Availability of a SCADA/OMS/DMS System – a Case Study

Martin Jensen, Cumhur Sel, Ulrik Franke, Student Member, IEEE, Hannes Holm, Lars Nordström, Member, IEEE

Abstract—With the advent of the smart grid, new challenges arise for electricity distribution. In particular, reliable power distribution will become evermore dependent upon information and communication technology (ICT). With this increasing dependency comes a need for a deeper understanding of the availability of those ICT components that maintain the power grid.

This paper presents a study in which all components of a supervisory control and data acquisition (SCADA), Outage Management (OMS) and Distribution Management (DMS) system at a power utility are analyzed from an availability perspective, identifying the parts of the system that contribute the most to overall system downtime. Furthermore, the case study involves a downsizing regarding the IT system architecture redundancy. This downsizing makes it very interesting to investigate how hardware redundancy relates to the overall SCADA/OMS/DMS system availability. Such knowledge is required to assess the rationality of the architectural restructuring decision, as well as for more general rational decision making when it comes to the ICT components of the power distribution grid.

It is concluded that even in the new architecture, the remaining hardware redundancy level is enough. Instead, it is found that most of the downtime of the SCADA/OMS/DMS system is caused by failing software, causing all the redundant hardware to become unavailable at the same time. Since the software is a third party piece from the supplier of the system, one important source of downtime can be seen as emanating from the requirements and procurement process of the company.

Index Terms—Availability, SCADA, OMS, DMS, ICT, Smart grid, Communication system, Critical information infrastructure

I. INTRODUCTION

Today, electricity distribution is facing many challenges: the lack of transmission capability, grid operation in a competitive market environment, the impact of competition on power system planning and operation, the determination of the optimum type, mix, and placement of sensing, communication, and control hardware and the coordination of centralized and decentralized control [1]. These challenges, and others, have lead to the proposal of the smart grid concept – the creation of a distribution grid that is secure, available and reliable, self-healing and redundant, massively customizable, and rapidly reconfigurable [2]. Smart grids are, according to the European Strategic Technology Platform, a vision for creating a flexible, accessible, reliable and economical grid for the future [3].

The challenges of the smart grid are inextricably linked to the continuous and reliable use of information and communication technology (ICT). It is clear that ICT in general is a key enabler for many of the features associated with the smart grid concept, such as intelligent load adjustment, decentralized power generation, optimal management of intermittent power sources and more sophisticated markets where price information is being signaled in real time to all market actors, including the consumers. Technological enablers such as smart meters, phasor measurement units and advanced supervisory control and data acquisition (SCADA) systems also hinge on state-of-the-art high availability ICT systems. As is pointed out by [2], this means that two infrastructures need to be developed and integrated – both the power delivery and the information infrastructure.

In this sense, making the grid smarter also means making it more dependent upon information systems. In the words of [2], "the electric power industry should recognize that the distributed computing infrastructure must be engineered and designed with as much technical discipline as the power system". This is very interesting from the perspectives of contingency planning and continuous availability – bearing in mind that the essential requirement of any modern day power system is that it be utterly reliable [4] – since the increased importance of software systems performing critical and complex functions increases the risk of software-caused failures. Internet server farms, data processing systems, financial services, telecommunications providers, microchip manufacturing plants, and digitally controlled manufacturing are some examples of businesses with very high availability requirements when it comes to uninterrupted power supply [2].

Loosely speaking, this increased dependence of the (smart) power grids on information and control systems is the motivation for the present paper. Along with this dependence comes the need for more thorough studies of the availability of the supporting ICT infrastructure, to ensure that it is – and will remain – sufficient. In particular, the present paper reports a study conducted at a power utility, investigating the availability of a SCADA/OMS/DMS (Outage/Distribution Management System) system used in a distribution network (0.4 to 130 kV). The system is used for managing the electricity grid, including locating and fixing outages. Furthermore, the study involves a downsizing regarding the IT system architecture redundancy. The rationale for the restructuring was economical.

