Systematic approach to secure automation – coordinated voltage control use-case

Mikko Salmenperä, Jari Seppälä, Hannu Koivisto*
Tampere University of Technology, Department of Automation Science and Engineering, P.O.Box 692, FI-33101 Tampere, Finland
Tel: +358 40 849 0061, E-mail: mikko.salmenpera@tut.fi, http://www.tut.fi/ase

Shengue Lu, Sami Repo
Tampere University of Technology, Department of Electrical Engineering,, http://www.tut.fi/dee

KEY WORDS Smart Grid, dependability, secure lifecycle

ABSTRACT

New emerging Smart Grid business possibilities require information integration in massive scale. One key problem is that business area tradition is to use point-to-point links, which are not suitable for the massive online integration requirements of this trend. The most promising business cases are implemented as a collection of various systems, thus the integration applications should also be treated as more than separate interconnections between systems. In this paper we focus one such use case - the Coordinated Voltage Control in Median and low voltage networks. We apply Information flow based approach analysis tool titled PICARD to derive requirements for the participating systems, middleware and communication links. The results show that this approach aids understanding complex systems and provides valuable information for the actual integration development process.

1 INTRODUCTION

Emerging Smart Grid requires information integration in massive scale. The most promising business cases require new functionality implemented as a collection of various systems, thus the integration applications should also be treated as more than series of interconnections between systems.

Integration the automation systems has various hard real-time and reliability properties which are critical compared to more traditional integration applications. These requirements must be understood and taken into consideration when designing and implementing the integration solutions. The requirements originate from the cyber-physical nature of automation and especially from the direct contact with physical world. The PICARD method is an information flow based method for researching and refining these automation requirements while taking into account integration, security and automation specific properties /1/, /2/. This modeling technique begins the essential business case. From this the information flows are deducted as the flow of data is the prime aspect for the analysis of the system. These flows are then refined into specific requirements corresponding to integration links between various systems. After the modeling, requirements are utilized in design and

implementation of the actual integration application.

Under Finnish Cluster for Energy and Environment (CLEEN) research program SGEM (Smart Grids and Energy Markets) a research environment for future smart grid functionality was planned and realized in TUTCyberlabs environment /3/. In this paper we present the Coordinated Voltage Control use case from real life smart grid environment that is being researched in TUTCyberLabs environment. We detail a method titled PICARD to analyze the CVC use case on an abstract level. As a result of the analysis we get a model of automation specific and security requirements. These requirements can then be used in later phases of integration application design.

2 COORDINATED VOLTAGE CONTROL USE CASE

Coordinated voltage use case is a process aimed to solve a voltage violation in electrical grid /4/. From algorithm point of view this problem is widely researched in smart grid community. Focus of the paper is on automation and security requirements analysis. Following datasources and systems are participating in CVC implementation:

- **Data Aggregator** collects consumption and production data from individual distributed energy resources (DER) such as home energy managements system (HEMS). It can also control the DER when required by the CVC Algorithm /5/.
- **Advanced metering infrastructure (AMI)** data consists of voltage, current, active and reactive power measurements. AMI can also provide demand-response behavior in order to control customer load as described in /6/.
- **SCADA** provides access to data from electrical grid operation. It also processes the new set of calculated set points from CVC output.
- **State Estimator** is an active agent creating a situational awareness view to current medium (MV) and low voltage (LV) electrical grid beyond actual measurements. It uses all the available data from the grid gathered by SCADA and AMI systems. State estimator also utilizes load profile based pseudo measurements. These load profiles used by the state estimator might be improved significantly based on AMI data, by classifying customers to correct customer class (each class has its own load profile) and by adapting load profile to real behavior of customers /7/.
- **Distribution management system (DMS)** provides topology and connectivity data of the distribution network. Static network structure and dynamic status of switches are combined for each execution cycle of CVC algorithm.

3 PICARD DEPENDABILITY MODEL

PICARD dependability modeling approach abstracts the implementation and system details. Focus is on what is important – information and it's flow through the system. In PICARD method the information flow is used to model requirements of each interconnection between processes. PICARD is not an alternative to existing threat model categorization methods, like Microsoft's STRIDE approach /8/, which is good tool after the system behavior is understood. STRIDE is suitable for software development but not for high level information flows used as basis for discussions between parties related to the project.

The PICARD dependability model uses classification suitable for automation. It contains two new features for the standard information flow diagrams. Compared to the traditional information flow, in our approach the flow is an object containing the information data of the flow. The first extension is security and automation requirements of the information inside the flow. This is marked as text PICARD where the interpretation of individual letters is described in Table 1.

Table 1. Description of PICARD extension. The requirement for information flow is presented as bold letters in flow diagram.

