Security Risk Assessment-based Cloud Migration Methodology for Smart Grid OT Services

Bojan Jelacic, Imre Lendak, Sebastijan Stoja,
Marina Stanojevic, Daniela Rosic

Faculty of technical sciences, University of Novi Sad
Trg Dositeja Obradovica 6, 21000 Novi Sad, Serbia
E-mail: bojan.jelacic@uns.ac.rs; lendak@uns.ac.rs; sebastijan.stoja@uns.ac.rs; marina.stanojevic@uns.ac.rs; drosic@uns.ac.rs;

Abstract: The primary goal of this paper is to present a security risk assessment-based methodology for migrating sensitive Smart grid operational technology (OT) services to the computing cloud, either on or off-premise. We created a baseline system architecture diagram for smart grid Industrial Control Systems (ICS) aligned with the IEC-62443 model of security zones. We identified potential threat sources and threats which might affect the confidentiality, integrity, and availability (CIA triad) of OT services. We defined a threat impact and likelihood assessment strategy tailored for use in smart grids. Based on the combined impact and likelihood of threats we present a risk matrix, a tabular risk assessment template, and a baseline cloud migration strategy. We test our methodology on two cloud migration case studies, namely a large distribution system operator (DSO) with a complex OT environment; and a small DSO with limited OT capabilities, budget, and IT staff. As there are no risk assessment-based studies which tackle the problem of migrating smart grid OT services to a cloud computing architecture in a systematic way, our method will be a valuable asset for any smart grid system owner/operator. Which will be able to guide them in choosing an optimal cloud migration strategy, both fitting their specific requirements and maintaining an adequate level of information security.

Keywords: Smart Grid; Cloud computing; control systems; information security; IT/OT systems; risk analysis; SCADA systems

1 Introduction

Industrial control systems (ICS) allow the operators of various systems, ranging from food processing plants to electric power systems, to remotely monitor and control the underlying physical processes. Modern ICS are complex and heterogeneous information systems, which can be regarded as a critical link connecting the cyber with the physical, i.e. connecting the hardware components in the process environment with the software used to monitor and control the industrial processes, thereby gluing the system together into a true cyber-physical system. Modern smart grid ICS consist of a diverse range of software-intensive solutions and services, e.g. the Supervisory Control and Data Acquisition (SCADA) allows remote monitoring and control, the Outage Management System (OMS) allows operators to handle planned and unplanned outages, Geographic Information Systems (GIS) are used to manage a company's assets, and Meter Data Management (MDM) systems handle large volumes of data collected by myriads of smart meters installed. Although the list of services used is usually quite different for each smart grid system operator, there are common elements, which allow us to perform their comprehensive security analysis. There are specific cloud migration challenges in smart grids as they are critical infrastructures whose continuous operation is of utmost importance to their owners, customers and the Nation. Their dual information systems consist of the information technology (IT) and operational technology (OT) elements tasked with business and real-time operations. Although these systems (IT and OT) worked as separate entities traditionally, the latest trends show that the two 'silos' converge. This IT-OT integration is regarded as a vital steppingstone towards a successful smart grid.

Different actors consider the integration of cloud computing into their (control) systems as the cloud would allow them to outsource hardware acquisition and maintenance costs. Obviously, cybersecurity is a highly relevant aspect of any cloud migration strategy, as cyber-attacks might impact national security, the economy, and the safety of the general population. Therefore, the goal of this paper is to propose a risk assessment-based methodology which can be systematically used by smart grid system owners and/or operators to create a tailored cloud migration strategy for their OT services. Our method is aligned with the Federal Information Processing Standards (FIPS) 199 security categorization of information and services [1] and the IEC-62443 model of security zones [2].

Apart from this introduction, the paper consists of three sections. In section two we overview the state-of-the-art in smart grid security, cloud security, and risk assessment. In the third section we formalize the security risk assessment methodology for smart grid OT environments. In the fourth section we present two case studies in which significantly different smart grid OT systems are migrated to the (hybrid) computing cloud using the proposed methodology.

2 Related Work

In this section, we overview the state-of-the-art in the fields of smart grid security, cloud computing security, risk assessment, and the intersections of these three domains.

2.1 Smart Grid Security

While bringing along substantial benefits in automation, supervision, real-time monitoring, and control throughout the system, modern power systems introduce new vulnerabilities and security issues [3]. The threat to energy firms is likely to increase in the coming years as new developments, such as further extensions of smart grids and smart metering expose more of their infrastructure to the Internet [4]. The Stuxnet sabotage attack against nuclear facilities in Iran made clear what could be done through cyberattacks [5]. The Ukraine 2015 and 2016 cyberattacks against selected elements of the state's electric power system showed that such attacks against cyber-physical systems can have significant consequences in the form of power outages, which in 2015 lasted 1-6 hours and affected ~225,000 customers [6].

