Expertise
and insight
for the future

Miska Koskelo

OT-asset CMDB Solutions

Metropolia University of Applied Sciences

Bachelor of Engineering

Electrical Power Engineering

Bachelor's Thesis

20.5.2020

Author Title Number of Pages Date	Miska Koskelo OT-asset CMDB solutions 27 pages + 1 appendix 20th May 2020
Degree	Bachelor of Engineering
Degree Programme	Electric engineering
Professional Major	Electrical power engineering
Instructors	Tomas Nyström, Service Manager, Nuclear Eero Kupila, Senior Lecturer

The assets of most industrial control systems are not well-documented and therefore the implementation of a CMDB system is essential for secure and safe operations. The line between IT and OT is not always clear. Therefore this thesis aimed to define IT and OT and find the most suitable system for the management of OT-assets.

A survey was carried out to create an outlook into the solutions used currently in the industry by interviewing experts in the field. In addition an online search for asset management systems on the market was carried out.

The results confirmed the need for a flexible, versatile and user friendly system. At the same time suitable solutions were found through the survey and the online search and product analysis. A suitable solution was found and suggested for future implementation in the company. The definitions of IT and OT were carried out based on current literature.

Keywords	Operational Technology, Asset management, CMDB

Tekijä Otsikko Sivumäärä Aika	Miska Koskelo Teollisuuden automaatiojärjestelmien konfiguraatiohallintatietokantajärjestelmäratkaisut 27 sivua + 1 liite 20.5.2020
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	sähkötekniikka
Ammatillinen pääaine	sähkövoimatekniikka
Ohjaajat	Service Manager, Nuclear Tomas Nyström lehtori Eero Kupila

Insinöörityössä oli tavoitteena määritellä tietotekniikkajärjestelmien ja automaatiojärjestelmien omistuksien väliselle harmaalle alueelle selvä raja ja löytää Fortum Oyj:n automaatiojärjestelmille mahdollisimman toimiva sovellus konfiguraatiohallintatietokantajärjestelmän ylläpitoon. Suurimmaksi osaksi teollisuuden ohjausjärjestelmiä ei ole kunnollisesti dokumentoitu, jonka vuoksi konfiguraatiohallintatietokantajärjestelmän käyttöönotto on välttämätöntä turvallisuudelle ja toiminnan turvaamiselle.

Työssä toteutettiin kysely haastattelemalla alan asiantuntijoita nykytilan ratkaisumallien selvittämiseksi. Haastatteluiden tulosten lisäksi tehtiin verkkohaku markkinoiden järjestelmätarjonnasta. Haastatteluista ja verkkohausta saadut tulokset taulukoitiin projektiryhmän kanssa laadittujen haluttujen ominaisuuksien mukaisesti. Tulokset analysoitiin ominaisuuksien löytymisen perusteella. Määrittely tietotekniikkajärjestelmien ja automaatiojärjestelmien välillä toteutettiin pohjautuen kirjallisuuteen.

Tulokset vahvistivat, että joustava, monipuolinen ja käyttäjäystävällinen järjestelmä on tarpeellinen. Kyselyn ja verkkohaun perusteella löytyi ehdotettava ratkaisu yrityksen tulevaa käyttöönottoa varten. Ratkaisun perusteella projektiryhmä tekee päätöksen järjestelmän käyttöönotosta.

Avainsanat	Operational technology, konfiguraatiohallintatietokanta

Contents

List of Abbreviations

1 Introduction 1

1.1 Background and Problem Definition 1
1.2 Project Scope 2

2 Theoretical Background 2

2.1 Purdue Reference Model 3
2.2 Defining Information Technology 4
2.3 Defining Operational Technology 6
2.3.1 SCADA 7
2.3.2 DCS 9
2.3.3 PLC 10
2.3.4 Field Devices 11
2.4 Asset Ownership 11

3 Data Collection 12

3.1 Ideal System Features 12
3.2 Questionnaire 13
3.2.1 System Identification 14
3.2.2 Process Management 14
3.2.3 Asset Discovery and Documentation 14
3.2.4 Data Storage and Security 14
3.2.5 Asset Ownership 15
3.2.6 Modifications 15
3.2.7 User Satisfaction 15
3.3 System Product Analysis 15

4 Results 16

4.1 The Line Between IT and OT 16
4.2 Questionnaire Results 16
4.2.1 Manual CMDB Governance System 17
4.2.2 Microsoft Excel 17
4.2.3 ServiceDesk Plus 19

4.2.4 Claroty 20
4.2.5 Kaseya Virtual Administrator 21
4.3 Internet Searches 22
5 Discussion 24
5.1 Conclusions 24
5.2 Recommendations for Project Implementation 25
5.3 Ethics and Reliability 25
References 26
Appendices
Appendix 1. Questionnaire

List of Abbreviations

BT	Business Technology
CMDB	Configuration management data base
DCS	Distributed Control system
IoT	Internet of Things
IT	Information Technology
ITIL	Information technology infrastructure library
ITSM	IT service management
OT	Operational Technology
PLC	Programmable Logic Controller
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition

1 Introduction

1.1 Background and Problem Definition

The network of devices used to control industrial plants is called an industrial control system (ICS) network or an operational technology (OT-) network. Assets, or items of value, in those networks are often not documented to the level of detail and scope as would be needed to gain the satisfactory level of control. In general the documentation of OT-assets is not implemented as well as the documentation of assets used for sending and storing information, or information technology (IT-) assets, since many ICS were designed and implemented long before the era of digitalization and the idea of the internet of things (IoT). (Perelman 2016.)

With the evolution and modernization of the ICS it is evidently essential to keep its documentation of hardware and software components up to date. Maintenance and modernization projects are generally planned thoroughly, however if the plans are based on outdated documentations of the system, the project cannot be executed successfully. An up to date configuration management data base (CMDB) is necessary for operating and modifying of the ICS safely.

Moreover the data traffic in ICS used to be limited to factories or plants' inner network, that was closed off of everything outside the physical site. The centralization of the control equipment into remote control stations, demands data traffic from one private network to another via tunneling through a public network, such as the internet. This creates vulnerabilities and could make ICS networks targets for cyber-attacks. This problem becomes evident, when the vulnerabilities of outdated OT-elements are exploited in order to wreak havoc in industrial systems. Without a proper asset management system and an up to date CMDB neither the asset owners nor the corporate security can guarantee the security of the ICS network. (Green – Krotofil – Hutchison 2016: 93-101.)

