Framework for Threat Based Failure Rates in Transmission System Operation

Samuel Perkin,
Gudjon Bjornsson,
Iris Baldursdottir,
Magni Palsson
System Operation and Market
Landsnet
Reykjavik, Iceland
Email: samuelp@landsnet.is

Ragnar Kristjansson,
Hlynur Stefansson,
Pall Jensson
Department of Science and Engineering
Reykjavik University
Reykjavik, Iceland

Efthymios Karangelos,
Louis Wehenkel
Montefiore Institute
University of Liege
Liege, Belgium

***Abstract*—Reliability of electrical transmission systems is presently managed by applying the deterministic N-1 criterion, or some variant thereof. This means that transmission systems are designed with at least one level of redundancy, regardless of the cost of doing so, or the severity of the risks they mitigate. In an operational context, the N-1 criterion provides a reliability target but it fails to accurately capture the dynamic nature of short-term threats to transmission systems. Ongoing research aims to overcome this shortcoming by proposing new probabilistic reliability criteria. Such new criteria are anticipated to rely heavily on component failure rate calculations. This paper provides a threat modelling framework, using the Icelandic transmission system as an example, highlighting the need for improved data collection and failure rate modelling. The feasibility of using threat credibility indicators to achieve spatio-temporal failure rates, given minimal data, is explored in a case study of the Icelandic transmission system. The paper closes with a discussion on the assumptions and simplifications that are implicitly made in the formulation, and the additional work required for such an approach to be included in existing practices. Specifically, this paper is concerned only with short term and real-time management of electrical transmission systems.**

***Keywords*—failure rates; threat credibility indicators; power system operation; spatio-temporal risk; reliability management;**

I. Introduction

Electrical transmission systems are becoming more difficult to control given the installation of dynamic devices, a growing share of distributed generation in the energy mix, the liberalisation of energy markets, and reduced investment in new transmission infrastructure [1]. Operators are forced to drive the system closer to its limits, in order to provide the expected level of service, requiring more operational risks to be accepted.

Current practice in managing risk relies upon the N-1 criterion, such that system operators aim to maintain a reasonable level of service after the potential loss of any single major component (e.g. a transmission line, generator, transformer, or bus bar). The N-1 criterion is enforced by some regulators and is discussed within ENTSO-E policies [2]. The application of this criterion by transmission system operators (TSOs) varies due to different interpretations and system risks. However, the N-1 criterion does not adequately mitigate threats associated with exogenous phenomena (e.g. weather), system protection failure, common failure modes of multiple components, and uncertainty in load and renewable generation forecasts. It also fails to consider the likelihood and consequences of faults occurring [3], treating all N-1 faults with equal importance. Risks that aren't mitigated by the N-1 criterion alone tend to be indirectly assessed and managed through a range of tools (e.g. dynamic simulations, energy management systems, SCADA, WAMS) and operator experience [1].This can be defined as a Reliability Management Approach and Criterion (RMAC).

In order to upgrade TSO procedures to include probabilistic RMACs, such as those proposed in [4]–[12], there is a need to upgrade TSO data collection and modelling. Ideally, the data collection and models should allow the TSO to estimate the likelihood and consequence (i.e. risk) of all threats to which the system is vulnerable, at least those dependent upon exogenous variables. Specifically, there is a need to improve data collection and modelling of failure rates, and hence fault probabilities, for both short and long term risk assessments.

This paper investigates the data and modelling requirements for calculation of failure rates on the Icelandic transmission system, by providing a framework for threat based failure rates. This is done by exploiting the link between the occurrence of contingencies and specific threats to the system, given that some threats are somewhat predictable. The main operational threats are described and categorised, with a brief review of existing models and their data requirements. The data requirements to model these threats are then compared with existing data collection, to suggest why stochastic models are not already in wide-spread use. Methods of estimating contingency probabilities as a function of credible threats are then described, and briefly investigated for part of the Icelandic transmission system.

II. Linking threats and failure rates

Probabilistic RMACs that have been proposed in literature [4] deal with both discrete contingencies (e.g. line faults) and continuous uncertainty (e.g. load forecast error, variability

of renewable generation). The operation of the transmission system is then optimised to mitigate the risks associated with discrete and continuous uncertainty. The cause of the events within the discrete contingency set, and the calculation of their probabilities, is not often elaborated on [13]–[15]. It is often assumed that the probability of a contingency occurring is constant; calculated from historical fault data. The Nordic grid disturbance statistics suggest that failure rates/probabilities are not constant, given that they vary month by month due to the seasonality of specific threats [16]. Section 2 discusses this link, and proposes a framework for describing contingency probabilities as a function of threats and their individual failure rate models.

A. Main operational threats

Threats to electrical transmission systems are defined in [17] as "any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof". A threat can be categorized as a natural (exogenous) threat, human error, sabotage, or technical [18]. The probability of a threat causing damage to a system depends upon the system's susceptibility to the particular threat [15]. When a threat has been realised, it can be described as the "primary cause" of a fault [19].

A study by [20] describes the natural threats to the Icelandic electrical transmission system. These are listed below, along with some additional credible exogenous threats:

- Wind (galloping)
- Wind (structural failure)
- Ice loading
- Lightning strikes
- Earthquakes
- Landslides/Avalanches
- Volcanic eruptions
- Glacial floods (jokulhlaup)
- Snow accumulation
- Salt pollution
- Generator failure
- Load failure
- Solar flares
- Human error (random)
- Human error (control errors)
- Human error (due to proximity of planned work)
- Sabotage
- Technical
- Other (unknown/invisible cause)

The realisation of most of these threats depends upon some prevailing, observable environmental conditions. It is unlikely to have a failure due to snow accumulation in the middle of summer, or a structural failure due to wind loading on a calm day. Therefore, given a combination of data measurement and modelling, it should be possible to anticipate faults due to some of these threats or rule some of these threats out for particular time intervals. The considered elimination of threats should improve operator awareness of system risk, and hence their ability to calculate the likelihood of faults.

For an extended list of threats considered within each of the Nordic transmission systems, refer to the appendix of [19]. Major threats to the Portuguese system are looked at comprehensively in [13], [21], [22].

