of continuous power generation. It is a risk that applying security patches in timely manner is difficult. It has also very long life span compared to standard IT system. It causes old operating system are used continuously even after expiration of OS vendor support.

5. Actual incident case study

In power plants, those security risks have already caused real security incidents all over the world. It is owing to characteristics of operation and system of power plant control. The examples below are real cyber security incidents.

1) Stuxnet caused by USB stick (2010/11)

Impact :

At uranium enrichment plant in Iran, centrifugal separator were destroyed

Overview :

An infected USB stick was brought into the facility by an employee

Duplicating worms on Windows PCs in the facility

Penetrating the control system using zero-day vulnerability

Modifying target control system software to control the centrifugal separator illegally

Lessons:

Above of the many cyber security issues, at least the USB stick should not be used inside the facility.

2) Illegal use of user ID by retired person (2010/2)

Impact:

Illegal start/stop operation at remote automobile centre in Texas

Overview:

A retired person accessed remote automobile management service with his colleague ID

He operated automobile using the system as start/stop or disable horn

Though his ID was disabled after his retirement

Lessons:

He should not know user ID and password of his colleagues. If shared user ID was used and its password was not changed at his retirement, security risk would rise higher.

3) Ransom ware infection caused by not applied security pathes (2017/6)

Impact:

Monitoring system for the dismantled Chernobyl nuclear power station was forced to manual mode

Overview:

Ransom ware "Goldeneye(Notpeyta)" was infected in the system

A vulnerability which was used by the malware was same as used by famous Wannacry.

Its security patch was already released on 2017/3.

Lessons:

If proper security patches were applied to the system on timely manner, the infection would not happened.

6. Cyber security risks residing in power plant control system should be considered

As explained above, risk of cyber-attack to power plant control system is growing bigger and bigger. The reasons are summarized as follows.

1) Power plant control system is changed to "connected" to outside comparing to segregated environment in past. It is because power plants have started using advanced digital services.
2) Power plant control system has been adopting standard OS or other middleware/protocols instead of proprietary vendor technology. It makes those systems easier to attack by malicious people
3) Malicious attacks have been getting more sophisticated as APT(Advanced Persistent Threat) or using distributed high capability open source tools.

To cope with those threats traditional cyber security mind set and measures are considered as not sufficient. Power plant has to handle new cyber security risks for cloud services etc. as well as potential problems that have been existing long time in control system.

III. Required cyber security measures for digital power plant

1. Overview

In the previous chapter, we have described new cyber security risks when utilizing advanced digital services and potential problems residing in power plant control system.

To handle those risks with reasonable costs, we need to plan and execute necessary and sufficient countermeasures for them. This chapter shows those countermeasures with categorizing three areas as cloud, perimeter between cloud and power station and power station itself.

2. Utilizing cloud services with effective security measures

On advanced digital services, power plant process data and additional information are extracted, processed and stored, in many cases, in cloud services.

We need to focus on the following cyber security points in this case

- Physical security : robust facility and management system
  disaster prevention, entry management, lock system, security camera etc.
- Logical security : advanced tools and management
  Authentication, credential, encryption, monitoring system etc.
- Guidelines : following several cyber security guideline
  NIST SP800-53, ISO27017, etc.

Major cloud services are performing necessary cyber security countermeasures on it continuously. Those cloud services are usually providing advanced tools to help cloud users to achieve the above.

On cloud system, with those tools, cloud users are able to perform required security counter measures. In contrast user themselves have to develop and maintain those measures/tools if they choose on premise system. It would require more man power, cost and period.

Thus we should choose cloud service where "sufficient and necessary" cyber security operation and support tools are ready.

3. Gate to prevent penetration from outside

To utilize advanced digital services, it is required to connect to outside for sending data to cloud systems. It is very important to create robust cyber security perimeter between power station and outside to prevent illegal access which would lead cyber security incidents such as data exposure or cyber-attack to power station.

For transmitting data from power station to cloud services, it is not necessary to access inside of power station. A good measure is limiting data flow to only coming from power station. If it is realized as physical one way data flow, robustness is practically very high level.