A proper CMDB is essential for a safe and secure operation, maintenance and development of an ICS, because without the knowledge of the components of a system, the reaction time to any unforeseen incidents is slow. This can lead to monetary, safety or

quality deficits in the production. Here, I present different aspects and definitions of IT- and OT-assets and describe a suitable solution for the CMDB governance of OT-assets.

1.2 Project Scope

This thesis work was done for the Business Technology (BT) department of the energy company Fortum Oyj. The terms IT and OT are defined at the beginning of this thesis, in order to understand the differences between the two. Physical assets are divided between the two based on literature research and for example the Purdue reference model. The information for this was collected from literature and online articles on ICS security, written by professionals of the field.

After creating a theoretical base for the thesis work, the situation in the company was researched, since the views between theory and practice may differ among different business units of the company. This information was gathered using a questionnaire, which was created in collaboration with the OT-asset owners, BT-coworkers and the corporate security unit. The questionnaire was sent to the OT-asset owners of Fortum power plants and other companies' ICS professionals to create an insight into different industry branches. The questionnaire results were anonymized and collected into a tabular for visualization of the results.

This thesis also creates an insight into the possibilities of managing OT-assets and intends to find the best management solution for Fortum based on the literature and online search and the questionnaire results. The results serve as a guideline into the project to create a companywide directive on how to manage the assets, if this is proven to be possible.

The objectives in this thesis work were to 1) clearly define IT and OT, 2) create an insight into the governance alternatives of OT-assets and 3) suggest the most suitable governance alternative to be introduced for Fortum.

2 Theoretical Background

Generally assets cannot be categorized into IT or OT based on simply what they are, but rather on the network they are in. Some assets can only be found in one of the two.

hence it is clear, whether they are defined as IT- or as OT-assets. Other assets can be found to some extent on any network, hence they are in the gray area what they are defined as. (Weiss 2010: 33.)

2.1 Purdue Reference Model

A possible method for defining assets is through the Purdue reference model, which segments network levels within an enterprise network. Depending on their intended use IT- and OT-assets are allocated to these levels. The Purdue reference model (figure 1) was first introduced in the ISA-99 standard. It divides the network into the Enterprise Zone, the Demilitarized Zone and the Industrial Zone. The enterprise zone consists of levels 5 and 4, the 5th level being the outward facing enterprise network with the internet facing demilitarized zone (DMZ) and connection to the internet, and the 4th level being the local enterprise network. These levels are inhabited solely by IT-assets. The industrial demilitarized zone (IDMZ) between levels 4 and 3 is used to prevent direct data transfer from the Enterprise zone to the Industrial zone and vice versa. The Industrial zone consists of levels 3 to 0 of the Purdue reference model, where levels 2 to 0 can be considered as individual cell or area zones, that are controlled from level 3. (Ackerman 2017: 16-22.)

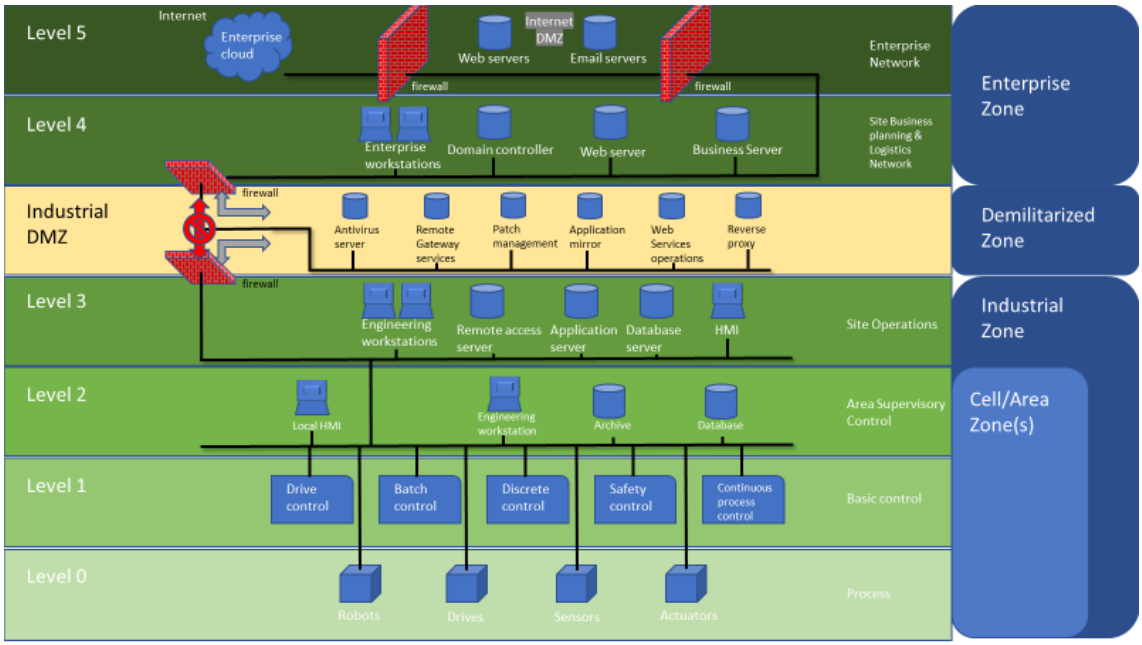

Figure 1. The Purdue reference model as introduced in the ISA-99 standard

The Purdue reference model can be divided into sub levels for more granular segmentation of the assets. A simplified interpretation of the Purdue reference model is, that the highest levels of it are purely ones and zeros, whereas lower levels are at the heart of the physical process.

2.2 Defining Information Technology

Information technology is “the science and activity of using computers and software to store and send information” (Cambridge Business English Dictionary, 2020). IT assets can be divided into physical assets, which range from handheld mobile devices to servers, and non-physical assets, such as user IDs, Active Directory (AD-) groups, software publications and virtual servers. These live mostly in the upper levels of the Purdue reference model. (Ackerman 2017: 19.)

