Improved methods for reporting, storing and visualising data according to the incident classification scale used in the power transmission system

Henrik Hillner

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.

Espoo 8.4.2019

Supervisor

Prof. Matti Lehtonen

Advisor

M.Sc Markku Piironen

Aalto University
School of Electrical
Engineering

Aalto University
School of Electrical Engineering

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi
Abstract of the master's thesis

Author	Henrik Hillner
Title	Improved methods for reporting, storing and visualising data according to the incident classification scale used in the power transmission system
Degree programme	Automation and Electrical Engineering
Major	Electrical Power and Energy Engineering — **Code of major** ELEC3024
Supervisor	Prof. Matti Lehtonen
Advisor	M.Sc Markku Piironen
Date	8.4.2019 — **Number of pages** 37+24 — **Language** English

Abstract
The incident classification scale used in the Pan-European power systems is a set of rules for classifying incidents affecting the security of a power system and reporting them. Furthermore, transmission system operators administering the Pan-European power system are obligated to report this data to the European Network of Transmission System Operators for Electricity, ENTSO-E. This thesis reviews the current incident classification scale and interviews 6 transmission system operators to find points of improvement and form improvement suggestions. The biggest issues found were unclear definitions and an immense workload for some transmission system operators. The most significant improvement would be to make the incident reporting fault-oriented instead of consequence-oriented. This change would decrease the workload by making the incident classification scala reporting utilise existing data gathered from reporting. Additionally, data collection could be better delegated to persons with correct expertises. Another significant improvement would be to include all individual incidents in the reporting instead of aggregating them to one single event. This modification would improve the data quality remarkably and allow new possibilities of data analysis.

Keywords Incident classification, power system security, statistics, wide-area incidents

Aalto University
School of Electrical Engineering

Aalto-universitetet, PB 11000, 00076 AALTO
www.aalto.fi
sammandrag av diplomarbetet

Författare Henrik Hillner

Titel Förbättrade metoder för rapportering, sparande samt visualisering av data enligt incidentklassifieringsskalan som används i elkraftnätet

Utbildningsprogram Automation och elektroteknik

Huvudämne Elkraftteknik **Huvudämnets kod** ELEC3024

Övervakare Prof. Matti Lehtonen

Handledare DI Markku Piironen

Datum 8.4.2019 **Sidantal** 37+24 **Språk** Engelska

Sammandrag

Incidentklassifieringsskalan som används i elkraftnäten i hela Europa är en samling regler för att klassificera händelser som påverkar elkraftnätets säkerhet. Stamnätsbolagen är även lagligt bundna till att leverera denna data till det Europeiska Nätverket för Stamnätsbolag inom Elektricitet, ENTSO-E. Detta diplomarbete granskar den nuvarande incidentklassifieringsskalan, intervjuar sex stamnätsbolag och undersöker sätt att förbättra de rådande processerna. De största problemen var oklara definitioner och ytterst höga arbetsbördor för stamnätsbolag för att rapportera data. Det mest betydande förbättringsförslaget skulle vara att rapportera händelser på ett felorienterat sätt istället för ett konsekvensorienterat sätt. Detta skulle minska stamnätsbolagens arbetsbörda och utnyttja data, som redan samlas in i dagens läge. Dessutom kunde man delegera arbetet bättre till mänskor som specialiserar sig inom det aktuella området. Ett annat betydande förbättringsförslag skulle vara att rapportera alla enskilda incidenter istället för att aggregera alla relaterade händelser till en. Denna förbättring skulle öka datakvalitén och möjliggöra nya sätt att analysera denna data.

Nyckelord Incidentklassifierings, säkerhet i elkraftnätet, statistik, omfattande händelser

Preface

I would want to thank most my advisor Jørn Schaug-Pettersen, who helped me through tremendously with making this thesis. His expertise in power systems has been invaluable and I have learned a lot during this project.

Furthermore, I would like to thank my second advisor Markku Piironen for being my official advisor and Professor Matti Lehtonen for believing in me being able to return this thesis in time.

Lastly, I want to thank my mother, who has had patience with my studies and graduation, and all my friends who have made my time at Aalto University, and especially at Teknologföreningen, worth it.