The importance of security and privacy in smart grids is explained through a systematic study of thirty-six publications on this topic [7]. In reference [8] the authors claim that cyberattacks on power grid could result in significant damages and they describe a cybersecurity protection approach to assist in the design and implementation of power grid protection systems. Others believe that cyberattacks on power grids are pushing threat and risk assessment to another complexity level [9]. The Security for Smart Electricity Grids (SEGRID) project was tasked with building on existing methods to address the inter-dependencies characteristic of a smart grid [10]. Reference [11] contains a vulnerability analysis of a simultaneous attack scenario, using a modified cascading failure simulator. The authors claim that their simulator can automatically find the strongest attack combinations for reaching maximum damage in terms of generation power loss and time to reach black-out. The authors of reference [12] claim that one way to ensure vital asset protection is to look for vulnerabilities from an attacker's viewpoint. High-priority and prescriptive compliance frameworks (e.g. the NERC CIP requirements [13]) require IT staff and OT staff to work together in new and innovative ways to share documentation and collaborate on risks and mitigation [14].

2.2 Cloud Computing Security

The National Institute of Standards and Technology (NIST) outlines four cloud delivery models [15] [16]: *public clouds* available to the public, *private clouds* operated solely by or for a single organization, *community clouds* shared by a specific community, as well as *hybrid clouds* which are compositions of two or more of the above three models. References [17] [18] assess the various technical aspects of cloud migration in different settings. One of the main challenges in the wider adoption of any of the above cloud computing delivery models is (information) security. This challenge is even higher when the migrated systems are involved in national security, disaster response, defense, or homeland security missions, where the criticality of service availability is elevated [19]. The authors of references [20] and [21] report a detailed analysis and categorization of various security threats in a cloud computing environment. The Cloud Security Alliance (CSA) listed the "Treacherous 12," the top 12 cloud computing threats organizations (both cloud customers and providers) faced in 2016 that can erase any gains made by the switch to cloud technology [22]. A survey conducted with IT managers found cost efficiency and data security the top two most sensitive aspects in cloud platform adoption [23]. The most important challenges to be solved before organizations and individuals will have the trust to deploy their systems in cloud environments are security, privacy, power efficiency, compliance, and integrity [24]. A recent study [25] indicated that the ideal ratio of a hybrid cloud environment is around 60 percent cloud and 40 percent physical servers.

In general, most studies about cloud computing applications in power systems are from the performance and/or cost perspectives. According to the authors of reference [26], cloud computing can significantly improve the operational performance of power systems. Reference [27] presents a methodology for deploying a monolithic Advanced Distribution Management System (ADMS) in the cloud without impacting its operational performance.

2.3 Risk Assessment and Threat Modeling

Information security risks arise from the loss of confidentiality, integrity, or availability (i.e. the CIA triad) of information or information systems and reflect the potential adverse impacts to (organizational) mission, functions, image, or reputation [28]. Risk assessment is the process of identifying, estimating, and prioritizing information security risks. The Federal Information Processing Standards (FIPS) 199 establishes three security categories for information and information systems [1], based on the potential impact on an organization if certain events occur: low, moderate, and high.

The European Network and Information Security Agency (ENISA) analyzes threats against smart grids and concludes that availability and integrity are of higher importance in time-critical industrial control systems, while confidentiality is important in enterprise services provided to end customers or businesses [29]. Threat modeling allows us to identify and rate the threats associated with a system. It might be implemented using one of the following three approaches: asset-centric, software-centric, and attacker-centric. The authors of [30] propose a software-centric threat analysis-based cloud migration strategy for smart grid ICS, based on Microsoft's STRIDE methodology.

Based on the above state-of-the-art review, we conclude that there are no risk assessment-based studies that specifically tackle the problem of systematically migrating smart grid OT services to a system architecture utilizing the benefits of cloud computing. That is the gap we intend to fill by proposing a method that can be used by any smart grid owner/operator in need to devise an optimal cloud migration strategy.

3 Risk Assessment Methodology

In this section, we describe the vital elements of our risk assessment method. We list threat sources and (most likely) threats, domain-specific definitions of impact, and likelihoods. We define a risk matrix, a risk assessment template, and a baseline (risk assessment-based) migration strategy to a cloud computing environment.

3.1 Threat Sources and Threats

Most likely smart grid-specific threat sources are insiders, state-sponsored actors deploying advanced persistent threats (APT) or professional hacker groups executing attacks in hope of reaping some form of financial reward, e.g. through ransomware attacks. We grouped a non-definite list of most likely smart grid OT threats based on which element of the CIA triad might be most affected if they were realized. The resulting threat grouping is shown in the table below.

Table 1
CIA-based grouping of smart grid ICS threats

CIA	Threats
Confidentiality	Confidentiality loss of configuration data
	Confidentiality loss of operational data
Integrity	Unauthorized modification or deletion of configuration data
	Unauthorized modification or deletion of operational data
Availability	Denial of service attack on backend services
	Backend service failure due to bad data
	Denial of service attack on communication channels, e.g. mobile or network communications unavailable due to an attack
	Denial of service attack on the human-machine interface

As our analysis is mainly focused on the OT subsystem, we consider confidentiality and integrity of operational and/or configuration data. With availability, being a key security goal in OT systems, we identified four threats, which might affect the backend services, human-machine interface or the communication layer of the smart grid, caused by either the insertion of bad data or a Distributed DoS (DDoS) attack.

3.2 Likelihoods

Due to the relatively small number of publicized cyberattacks against smart grids, assessing the likelihood of such attacks is a considerable challenge. We hereby propose an industry-specific likelihood classification based on the following threat actor and smart grid characteristics:

- Existence of vulnerabilities in the smart grid services or infrastructure, ranging from serious to none.
- Known exploits and the level of difficulty to execute them remotely, via physical access and/or by gaining elevated privileges.
- Workforce loyalty and insider threat monitoring capabilities.
- Existence of capable threat sources and level of their motivation to execute attacks.
- Level of staff information security training, especially in the OT department(s).
- Level and quality of IT/OT system segmentation into security zones.