The availability requirement on the SCADA/OMS/DMS system studied is that it must be available at all times (compare [4]). It is therefore important for the company to gain an in-depth understanding of the system availability and the factors that determine it. Specifically, due to the ongoing changes in system architecture, it is of great interest to understand how site and component redundancy are related to total system availability. The specific research aim of the case study is to
find (i) the worst case availability of the SCADA/OMS/DMS system and (ii) the factors that determine the system availability.

The remainder of this paper is structured as follows. Section II contrasts the present contribution with some related work in the fields of availability analysis within the electric power industry. Section III introduces some basic availability theory. In section IV, the architecture framework used throughout the study is presented. It is followed, in sections V and VI, by the main contribution: the results of the case study conducted and a discussion of their significance. Some concluding remarks are given in section VII.

II. RELATED WORK

A general and widely cited description of IT systems availability found in [5], where the authors present an "availability index" describing the relationship between various availability-increasing measures and their costs. The presented availability index gives guidance on improving systems availability, but it is not empirically validated in a structured way.

In [6] the authors present an approach for analytical service availability assessment, mapping dependencies between low-level ICT infrastructure and high-level services. The mapping, however, does not give a detailed description of the supporting ICT infrastructural elements, nor any weighting of how each element impacts the service availability. In [7] a similar mapping is presented, but here the focus is the impact of ICT infrastructure availability upon business processes, rather than upon availability assessment as such.

An effort to identify factors impacting software reliability is presented in [8]. The article includes the identification of 32 factors involved in the software development process, all of which impact software reliability. A ranking based on empirical research from 13 companies working with software development is presented, highlighting the most important factors influencing the software reliability. However, only the software development phase is addressed – how to ensure availability once systems already taken into service is not mentioned.

ICT system characteristics and their impact on future electricity distribution grids is addressed in [9], but this is a pure method paper without empirical content. In the later work [10], a more mature framework for reliability assessment of the interdependencies ICT systems and the power grid is presented, but there is still no empirical content.

III. AVAILABILITY

The availability of an item, whether a single component or a larger system, is often defined as

\[ A = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \]  \hspace{1cm} (1)

where MTTF denotes "Mean Time To Failure" and MTTR "Mean Time To Repair", respectively. The quotient is easy to interpret as the time that a system is available as a fraction of all time [11]. A more cautious availability estimate is found by instead using the "Maximum Time To Repair", corresponding to a worst-case availability \( A_{wc} \) scenario [5].

Due to the critical nature of power systems operation and control, this study has elected to use the more cautious "Maximum Time To Repair" estimate. Therefore, the availability calculated for the SCADA/OMS/DMS system in this study does not correspond to an average availability, but rather to a worst case scenario deemed most appropriate for the power distribution business.

The exponential distribution is central in most reliability work and the distribution most commonly used in applied reliability analysis. The reason for this is its mathematical simplicity and the fact that it gives realistic lifetime models for certain types of items, at least as a first approximation [11].

If the time to failure \( T \) of an item is exponentially distributed, it has the following well-known probability density function:

\[ f(t) = \begin{cases} \lambda \cdot e^{-\lambda t} & \text{for } t > 0, \lambda > 0 \\ 0 & \text{otherwise} \end{cases} \]  \hspace{1cm} (2)

The corresponding MTTF is simply the reciprocal of the parameter \( \lambda \):

\[ \text{MTTF} = \frac{1}{\lambda} \]  \hspace{1cm} (3)

The assumption of exponentially distributed lifetime has two important implications [11]:

1) A used item is stochastically as good as a new, i.e there is no reason to replace a working item.

2) When estimating MTTF etc. it is sufficient to collect data on the observed time in operation, and the number of failures. There is no need to keep track of the age of items.

It is worth noting that the second assumption is (at least implicitly) made in the ISO 9126 definition [12] of availability.

Making the same assumptions about the MTTR, this distribution can similarly be described by a parameter \( \mu \):

\[ \text{MTTR} = \frac{1}{\mu} \]  \hspace{1cm} (4)

The worst case availability \( A_{wc} \) of a component can now be computed from Eq. 1:

\[ A_{wc} = \frac{\mu}{\mu + \lambda} \]  \hspace{1cm} (5)

Again, this corresponds to the definition given in the ISO 9126 standard [12], viz. operation time divided by the sum of operation time and time to repair.