With firewall which are used in standard IT system, there would be still some possibility to be attacked using equipment vulnerability etc.

4. Necessary and sufficient cyber security countermeasures for whole power plant

As work, operation and systems are varying on each power plant, required cyber security measures also differ for each plant. Firstly we have to get a comprehensive view of target power station, find where risks exist and plan how to cope with them.

1) Bad practice

   In spite of adopting high quality cyber security solutions and starting security operation team, there still happen security incidents.

- Not knowing where cyber risks exist in power plant
- Adopting retail security solution without understanding what effect is for power plant

- Executing security measures without appropriate planning

Those might result in non-used expensive security appliance, ignored security rules or disregarded security team

Then how can we plan and execute effective cyber security measures for our power plants?

2) Good practice we recommend

Firstly understanding current cyber security issues on whole power plant, and making efficient action plans to achieve necessary and sufficient measures

- Understanding overall security risks
  Find where security risks exist with having comprehensive view of power plant
  Instead of detail security analysis, it is important to get security overview
  Not only system or equipment, but also management, organization, rules and processes
  For example illegal use of USB stick cannot be found only from system point of view

- Planning necessary and sufficient actions
  Make "necessary and sufficient" countermeasures for found risks
  Good way is to come up with mitigating or avoiding those risks
  Focusing on coping with what we are not doing. Not blushing up what we have been doing
  Reconsidering current work flow or process could be same value as expensive security appliance
  Create practical countermeasures which could be done by current power plant personnel

- Prioritizing those actions
  Planning priorities of those measures to execute in proper order
  Good action plans are not always leading to best results
  To decide priorities, it is important to see what risks, how important, where exist, difficulties or how much cost required.
  First for high risk without any actions taken yet, then risks already coped with
  Low cost than expensive one
  Important to make most efficient order of actions within limited resources

Those three steps will lead to the best effective execution plan of "necessary and sufficient" cyber security actions

Even though we could follow the action plan, it is better to get feedback and modify the plan because environment or timing would affect those cyber security risks

Ex. Change of company organization, added systems, unexpected new cyber security risk

There is no silver bullet for what everyone is struggling. Only steady work could be solution as understanding current status and taking planned actions.

5. Control system security regulations and guidelines

As growing of cyber security incidents on critical infrastructure, security regulations and guidelines for control systems have become popular. Those guidelines are usually categorized to management layer, system layer and component layer. For system and component layers, it is important to choose appropriate system and appliance vendors. In contrast it is required to plant owners to cope with the management layer.

As many guidelines are becoming popular, the below shows important ones

- IEC62443 series : global standard as general common criteria
  Created as generic security standard from various rules in various industries
  This series covers all layers as management(IEC62443-2), system(IEC62443-3) and component(IEC62443-4)
- Power industries
  NERC CIP : power utilities standard in united states FERC firstly approved ver.1 in 2008 the latest one is ver.6 and operated with real penalty
  In Japan “Security guideline for power plant control system” was released in 2016 referring to NERC-CIP standard

Various situations in countries, regions and industries should be considered when making security action plans.

Also those guidelines could be good resources as baseline to grasp security risks because those have exhaustive necessary security countermeasures.