Table 2
Smart grid ICS threat likelihoods

Likelihood	Threat source/system characteristics
Very likely	Serious security flaws in the smart grid services or underlying infrastructure (e.g. operating systems)
	Known exploits can be launched from the Internet, semi-trusted or untrusted networks
	No insider threat monitoring, workforce loyalty issues
	Highly motivated and capable threat-source
	OT personnel without proper security training
	Highly integrated IT-OT systems exposing the OT environment
Moderate	Limited security flaws in smart grid services and infrastructure
	Known exploits can be launched only via physical access to the target system
	Loyal workforce and limited insider threat monitoring in place
	Limited threat source motivation, due to limited political or financial impact of potential attacks
	Limited security training for OT personnel
	Custom IT-OT system segmentation, limited OT system exposure
Low	No known security flaws in the smart grid services and infrastructure
	No known exploits, malicious users need physical access and elevated privileges in the target system
	Loyal workforce, advanced insider threat monitoring
	No threat source motivation due to minimum political or financial impact
	Well-trained OT workforce knowledgeable about the latest threats
	Excellent IT-OT system segmentation, no OT system exposure

Obviously, any occurrence of 'very likely' threats should be mitigated first by putting proper security controls in place. Possible threats in the 'low' likelihood class might be tackled last.

3.3 Impact

We propose the following three-level, smart grid-specific impact classification based on a theoretical attack's possible effect on (1) the correct operation of the smart grid and (2) the operating company's public image.

- **High-severity** impacts include loss of human lives or serious injuries of employees or customers, widespread power outages, severe infrastructure damage, and critical service malfunctions (e.g. prolonged SCADA outage).
- **Medium-severity** impacts include availability loss of non-critical services (e.g. GIS or EMS) or (limited) access to sensitive information (e.g. personally identifiable information or sensitive business data). These might cause reputation damage, significant client dissatisfaction, and possibly even penalties imposed by regulatory bodies and government agencies.
- **Low-severity** impacts do not lead directly to the failure of critical services or confidentiality loss of sensitive business or customer data. However, they cause delays in non-critical services or information disclosure that does not have a direct business impact, but may lead to exploitable vulnerabilities.

The above listed possible impacts are summarized in the table below.

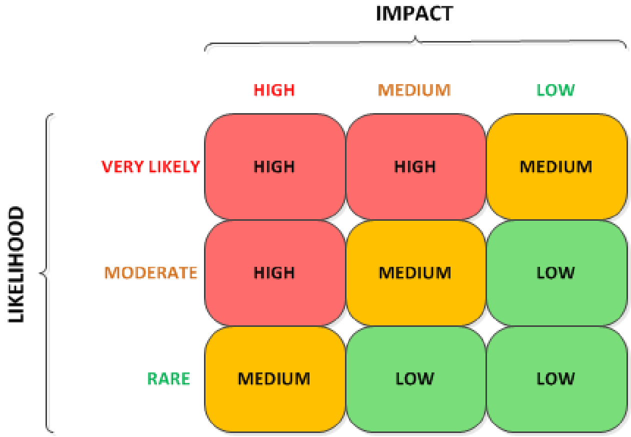
Table 3

Smart grid ICS impact levels

Level	Impact description
High severity	Loss of human lives or serious injuries
	Widespread power outages
	Severe infrastructure damage (e.g. high voltage transformer damage)
	Prolonged critical service malfunctions (e.g. SCADA)
Medium severity	Exposure of personally identifiable information or sensitive business data
	Very limited power outages
	Limited infrastructure damage (e.g. single transformer)
	Prolonged non-critical service malfunction (e.g. GIS)
Low severity	Limited unavailability of non-critical services
	Information disclosure without direct financial impact or adverse impact on company image

3.4 Risk Matrix

Based on the above-presented likelihood and impact classifications we determined the risk rating matrix shown in Figure 1. Impact is on the horizontal axis, likelihood on the vertical axis, and the rounded rectangles in the center of Figure 1 represent risk levels.



		IMPACT		
		HIGH	MEDIUM	LOW
LIKELIHOOD	VERY LIKELY	HIGH	HIGH	MEDIUM
	MODERATE	HIGH	MEDIUM	LOW
	RARE	MEDIUM	LOW	LOW

Figure 1
Risk rating matrix

We identified three risk levels: low, medium, and high. High risk is associated with those threats which are both likely and have a medium to high impact, e.g. a known vulnerability with an existing exploit in OT systems which might be used to cause a major power outage. The Ukraine 2015 attack falls into this category because the attack was very likely, due to weaknesses in personnel and IT systems security, as well as the geopolitical situation in 2015. Converged IT-OT privileged account management allowed the attackers to gain access to the OT system and execute commands which led to widespread power outages, i.e. had a high impact.

It is important to note that the threat sources, threats, impacts, likelihoods, and risk levels defined in this section are not definite and might be tailored for different OT environments based on their specific requirements. If the levels proposed in this paper are modified, then the migration strategies outlined in the following chapters might change as well.