Letter	Short for	Description
P	Privacy	Personally identifiable information (PII)
I	Integrity	Integrity of the information is required
C	Confidentiality	Information is confidential e.g. process optimization configurations, or material requiring IPR protection
A	Alarm	Event based information requiring prioritization
R	Real-time	Cyclic information which must be deterministic i.e. delays are known and without unspecified variation.
D	auDiting	Information has auditing requirements e.g. Sarbanes-Oxley [11].

The second extension is color-coding of the link, process or storage according to the trust that can be placed on it. For example, red can be untrusted link over Internet. Green can be trusted link inside the automation network.

The main idea of extended model is simple and can be divided into 10 phases:

1. Create context model of the use case with external entities. This can be extracted from the previously defined explicit use cases.
2. Identify the trust boundaries.
3. Color-code the components based on trusts.
4. Create next level information flow diagram.
5. Identify the trust boundaries.
6. Color-code the components based on trusts.
7. Add security requirements to flows (apply caps/bold to letters P, I, C).
8. Add automation requirements to flows (apply caps/bold to letters A, R, D).
9. Add red color code to untrusted/unsafe flows from automation perspective (e.g. over Internet over office network). Leave unclassified to black.
10. Iterate from 4 until desired detail level is achieved.

The STRIDE approach is used to analyze and decide mitigation strategies whereas the PICARD is more suitable for modeling information flows inside an automation system. Another difference between STRIDE and PICARD is that PICARD's target is not to prioritize the threats rather classify the trust and requirements of the paths, processes, storages and external entities related to information flow. Reference /9/ details PICARD method in more detail.

4 PICARD DEPENDABILITY ANALYSIS OF THE CVC USE CASE

PICARD method begins with essential model derived from this use case. CVC use case is described in chapter 2 and the essential model used for the PICARD is derived from that. As CVC use case is too complex to depict in one diagram we choose to draw each end system separately. In this paper we use the flow of information to/from

State Estimator system as an example how this method is applied. Resulting diagram is depicted in Figure 1.

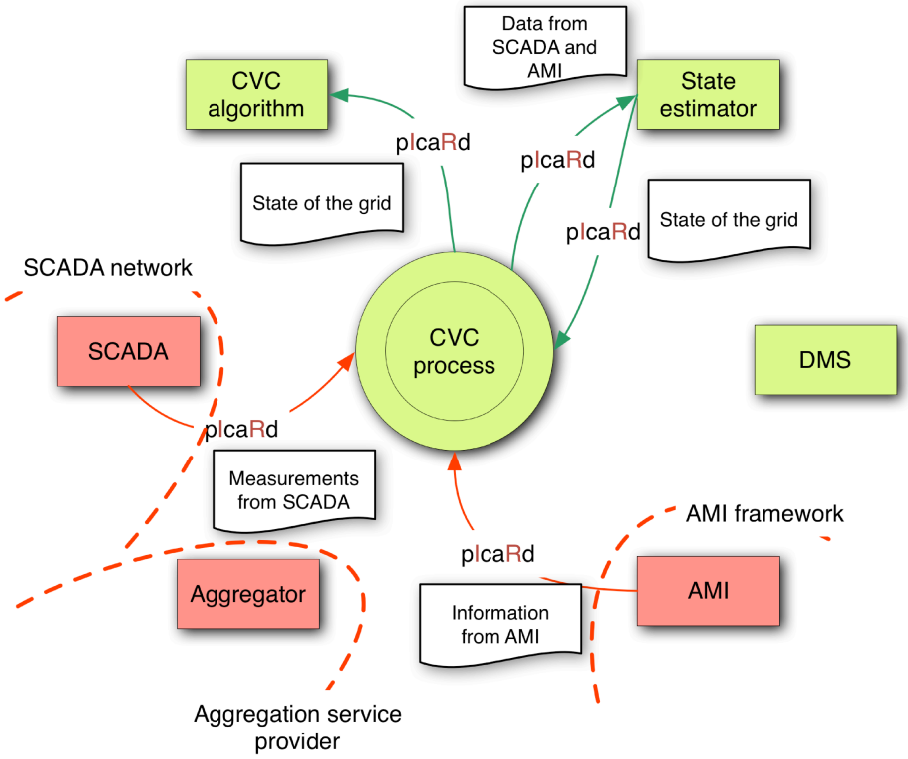

Figure 1: State estimator related information flows

Green components are trusted or owned systems which we know and can rely on. Similarly green arrows indicate trusted information flow path. These require less scrutiny when actual integration solution is designed. Red color indicated untrusted or external system, which pose a need to establish the trust with some explicit way when the system is implemented.

Dotted red lines between systems indicate truest boundaries between systems. This means that the end systems on the other side of the boundary are in separate networks and are possibly a responsibility of an other party. This poses an additional requirement for the integration application as the trust must be re-established somehow before we can accept the information crossing the boundary.