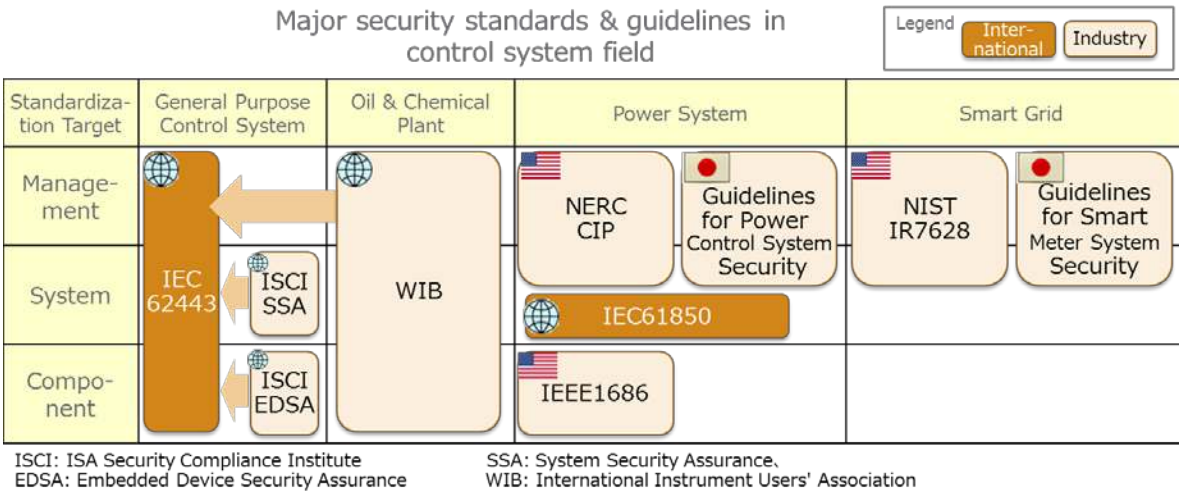

Figure 5: Main cyber security standard for control systems [ref5,6]

IV. Cyber security solutions of MHPS-TOMONI

1. Overview

In the previous chapter we explained necessary cyber security actions for power plant incoming digital era. MHPS-TOMONI provides supporting services and solutions covering from power plant control system to cloud services.

- MHPS-TOMONI Cloud : Secure cloud environment for advanced digital services
- Netmation secure gateway : One way data gateway
- MHPS-TOMONI cyber security planning : Supporting service for power plant security action palnning

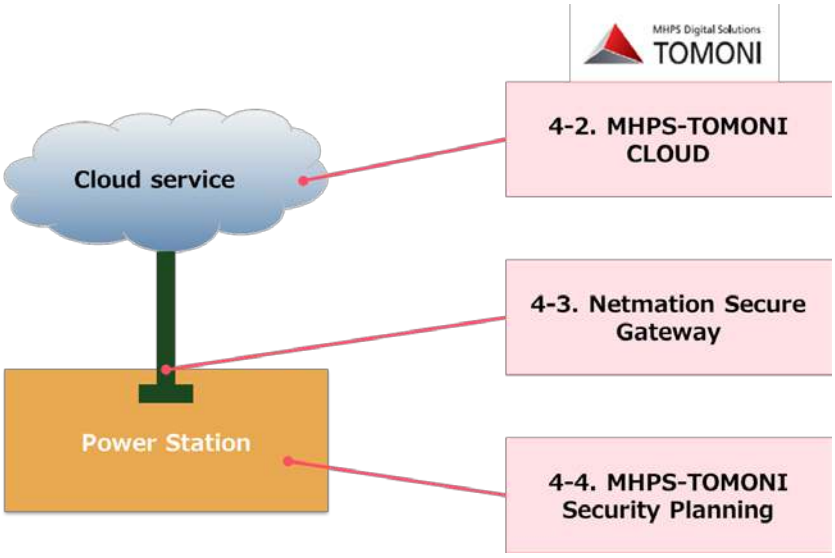

Figure 6: MHPS-TOMONI Cyber security solutions/services

2. MHPS-TOMONI CLOUD

MHPS-TOMONI CLOUD is located on Microsoft Azure cloud service, which applies plentiful security actions based on ISO27001, 271017 guidelines etc.

- Physical security : robust facility and management
  Disaster prevention, in/out control, locking system, monitoring camera etc.
- Logical security : Advanced security systems, services and tools
  Authentication, credential, encryption, monitoring system

We are effectively using cyber security tools equipped in Azure to maintain extremely high MHPS-TOMONI security level

- OMS(Online Management Suite) : Detecting security incidents, analysing influences and suppressing security incident damage
- Security centre : Detecting and mitigating malicious behaviour or malware with advanced technologies such as machine learning algorithms
- Azure Active Directory, multi-factor authentication etc.
  Proven authentication system with not only user ID and password