3.5 Risk Assessment Template

Based on the above analysis of the possible threats, likelihoods and impacts, we created a risk assessment template, which can be used by smart grid owners/operators to document their risk assessments. For each identified threat we added one row, and each OT service should be entered as columns. After that, it is necessary to assess the impacts and likelihoods of the threats for each OT service (i.e. in each row) and to enter their ratings under column headers “I” and “L”. The cumulative risk is determined based on the risk rating matrix shown in Figure 1 and should be entered into the lower parts of the three-element cells with darker backgrounds in the risk assessment template below.

Table 4
Smart grid ICS risk-assessment template

Threat / Service	OT Service #1		OT Service #2		…		OT Service #N	
	I	L	I	L	I	L	I	L
Confidentiality loss of configuration data								
Confidentiality loss of operational data								
Configuration data integrity loss								
Operational data integrity loss								
Backend service failure due to bad data								
DoS against backend services								
DoS against the communication system								
DoS against the human-machine interface								

This risk assessment template can be generalized, as both the list of threats in the rows, as well as the list of IT/OT services in its columns can be tailored and aligned with specific smart grid system architectures. It can be tailored to other critical infrastructures or any industrial systems as well.

3.6 Baseline Cloud Migration Strategy

We propose the following baseline cloud migration strategy when deciding whether to keep an OT service on-premise (i.e. on physical servers or a private cloud), or deploy it in a community cloud:

- Keep services on-premise if they directly interface (i.e. connect to) physical equipment and do not have extremely high storage and/or processing requirements.
- Keep workstations in the control center so that the operators monitor and control the smart grid from a physically secured location.
- Move all low (L) and medium (M) risk services to the community cloud.

- Assess all high (H) risk services and move them to the community cloud if their storage or processing requirements are high[1].

Obviously, the above rules might be tailored according to the risk 'appetite' of smart grid owners/operators, i.e. aligned with their willingness to accept certain levels of risk.

4 Case Studies

We used the risk assessment method presented in the previous sections to analyze two significantly different case studies, in which different types of distribution system operators (DSO) migrate parts of their OT systems to the computing cloud. In the first case study, we performed a risk assessment based on which we proposed a hybrid cloud-based architecture for a large, multi-state and/or international DSO. In the second case study, we did the same for a (very) small DSO. We also present the most relevant characteristics of these two types of systems, document our risk analysis approach, and draw future, cloud-based system architecture diagrams. As a guide in any OT-to-cloud migration, we developed a somewhat simplified smart grid IT/OT control system architecture shown inFigure 2. In line with the IEC-62443 model [2], the building blocks of this system architecture are grouped into the following five security levels:

- **Level 1: Process Environment** - Contains the process subsystem, e.g. substations, remote terminal units (RTU), local SCADA (not shown in Figure 2).
- **Level 2: Operational Technology (OT)** – Consists of the services which allow system owners/operators to remotely monitor and control the smart grid from a control center. A subset of such services is shown inFigure 2: Supervisory Control and Data Acquisition (SCADA), Energy/Distribution Management System (EMS/DMS), Switching Management (SM), Outage Management System (OMS) and Meter Data Management (MDM) services. The MDM usually does not share its communication infrastructure with the SCADA.
- **Level 3: OT DMZ** – It is the main link between the OT and IT domains, allows data to flow in a tightly controlled manner between these two zones. In our, simplified smart grid system architecture it contains (only) the Historical and Security Information and Event Management (SIEM) services.

[1] The definition of 'high' will obviously vary between smart grids, and it will not be possible to exactly specify it here. Each system owner/operator will measure it based on its current and (planned) future capabilities.

- **Level 4: Information Technology (IT)** – The majority of IT services are hosted in this environment. We consider only the Geographic Information System (GIS), as it is often the master source of the network model, i.e. the asset information is exported from the GIS and imported into different OT services, e.g. SCADA, EMS, OMS, DMS, whose operation relies on having access to the up-to-date network model of the electric power system.
- **Level 5: IT DMZ** – Usually hosts services accessible from the Internet and/or interfacing information systems maintained by other smart grid actors, e.g. regulators, adjacent generation, transmission or distribution systems.