IT systems are often well documented and follow predetermined procedures, when faced with IT issues. These procedures are defined in the Information Technology

Infrastructure Library (ITIL). The processes ensure that IT services are delivered to customers in the most efficient way. (Taylor – Cannon – Wheeldon 2007: 35.) Another purpose of the processes is to guarantee the data security within the network. Considering the CIA-triad (figure 2), IT systems prioritize the confidentiality, integrity and availability of data in that order. Confidentiality of data means, that the data is intended for restricted audiences only. Confidential data must not be able to be read or taken advantage of by unauthorized persons. Integrity of data implies, that the data has not been modified without authorization. Availability of data means, that persons with proper authorization to read and modify data can do so whenever convenient. The availability can be compromised for example with denial of service (DoS) attacks. (Samonas – Coss 2014.)

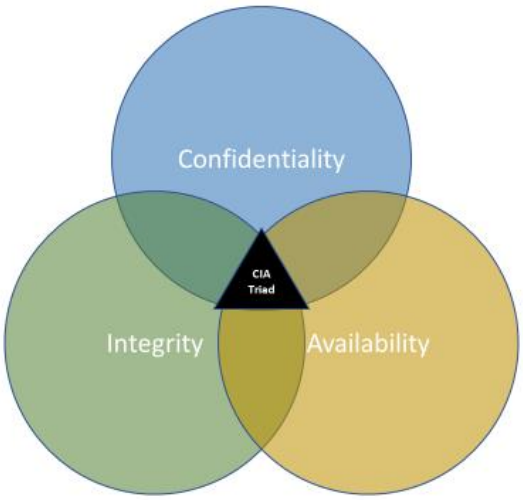

Figure 2. CIA Triad (modified from: Samonas – Coss 2014.)

In the IT world systems are evolving towards centralization and consolidation for lowering operational costs. The CMDB as an ITIL database documents all assets within an enterprises possession. A big difference between IT and OT is, that the main users of IT-assets are mostly humans, whereas the OT assets are generally used by computers or

other intelligent control devices. This distinction is to be considered when operating the different networks, since human error plays a greater role in one and lack of human common sense in the other. (Weiss 2010: 209.)

2.3 Defining Operational Technology

Operational technology (OT) consists of hardware and software assets, that monitor or control industrial networks. These assets live in the levels 0 to 3 of the Purdue reference model, where level 3 is the gray area between IT and OT, where the two share data. The lower the level gets, the clearer the assets can be defined as OT assets. Everything, that has power over a physical process can be considered to be OT rather than IT. (Operational Technology, Gartner Glossary 2020)

Another major difference between IT and OT is that OT assets follow the CIA triad philosophy as well, but prioritizes it in the reverse order: AIC. The availability in an OT-network connection is more important than the confidentiality of data. It is irrelevant, how many parties in an ICS receive a control command, as long as it is delivered to the correct asset and with the correct content. Hence the availability trumps integrity, which trumps confidentiality. (Ackerman 2017: 11.)

To ensure the availability of connections in an ICS, it might be beneficial for most of them to be built with a redundancy. Two physically separated cables run a loop, connecting all devices controlled by a single controller. An example of this is presented in figure 3, where actuator number 5 is malfunctioning and needs to be stopped. The controller unit addresses actuator 5 with the stop-command, which is sent via all available connections to all devices within the loop. The command can be ignored by the devices, that are not addressed by it, while actuator 5 notices that the command is intended for it and obeys the stop-command.

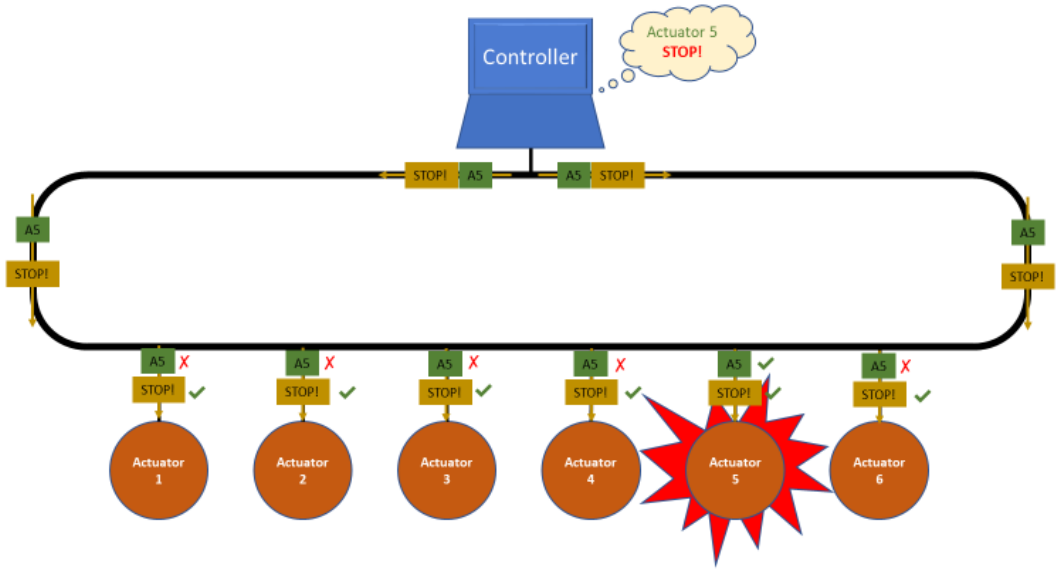

Figure 3. A redundant control network loop picturing AIC triad philosophy preferencing

Redundancy in the pictured control network in figure 3 permits the breaking of the connection at any one point in the loop and every device in the network still being able to communicate with any other. With this the availability of communication is improved. The integrity of data could be compromised, if bit errors occurred due to signal noise, interference or distortion, and changed the command or the addressee. The needed integrity of the signal can be ensured by adjusting the expected bit error ratio to the address or command size in bits. Confidentiality of data in the ICS-network in such scale can be considered inconsequential, as every device in the network is a machine. For a larger scale contemplation the types and components of industrial control systems must be considered.