Human error involves the random failure of one or more components due to physical damage (i.e. during maintenance or adjacent construction) or by incorrect control (accidentally switching the state of a component). Trivially, the occurrence of human error depends on the presence of humans [23]. Therefore, all controllable components are only at risk of human errors due to incorrect control. All other components are at risk of physical damage due to human error when humans are present. Therefore, knowledge of maintenance activities or nearby construction can be used as an input for a model to anticipate random human error.

Literature on antagonistic damage to electrical power systems is largely based upon attacker-defender simulations, with a heavy emphasis on game theory and trying to find optimal defence strategies in response to different attack strategies. The probability of sabotage is not easily calculated given the classified nature of data related to the subject. Sabotage of transmission systems may also take the form of cyber-attacks [24]. In general, some latent possibility of sabotage can be modelled by increasing the failure rate of all components slightly, as done with human error. Possibly with adjustment factors based on the accessibility of the component to the public, its visibility, and its perceived (or actual) importance to the system. Alternatively sabotage may be modelled by considering an informed attacker who optimises their attack to maximise consequences, given some finite resources (e.g. manpower) [25].

Technical failures can be described as those that occur due to continued use and wear of components, or due to hidden damage of components. They occur due to no apparent forcing by exogenous variables at the time of failure. When potential for a technical failure is observed, it is normally corrected through maintenance activities. Therefore, given adequate observation and maintenance, any residual risk of technical failure must be due to hidden or irreparable damage. Under the assumption of perfect maintenance, technical failures can be considered to have a constant failure rate [25]. However, it may be argued that a component operated close to its limits is more likely to undergo a technical failure than one that is lightly-loaded. Significant literature exists on linking maintenance, component age and component health to failure rates, but is not discussed in this paper.

B. TSO modelling of failure rates

No stochastic models related to operational risks are presently used for system operation in Iceland. This is due to a combination of the following reasons:

- A lack of proven economic value in updating existing practices
- Intuitive approach is currently fit-for-purpose
- Low confidence in the accuracy of some models
- Distrust of black-box models

- Models still considered to be in research and development phase

As discussed in [3], TSOs commonly test that their system can survive N-1 or even N-1-1 faults (occurrence of two independent N-1 events) without significant loss of load. A number of probabilistic risk-assessment tools are already being developed and tested by various TSOs in planning and operation [1]. The Nordic countries collect and share fault statistics, and categorise faults by a number of causes [16]. Using these fault statistics, some Nordic TSOs and DSOs (Distribution System Operators) calculate historical failure rates for use in the Promaps reliability software package, described in [26], [27].

Another common use of fault statistics is to calculate multi-level failure rates, where the failure rate is separated into a "normal weather" failure rate and a number of "severe weather" failure rates, as described in [28]–[33]. This approach is generally used for planning longer term activities and not used within the short-term or real-time operational contexts. As stated in [34], the resolution of this approach might not be sufficient for operational purposes but it should suffice for long-term planning. It should be noted that "severe weather" is not a specific threat, but describes a broad environmental state in which some subset of threats become credible and more likely. Such an approach cannot distinguish between a storm that may cause icing and a storm that may cause line to line faults due to galloping, landslides or lightning strikes.

In a general sense the N-1 approach to reliability considers the vulnerability of the system without considering the specific threats to the system. It assumes that any component is capable of experiencing a fault at any time, without any consideration of how this may occur. Specific, high impact low probability (HILP) threats, such as sabotage and severe natural disasters, are generally considered as scenarios which are specifically prepared for using expert knowledge. On the Icelandic transmission system, outages due to storms are normally mitigated through expert knowledge and intuitive understanding of how a storm will affect outage probabilities. Despite the acknowledgement of a link between the likelihood of threats and the likelihood of contingencies, failure rates are not currently described in terms of specific threats.

C. Framework for threat based failure rates

The approach proposed by this paper is to use observational data and stochastic models to calculate the likelihood of failure, conditional on specific threats. Doing so will allow failure rates to be variable in the context of short-term transmission system operation. This approach is described by Fig. 1. This draws inspiration from the ideas discussed in [13], [18], [21], [35], putting such approaches into a generalized framework.

For a given component, there is some finite set of threats which may lead to failure. Those which can be discerned by the TSO are defined generally as visible threats whilst those that aren't are defined as invisible threats (equivalent to the "other" primary cause listed in the Nordic fault statistics [19]). Within the set of visible threats a particular threat may be

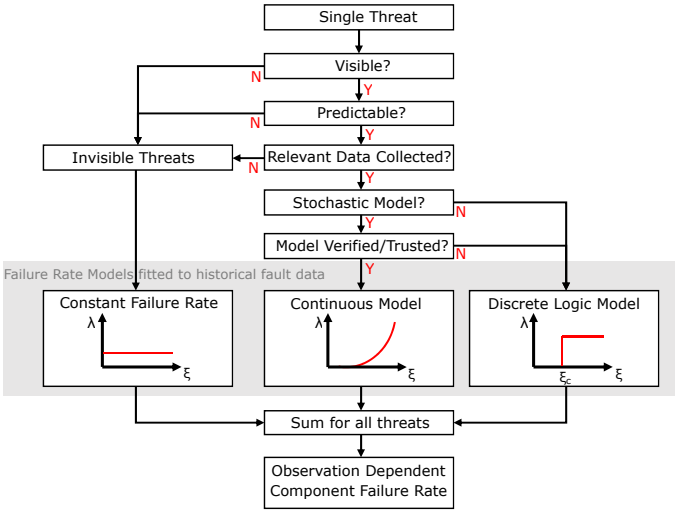

Fig. 1. Framework for the choice of a specific failure rate model given the nature of the threat, and the availability of data and trustworthy models

predictable or not. A predictable threat is one that, given some observational data, an expert can determine whether it is more or less likely for a fault due to the threat to occur. Those which are unpredictable can also be considered as invisible threats within the context of calculating failure rates, as they are essentially random. This is also the case for predictable threats for which the relevant data is not collected, as although it could be visible, it is invisible to the TSO due to the lack of data. All invisible threats must be lumped into a single random threat for which there is a constant failure rate, similar to how all threats are treated by TSOs at present.

A predictable threat for which the relevant data is observed may have an associated stochastic model. For example, a predictive model of icing on transmission lines may be based on temperature, wind and humidity data. Although such models exist, they may not be adopted by TSOs due to issues with verifying the model (i.e. lack of historical data) or a lack of trust in the model.