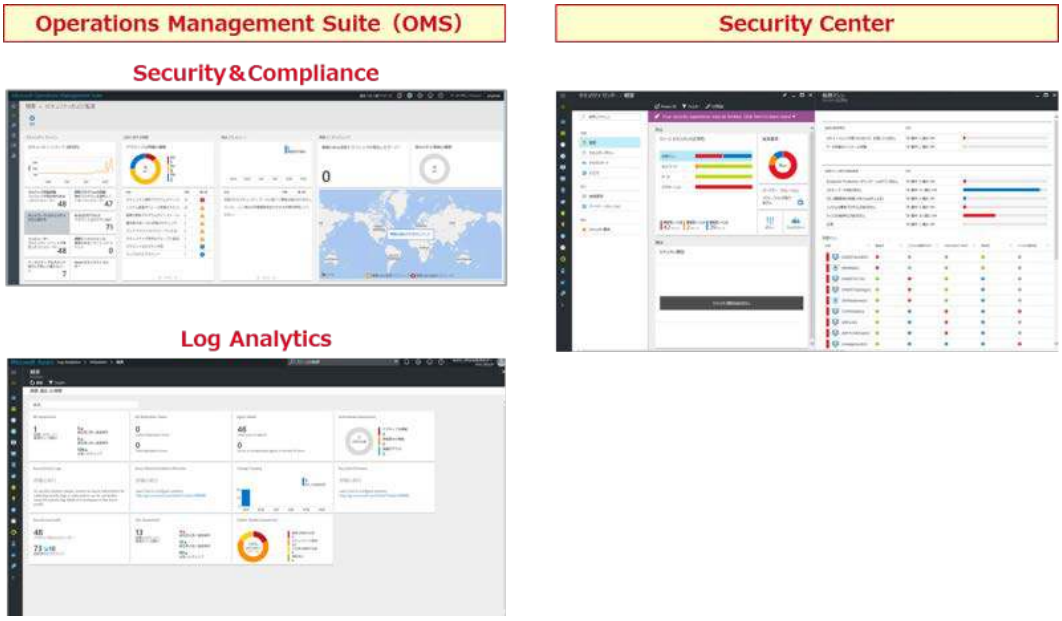

Figure 7: Various security tools on Microsoft Azure

3. Netmation Secure Gateway

Netmation Secure Gateway is designed by MHPS to provide flexible secure data access to power station with reasonable cost. It realizes physical one way data flow from inside to outside.

- Preventing intrusion to power plant
  One-way optical communication combined with non-routable serial communication to make it physically impossible for intrusion to plant network from outside.
- Preventing data leakage
  For data transmission to the cloud server, one to one security authentication using digital certificates is being used and it makes data leakage extremely difficult.
- Encrypting transmitted data
  SSL/TLS encryption makes it extremely difficult for eavesdropping and data exploitation.
- Transmitting through Internet
  No dedicated line or VPN needed. Netmation Secure Gateway achieves strong security using standard Internet connection

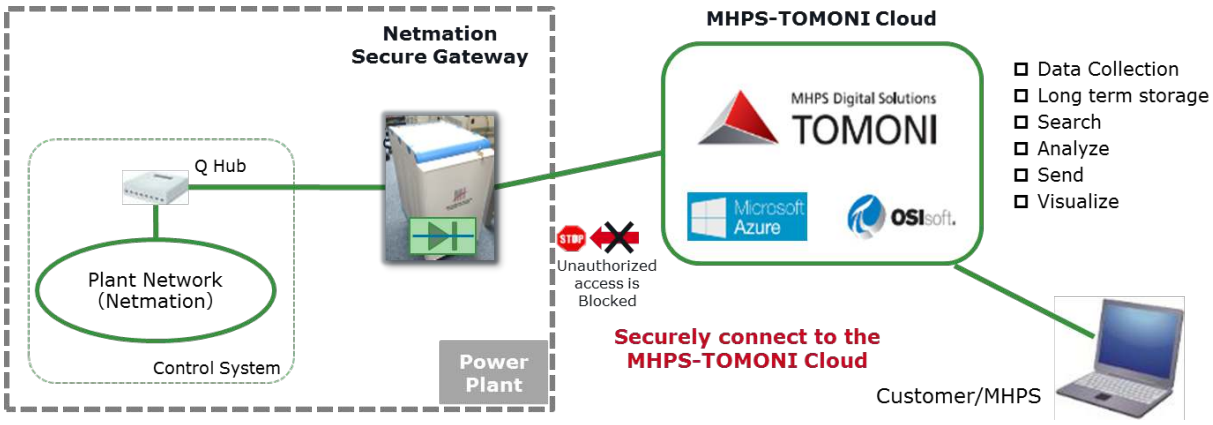

Figure 8: Netmation Secure Gateway

4. MHPS-TOMONI Security Planning

As described in the previous chapter, first step to achieve good cyber security is understanding current security overview in power plant and planning security actions with considering priorities based on necessity and cost.