2.3.1 SCADA

The Supervisory Control And Data Acquisition (SCADA-) systems are used for controlling large systems, that can be distributed over wide distances. A SCADA system is a wide network of ICS assets. The assets at the control center consist of a Human Machine Interface (HMI) and the SCADA Master, that serves as the main control unit of the

SCADA system (figure 4). The SCADA master can be connected to multiple Remote Terminal Units (RTUs) or Programmable Logic Controllers (PLCs), which are located at the sites controlled by the SCADA system. The RTUs or PLCs control the factory level equipment at the sites. They can also be controlled locally by HMIs, which mostly are dominant towards the SCADA master, since these can also control processes like emergency shut downs and other crucial processes, that require fast reacting. The SCADA master has a data storage for logging measurement data from the system, so that the process can be evaluated and optimized. (Weiss 2010: 8-16; Colbert – Kott 2016: 26-27.)

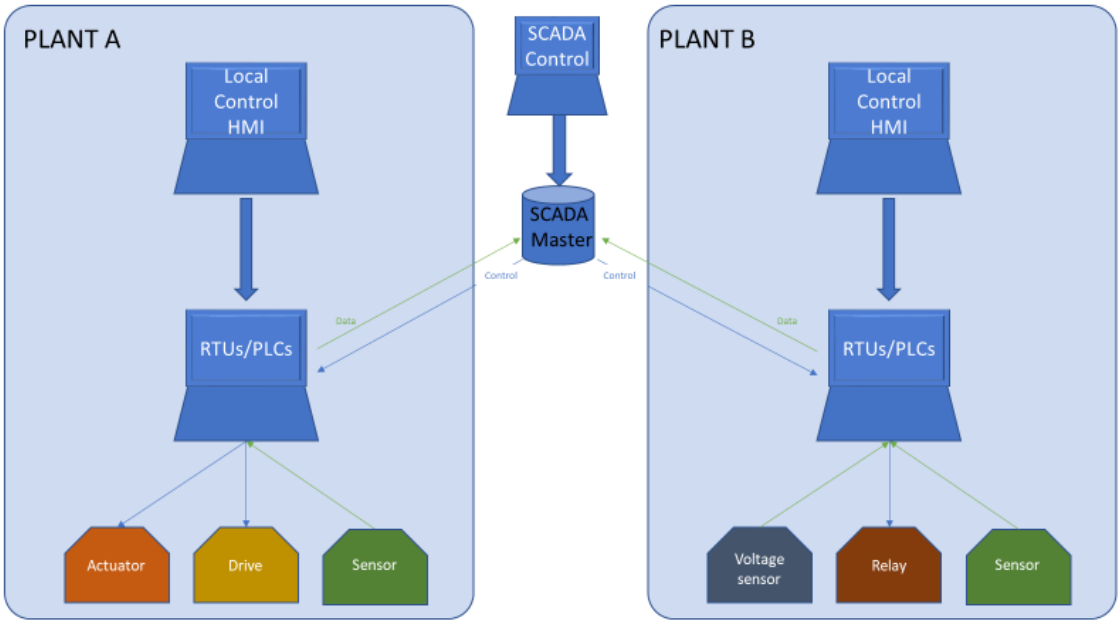

Figure 4. Basic structure of SCADA system

The communication between the centralized control station and the substations within a SCADA system is executed either via direct wiring of copper or optical fiber cable or wirelessly via radio communication. (Weiss 2010: 13) The SCADA system reaches from the process level (level 0) to the site operations level (level 3) of the Purdue reference model.

2.3.2 DCS

Distributed Control systems (DCSs) are, as the name suggests, systems, where the control and data acquisition are distributed to a number of processor units among the ICS devices within a plant. A DCS is used for continuous control of a larger or complex system, where different processes have relations with each other. (Weiss 2010: 16-18.)

The operator stations (OSs) are the HMIs of the DCS and control the processes. These are connected to the data servers, archives and engineering workstations via industrial Ethernet TCP/IP. Servers within the DCS manage the communication, like warnings or alarms from the process level to be visualized on the HMIs, or control commands from the OSs to the processors. Archiving servers store the process data for later use in process optimization or troubleshooting with production errors. The engineering workstations within a DCS are used for designing the hardware configuration of the field devices, programming the processor logic, by which the field devices are controlled, creating the HMI frontends of the OSs and administering the whole DCS (figure 5). Processors on the plant floor are connected to the servers, archives and engineering workstations via Ethernet TCP/IP or fiber optics. They control the field devices, such as actuators or drives, by executing the programmed logic and collect data from sensors. (Weiss 2010: 16-18; Colbert – Kott 2016: 24-25.)

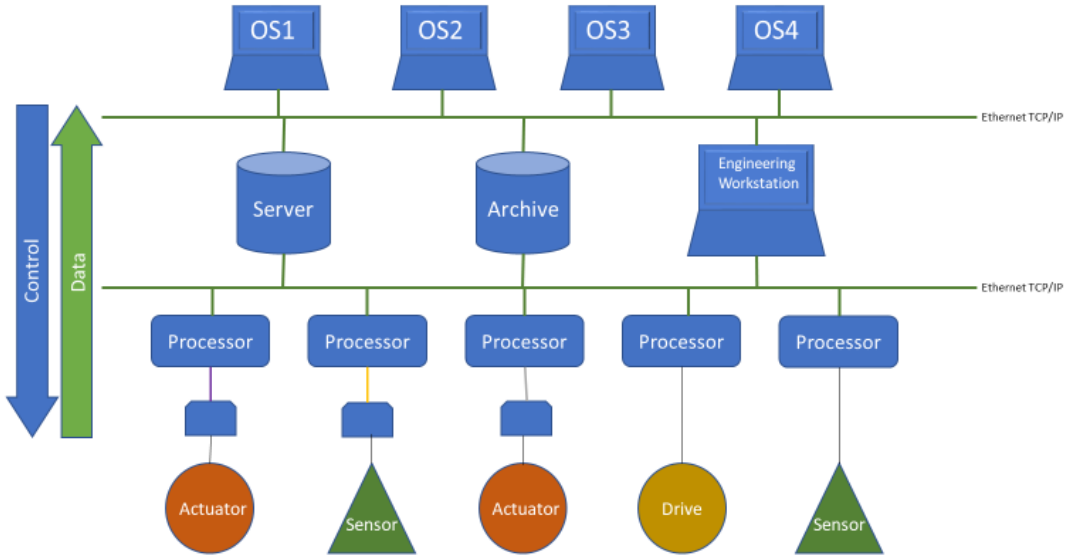

Figure 5. Basic structure of a DCS (modified from: What is DCS 2019).