The proposed framework contains the present day approach (all threats are considered as invisible), outlines the requirements to transition to full stochastic modelling, and suggests a discrete logic model as an intermediate step to overcome a lack of historical data. This framework allows for a gradual transition towards the ideal approach of spatio-temporally variable failure rates.

1) Data set description: We presuppose there exists a finite set of M independent and mutually exclusive threats defined by $\Psi = \{\psi_1, ..., \psi_M\}$. Furthermore, for a given component and an observational period of $[0, T]$ we define a dataset, F, of N observed failures as:

$$F = \{(t^1, \psi^1), ..., (t^N, \psi^N)\}, \quad \text{where } \forall i : t^i \in [0, T] \text{ and } \psi^i \in \Psi. \quad (1)$$

The pair (t^i, ψ^i) is interpreted as meaning that a failure

occurred at some time $t^i \in [0, T]$ and its root cause was attributed to threat ψ^i. It should be noted that no information regarding outage duration is used, even if this information is recorded in practice.

Given this data set, F, we denote by x_t a time-series of failures, defined as $x_t = 1$ whenever $t = t^i$ for some failure occurrence i in F, and 0 otherwise. Similarly, we denote by $x_{k,t}$ the time-series of failures attributed to threat ψ_k, defined as $x_{k,t} = 1$ whenever $t = t^i$ and $\psi^i = \psi_k$ within F and 0 otherwise. Note that $x_t = \sum_{\psi_k \in \Psi} x_{k,t}$, since at most one failure may occur at any moment in time, and can only be attributed to a single threat. We furthermore denote by $\sum_t x_{k,t}$ the total number N_k of failures in F attributed to threat k. Note also that $\sum_{\psi_k \in \Psi} \sum_t x_{k,t} = N$.

For the purpose of modelling component failure rates, we decompose our set of all possible threats, Ψ, into three mutually exclusive and exhaustive subsets of threats, denoted respectively by Ψ_u, Ψ_v, and Ψ_d, where:

- the subset $\mathbf{\Psi}_u$ contains the unpredictable threats whose induced failures will be modelled by a constant failure rate;
- the subset $\mathbf{\Psi}_v$ contains those threats whose induced failures will be modelled by a variable failure rate;
- the subset $\mathbf{\Psi}_d$ contains those threats whose induced failures will be modelled by a discrete logic model.

For the remainder of this document, the indices $\{i, j, k\}$ are used to represent a specific threat that is contained within Ψ_u, Ψ_v, or Ψ_d, respectively.

2) Constant failure rate model: For an unpredictable threat $\psi_i \in \Psi_u$, we assume a constant threat-specific failure rate, estimated from our data set by:

$$\lambda_i = \frac{\sum x_{i,t}}{T}. \tag{2}$$

This is simply a statistical mean rate of failure and would be expected to equal the true failure rate given a long enough period of time.

3) Continuous failure rate models: For those threats $\psi_j \in \Psi_v$ that are modelled by general (possibly continuous) failure rate models, we denote by $\lambda_j(\xi_t)$ their failure rate function, where ξ_t is an observation or forecast of one or more exogenous variables at time t. We do not elaborate on the types of functional dependencies, nor on the procedures for estimating their parameters from the available data set $x_{j,t}$. An example of a continuous model for transmission system reliability is discussed in [36], where the failure rate is a linear function of temperature and wind speed, although this particular example does not describe a threat-specific model.

For cases in which a stochastic model is not sufficient for the calculation of failure rates (due to problems with verification or a lack of trust in the model), the model should be simplified as a discrete logic model.

4) Discrete logic model: For each threat $\psi_k \in \Psi_d$ to be represented by a discrete logic model, we assume that a threat specific credibility indicator, $\alpha_k(\xi_t) \mapsto \{0, 1\}$, is given and which must satisfy the following condition:

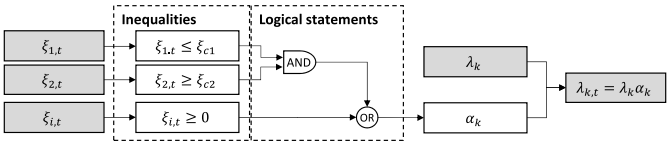

Fig. 2. Example of how observations of exogenous data can be used in combination with inequalities and logical statements to calculate a threat credibility indicator, and hence a threat conditional failure rate at some point in time.

$$x_{k,t} = 0, \text{ whenever } \alpha_k(\xi_t) = 0. \tag{3}$$

That is, a fault due to ψ_k should only be historically observable only when it is defined to be credible. This feature is required for discrete logic models to be feasible. and we model the failure rate of threat ψ_k by:

$$\lambda_k(\xi_t) = \lambda_k \alpha_k(\xi_t). \tag{4}$$

In other words, the logical condition $\alpha_k(\xi_t) = 0$ is interpreted as meaning that the threat can not be present, while $\alpha_k(\xi_t) = 1$ means that the threat may be present. The simplest example of a discrete logic model would be a threshold function, defined as:

$$\alpha_k(\xi_t) = \begin{cases} 1, & \text{for } \xi_t \geq \xi_c \quad (5) \\ 0, & \text{otherwise.} \quad (6) \end{cases}$$

Where ξ_c defines some critical limits above which threat ψ_k is credible. An alternate example of a discrete logic model is shown in Fig.2, where a set of relevant observations are treated by a combination of inequalities and logical rules. The setting of the critical limits, ξ_c, and of the discrete logic model may be determined by a stochastic model, machine learning, or expert opinion. It should be noted that the threat credibility indicator, $\alpha_k(\xi_t)$, does not depend upon the fault statistics, F, but instead depends only upon exogenous data.

The threat specific failure rate, λ_k, in (4) is hence estimated by:

$$\lambda_k = \frac{\sum_t x_{k,t}}{\int_0^T \alpha_k(\xi_t) dt}, \tag{7}$$

Which is the number of failures due to the k^{th} threat divided by the period of time for which the credibility indicator function was active.

For some threats, there may be no historical data from which to calculate failure rate statistics. In which case, expert knowledge may be used to assume failure rates.