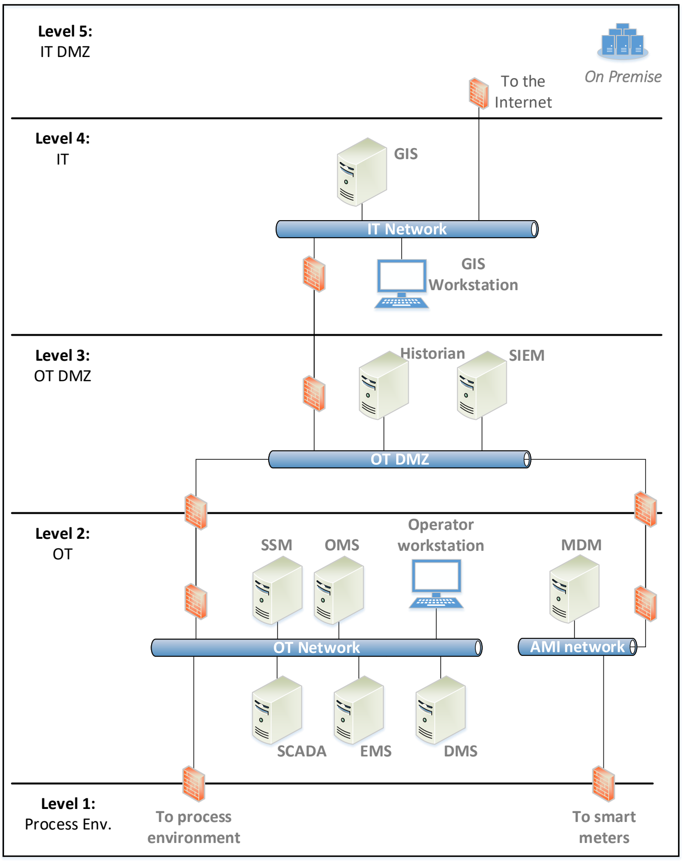


Figure 2
Original large DSO system architecture

Levels 1 and 2 correspond to the OT environment. Levels 4 and 5 are constituents of the IT environment. Level 3 is an IT/OT hybrid.

4.1 Large DSO Cloud-Based System Architecture

We define the large DSO as a system supplying at least one million customers either in a densely populated, urban area or in a larger geographic area. As additional inputs to the risk assessment, our theoretical DSO possesses the following specific characteristics:

- There is only one, primary data center. There is no disaster recovery (DR) center, but the DSO plans to invest in DR capabilities.
- There are no known vulnerabilities on the servers, workstations, and underlying communication infrastructure.
- There are no known exploits that can be launched from untrusted networks or via gaining physical access to the system or gaining elevated privileges.
- There are highly motivated state-sponsored and other threat sources.
- Loyal, tightly controlled, and security-aware workforce.
- Adequate IT budget and staff. A small but dedicated information security team.
- Clearly separated security zones aligned with IEC 62443 (seeFigure 2).

4.1.1 Impact Assessment

In the above-described setting and by using the impact classification template in Table 3 we identified the following high impact threats, either leading to (1) loss of human lives or injury (e.g. field crew affected), (2) widespread outages, (3) severe infrastructure damage (e.g. critical power transformer failure), or (4) prolonged critical service malfunctions (e.g. SCADA failure):

- Integrity loss of SCADA operational data if it leads to infrastructure damage.
- Integrity loss of operational EMS/DMS data if it leads to service or power outages, which is likely if they operate in a closed-loop and automatically issue commands via the SCADA.
- Integrity loss of SM operational data if it leads to personnel injury.
- Any availability loss of SCADA (backend) services.

We identified the following groups of medium impact threats:

- Exposure of personally identifiable (operational) data in the MDM or OMS, which handles customer information.
- Any DoS attack against any of the (non-critical) backend services.
- Any operational data confidentiality loss, as all services handle sensitive business data.

4.1.2 Likelihood Assessment

We assessed likelihoods in line with the specific case study setting, in which there are no known vulnerabilities, but there are highly motivated threat sources that might exploit zero-day vulnerabilities. As we identified a loyal and well-monitored workforce, we will consider insider threats infiltrated by threat actors as unlikely. Threat sources might initiate attacks from untrusted networks (i.e. the Internet), the public switched telephone network, or the process environment by gaining physical access to the geographically dispersed assets of the DSO. In such a setting DoS attacks against the GIS backend services from the Internet or hacked assets in the IT network are very likely.

As far as the moderately likely threats are concerned, we identified the following:

- All threat types against the Historian and SIEM due to their more exposed position towards untrusted networks in the OT DMZ.
- All remaining threats against the systems which are more exposed to attacks from the process environment, i.e. SCADA, MDM.
- All threat types against the OMS/SM which might be carried out via the mobile devices of the field crew or the public switched telephone network.
- EMS/DMS service failure caused by operational or configuration data integrity loss, e.g. intentional insertion of bad data.

Denial of Service attacks against the OMS/SM backend services, initiated either from the public switched telephone network, or the mobile devices carried by field crews.

4.1.3 Risk Assessment Results

Based on the above impact and likelihood analysis, as well as the risk matrix in Figure 1 we populated the risk cells in the risk assessment template below.

Table 5
Large DSO’s risk assessment

Threat / Service	SCADA		OMS \ SM		DMS \ EMS		GIS		MDM		HIS \ SIEM	
	I	**L**	**I**	**L**	**I**	**L**	**I**	**L**	**I**	**L**	**I**	**L**
Confidentiality loss of configuration data	M	L	M	L	M	L	M	M	M	M	M	M
	L		L		L		M		M		M	
Confidentiality	M	M	M	M	M	L	M	V	M	M	M	M

loss of operational data	H		M		L		H		H		M	
Configuration data integrity loss	M	L	M	L	M	L	M	M	M	M	M	M
	L		L		L		M		M		M	
Operational data integrity loss	H	M	H	M	H	L	M	V	M	M	M	M
	H		H		M		H		H		M	
Backend service failure due to bad data	H	M	M	L	M	M	M	M	M	M	M	M
	H		L		H		M		M		M	
DoS against backend services	H	M	M	M	M	L	M	V	M	M	M	M
	H		M		L		H		M		M	
DoS against the communication system	H	M	M	M	M	L	M	V	M	M	M	M
	H		M		L		H		M		M	
DoS against the human-machine interface	L	M	L	L	L	L	L	M	L	M	L	M
	L		L		L		L		L		L	

The baseline cloud migration strategy presented in section III/F was slightly adapted in the following manner to further distinguish high-risk services:

- Keep services on-premise if they directly interface (i.e. connect to) physical equipment.
- Keep all high (H) risk services on-premise if their impact rating is also high.
- Assess all (high risk, medium impact) and medium risk services. If their storage and/or processing requirements are high, then move them to a community cloud. The SIEM and the Historian usually fall into this category.
- Move all low (L) risk services to the community cloud.
- Move the disaster recovery center to a community cloud. The DR services physically interfacing equipment in the process environment (e.g. SCADA) need to be kept on-premise.