A DCS ranges from the process level (level 0) to the area supervisory control level (level 2) of the Purdue reference model.

2.3.3 PLC

A Programmable Logic Controller (PLC) is an ICS asset, that are used to reliably automate a processes within industrial systems. They have analog and digital inputs, for receiving measurement values of the process, and outputs, for controlling the process according to the programmed logic. PLCs have a fast processing speed and are very customizable. Therefore they are often used for simple and fast recurring processes. The field devices are connected to the analog or digital inputs and outputs via Data cables. PLCs are controlled by a graphical interface like SCADA. (Weiss 2010: 18-19; Colbert – Kott 2016: 16-17.)

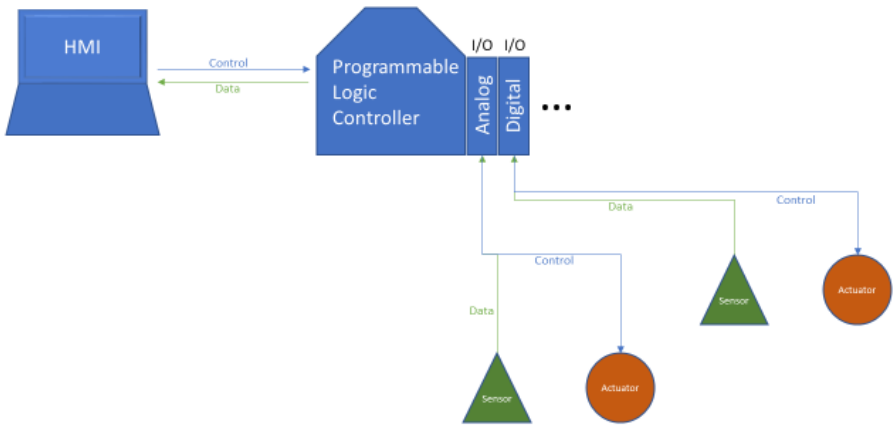

Figure 6. Basic structure of a programmable logic controller (modified from: What is DCS 2019).

PLCs belong to the basic control level (level 1) of the Purdue reference model.

2.3.4 Field Devices

Field devices in an ICS network are products in the plant production area, that measure physical values or make physical changes within a process. Such devices range from temperature-, pressure- or photo-sensors to actuators, electrical motors and valves. The Process level (level 0) of the Purdue reference model consists of field devices. (Colbert – Kott 2016: 22-23.)

2.4 Asset Ownership

An asset is an item, that has some value to a company or person. When an asset is acquired or created, it should be assigned to the portfolio of an owner, who is responsible for the management of the asset over its whole life cycle. The asset owner should ensure, that all assets are inventoried, classified, protected and at the end of their life cycles

deleted or destroyed. The owner is also responsible for access control policies regarding the asset. (Biswas 2019.)

Commonly, IT-assets are owned by the IT division of a company, whereas OT-assets are owned by the business divisions. The asset owner alone is accountable for the asset, which makes collaboration between the divisions necessary, since IT- and OT-assets have similar needs and issues, as they are used for information collection, transfer and visualization. Without a proper CMDB governance, the asset owners cannot collaborate with the IT- or corporate security professionals about the possible vulnerabilities in their systems.

3 Data Collection

The data for this thesis was collected by first defining the desirable features of an asset management system. The features were discussed and evaluated with project members. After the definition of an ideal system, a questionnaire was constructed based on the selected ideal features. The questionnaire, along with an interview invite, was sent to carefully selected representatives of Fortum generation division and of other companies. Concurrently with the interviews asset management systems were searched online.

3.1 Ideal System Features

While creating the questionnaire the ideal aspects of an OT-asset management system were considered with essential parties in the project. An asset management system should possess all the defined features (table 1) in order to fulfil all needs required from the system.

Table 1. OT asset management system ideal features and explanations.

Feature	Explanation
Suitability	The system must be applicable for OT-assets in the energy production sector.
Security	Connections and access to the CMDB must be secure due to the sensitivity of the data.
Process management	A CMDB tool should enable the undertaking of asset management processes.
Automated asset discovery	ICS networks of a company can include thousands of devices and hence require automation for a precise and fast asset documentation.
Usability	As one system should satisfy all users, like asset owners, cyber security professionals and field engineers, the system should be multifunctional and allow use from all users' standpoints.
Mobile application	A mobile use of the system would be beneficial for workorders concerning certain assets.
Integrations	Users should be able to import and export data from and to the system if needed.
Support	Reliable application support should be available on short notice.
Modifiability	Features should be requestable and removable to or from the system for it to be tailored to the task and environment.
User friendliness	Users should be satisfied to use the system in their work.

3.2 Questionnaire

This survey was constructed of open-ended questions with an aim for a specific answer. Each question has an investigative purpose for figuring out the capabilities of the asset governance system in use. The survey was conducted via Microsoft Teams meetings with the workers responsible for the OT-assets at the respective plants. The questionnaire aims to define and find out, how well the system used corresponds to issues, and how well it performs documentation. The questions focus on system identification,

process management, asset discovery and documentation, data storage and security, asset ownership, modifications and customer satisfaction.

3.2.1 System Identification

Identification of the system is essential for the creation of an insight into the systems currently in use and defining the best suited system for Fortum. In the first question the system was identified by resolving the product name, vendor and producer of the system.

3.2.2 Process Management

As management of processes is a feature of an ideal system, it is important to question, whether processes are defined at all. Since the processes exist in any case the question at hand is, where these are documented, if at all.

3.2.3 Asset Discovery and Documentation

The scalability of the asset management system is dependent on how easily asset data can be added to the system, considering that a single powerplant can have thousands of OT-devices. In order for suck system to be suitable for a company wide use, an automated asset discovery function is essential.