Systems rarely consist of a single component and oftentimes these components are connected in parallel. The case where we have \( s \) subsystems, where each subsystem \( i \) consists of \( k_i \) parallel components, and where the subsystems are connected in series is depicted in Fig. 1.

Assuming exponentially distributed MTTF and MTTR, the worst case availability for this general case can be obtained thus:

\[ A_{wc} = \prod_{i=1}^{s} \left( 1 - \left( \frac{\lambda_i}{\lambda_i + \mu_i} \right)^{k_i} \right) = \prod_{i=1}^{s} \left( 1 - (1 - A_i)^{k_i} \right) \]  \hspace{1cm} (6)
As seen in Equation 6, this assumes that the failure and repair rates are the same ($\lambda_i$ and $\mu_i$) for all components in a subsystem $i$.

IV. ANALYSIS FRAMEWORK

In this section a theory for assessing the availability of systems similar to the SCADA/OMS/DMS system is developed. The aim of the analysis framework is two-fold: first to provide a (worst-case) assessment of the system availability, and second to give an understanding of how the on-going changes in the configuration (redundancy) of the system will affect the overall system availability.

A. Causal Enterprise Architecture Analysis

The method proposed in this paper aims to aid rational decision making when designing ICT systems and infrastructure for control and automation systems in power distribution grids. To achieve this, we depart from a tradition within Enterprise Architecture focusing on decision-making using scenario-analysis, delineated in [14], [15] and recently described as a causality-based approach to Enterprise Architecture [16].

The basic idea is simple. To provide relevant decision-support, the goals must first be identified. In our case, the goal is high availability of a SCADA/OMS/DMS system. For analysis, the goal is decomposed into clearly operationalized sub-goals, viz. component availabilities of the system. Also, the architecture of the system needs to be documented, so that the interactions of the component availabilities can be properly taken into account.

The formal machinery of availability calculations, constituting a crucial aspect of the approach, was presented in section III.

B. An analysis framework based on component MTTF and MTTR

To conduct the analysis of system availability, a model of the system architecture is required. The analysis framework is presented as a meta-model containing entities and attributes amenable for availability calculations. Instantiating the meta-model yields not only a system model in general, but also the mathematical framework for availability analysis according to section III.

Figure 2 shows multiplicities for the relations between entities. These multiplicities form the basis of redundancy modeling, together with the information about what kind of redundancy – serial, parallel or $k$-out-of-$n$ – is present with respect to the various entities. The following entities make up the metamodel:

- **System** The system of interest for availability assessment. The SCADA/OMS/DMS system is the objective of this case study.
- **Site** A complete redundant installation of the system.
- **FEP** A hardware/software combination that is responsible for communicating with Remote Terminal Units (RTU:s), sensors and control units in the power grid that the SCADA/OMS/DMS system controls and acquires data from.
- **LAN** Connects components of a site to each other. Notably, clients are connected to servers. In the case of the SCADA/OMS/DMS system, the LAN:s are Ethernet based networks.
- **Communication System** Needed for system operators to be able to communicate with electricians in the field.
- **Client** Devices that are used by system operators to use and control the system. Clients consist of software and hardware. The SCADA/OMS/DMS system clients are often referred to as workstations.
- **Server** The main computers storing and processing data. Clients connect to these to view and manipulate data. Besides consisting of software and hardware, servers are also considered to consist of data.

The data entity deserves some extra explanation. It has been modeled the way it is as a way to balance resemblance of the real world with a model that is simple enough to be manageable. In the real world, data does not have MTTF or MTTR values. However, by modeling backup properties as data MTTR and MTTF values, information about backups can be fitted into the analysis framework. MTTF in this case refers to how often data becomes unavailable. MTTR refers to how long it takes from the time data is lost until it is restored to the previous state. Notably, backup frequency is only indirectly involved in the latter measurement. This simplification has been made to keep the investigation manageable, but may have consequences for the reliability and validity for the study.

The analysis framework presented can be used for decision making. As pointed out by [10], one may model and analyze the present situation and any planned changes, scenarios, in the IT architecture. In the real world, experimenting with different scenarios would be an expensive and difficult process, causing unreliable and unpredictable systems. Modeling using the analysis framework allows the impact on availability caused by possible changes within the scope of the framework to be analyzed before any changes are actually implemented.