5) Sum of threat-specific failure models: If a failure rate model is established for each threat, for a specific component, the total failure rate at some instant in time, t, given some observations, ξ_t, is then estimated by:

$$\lambda(\xi_t) = \sum_{\psi_i \in \Psi_u} \lambda_i + \sum_{\psi_j \in \Psi_v} \lambda_j(\xi_t) + \sum_{\psi_k \in \Psi_d} \lambda_k \alpha_k(\xi_t). \tag{8}$$

The probability of occurrence of a failure within a time frame $[t_1, t_2]$, is obtained:

$$\pi(t_1, t_2) = 1 - e^{-\int_{t_1}^{t_2} \lambda_t dt}, \tag{9}$$

and if the interval is short enough to consider ξ_t as constant over $[t_1, t_2]$, this reduces to:

$$\pi(t_1, t_2) = 1 - e^{-\lambda_t (t_2 - t_1)}. \tag{10}$$

There is no need to use Markov models in the real-time operational context, as within a time frame of days the operator is interested in the probability of any fault occurring, and not necessarily the expected proportion of component availability to unavailability. The operator is only interested in the first transition of a component from an operational state to an inoperable state, how likely this is, and its potential consequences.

6) Treatment of line segments: Transmission lines are a special case of components in terms of threats, as a threat may be credible only on a segment of the line, such as a line that is exposed to high winds for only a few spans. Experience from operators at the Icelandic TSO suggests that if a line fails due to a particular threat, it normally occurs in one of a few locations that are especially susceptible to it due to local topography and line orientation. Given that line segments are discernible from one another in this regard, a single transmission line component model may be broken down into a sequence of individual line segment models in series for relevant threats. This however depends upon the spatial resolution of both observational data and fault statistics. The failure rate of the entire transmission line is simply the sum of the constant failure rates at a given point in time.

D. Data requirements

Table I describes the threats to the Icelandic system within the proposed framework, and identifies the potential to improve data and modelling for individual threats. It should be noted that for some threats, partial data may still allow for the creation of a valid credibility indicator function. Most of the data required is already measured by the Icelandic TSO at present (salt measurements, reservoir levels, maintenance crew locations), or by meteorological bureaus. However, not all of the data is collated in a useful format, or at useful spatial/temporal resolutions, which are practical barriers to implementation of the proposed method. A threat is assumed to be predictable if there exists some observable parameter that would allow a TSO to adjust their risk assessment of that particular threat, with enough time to react before its occurrence (i.e. at least 15 minutes ahead).

The present data collection is minimal, and therefore it is not possible to thoroughly implement the approach discussed in this paper at present, despite thorough historical fault records. Data collection activities and the development of stochastic models can both be costly endeavours with difficult to quantify value to the TSO. It is likely that the usefulness of the logical models will need to be proven in order to initiate the collection of data, either through convincing simulations or initially using cheap low resolution/quality data. Once data collection is under way, the development of stochastic models can be accelerated due to the improved availability of data for future model fitting.

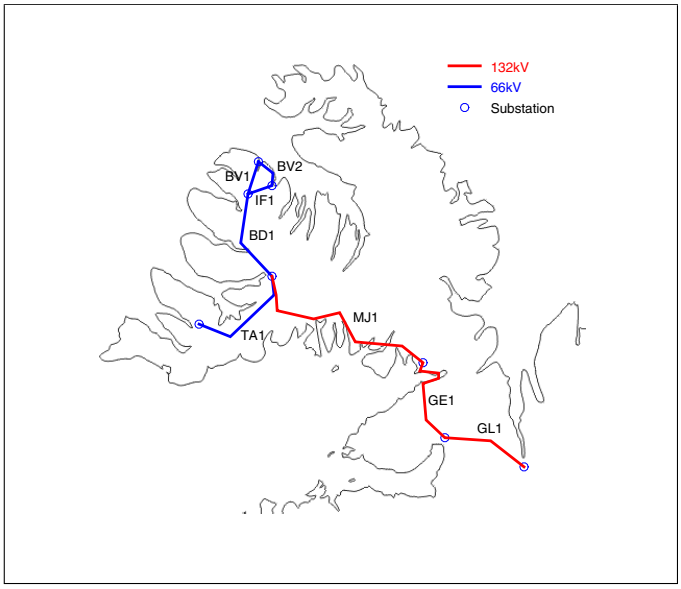

Fig. 3. Overview of the electrical transmission system in the West Fjords, Iceland

It is apparent from Table I that a lack of data collection (especially related to weather) is a significant bottleneck to the adoption of stochastic models in practice. It is therefore important to identify ways to overcome this bottleneck, by justifying the costs of incremental improvements to data acquisition and storage.

III. Case Study: Part of Iceland

The case study demonstrates the application of the credibility indicator functions, using a segment of the Icelandic system that is susceptible to a particular threat. This study uses historical fault data and simulated credibility indicators to show the effectiveness of using threat credibility indicators compared with the present day approach. The simulated credibility indicators are used in lieu of actual weather data, which is unavailable at present.

A. Description of case study area

The least reliable region of the Icelandic transmission system is the West Fjords, located in the country's North West [66], shown in Fig. 3. Of all transmission line faults that have occurred in the region, 32% have been due to icing, as determined using the historical fault statistics. This region is a radial connection from the main network, consisting of transmission lines operated at 132 kV, 66 kV and lower voltages. The transmission shown as BV2 is an underground cable, and therefore is not susceptible to icing.

TABLE I

MAIN THREATS TO THE ICELANDIC TRANSMISSION SYSTEM, DESCRIBED IN THE CONTEXT OF THE PROPOSED THREAT MODELLING FRAMEWORK. ALL THREATS THAT ARE DEFINED AS PREDICTABLE SHOULD BE POSSIBLE TO MODEL STOCHASTICALLY OR LOGICALLY. SOME ADDITIONAL THREATS MAY BE DEFINED AS A COMBINATION OF A SUBSET OF THREATS (E.G. WIND AND ICING).