3.2.4 Data Storage and Security

Legislative reasons in some countries convey that the ICSs of critical infrastructure providing plants must be documented (Laki kaksikäyttötuotteiden vientivalvonnasta 26.7.1996/562). These documentations must be stored securely, since revealing the inventory of a plant creates security risks. As the energy production sector is part of the critical infrastructure for a society, it is important to consider the method of data storing.

3.2.5 Asset Ownership

As asset owners are responsible for the assets, they should be able to access the inventory and manage their own resources and delegate tasks to other parties. The usability of the system depends on how well different parties have access to it.

3.2.6 Modifications

The system should fulfill all the needs of the customer. Therefore the producer should be cooperative in modifying the system and tailoring it to the customer's needs. This includes the support provided by the producer or vendor of the system.

3.2.7 User Satisfaction

Productive working requires a good working environment and good tools. If a worker is dissatisfied with either one, productivity and work morale decrease. User satisfaction is therefore an important aspect to be considered. The dispersion of the system within a company as well as direct questions indicate the satisfaction of system users.

3.3 System Product Analysis

The system product analysis was conducted by overlooking the market currently, searching products on companies' websites with keywords "OT-asset management system" and "ICS asset management system". The systems that were found were evaluated based on the website professionality and company credibility, contact information availability, and product descriptions. Multiple asset management systems were found in the online search. OT Base, Nozomi Networks solution and SilentDefence were chosen based on the accuracy of the entries or suggestions from professionals of the field.

4 Results

4.1 The Line Between IT and OT

The definitions of IT and OT and the Purdue reference model in the theoretical background help separating the two. As discussed in the theory part of this thesis, some levels of the Purdue reference model are inhabited by solely IT- and others solely by OT-assets. The definitions of assets should therefore start by considering the level of the Purdue reference model and the network the asset is in. If the asset cannot be defined distinctly by the network level, the second step should be to examine whether the asset is part of a larger system, like SCADA or DCS, which are OT, or a public address system, which is IT. In case the assets affiliation cannot be determined by the network level, nor does it belong to a system. The rule of thumb is, that everything that has the possibility to affect a physical process is OT and everything else is IT. When considering the CMDB it is essential, that all assets are documented and assigned an asset owner.

4.2 Questionnaire Results

The interview invite was sent to 11 different parties, of which eight accepted the invite and provided a response, one participated, but refused to give response and two did not participate. Data collected via interviews with the asset owners was documented in the questionnaire form (appendix 1) and checked by the interviewee during the interview. The questionnaire form was then named after the site or company and saved as a PDF-file. The raw data of the questionnaires was analyzed and summarized into tables that were prepared for the individual products. The table consists of one feature column, stating the ideal features of an asset management system, and another column for the availability of a feature in the system, in which a “1” indicates the presence of a feature, a “0” the absence of it and a “-“ means, that the feature is either only partly included or it is unknown, whether it is included. In case multiple questionnaire results were based on similar systems consisting of the same components, all results were summarized into one table.

4.2.1 Manual CMDB Governance System

One questionnaire result showed a system, where the CMDB was kept manually. The outdated governance of OT-asset is possible, however it lacks almost every desired feature. The documentation is kept in a fireproof safe and is available for a restricted group of users only.

Table 2. Questionnaire results for a manual system. A “1” indicates the presence of a feature, a “0” the absence of it and a “-“ means, that the feature is either only partly included or it is unknown, whether it is included

Feature	**-**
Suitability	**-**
Security	**1**
Process management	**-**
Automated asset discovery	**0**
Usability	**-**
Mobile application	**0**
Integrations	**0**
Support	**0**
Modifiability	**0**
User friendliness	**0**

A manual CMDB is a good backup plan for example in a situation, where non electrical technology must be relied on, hence it is useful to have one. However this does not appear to be a desirable system for primary use.

4.2.2 Microsoft Excel

Surprisingly many questionnaires show, that Microsoft Excel is used often for asset inventories, although it is a spreadsheet program. As is summarized in the second column of table 3, Excel is suitable to document the asset inventories of plants and the documentation can be opened by anyone with access to the file on the mobile version of the software. The import and export of excel data is fairly simple and Microsoft updates the

office tools regularly. Excel does not scan any networks for assets and it cannot be modified to do other desired tasks. As human error plays a factor in the use of Excel as a documentation tool, it cannot be considered to be user friendly. Data security is not built in to excel as the master file can be easily compromised by human error, unless it is handled correctly. Process management can only be documented in Excel but not carried out in it.

One questionnaire shows also Icinga, an open source software, used for IT network monitoring. When being used alongside Excel it brings additional features to the system. Icinga can scan networks for the components using a limited range of protocols, which improves the security of the system, since an up to date version of the documentation can be created at any time. Icinga can also be used for process management but as it does not have a mobile application and the availability of its support is unknown, the resulting system has some disadvantages towards only Excel. The questionnaire results are summarized in column 3 of table 3.

Another system of a respondent included Excel with IBM Maximo, an enterprise asset management system that can be used for procurement and work management processes. The asset inventory can be exported from the system, thus improving the security, but as it requires licenses for all users, it is not profitable to grant all users these rights. Maximo has no mobile version of the application but it can be modified to some extent to fit the company's needs. Column 4 of table 3 summarizes these results.

The 5th column of table 3 summarizes a system with Excel and IFS Enterprise resource planning software, that can be used for managing the production, distribution, inventory, billing and bookkeeping of a company. Like in Maximo, the asset inventory can be exported into Excel, which again improves the security aspect, since a new asset inventory can be created, whenever needed but only part of the users have access to create the reports. The support agreement terms of the software were unknown at the time of the interview.

Table 3. Questionnaire results for MS Excel with additional components. A “1” indicates the presence of a feature, a “0” the absence of it and a “-“ means, that the feature is either only partly included or it is unknown, whether it is included

Feature	MS Excel	Icinga + MS Excel	IBM Maximo + MS Excel	IFS ERP + MS Excel
Suitability	1	1	1	1
Security	-	1	1	1
Process management	-	1	-	-
Automated asset discovery	0	-	0	0
Usability	1	1	-	-
Mobile application	1	-	-	-
Integrations	1	1	1	1
Support	1	-	1	-
Modifiability	0	0	-	0
User friendliness	0	0	0	0

Microsoft Excel can be used to document assets and to monitor processes to some extent. Adding another software to form a combination can improve the quality of the overall system but the resulting system still does not satisfy all needs.