C. Data collection through interviews

Personal interviews played a vital role in gathering the data for the study. Interviews were used at the following stages in the study:

1) To gain a general understanding of the SCADA/OMS/DMS systems, informal interviews...
2) Interviews were used to collect the qualitative empirical data required to construct the metamodel (and model) used for analyzing the availability of the system. This information is thus the main basis for Fig. 2. The interview concerned the components that constitute the SCADA/OMS/DMS system, the connections between these, and which components need to be available for the system as a whole to be available.

3) Interviews were conducted with informants 1 through 4 to collect the quantitative empirical data that, when fed into the analysis framework, allows for the calculations of system availability. In the present study, this information is estimates of how often components fail on average – MTTF – and how long it takes to repair them in a worst-case scenario – MTTR.

Written documentation about the system was initially believed to be a good and accurate source of data for information about the system configuration at the component level. However, it turned out that the company was not be able to assist the study with this data. Instead, interviews with system experts had to be used to document the configuration of the system.

The interviews can be considered a mixture between an open-ended (unstructured) interview approach and a closed, fixed-response (structured) interview approach. First, all informants were told about how the analysis framework was constructed and that the interview goal was to find accurate values for the MTTF and MTTR of system components. The informants were allowed to ask questions until the interviewers felt certain that the goal of the interview was well understood by the subject. Then, the subjects were asked to answer the questions outlined in Table I.

### TABLE I
**INTERVIEW QUESTIONS FOR MTTF AND MTTR**

1. How long has the type of component been in use and observed by you? (Observed time, OT)
2. How many times has the system failed during this time period? (Number of failures during the time period, NF)
3. What is the worst case repair time for this component? (MTTR)
4. How many of these components are there? (Redundancy)
5. How many, and which, of these components must be available in order for the entire system to be available? (Redundancy)

The same questions were asked for all entities, mutatis mutandis (i.e. small modifications to fit data being available in databases as opposed to system components being available).

Answers to questions about component MTTR and MTTF values had to be converted into availability measurements. While MTTR was asked for explicitly, MTTF had to be determined from the interview questions asked about observed time, OT, and number of failures during that time, NF. In other words, $MTTF = OT/NF$. OT and NF could be determined directly from interview questions. The special case where
NF = 0 is handled by taking the limit as NF approaches 0:

\[ A_{\text{inf}} \bigg|_{NF=0} = \lim_{NF \to 0^+} \frac{\text{OT}}{\text{NF} + \text{MTTR}} = 1 \quad (7) \]

The interpretation of components that never fail will be further discussed in section VI.

V. CASE STUDY DATA

This section describes the data collected through the interviews, and gives some background on the informants who provided the information. Table II contains the quantitative data collected as well as the corresponding calculated availabilities.

A. Informant 1

Informant 1 has a background consisting of many years of experience from both the supplier of the system and with the actual system at the company. He has been working with the SCADA/OMS/DMS system as a systems engineer for several years, and confirmed that no components important for the system had been left out in the model used in the study.

The system consists of several different servers. Many component have been upgraded or changed during the last years, making one year a good time frame for understanding the availability of today’s components. The supplier regularly provides software updates, adding new features and fixing problems. For most of the hardware there are two kinds of SLA:s:

1) 24/7, meaning that the consumer can get support any time of the day with a calling-up time of four hours.
2) 13/5, meaning that support is available weekdays 7.00 a.m. – 8.00 p.m. with a calling-up time of four hours. In this case, if a failure occurs 8.00 p.m. on a Friday the consumer cannot get support until 7.00 a.m. Monday (59 hours) with an additional four hour for calling-up time, i.e. 63 hours.

Informant 1 pointed out that although there is only one report server at each site, in case of a failure, it is very likely to be possible to redirect traffic to the report server at the other site. This means that the repair time is very short – only a few minutes.

Data from the interview is presented in Table II, giving the data for the observed time periods, failures during that time period, and repair times.