Letters in the data flows indicate specific requirements corresponding to each flow. Red capital letter show which requirement is in effect. In this case all data must be guaranteed to have integrity i.e. No changes can occur during the transfer. Real time requirement is also present, as the CVC algorithm needs timely execution in case of being triggered by voltage limit violation.

By drawing all of the PICARD flow diagrams we explicitly document the security and automation specific

requirements of the use case. This information can then be passed to integration/software development team and formulated to more traditional software requirements form. From the shown diagram we can formulate following requirements for state estimator data flow:

1. Connection to SCADA systems needs to be authenticated to enable the trust to it.
2. Connection to SCADA system needs to be secure so the authentication can be trusted.
3. Communication to SCADA needs to protected agains transfer errors.
4. Communication to SCADA must be reliable to enable the real-time requirement of data transfer. This requirement is soft realtime meaning that there is no clear time line after which the data becomes obsolete. Rather the usability of data is a slowly declining cost function reaching no value at some time after the process being started,

To satisfy these requirements following design choices were made for implementation to TUTCyberlabs:

1. Reliable communication path to SCADA is provided by using multi path network equipment from AJECO. /10/
2. Communication protocol used is OPC Unified Access. OPC UA provides strong authentication, reliable communication and timely operation for the data link. SCADA system supports only OPC Classic so a OPC UA Gateway is needed /11/.
3. Network and system loads are designed so that no congestion occurs, enabling soft real time processing of data.

Similarly analysis of other data flows participating in CVC use case is done and a resulting portfolio of PICARD diagrams forms a dependability model of the use case. This dependability model is used as input into company's Secure Development Lifecycle. /12/.

5 CONCLUSIONS

CVC use case is a complex and challenging new functionality planned for future smart grid. It gathers a lot of information from various existing systems and refines it to enable new features required by the smart grid. PICARD method based dependability model was used to document the requirements of this use case. The resulting portfolio can be used as a base line for defining automation and security requirements for research environment used in this project.

The created dependability models are as good as the information used to create them. They must be updated when new technology is presented into the environment or into the automation system. This is similar to updating the automation schematics when a process change is introduced.

It was found that drawing these diagrams was a good way to analyze and document the complex system. They form a solid foundation which can be used to explain and discuss the requirements and selected solutions. We also have found that the high abstraction level of this method enables people of different backgrounds to communicate more easily. For instance automation, IT and software engineers are all able to discuss the modeled requirements more easily as each party is forced to use similar vocabulary and concepts.

6 REFERENCES

/1/ Salmenperä, Eerola, Seppälä,Koivisto. Design and analysis of secure integration solution for Smart grids, 2013, Automaatiopäivät 2013.

/2/ Eerola R. Analyzing Integration and Information Security: Enterprise Service Bus for Smart Grid, Master's Thesis. Tampere University of Technology, Tampere 2013.

/3/ Seppälä, Salmenperä, Harju, Repo, Koivisto, Holmström. Towards automation security research and training environment. Automaatioseminaari XXI, 2015

/4/ J. Tuominen, S. Repo, and A. Kulmala, "Coordinated voltage control algorithms tested in real time digital simulator," To appear in Proc. Power System Computation Conference, Wroclaw, Poland, Aug. 2014.

/5/ A. Koto, S. Lu, T. Valavaara, A. Rautiainen, and S. Repo, "Aggregation of small-scale active resources for smart grid management," in Proc. IEEE PES ISGT Europe 2011 Innovative Smart Grid Technologies, Manchester, UK, Dec. 2011.

/6/ P. Koponen and J. Seppälä, "Market price based control of electric heating loads," in Proc. 21th International Conference on Electricity Distribution, Frankfurt, Germany, Jun. 2011.

/7/ A. Mutanen, M. Ruska, S. Repo, and P. Järventausta, "Customer classification and load profiling method for distribution systems," IEEE Transaction on Power Delivery, vol. 26, pp. 1755–1763, Jul. 2011.

/8/ Yourdon, P. and Constantine, L. L.: Structured Design: Fundamentals of a Discipline of Computer Program and Systems Design. 1 edition, Prentice Hall, 1979, ISBN: 978-0138544713, p. 473.

/9/ Jari Seppälä, Mikko Salmenperä and Hannu Koivisto, Making sense of information security in real time automation - information flow approach. Automaatioseminaari XX, 2013

/10/ Rajamäki J., Holmström J. and Hult T., The future solutions and technologies of public safety communications - DSiP traffic engineering solution for secure multichannel communication. International Journal of Communications, Issue 3, Volume 5, 2011.

/11/ Hannelius, T.; Salmenpera, M.; Kuikka, S., "Roadmap to adopting OPC UA," Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on, vol., no., pp.756,761, 13-16 July 2008

/12/ Microsoft. Security Development Lifecycle. http://www.microsoft.com/security/sdl/default.aspx [accessed February 24 2015]