4.2.3 ServiceDesk Plus

The questionnaire results for ServiceDesk Plus show, that ServiceDesk Plus is an IT help desk system by ManageEngine, which can be used for the documentation of the asset inventory, including contract and license management and change and incident management. The assets, that support the protocol, are discovered via simple network management protocol (SNMP) and the data is stored securely on a local server. All users with the need have access to the asset inventory, the system has interfaces with the IT and OT databases and system support is provided by the vendor. To the knowledge of the interviewee the system is not modifiable and it does not have a mobile application. The users are satisfied with the system and would recommend it to other companies as well. The results are summarized in table 4.

Table 4. Questionnaire results for ServiceDesk Plus. A “1” indicates the presence of a feature, a “0” the absence of it and a “-“ means, that the feature is either only partly included or it is unknown, whether it is included

Feature	ServiceDesk Plus
Suitability	**1**
Security	**1**
Process management	**1**
Automated asset discovery	**-**
Usability	**1**
Mobile application	**-**
Integrations	**1**
Support	**1**
Modifiability	**-**
User friendliness	**1**

ServiceDesk Plus fulfills most of the important functionalities of the ideal asset management system. It was described to be sufficient for use but as it does not fulfill all requirements, it is not ideal.

4.2.4 Claroty

The questionnaire results, summarized in table 5, discuss a system by Claroty Ltd., which is a cyber security provider, that focuses on OT-network security. Their product, also called Claroty, is created for the sole purpose of creating a configuration management database for OT-assets. The data is stored securely on the applications servers where access is granted via the application access management to any needed user. Assets are discovered via multiple protocols and processes can be handled within the system. The system integrates with existing infrastructure seamlessly and could be used via the browser on a tablet computer. Support is provided by the vendor and the system has only positive user experiences. The interviewee unsure, whether the system can be modified, as there has not been a need for that.

Table 5. Questionnaire results for Claroty. A “1” indicates the presence of a feature, a “0” the absence of it and a “-“ means, that the feature is either only partly included or it is unknown, whether it is included

Feature	Claroty
Suitability	**1**
Security	**1**
Process management	**1**
Automated asset discovery	**1**
Usability	**1**
Mobile application	**1**
Integrations	**1**
Support	**1**
Modifiability	**-**
User friendliness	**1**

Claroty was the only system found in the survey, that is actually intended for this specific use. It fulfills most required needs, and according to the interviewee has only few deficits. In 2019 Claroty was awarded with the SAFETY Act approval by the U.S. Department of Homeland Security (Safety act 2019, Homeland Security).

4.2.5 Kaseya Virtual Administrator

The virtual system administrator by Kaseya was found to be used through one questionnaire. The system’s main functionality seems to be the administration of IT networks, rather than the management of an OT CMDB. The system data is stored securely on an application server. Some processes can be handled with the system. An automated asset discovery is possible and integrations to the system are possible, but were not used in the interviewees system. The facilities do not have access to the system data, however all other necessary parties can access it. There was no mention about a mobile application, support for the system or it’s modifiability in the interview. The users were not dissatisfied with the system, but would not recommend it to other organizations either.

Table 6. Questionnaire results for Kaseya virtual administrator. A “1” indicates the presence of a feature, a “0” the absence of it and a “-“ means, that the feature is either only partly included or it is unknown, whether it is included

Feature	Kaseya virtual administrator
Suitability	**1**
Security	**1**
Process management	-
Automated asset discovery	**1**
Usability	-
Mobile application	-
Integrations	**1**
Support	-
Modifiability	-
User friendliness	-

Although the system shows the capability to handle many of the wanted features, it does not handle these well enough. The system was described to be more suitable for an IT service desk than for asset CMDB governance.

4.3 Internet Searches

The systems from the internet product searches were chosen for the following reasons. OT Base by Langner Inc. was chosen, because it is the first system in the online search on all search engines. The Nozomi Networks solution was discussed in the project group during the defining of the ideal features and therefore included. SilentDefence was a candidate in an interviewed company’s project for implementing an asset management system for OT assets. Support, modifiability and user friendliness of these systems cannot be commented, since there is no reliable data to be found on these topics.

OT-Base, an asset management system by Langner Inc., was the first entry in all search engines. It is, like Claroty, a system built for the purpose of creating a CMDB for OT-

assets. The data is stored on an application server within the industrial network and the system can be used for processes involving the assets. All users of the system have access to the data, that can be limited by user groups within the application. It has an automated asset discovery and data can also be imported and exported to and from the system. There is no mobile application of the system. The results are summarized in table 7 column 2. (OT Base 2020.)

The Nozomi networks solution is system for managing and securing industrial control systems, that was recommended for this thesis by a company internal party. Its features are summarized in column 3 of table 7. The asset discovery is automated and integrations are available to the system. The website does not provide sufficient information on whether the system can be used via mobile devices or whether all users can use it. Some processes can be managed with the system. (Asset Intelligence datasheet 2020.)

SilentDefence is an OT network monitoring and intelligence platform by SecurityMatters. It was recommended for this thesis by an external party. Asset discovery is automatic and integrations are possible. It is unknown, whether processes can be managed with the system, or whether all users can use it. There is no mention of a mobile application of this system. (SilentDefence datasheet 2020.) The results are summarized in column 4 of table 7.

Table 7. Online search results. A “1” indicates the presence of a feature, a “0” the absence of it and a “-“ means, that the feature is either only partly included or it is unknown, whether it is included

Feature	Langner, Inc. OT-Base	Nozomi Networks solution	Security Matters SilentDefence
Suitability	1	1	1
Security	1	1	1
Process management	1	-	-
Automated asset discovery	1	1	1
Usability	1	-	-
Mobile application	0	-	-
Integrations	1	1	1
Support	-	-	-
Modifiability	-	-	-
User friendliness	-	-	-

5 Discussion

5.1 Conclusions

The goal in this thesis work was to find the best solution for the OT-asset management at Fortum. Solutions were searched via a questionnaire and online search. As can be seen from the questionnaire results presented in this thesis, the governed CMDB of OT-assets truly is a widespread necessity. Many interviewees confirmed, that a system with the named ideal features would be desirable and although all systems in the survey and the internet searches fulfil the minimal requirements for being considered for implementation, most interviews showed a dissatisfactory user friendliness and therefore a desire to modernize their current system. The problem for many parties seemed to be an

unwillingness to invest into a new system to replace a running one. As seen in the results, a system built for this exact purpose fulfills almost all needs in OT-asset management and hence either Claroty by Claroty Ltd. or OT-Base by Langner, Inc. could be the most suitable options.