B. Informant 2

Informant 2 is responsible for the telephone communication system and has been working with the SCADA/OMS/DMS system for as long as the system has been in use, approximately five to six years as a systems engineer.

The telephone system consists of one switch which has two CPU halves and has been used for six years. The switch is connected to a server named Computer Telephony Integration (CTI) server. The switch is newly installed, but very similar to a system that has been used for six years. Informant 2 concludes that since the components and configurations are the same, there is no problem using his observations of the old installation as data for calculations.

That CTI servers’ job is to direct received calls from electricians working in the field to the correct operator, i.e. to the operator who currently is controlling the part of the grid where the electrician is. If something happens to the CTI server, there is a fall back system which is based on that electricians in the field will have to call a phone number to an operator who in that turn manually directs the call to the right operator. That however, works only in low stress situations – not in outage situations.

There is one CTI server at each site. Data from the interview is presented in Table II.

C. Informant 3

Informant 3 has worked with the SCADA/OMS/DMS system since September 2009 and is responsible for data backups and data availability.

Data is backed up from the Main NMS Servers, the Main Database Servers and the Reports Database Servers. The backup is made once a week. It takes up to two hours to take the backup and it takes place some night between Saturday and Tuesday. One Main NMS server and one database server is stopped in order to take the backup. So the NMS server that has been taken down has to “catch up” after the backup and this can take up to two hours. The database catch up takes less than one hour. A full backup restore takes about 12 hours, both for NMS and database. There has not occurred a single time for the last twelve months that data had to be restored from a backup. This was confirmed by Informant 1.

Data sticks caused by software bugs are a big problem on the NMS servers. This has occurred two times in one year and it can take up to three hours before the stick is fixed. During a stick the system is very complicated to use, i.e. the NMS data cannot be seen as available during this time period. However, once the stick is fixed, the system is available immediately. There is no need to restore any data from backups. The data stick bug has been around for several years. Data from the interview is presented in Table II.

D. Informant 4

Informant 4 is a systems engineer and an expert on the Front End Protocols (FEPs) and the Local Area Network (LAN). He has been working with the SCADA/OMS/DMS system for more than five years.

Informant 4 points out that the network that connects all the sites and component out in the grid is highly redundant, complex and so large that it would need a case study itself. It is not considered a part of SCADA/OMS/DMS and he knows very little about it, as all people at the SCADA/OMS/DMS department do.

The Local Area Network (LAN) is redundant with a double network on each site, so every component has two separate network lines to the separate LANs. This means that if one LAN fails there is a backup LAN available right away. So, for the LAN to become unavailable, both LANs must fail.
Informant 4 could not recall the maximum repair time for the FEP hardware so he instead referred to the support agreement with the vendor, which was a 13/5 agreement. Data from the interview is presented in Table II.

### E. Informant 5

Informant 5 has been the contact person for the study at the company. He is the head of the system group responsible for running the SCADA/OMS/DMS system. According to Informant 5, after the downsizing the number of workstations (clients) at a Backup site will be only 15% of the number at a Primary site.

However, in a "normal outage situation" at least 20% of the workstations at a Primary site will be needed to handle and control the SCADA/OMS/DMS system. Informant 5 also points out that if a major outage situation occurs, the system requires approximately 78% of all workstations to control and handle the situation. Thus, there is a discrepancy between the fact that 20% of all workstations are needed to handle a normal outage situation, but only 15% are planned to be at a backup site.

### VI. ANALYSIS AND DISCUSSION

This section aims to discuss and interpret the data presented in the previous section. First, the concept of system availability is dissected. Since a SCADA/OMS/DMS system has a lot of somewhat independent functionalities, it is a non-trivial matter to draw the line between the system being up and down, respectively. A tentative definition is given. Second, the availability under the definition adopted – of the SCADA/OMS/DMS system is discussed. The section is concluded with a sensitivity analysis of which factors are the most amenable to improvement, i.e. an attempt to find the most bang for the bucks strategy for availability improvement.