Threats	**Visible?**	**Predictable?**	**Relevant Data**	**Data Collected**		**Model Examples**	
				Now	**Potential**	**Used Now**	**In Literature**
Wind - Galloping	Yes	Yes	Wind speed, wind direction, topography	No	Yes	No	[37]–[41]
Wind Structural Failure	Yes	Yes	Wind speed, wind direction, topography	No	Yes	No	[20]
Ice loading	Yes	Yes	Existing ice load, precipitation, temperature, humidity, wind speed	Partial	Yes	No	[42]–[48]
Lightning strikes	Yes	Yes	Temperature, humidity, precipitation, atmospheric voltage potential	No	Yes	No	[49]–[53]
Earthquakes	Yes	No	-	-	-	-	-
Landslides/avalanches	Yes	Yes	Topography, temperature, wind speed, wind direction, precipitation, snow depth	No	Yes	No	[20]
Volcanic Eruptions	Yes	Yes	Risk indicators, seismic activity, atmospheric sulphur, snow/ice melting, topography	No	Yes	No	[54]–[56]
Glacial floods (jokulhlaup)	Yes	Yes	Topography, seismic activity	No	Yes	No	[57]–[59]
Snow accumulation	Yes	Yes	Precipitation, snow depth	No	Yes	No	[60]–[62]
Salt pollution	Yes	Yes	Salt measurements, wind speed, wind direction	Partial	Yes	No	[63]
Generator/load failure	Yes	No	-	-	-	-	-
Solar flares	Yes	Yes	Solar flare warnings	No	Yes	No	[64], [65]
Human error (random)	Yes	No	-	-	-	-	-
Human error (control)	Yes	No	-	-	-	-	-
Human error (proximity)	Yes	Yes	Maintenance crew locations, public work notifications	Yes	Yes	No	-
Sabotage	Yes	No	-	-	-	-	-
Technical	Yes	No	-	-	-	-	-
Other	No	No	-	-	-	-	-

B. Threat modelling

It is assumed that icing events can only occur from August to March, based on historical fault data provided by the Icelandic TSO. It is also assumed that within these 8 months, icing faults are credible for 20% of the time (equivalent to 1170 hours per year). These assumptions are based on operator experience, and are made due to a lack of historical weather and icing data. For simplicity, all other threats are considered as invisible threats. Given the Icelandic fault statistics, which provide a time series of faults categorized by their root cause (x_k), and the above assumption that icing is credible 20% of 8 months of the year ($\sum \alpha_k = (0.2)(\frac{8}{12})T$), the conditional failure rates due to icing (ψ_k) can be calculated by (7).

The residual failure rate, λ_r, capturing failures due to all other possible threats (and which are considered as unpredictable for this case study), is estimated by:

$$\lambda_r = \frac{\sum(x_t - x_{k,t})}{T} = \sum_{\psi_i \in \Psi_u} \lambda_i. \tag{11}$$

The failure rate of each component at some point in time can then be calculated using (8) as:

$$\lambda_t = \lambda_r + \lambda_k \alpha_k(\xi_t). \tag{12}$$

For the case study, the resulting failure rates are shown in Fig. 4, alongside the original failure rates. These failure rates are based on 30 years of fault records collected at the Icelandic TSO. The relevant information included in these records include failure time, duration, component, and a description of the root cause and nature of the fault.

The lack of historical weather data makes it difficult to realistically simulate a storm. Therefore credibility indicator values are assumed to describe a storm moving across the West Fjords region, over the course of a day, gradually affecting the transmission lines from the NW to the SE. For simplicity, weather is considered to affect either the whole of the line or not at all. The simulation is run hourly, over the course of a day, with the storm affecting the lines in the manner described by Table II.

C. Hourly fault probability

For the assumed storm and credibility function accuracy, the hourly probability of one or more faults in the region was calculated. This is shown in Fig. 5, with the existing method (constant failure rate) shown for comparison. The use of component specific threat credibility indicators results in spatio-temporal failure rates, and allows for the risk associated with a particular storm to be quantified and visualised. The accumulated risk of at least one fault occurring in the West

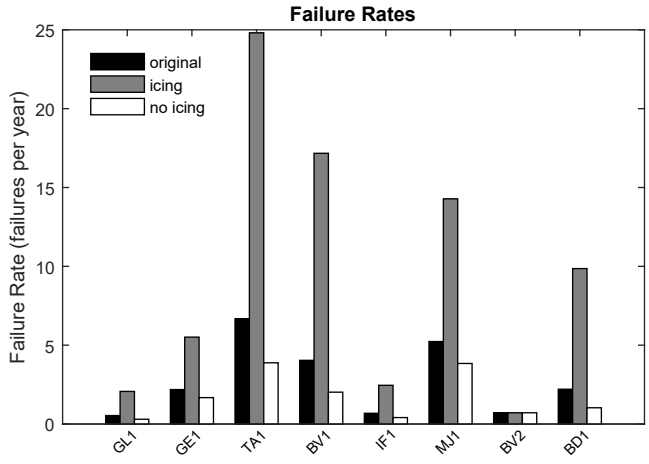

Fig. 4. Transmission line failure rates, with the standard failure rate compared with the failure rates that are conditional on the credibility of icing.

TABLE II
HOURLY CREDIBILITY OF ICING THREATS IN THE WEST FJORDS DUE TO A STORM MOVING OVER THE REGION

Transmission Lines	Hours of credible icing threat ($\xi_t \geq \xi_c$)
BV1 and IF1	2 to 14
BD1	5 to 17
TA1 and MJ1	7 to 19
GE1	9 to 21
GL1	12 to 24
BV2	icing not credible (underground cable)

Fjords region for the duration of the simulated storm is 12.3%, which is more than double the accumulated probability when using a constant failure rate (5.9%). The spatial variability of fault probabilities is not shown, as it simply follows the timing shown in Table II, proportional to the conditional failure rates shown in Fig. 4.

An interesting outcome of using threat credibility indicators, is that the failure probability in the region decreases below the probability calculated using existing methods (i.e. constant failure rate for the entire year), given that the probability of icing faults is zero. That is, in this case study, periods in which icing is not credible allow for 32% of faults to be removed from the fault statistics hence leading to a lower failure rate. This implies that current practice of constant year-round failure rates over-estimate fault probabilities in calm summer periods.