Based on the case study definition and our risk assessment, we propose that the large DSO migrates its OT services to the cloud-based system architecture shown in Figure 3.

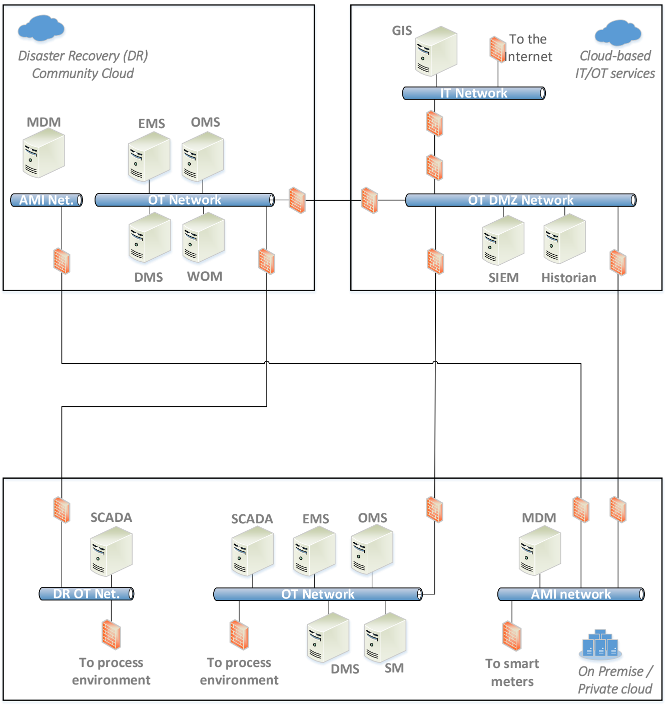


Figure 3
Large DSO's cloud-based OT system

The most notable advantages of this solution compared to the original solution (and to those operated by most modern, large DSOs) are the following:

- Potentially improved security monitoring and awareness capabilities via a community cloud-based SIEM, which might have insight into the security posture of multiple smart grid actors if they shared a Security Operations Center (SOC).
- Lowered disaster recovery costs[2].
- Seamless upgrades to new versions of the services utilized, as the community cloud service provider (CSP) might perform regular system upgrades as part of its service level agreement (SLA).

It must be noted that seamless upgrades to new versions for different large DSOs using a solution offered from the same computing cloud would be complex undertakings, as large DSOs tend to have different internal processes and (a plethora of) customer-specific requirements. It must be mentioned that a vital

[2] Costs can be lowered if the DR deployment is minimal.

precondition for the creation of such system architectures is the existence of community clouds for smart grids, which would be similar to the federal cloud in the USA.

4.2 Small DSO Cloud-based System Architecture

One possible criterion for identifying a small DSO is to check the number of customers and characterize it as ‘small’ if it has up to 100,000 (one hundred thousand) customers in a small or larger, but sparsely inhabited geographic region. Today such companies (usually) have limited IT budgets, which in turn means that their spending on computing hardware and information security capabilities is also limited. Regardless of the limited IT budgets, these companies still need at least asset and outage management (i.e. GIS and OMS) capabilities, which allow them to have insight into the up-to-date inventory of equipment owned, and timely outage management necessary for an acceptable level of customer satisfaction. Depending on their needs, they might invest into fully featured SCADA, MDM, DMS or SM solutions. Their day-to-day operations will most often be carried out without the benefits of having a SIEM and/or Historian. These systems usually do not fall under the jurisdiction of NERC CIP [13] or similar mandatory security requirements imposed by regulatory bodies. As additional inputs to the risk assessment, our theoretical (small) DSO possesses the following specific characteristics:

- There is only one, primary data center without a DR center or plans for setting it up in the future.
- There is an unknown number of vulnerabilities in the integrated IT/OT environment.
- There are known exploits that can be launched from untrusted networks or via physical access.
- There are no highly motivated state-sponsored and other, high-profile threat sources.
- Loyal, tightly controlled, but security-unaware workforce.
- No IT budget and staff. No information security team.
- Tightly coupled IT and OT zones.

In summary and based on the above introduction, we conclude that such systems possess limited capabilities in the following domains: No security monitoring and awareness without a SIEM; No analytical capabilities without a DMS/EMS; No audit capabilities without a Historian and/or a SIEM; Limited automation and remote-control capabilities without a SCADA; There is no disaster recovery center (DR).

We analyzed the above-described system and we classified operational data integrity loss in the OMS as high impact because such threats can lead to service personnel injury or extended power outages. We considered attacks against both the OMS and GIS more likely than in the large DSO scenario, as they are usually more exposed to untrusted networks in smaller systems (with lower IT and cybersecurity budgets).