5.2 Recommendations for Project Implementation

The project for selecting and implementing a companywide solution for OT-asset management is in its planning phase. The results found in this thesis work will be used, when choosing the system to be implemented. The most suitable options were selected based on the available data. However, the limited quantity of systems found in the online search and the subjective nature of interview answers, must be taken into consideration before the implementation. This thesis work only focused on the functionality of the systems and not the expenses connected with them. More information about the considered systems should be requested from the vendors.

5.3 Ethics and Reliability

This study was carried out by describing the data collection and data description accurately and truthfully. All the data is stored and documented, and all the relevant data is presented in this thesis. The questionnaire answers were anonymized to protect the identity of participating companies and their employees. There were no conflicts of interest declared. The thesis project was carried out transparently.

The questionnaire used in the data collection was created in close collaboration with cyber security professionals to ensure, that no sensitive or confidential data was inquired. The invite was sent along with the questionnaire form to 11 carefully chosen parties, of which nine agreed to an interview and two did not participate. Of the nine interviews eight resulted in data for the thesis and one refused to answer questions due to legislative reasons. All interviewees were informed at the beginning of the interview, that the results will be published with this thesis without mentioning the company or employee name.

References

Ackerman, Pascal 2017. Industrial Cybersecurity. Packt Publishing Limited

Asset intelligence datasheet. 2020. Online document. Nozomi networks. <https://www.nozominetworks.com/products/asset-intelligence/> Accessed 11.5.2020

Biswas, Pretesh. 2019. Online document. Trace International. 8.12.2019. <https://iso-consultantkuwait.com/2019/12/08/iso-270012013-a-8-asset-management/> Accessed 9.5.2020

Cambridge Business English Dictionary, https://dictionary.cambridge.org/dictionary/english/information-technology

Colbert, Edward J.M. – Kott, Alexander 2016. Cyber Security of SCADA and Other Industrial Control Systems. Springer International Publishing; Switzerland.

Green, Benjamin – Krotofil, Marina – Hutchison, David 2016. Achieving ICS Resilience and Security through Granular Data Flow Management. Association for Computing Machinery. Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy.

Laki kaksikäyttötuotteiden vientivalvonnasta 26.7.1996/562. Finlex. Available online <https://www.finlex.fi/fi/laki/ajantasa/1996/19960562>

Operational Technology (OT). Gartner Glossary 2020. Online Document. <https://www.gartner.com/en/information-technology/glossary/operational-technology-ot> Accessed 14.5.2020

OT Base. Online document. Langner Inc. 2020. <https://www.langner.com/ot-base/> Accessed 11.5.2020

Perelman, Barak 2016. The Role of Asset Management in ICS network. Security Week December 13. Available online <https://www.securityweek.com/role-asset-management-ics-network>

Safety Act. Online document. Homeland security. 25.10.2019. <https://www.safetyact.gov/lit/at/aa> Accessed 5.5.2020

Samonas, Spyridon – Coss, David 2014. The CIA strikes back: Redefining confidentiality, integrity and availability in security. JISSec Journal of Information System Security. Volume 10 Issue 3

SilentDefence datasheet. Online document. SecurityMatters. 2020. <https://cdn2.hubspot.net/hubfs/2951224/Security_Matters-March2017/PDF/SilentDefense_datasheet_US.pdf?t=1502461533758> Accessed 11.5.2020

Taylor, Sharon – Cannon, David – Wheeldon, David 2007. ITIL Service Operation. TSO

Weiss, Joseph 2010. Protecting industrial control systems from electronic threats. Momentum press

What is DCS. 2019. Online document. REALPARS 13.5.2019 <https://realpars.com/dcs/> Accessed 17.3.2020

Questionnaire

This questionnaire was used for the data collection in this thesis. The PDF file consists of 8 questions on 4 pages.

OT-asset CMDB solutions questionnaire

This questionnaire serves for gathering information for my thesis on OT-asset CMDB solutions to Helsinki Metropolia University of Applied Sciences and Fortum Power and Heat Oy.

The Thesis results will be published but all answers will be anonymized so companies will not be mentioned in connection with the results.

1. a) What system is used for the OT-asset management?
   b) Is it used on all sites of your company?
   c) Why have you chosen this Tool? What main functionalities are important?

Producer:
Vendor:
Product:
b) [Yes/No] (if "No" what Tools are used in them?)
c)

2. a) Have you defined processes for OT-assets (for example for change management) like in ITIL and does your asset management system enable their undertaking?

[answer here]

b) If yes, what are those processes? Are the processes handled within the tool, documented in it or not at all related to the tool?

[answer here]

3. Is the asset discovery done manually, automatically with the same system, that is used for asset management or a different tool?

[answer here]

4. a) How and where is the data stored? Is there a centralized data storage or is the asset data stored on a local server?

[answer here]

b) Are there legal reasons connected with the location of the data storage (For example with assets in different countries) the encryption and securing of data and the access management to the data?

[answer here]

5. a) Who/which department owns the OT-assets? To be more presise: who is responsible for:

Industrial cyber security: life cycle management: Change management: Business continuity management: Security monitoring and logging: Physical and environmental protection: Access management: Network connections:

b) Do all parties above have access to the system and the asset CMDB? If not, who is responsible of informing the individual parties of tasks in their area?

[answer here]

6. Do you have any integrations to your system or is it possible to add integrations? Are there still functional requirements?

[answer here]

7. What could be improved within your OT-asset management system? What are the worst aspects of it?

[answer here]

8. Are you satisfied with your OT-asset management system? Would you recommend it to colleagues?

[answer here]