MHPS-TOMONI Security Planning provides this action plan with following steps.

Step1: Importance analysis of power plant systems

Evaluate power plant systems from CSMS point of view

Step2: Assessment of current status and analysing risks

Assess current security status based on global standard and guidelines
IEC62443-2-1, NERC-CIP ver.6 and Japanese security guideline for power plant control system are used for this purpose

Step3: Making security measures

Making practical security countermeasures for current status

Step4: Creating action plan

Prioritizing countermeasures with considering system importance, vulnerability, cost, difficulties
, then creating final security action plan

Those steps could be done only by experts of power plant and MHPS is the one based on long experience as main equipment OEM and EPC contractor. We are providing those services from customers standing point.

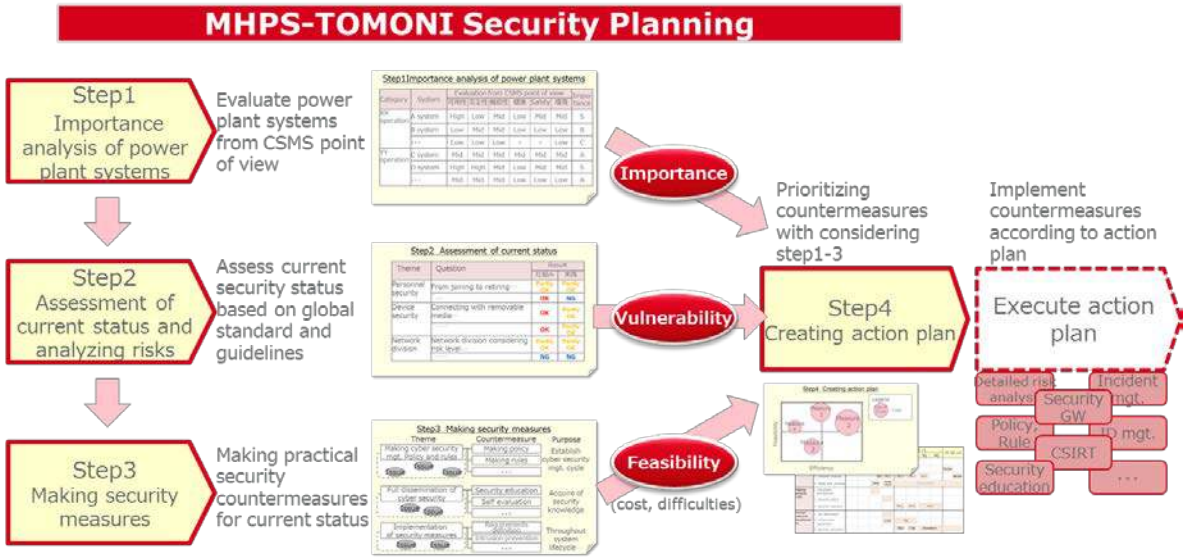

Figure 9: Overview of MHPS-TOMONI Security Planning

V. Conclusion and Future vision

1. Cyber security risks and actions for digital power plant

This paper described new security risks coming from advanced digital services and existing potential risks of power plant. Solution was also explained for those new and old risks.

(1) New cyber security risks on utilizing advanced digital services

- Concerns for cloud services

Answer: Utilize appropriate and robust cloud service with utilizing their capability

- Concerns of connecting power plant to outside

Answer: Use security devices which prevents penetration from outside absolutely

- Potential cyber security risks which have been existing from past

Answer: Understanding overview of systems and risks, making actions, prioritizing them and developing action plan

2. Cyber security solutions of MHPS-TOMONI

MHPS-TOMONI provides necessary and sufficient security solutions and services for power plant customers. Those solutions are based on MHPS expertise, experiences as OEM and EPC.