We populated the risk assessment template presented in Table 4. The resulting risk assessment results are shown in Table 6.

Table 6
Small DSO's risk assessment

Threat / Service	**OMS**		**GIS**	
	I	**L**	**I**	**L**
Confidentiality loss of configuration data	M	L	M	L
	L		L	
Confidentiality loss of operational data	L	V	L	V
	M		M	
Configuration data integrity loss	M	L	M	L
	L		L	
Operational data integrity loss	H	V	L	V
	H		M	
Backend service failure due to bad data	M	L	M	L
	L		L	
DoS against backend services	M	L	M	L
	L		L	
DoS against the communication system	M	L	M	L
	L		L	
DoS against the human-machine interface	L	V	L	V
	M		M	

We identified the following high and medium risk threats: H: Integrity loss of OMS operational data; M: Confidentiality loss of OMS operational data; M: Confidentiality loss of GIS operational data; M: Availability loss of OMS clients; M: Availability loss of GIS clients.

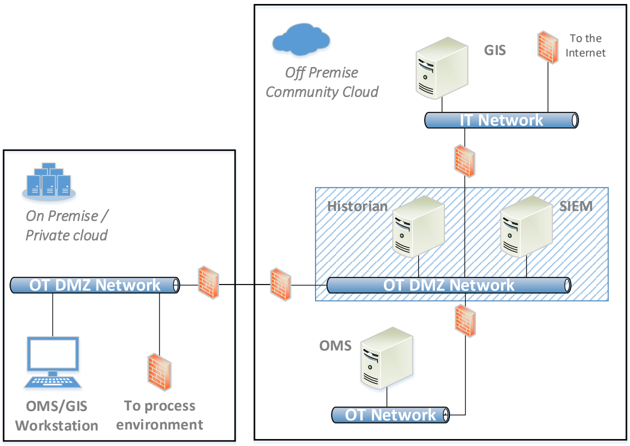


Figure 4
Small DSO's cloud-based OT system

Most of the above listed common disadvantages and risks identified can be mitigated if the small DSO switches to a hybrid cloud-based system architecture presented in Figure 4.

In this architecture, the DSO keeps in its control center only the operator workstations. The GIS and OMS are migrated to a remote community cloud data center. The high and medium risks identified during risk assessment are mitigated by the introduction of the SIEM and Historian, which are offered to all cloud customers by the cloud service provider (CSP). The most notable benefits of this system architecture compared to the original solution are the following:

- Information security is improved via segmenting the networks into OT, OT DMZ, and IT zones, aligned with IEC-62443.
- Security monitoring, awareness, monitoring, and audit capabilities via the SIEM and Historian in the cloud. These services reside in the OT DMZ and are differently shaded in Figure 4.
- Seamless upgrades to new versions of the OT services, i.e. the small DSO does not have to upgrade its sub-systems every 7-10 years as the community cloud provider will do that as part of its SLA.

A downside of this system architecture is that disaster recovery is not addressed. If the (small) DSO’s budget permits, it might maintain a cold or warm start subsystem in a separate community cloud in a different (geographic) location as a DR solution.

Conclusions

Based on our state-of-the-art review we concluded that there are no risk assessment-based studies that specifically tackle the problem of migrating smart grid OT services to a cloud computing architecture in a systematic way. That is the gap that we filled with the research presented in this paper. We presented a method valuable to any smart grid system owner and/or operator, which can help them to choose an optimal cloud migration strategy, fitting their specific requirements and maintaining an adequate level of information security.

We presented a baseline smart grid OT system architecture aligned with the IEC-62443 model. We identified smart grid-specific threat sources, threats, likelihoods, and potential impacts. We performed a detailed risk analysis of the common OT services from the confidentiality, integrity and availability (CIA triad) perspective. Additionally, we defined a baseline cloud migration strategy for smart grid OT services. We applied our risk assessment methodology in two cloud migration case studies. Our first case study involved a large DSO with complex OT capabilities. We theorized that there were highly motivated and capable threat sources, numerous IT and OT services, and possible attack vectors from untrusted networks, via physical access to the equipment in the field or via the communication infrastructure. We applied the proposed method and presented a hybrid cloud-based smart grid ICS architecture with disaster recovery (DR) capabilities. In the second scenario, we analyzed the security risks in a small DSO with a limited budget and IT staff. We applied the method again and proposed a fitting, mostly (community) cloud-based system architecture.

This work focused on information security. Therefore, the proposed cloud migration strategy and the case studies analyzed did not include additional key metrics, e.g. personnel and cloud service costs, level of management support, compliance with relevant standards and specifications (e.g. NERC CIP), or the temporal aspect of threat sources and threats, i.e. the fact that threat sources and threats change in time. The authors intend to incorporate these measures as part of their future work. Also, as part of their future work, the authors plan to research the technical details of cloud architecture model and migration processes represented in [17] [18], and to implement and test the presented risk assessment methodology in practice. Additionally, this research can be expanded by exploring and proposing the implementation of various mitigations based on the risk assessment methodology presented.