#### A. When is the system available?

In most cases, the data received regarding what components need to be available for the system as a whole to be available is unambiguous. However, there are some cases where a short discussion is needed before the data analysis is continued. In the following analysis, the logic that has been used is that there is no point having an outage management system that does not have the capacity to handle an outage situation. Therefore, in system states where SCADA/OMS/DMS system would not be able to handle an outage situation, the SCADA/OMS/DMS system is considered unavailable.

Even though it is possible to use the telephony system when the CTI system is down (through manual call diverting) the backup solution does not have capacity enough to work in an outage situation. Therefore, the telephone system, and thus the
SCADA/OMS/DMS system, is defined as unavailable when the CTI system is down. Data sticks are such major problems that all the NMS servers and thus SCADA/OMS/DMS system are considered unavailable in a data stick state.

If the connection to any set of RTUs (grouped by a FEP) is lost, the connection to at least 50 RTUs is lost. This means both that it will be impossible to fix outages in areas covered by those RTUs and that it will be likely that new outages occur in these areas. Therefore, SCADA/OMS/DMS system is considered available when connections are available to all sets of RTUs.

Following the reasoning outlined in section V by informant 5, a site is defined as available only if there are at least 20% (the number needed to handle an outage situation) of all clients available at that site. Notably, that means that a backup site will never be considered available, since there are only 15% of all clients there.

B. SCADA/OMS/DMS system availability

Under the definition given above, the worst case availability of a SCADA/OMS/DMS system consisting of only a Primary and a Backup site is 92%. This refers to full availability, i.e. all system functions are available. However, most of this unavailability corresponds to the system being almost available, i.e. having lost connectivity to only a few RTUs. Table III summarizes the component-wise availabilities, as well as the overall subsystem and system availabilities.

<table>
<thead>
<tr>
<th>Component and System Availability</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTI server</td>
<td>0.99932</td>
</tr>
<tr>
<td>Main NMS Servers</td>
<td>0.99932</td>
</tr>
<tr>
<td>Workstations</td>
<td>1 for primary site, 0 for backup</td>
</tr>
<tr>
<td>LAN A</td>
<td>1</td>
</tr>
<tr>
<td>LAN B</td>
<td>1</td>
</tr>
<tr>
<td>IIS Report Server</td>
<td>1</td>
</tr>
<tr>
<td>LV-Web Server</td>
<td>0.99977</td>
</tr>
<tr>
<td>CTS Server</td>
<td>0.99863</td>
</tr>
<tr>
<td>Main Database Servers</td>
<td>1</td>
</tr>
<tr>
<td>Report Database Server</td>
<td>0.99286</td>
</tr>
<tr>
<td>Telephone Switch</td>
<td>1</td>
</tr>
<tr>
<td>Primary site</td>
<td>0.98991849</td>
</tr>
<tr>
<td>Backup site</td>
<td>0</td>
</tr>
<tr>
<td>FEPs</td>
<td>0.93515018</td>
</tr>
</tbody>
</table>

The main components causing downtime are the following:
- The various supplier software running on the FEPs
- The lack of clients at the backup site
- The NMS software causing data sticks
- The CTS server software
- The CTI server software

It deserves to be mentioned that the FEP software failures only causes the SCADA/OMS/DMS system to lose contact with some parts of the grid and that the CTI server only reduces the SCADA/OMS/DMS system capacity. The NMS software data stick bug however renders the entire SCADA/OMS/DMS system and all its sites fully unavailable.

The high level of redundancy leads to very little downtime caused by failing hardware. Rather, software faults that occur simultaneously throughout the redundant hardware architecture is the major cause of downtime.

C. Sensitivity analysis

From the perspective of a decision maker aiming to increase the overall system availability of a SCADA/OMS/DMS system, it is interesting to investigate how improving the availability of the different components impacts the overall system availability. Such a sensitivity analysis is shown in Table IV. For each component listed, the increase in system availability in case the component at hand was completely available is given. This gives a hint of the relative importance of the various components from an availability perspective.