- MHPS-TOMONI Cloud : Secure cloud environment for advanced digital services
- Netmation secure gateway : One way data gateway
- MHPS-TOMONI cyber security planning : Supporting service for power plant security action palnning

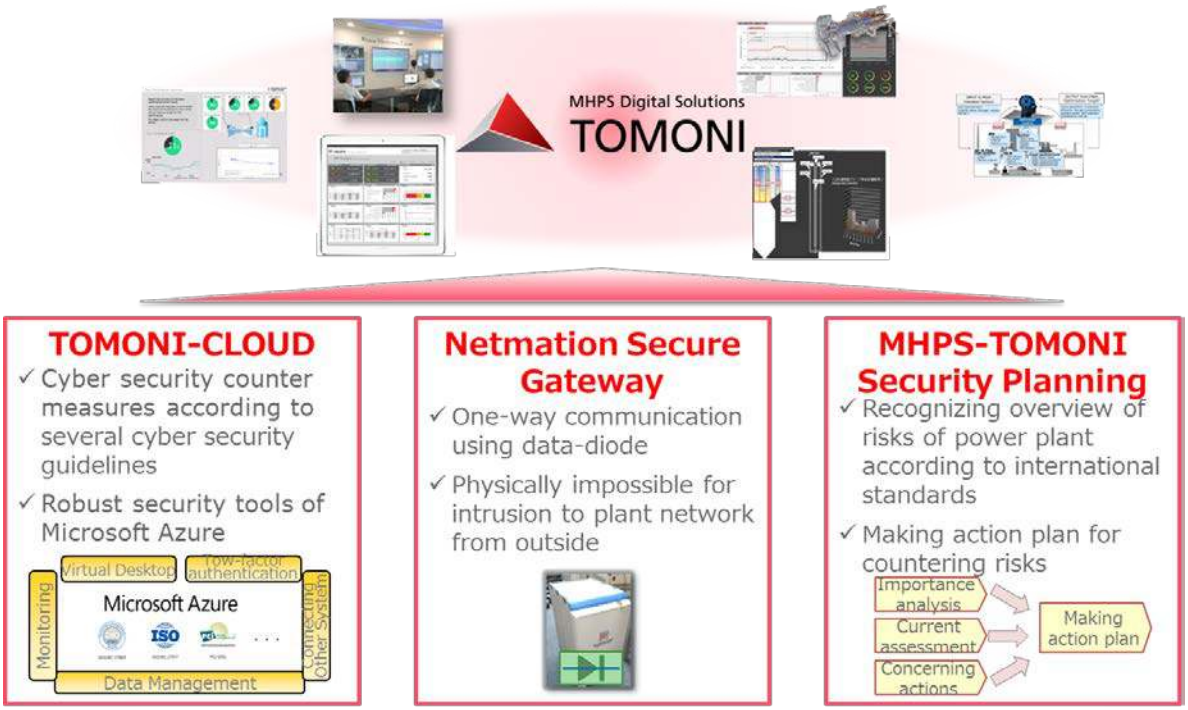

Figure 10: MHPS-TOMONI cyber security solutions and services

References

1. Michael Holloway. 2015, "Stuxnet Worm Attack on Iranian Nuclear Facilities", Submitted as coursework for PH241, Stanford University
2. D. Kushner. 2013, "The Real Story of Stuxnet," , IEEE Spectrum 53, No. 3, 48
3. Kevin Poulsen. 2010, "HACKER DISABLES MORE THAN 100 CARS REMOTELY", WIRED
4. NICOLE PERLROTH, MARK SCOTT and SHEERA FRENKEL. 2017, "Cyberattack Hits Ukraine Then Spreads Internationally", The New York Times
5. Hideaki Kobayashi. 2013, ”Overview of IEC62443 and authentication”, Control System Security Center

6. Yasunori Irisawa. 2013, “Control system security standard”IEC62443”, Nikkei Technology online