D. Model sensitivity

Fig. 6 shows the relationship between the accuracy of the credibility function and the hourly failure probability, for the simulated 24 hour period. Trivially, Fig. 6 shows that assuming icing threats are credible 100% of the time is equivalent to using a single, constant failure rate. This implicitly assumes that icing is an invisible, unpredictable threat, which is contrary to expert opinion. It is therefore important to define a credibility function that can exclude as great a proportion of time as possible. The choice of models

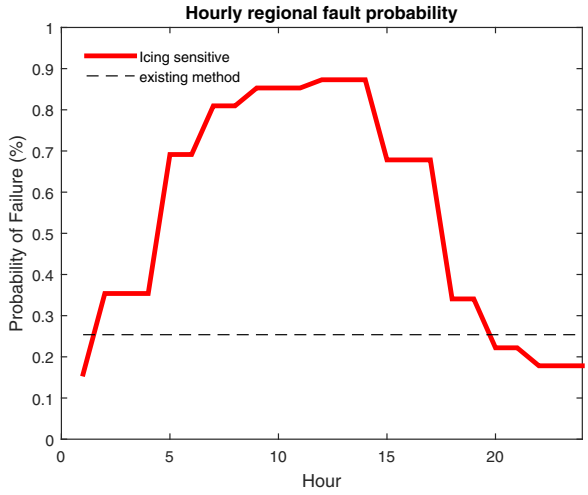

Fig. 5. The probability of one or more faults at each hour of the simulation, equivalent to the complement of the probability of all components surviving each hour

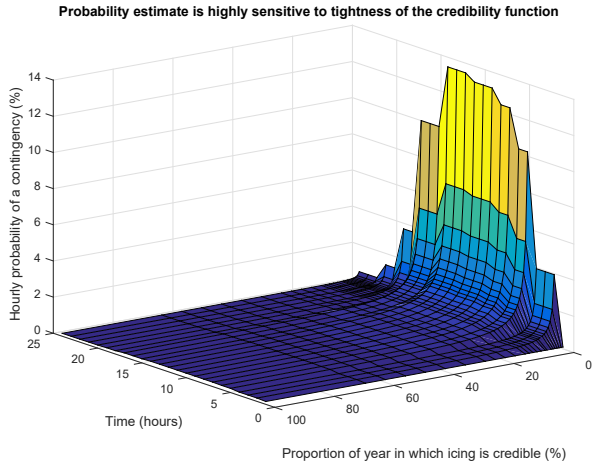

Fig. 6. Sensitivity of the simulated logical failure rate model to the tightness of the credibility indicator function. A tight credibility indicator function means one which is active for a minimal proportion of the year.

or rules which inform credibility indicators must be trusted by operators, and verifiable with data, if the outcome is to be of any use in real-time operation. It is anticipated that it is easier to gain the trust of operators with the simple, binary rules of credibility indicators, than with the continuous regression models proposed in the literature to date.

IV. DISCUSSION

In the context of the proposed framework, outlined by Fig. 1, most TSOs make the implicit assumption that all threats are invisible by using constant failure rates. State of the art literature concentrates on continuous, regression-based models to connect failure rates to exogenous variables, but requires historical data that TSOs don't necessarily possess and may not be trusted by operators. The proposed logical modelling method, which relies on threat credibility indicators, may over-

come these issues and would allow TSOs to implement spatio-temporal failure rates into their RMAC. They would also encourage TSOs to begin collecting data in order to tighten the credibility indicator functions, without requiring a pre-existing database of exogenous data. This may eventually lead to TSOs possessing the data required to develop and implement the regressive continuous models already discussed in literature. Therefore the proposed modelling framework and technique may provide a pathway for the eventual implementation of more robust stochastic models in practice.

If a TSO were to transition towards a probabilistic RMAC without considering the effects of exogenous factors on failure probabilities, their approach would overlook a substantial source of system risk in an operational context. There is a need to quantify threats before they are realised, such that they can be adequately addressed in a preventative, rather than corrective, manner. Until threat based failure rates are modelled and adopted, a TSO using a probabilistic RMAC must rely solely on operator intuition to react to dynamic threats to the system.

In an operational context, it is not expected that implementing spatio-temporal failure rates will affect decision making (the choice of control actions) significantly, but rather confirm what is already intuitively known by operators. The proposed modelling method provides a way of quantifying what is already described/used qualitatively, and may be used to help operators and TSOs justify the outcomes of their decision making process.

V. Conclusion

There is growing pressure on TSOs to operate their system closer to the limits, and doing so requires TSOs to be increasingly aware of these limits in real time. TSOs currently rely on operator experience and judgement to manage the short-term threats to the system, the likelihood of these threats leading to a failure, and the severity of their occurrence. Quantifying the risks to the transmission system is an active topic of research, and this paper suggests a pathway to transition from static failure rates towards more complex models. The success of such a transition relies on long-term, consistent data collection. The use of the suggested method is justified by the case-study which uses fault information from a European TSO and shows how the use of simple logical rules can improve the quantification of the transmission system's reliability.

Further research required on this topic will be in defining trustworthy credibility indicators for threats, combining the method with consequence modelling (calculation of expected lost load) and showing its potential to drive decision making, proving the practical accuracy of credibility indicators using real weather data, and comparing the efficacy of logical models with continuous models.

Acknowledgment

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n^{o} 608540.

The authors would like to thank Landsnet for allowing the use of data, and members of the GARPUR project for many useful discussions, especially Liisa Haarla from Aalto University for her ideas on the summation of partial failure rates.

References

[1] P. Pourbeik, B. Chakrabarti, T. George, J. Haddow, H. Illian, R. Nighot, *et al.*, *Review of the Current Status of Tools and Techniques for Risk-based and Probabilistic Planning in Power Systems*. CIGRE, 2010.

[2] ENTSO-E, "Network Code on Operational Security," 2013.

[3] GARPUR Consortium, "D1.2 Current practices, drivers and barriers for new reliability standards," tech. rep., EU Commission grant agreement 608540, 2014.

[4] F. Capitanescu, J. Martinez Ramos, P. Panciatici, D. Kirschen, A. Marano Marcolini, L. Platbrood, and L. Wehenkel, "State-of-the-art, challenges, and future trends in security constrained optimal power flow," *Electric Power Systems Research*, vol. 81, pp. 1731–1741, Aug. 2011.

[5] C. Hamon, M. Perninge, and L. Soder, "A computational framework for risk-based power systems operations under uncertainty. Part I: Theory," *Electric Power Systems Research*, vol. 119, pp. 45–53, Feb. 2015.

[6] E. Karangelos, P. Panciatici, and L. Wehenkel, "Whither probabilistic security management for real-time operation of power systems?," in *Bulk Power System Dynamics and Control - IX Optimization, Security and Control of the Emerging Power Grid (IREP), 2013 IREP Symposium*, pp. 1–17, Aug. 2013.

[7] C. E. Murillo-Sanchez, R. D. Zimmerman, C. L. Anderson, and R. J. Thomas, "A stochastic, contingency-based security-constrained optimal power flow for the procurement of energy and distributed reserve," *Decision Support Systems*, vol. 56, pp. 1–10, Dec. 2013.