References

[1] New Standards for Security Categorization of Federal Information and Information Systems, NIST Federal Information Processing Standard (FIPS) 199, Feb. 2015

[2] International Electrotechnical Commission. Industrial communication networks - Network and system security - Part 3-3: System security

requirements and security levels. IEC 62443-3-3, Geneva, Switzerland, 2013

[3] D. Rosic, I. Lendak, and S. Vukmirovic, "A Role-Based Access Control Supporting Regional Division in Smart Grid System", *Acta Polytechnica Hungarica*, Vol. 12, No. 7, pp. 237-250, 2015

[4] D. Healey, S. Meckler, U. Antia, E. Cottle, "Cyber Security Strategy for the Energy Sector", ITRE Committee, Oct. 2016

[5] D. Kushner, "The real story of Stuxnet", IEEE Spectrum, Vol. 3(50), 2014

[6] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid", Defense Use Case, SANS ICS, Mar. 2016

[7] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids – A comprehensive survey", *Computer Standards & Interfaces*, Vol. 56, Feb. 2018

[8] J. Jarmakiewicz, K. Parobczak, and K. Maślanka, "Cybersecurity protection for power grid control infrastructures", *International Journal of Critical Infrastructure Protection*, Vol. 18, pp. 20-33, Sep. 2017

[9] J. E. Y. Rossebo, R. Wolthuis, F. Fransen, G. Björkman, and N. Medeiros, "An Enhanced Risk-Assessment Methodology for Smart Grids", *IEEE Computer*, Vol. 50, No. 4, pp. 62-71, Apr. 2017

[10] "Security for smart Electricity GRIDs", SEGRID Whitepaper, Edited by F. Fransen, and R. Wolthuis, Jul. 2017 [Online] Available: https://segrid.eu/wp-content/uploads/2017/07/Whitepaper-SEGRID.pdf

[11] S. Paul, and Z. Ni, "Vulnerability analysis for simultaneous attack in smart grid security," in Proc. 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, USA, 2017, pp. 1-5

[12] S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques", *Computers & Security*, Vol. 70, Sep. 2017

[13] Critical Infrastructure Protection (CIP) Standards, Version 6, North American Electric Reliability Corporation (NERC), Jul. 2016

[14] R. Paes, D. C. Mazur, B. K. Venné, and Jack Ostrzenski, "A guide to securing industrial control networks — (IT/OT) convergence", in Proc. 2017 Petroleum and Chemical Industry Technical Conference (PCIC), Calgary, Canada, Dec. 2017, pp. 89-96

[15] Evaluation of Cloud Computing Services Based on NIST SP 800-145, NIST Special Publication 500-322, February 2018

[16] US Government Cloud Computing Technology Roadmap Volume I, High-Priority Requirements to Further USG Agency Cloud Computing Adoption", NIST Special Publication 500-293, Oct. 2014

[17] Pooyan Jamshidi, Claus Pahl, Nabor C. Mendonça, Pattern-based multi-cloud architecture migration, 03. October 2016

[18] Mahdi Fahmideh, Farhad Daneshgar, Fethi Rabhi, Ghassan Beydoun, A generic cloud migration process model, European Journal of Information Systems, Volume 28, 2019 - Issue 3

[19] R. Garcia, and C. E. Chow, "Identity considerations for public sector hybrid cloud computing solutions", presented at the *2015 International Conference Computer Communication and Informatics (ICCCI),* India, 2015

[20] P. Gayatri, M. Venunath, V. Subhashini, Syed Umar Securities and threats of cloud computing and solutions, Coimbatore, India, 2018

[21] P. Deshpande, S. C. Sharma, and P. Sateesh Kumar, "Security threats in cloud computing", in Proc. 2015 International Conference Computing, Communication & Automation (ICCCA), Noida, India, 2015, pp. 632-636

[22] R. Wynn, "The 2016 Dirty Dozen: 12 cloud security threats", Cloud Security Alliance Southwest Chapter meeting, Cloud Security Alliance, Apr. 2016

[23] J. Y. Kimm, and Y. Kim, "Benefits of cloud computing adoption for smart grid security from security perspective", *The Journal of Supercomputing*, Vol. 72, No. 9, pp. 3522-3534, Sep. 2016

[24] T. Radwan, M. A. Azer, and N. Abdelbaki, "Cloud computing security: challenges and future trends", *International Journal of Computer Applications in Technology*, Vol. 55, No. 2, 2017

[25] B. Fortna, "Securing the federal hybrid cloud", Industry Insight, GCN, 2018

[26] Z. Cao, J. Lin, C. Wan, Y. Song, Y. Zhang, and X. Wang, "Optimal Cloud Computing Resource Allocation for Demand Side Management", *IEEE Transactions on Smart Grid*, Vol. 8, No. 99, pp. 1943-1955, Jul. 2017

[27] N. Popovic, D. Popovic, and I. Seskar, "A novel cloud-based Advanced Distribution Management System solution", *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 8, pp. 3469-3476, Aug. 2018

[28] Risk Management Framework for Information Systems and Organizations, NIST Special Publication 800-37, October 2018

[29] Smart Grid Security: Recommendations for Europe and Member States, Annex II. Security Aspects of the Smart Grid, European Network and Information Security Agency (ENISA), 2012

[30] B. Jelacic, D. Rosic, I. Lendak, M. Stanojevic, and S. Stoja "STRIDE to a secure Smart Grid in a hybrid cloud", in Proc. European Symposium on Research in Computer Security, SECPRE 2017, CyberICPS 2017, Lecture Notes in Computer Science, Vol. 10683, Oslo, Norway, 2017, pp. 77-90