<table>
<thead>
<tr>
<th>Component set fully available</th>
<th>System availability</th>
<th>Change (percentage points)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Baseline)</td>
<td>92.57%</td>
<td>N/A</td>
</tr>
<tr>
<td>IEC-104 Software</td>
<td>95.13%</td>
<td>2.56%</td>
</tr>
<tr>
<td>FEP DDN Software</td>
<td>94.48%</td>
<td>1.91%</td>
</tr>
<tr>
<td>ICCP Software</td>
<td>93.52%</td>
<td>0.95%</td>
</tr>
<tr>
<td>NFE Software</td>
<td>93.38%</td>
<td>0.81%</td>
</tr>
<tr>
<td>Lack of clients at the backup site</td>
<td>93.37%</td>
<td>0.80%</td>
</tr>
<tr>
<td>CTS server software</td>
<td>92.69%</td>
<td>0.12%</td>
</tr>
<tr>
<td>CTI server software</td>
<td>92.63%</td>
<td>0.06%</td>
</tr>
<tr>
<td>Data sticks caused by NMS software bugs</td>
<td>92.63%</td>
<td>0.06%</td>
</tr>
</tbody>
</table>

D. Interview bias

Interview bias, often referred to as “the interview effect”, involves that a respondent is influenced in his or her attitudes or opinions through uncritical suggestion, rather than through critical weighing of the available facts upon both sides of an issue [17]. Two major reasons for interview bias include 1) the social distance between the interviewer and respondent, and 2) the perceived threat of the interview schedule question [18].

Regarding this study, there should not be any threats of interview bias due to social differences. The interview were also primarily of a structured form, which according to [19] reduces the threat of interview bias. However, the questions regarding availability could be perceived as “threatening” since they somewhat reflect the performance of the organization, and thus also the respondent. On the other hand, this does not pose much of a threat to the validity of the study since the involved measurement error presumably is evenly spread across the entire data set. Thus the analysis would still point in the same direction, but with availability scores slightly worse than assessed.
VII. Conclusions

It is not hardware problems that cause downtime. The level of hardware redundancy is sufficient, and further downsizing can certainly be warranted. In fact, there are arguments that the increased complexity caused by excessive hardware redundancy causes overall system availability to decrease [5], [20]. The return on availability investments is likely to be a lot higher if invested in eliminating single points of failure than in maintaining excessive hardware redundancy. Still, an example of a situation where more hardware is needed is the proposed backup site, since the number of workstations at a backup site is not enough to handle a normal outage situation.

The main causes of downtime in the SCADA/OMS/DMS system are various failing pieces of software. Since software that spans across several hardware machines constitute single points of failure, the failing software’s effect on downtime is independent of redundant hardware. Five of the pieces of software causing SCADA/OMS/DMS system downtime come from the supplier. Some of the problematic bugs in those pieces of software have been around for several years. The fact that the supplier during this time has provided several updates for software, adding new features, but not fixing the bugs indicates a procurement problem. The fact that it is likely to be possible to greatly reduce downtime by introducing a new procurement process, with requirements being set up is well aligned with the finding in [21] that requirements and procurement is one of the most important causally linked factors affecting system availability. The fact that software often causes problems is also confirmed by [21] as well as by [5], [20].

The most important factor determining the availability of the SCADA/OMS/DMS system is perhaps the definition of availability. In this study, the system has been considered available only when available enough to handle an outage situation anywhere in the grid controlled. If the definition is changed so that the system is considered available even when it has lost contact with some part of the grid (i.e. some FEP software has failed), the availability increases dramatically.

Since the maximum time to repair, rather than the mean time to repair, has been used throughout the present study, all figures represent the worst possible case. Although the worst possible case is interesting, it would also be interesting to re-do the study using the mean time to repair as the measurement. This way, it would be possible to translate the results regarding system availability into expected, rather than worst-case, downtime.

The focus in the present study has been structural redundancy. Most potential single points of failure discussed by [5], [20] and [21] have been eliminated in the SCADA/OMS/DMS system, by the introduction of redundancy. This is true for most hardware, but also for the network and even for the physical environment (multiple sites). If wanting to improve the availability of the SCADA/OMS/DMS system further, the company needs to look not at additional hardware redundancy, but rather at fixing existing single points of failure. This includes “soft” factors causally linked to availability such as procurement. Another such factor, found to be of major importance by [21] is change control.

ACKNOWLEDGMENTS

The authors would like to thank the informants and the company for their time and effort.

REFERENCES