[8] B. Stott and O. Alsac, "Optimal Power Flow - Basic Requirements for Real-Life Problems and Their Solutions," 2012.

[9] M. M. Bhaskar, S. Muthyala, and M. Sydulu, "Security constraint optimal power flow (SCOPF): A comprehensive survey," *Global Journal of Technology and Optimization*, vol. 2, no. 11, 2011.

[10] N. Yang and F. Wen, "A chance constrained programming approach to transmission system expansion planning," *Electric Power Systems Research*, vol. 75, pp. 171–177, Aug. 2005.

[11] W. Li and J. Zhou, "Probabilistic Reliability Assessment of Power System Operations," *Electric Power Components and Systems*, vol. 36, pp. 1102–1114, Sept. 2008.

[12] E. Ciapessoni, D. Cirio, S. Grillo, S. Massucco, A. Pitto, and F. Silvestro, "Operational Risk Assessment and control: A probabilistic approach," in *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*, pp. 1–8, Oct. 2010.

[13] S. de Almeida, R. Pesta, and F. Barbosa, "The main causes of incidents in the Portuguese Transmission System - Their characterization and how they can be used for risk assessment," in *6th International Conference on the European Energy Market, 2009. EEM 2009.*, pp. 1–6, IEEE, May 2009.

[14] M. Bollen, L. Wallin, T. Ohnstad, and L. Bertling, "On Operational Risk Assessment in Transmission Systems - Weather Impact and Illustrative Example," in *Proceedings of the 10th International Conference on Probabilistic Methods Applied to Power Systems, 2008. PMAPS '08*, pp. 1–6, May 2008.

[15] M. Hofmann, O. Gjerde, G. H. Kjolle, E. Gramme, J. G. Hernes, and J. A. Foosnaes, "Developing indicators for monitoring vulnerability of power lines-case studies," in *22nd International Conference and Exhibition on Electricity Distribution, CIRED 2013*, 2013.

[16] ENTSO-E, "Nordic Grid Disturbance Statistics 2013," tech. rep., ENTSO-E, Brussels, Belgium, 2014.

[17] EU Commission, "Green Paper on a European Programme for Critical Infrastructure Protection," 2005.

[18] O. Gjerde, G. Kjolle, N. Detlefsen, and G. Bronmo, "Risk and vulnerability analysis of power systems including extraordinary events," in *PowerTech, 2011 IEEE Trondheim*, pp. 1–5, June 2011.

[19] Nordel, "Guidelines for the Classification of Grid Disturbances," 2009.

[20] A. J. Eliasson, "Natural Hazards and The Icelandic Power Transmission Grid," in *7. konferenca slovenskih elektroenergetikov*, (Velenje, Slovenia), CIGRE, 2005.

[21] N. Machado, S. A. de Graaff, and R. Pestana, "Risk assessment methodology Running tests at the Portuguese TSO," (Paris, France), CIGRE, 2014.

[22] S. de Almeida, *Portuguese Transmission Grid Incidents Risk Assessment*. PhD thesis, FUEP, Portugal, 2010.

[23] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, *et al.*, "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance," *IEEE Transactions on Power Systems*, vol. 20, pp. 1922–1928, Nov. 2005.

[24] k. J. Holmgren, "A Framework for Vulnerability Assessment of Electric Power Systems," in *Critical Infrastructure* (P. A. T. Murray and P. T. H. Grubesic, eds.), Advances in Spatial Science, pp. 31–55, Springer Berlin Heidelberg, 2007.

[25] R. Billinton and R. N. Allan, *Reliability Evaluation of Engineering Systems: Concepts and Techniques*. New York: Springer, 2nd edition ed., June 1992.

[26] T. Digernes, A. B. Svendsen, Y. Aabo, C. Hernandez, and M. Palsson, "Analyses of delivery reliability in electrical power systems," 2007.

[27] A. B. Svendsen, T. Tollefsen, R. F. Pedersen, K. P. Petursson, D. Patel, and O. D. Lampe, "Abstract Representation of Power System Networks as a Function of Regularity Properties," 2014.

[28] R. Billinton and G. Singh, "Application of adverse and extreme adverse weather: modelling in transmission and distribution system reliability evaluation," *Generation, Transmission and Distribution, IEE Proceedings*, vol. 153, pp. 115–120, Jan. 2006.

[29] M. Rios, D. Kirschen, D. Jayaweera, D. Nedic, and R. Allan, "Value of security: modelling time-dependent phenomena and weather conditions," *IEEE Transactions on Power Systems*, vol. 17, pp. 543–548, Aug. 2002.

[30] Billinton and W. Li, *Reliability Assessment of Electric Power Systems Using Monte Carlo Methods*. Springer Science & Business Media, June 2013.

[31] B. John, U. H. Acharya, and A. K. Chakraborty, *Quality and Reliability Engineering: Recent Trends and Future Directions*. Allied Publishers, Apr. 2013.

[32] P. Wang and R. Billinton, "Reliability cost/worth assessment of distribution systems incorporating time-varying weather conditions and restoration resources," *IEEE Transactions on Power Delivery*, vol. 17, pp. 260–265, Jan. 2002.

[33] Y. Zhou, A. Pahwa, and S.-S. Yang, "Modelling Weather-Related Failures of Overhead Distribution Lines," *IEEE Transactions on Power Systems*, vol. 21, pp. 1683–1690, Nov. 2006.

[34] GARPUR Consortium, "D1.1 State of the art on reliability assessment in power systems," tech. rep., EU Commission grant agreement 608540, 2014.

[35] L. Haarla, M. Koskinen, R. Hirvonen, and P. Labeau, *Transmission Grid Security: A PSA Approach*. Springer, 2011.

[36] F. Xiao, J. McCalley, Y. Ou, J. Adams, and S. Myers, "Contingency Probability Estimation Using Weather and Geographical Data for On-Line Security Assessment," in *International Conference on Probabilistic Methods Applied to Power Systems, 2006. PMAPS 2006*, pp. 1–7, June 2006.

[37] G. McClure and M. Lapointe, "Modeling the structural dynamic response of overhead transmission lines," *Computers & Structures*, vol. 81, pp. 825–834, May 2003.

[38] Y. M. Desai, P. Yu, N. Popplewell, and A. H. Shah, "Finite element modelling of transmission line galloping," *Computers & Structures*, vol. 57, pp. 407–420, Nov. 1995.

[39] M. B. Waris, T. Ishihara, and M. W. Sarwar, "Galloping response prediction of ice-accreted transmission lines," in *The 4th International Conference on Advances in Wind and Structures: book of proceedings. Jeju (Korea)*, pp. 876–885, 2008.

[40] N. Nikitas and J. H. G. Macdonald, "Misconceptions and Generalizations of the Den Hartog Galloping Criterion," *Journal of Engineering Mechanics*, vol. 140, no. 4, 2014.

[41] A. S. Richardson, "A study of galloping conductors on a 230 kV transmission line," *Electric Power Systems Research*, vol. 21, pp. 43–55, Apr. 1991.

[42] A. J. Eliasson, A. B. Jonasson, and P. T. Gunnlaugsson, "Comparison of ice accumulation on simplex and duplex conductors in parallel overhead transmission lines in Iceland.," 2015.

[43] L. Makkonen, "Estimation of wet snow accretion on structures," *Cold Regions Science and Technology*, vol. 17, no. 1, pp. 83–88, 1989.

[44] L. Makkonen, "Models for the growth of rime, glaze, icicles and wet snow on structures," *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 358, no. 1776, pp. 2913–2939, 2000.

[45] G. Thompson, B. E. Nygaard, L. Makkonen, and S. Dierer, "Using the Weather Research and Forecasting (WRF) model to predict ground/structural icing," in *13th International Workshop on Atmospheric Icing on Structures, METEOTEST, Andermatt, Switzerland*, 2009.

[46] K. F. Jones and K. Z. Egelhofer, "Computer model of atmospheric ice accretion on transmission lines," tech. rep., DTIC Document, 1991.

[47] B. E. Kringlebotn Nygaard, H. Agustsson, and K. Somfalvi-Toth, "Modelling wet snow accretion on power lines: improvements to previous methods using 50 years of observations," *Journal of Applied Meteorology and Climatology*, vol. 52, no. 10, pp. 2189–2203, 2013.

[48] H. Olafsson, H. Agustsson, O. Rognvaldsson, and A. J. Eliasson, "Towards a method for estimating the risk of wet snow icing in a mountainous region," 2007.

[49] S. de Almeida, C. Loureiro, F. Barbosa, and R. Pestana, "Historical data analysis of lightning and its relation with the Portuguese Transmission system outages," in *PowerTech, 2009 IEEE Bucharest*, pp. 1–8, June 2009.

[50] IEEE, "Estimating lightning performance of transmission lines. II. Updates to analytical models," *IEEE Transactions on Power Delivery*, vol. 8, pp. 1254–1267, July 1993.

[51] E. W. McCaul, S. J. Goodman, K. M. LaCasse, and D. J. Cecil, "Forecasting Lightning Threat Using Cloud-Resolving Model Simulations," *Weather and Forecasting*, vol. 24, pp. 709–729, June 2009.

[52] C. A. Doswell III and D. M. Schultz, "On the use of indices and parameters in forecasting severe storms," *E-Journal of Severe Storms Meteorology*, vol. 1, no. 3, 2006.

[53] J. Wang, Q. Yang, X. Xiong, and S. Weng, "Short-Term Reliability Evaluation of Transmission System Using Lightning Strike Probability Prediction," *Journal of Power and Energy Engineering*, vol. 2, no. 04, p. 647, 2014.

[54] R. S. J. Sparks, "Forecasting volcanic eruptions," *Earth and Planetary Science Letters*, vol. 210, no. 1, pp. 1–15, 2003.

[55] J. Eliasson, G. Larsen, M. Tumi Gudmundsson, and F. Sigmundsson, "Probabilistic model for eruptions and associated flood events in the Katla caldera, Iceland," *Computational Geosciences*, vol. 10, pp. 179–200, May 2006.

[56] M. Bebbington, S. J. Cronin, I. Chapman, and M. B. Turner, "Quantifying volcanic ash fall hazard to electricity infrastructure," *Journal of Volcanology and Geothermal Research*, vol. 177, pp. 1055–1062, Nov. 2008.

[57] H. Bjornsson, "Jokulhlaups in Iceland: characteristics, prediction and simulation," *Annals of Glaciology*, vol. 16, pp. 95–106, 1992.

[58] H. Bjornsson, "Jokulhlaups in Iceland: sources, release, and drainage," *Megaflooding on Earth and Mars. Cambridge University Press, Cambridge*, pp. 50–64, 2009.

[59] M. T. Gudmundsson, H. Bjornsson, and F. Palsson, "Changes in jokulhlaup sizes in Grimsvotn, Vatnajokull, Iceland, 1934-91, deduced from in-situ measurements of subglacial lake volume," *Journal of Glaciology*, vol. 41, no. 138, pp. 263–272, 1995.

[60] D. G. Tarboton and C. H. Luce, *Utah energy balance snow accumulation and melt model (UEB)*. Utah Water Research Laboratory and Utah State University, 1996.

[61] C. H. Luce, D. G. Tarboton, and K. R. Cooley, "Sub-grid parameterization of snow distribution for an energy and mass balance snow cover model," *Hydrological Processes*, vol. 13, no. 12, pp. 1921–1933, 1999.

[62] E. Kuusisto, *Snow accumulation and snowmelt in Finland*. No. 55 in Vesientutkimuslaitoksen julkaisuja. Vesihallitus, Helsinki: Vesihallitus, 1984.

[63] R. Kristjansson, "Urvinnsla seltumaelinga Landsvirkjunar 1993-2000," tech. rep., AFL Engineering Ltd, Reykjavik Iceland, 2005.

[64] M. K. Georgoulis, "Toward an efficient prediction of solar flares: which parameters, and how?," *Entropy*, vol. 15, no. 11, pp. 5022–5052, 2013.

[65] A. Strugarek and P. Charbonneau, "Predictive capabilities of avalanche models for solar flares," *Solar Physics*, vol. 289, no. 11, pp. 4137–4150, 2014.

[66] K. Sigurjonsson, R. Stefansson, H. Halldorsson, K. Thorbergsdottir, J. Vilhjalmsson, and K. Reinholdsdottir, "Reliability of supply and quality of delivered electricity - performance report 2014," 2015.