Otaniemi, 8.4.2019

H. Hillner

Contents

Abbreviations

ACER	Agency for Cooperation of Energy Regulators
EAS	European Awareness System
ENTSO-E	European Network of Transmission System Operators for Electricity
EU	European Union
FCR	Frequency containment reserves
FRR	Frequency restoration reserves
FRRa	Automatic Frequency restoration reserves
FRRm	Manual Frequency restoration reserves
HVAC	High-voltage alternating current
HVDC	High-voltage direct current
ICS	Incident Classification Scale
PMU	Phasor Measurement Unit
RR	Replacement reserves
RSC	Regional security coordinator
SCADA	Supervisory Control and Data Acquisition
SOC	System Operations Committee
SPS	System protection scheme
TSO	Transmission System Operator

ICS abbreviations

F	Incidents leading to frequency degradation
G	Incidents on power generating facilities
L	Incidents on load
LT	Loss of tools and facilities
OB	Blackout
ON	N and N-1 violations
OV	Violation of standards on voltage
RA	Remedial action
RRC	Reduction of reserve capacity
RS	Separation from the grid
T	Incidents on transmission system elements

1 Introduction

The power systems today are an outcome of high-quality engineering for more than a hundred years. They have evolved from the earlier simple and robust systems, which were often operated by government bodies, to complex interconnected networks with multiple operators that we have today. However, the advancement in technology has not halted. Recent decades have introduced open energy markets, which have further increased the intricacy of the the power system [1]. Furthermore, there is an increasing trend of using more and more renewable energy sources and distributed energy production. There are also aims to increase it even further. For example, the ENTSO-E 2018 Ten Year Network Development Plan [2] has set a target that 58 % of the energy demand in Europe should be covered by renewable sources by year 2030.

The society today is immensely dependent on the supply of electricity to function, and disruptions have a great potential to cause high economical and societal impacts [3]. For example, the blackout on 14 August 2003 in Northern America and Canada affected 50 million people and caused about 4–10 billion US dollars of economic losses in the United States [4]. Therefore, it is essential to maintain high operational security in power systems to protect the energy supply.

The European initiative to guarantee the energy supply was to establish the European Network of Transmission System Operators for Electricity, ENTSO-E. ENTSO-E was established in 2009 with the aim to assure the security of energy supply and system reliability, the integration of renewable energy sources into the energy network and to complete the internal energy market [5]. The establishment was driven by EU's Third Legislative Package, and more specifically by the Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009 [6], giving ENTSO-E a set of tasks and responsibilities to ensure the successful implementation of the goals and to improve the cooperation between its 41 member transmission system operators (TSOs). These tasks and responsibilities were further updated by the Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation (SOGL) [7].

One of these tasks was to implement a common incident classification scale (ICS) methodology, as stated in Article 8(3) of Regulation (EC) No 714/2009 [6]. The current ICS was approved by the ENTSO-E System Operations Committee on 11 April 2018 and aims to [8]:

- provide an overview of operational security indicators related to operational security and planning, as stated in Article 15 of SOGL [7];
- identify necessary improvements to maintain a sustainable and long-term operational security;
- identify appropriate improvements to network operation tools required to maintain operational security. These improvements should relate to the real-time operation, operational planning and disturbance prevention and recovery in the TSO control areas, as stated in Article 55(e) of SOGL [7];

- explain the reasons of incidents at the operational security ranking scales 2 and 3, as stated in Article 15 of SOGL [7]. The explanations shall be based on an investigation by the TSOs, and the process shall be detailed by the incident classification scale.

To fulfil these tasks, the ICS defines the concepts and procedures needed to produce an annual report. The defined concepts include the incident classification scale and the operational security indicators.

The incident classification scale categorises the system state into 4 levels of security: normal state, alert state, emergency state and blackout state, as described in Article 18 of SOGL [7]. These system states are also the same system states used in the ENTSO-EAwareness System (EAS). The EAS is a real-time system that informs the current system state of each connected TSO to the other TSOs. Therefore, it is of significant interest to maintain compatibility between the ICS and EAS definitions. However, EAS and ICS may sometimes classify the system state differently as EAS only has limited information available due to its real-time nature.

The defined operational security indicators are separated to indicators relevant to operational security and indicators relevant to operational planning, which are listed in Article 15 of SOGL [7]. Furthermore, additional security indicators may be introduced when deemed necessary for operational security.

Every TSO member of ENTSO-E must report the necessary data and information needed to produce a report based on ICS methodology, as stated in Article 15(2) in SOGL [7]. Therefore, it is essential that the ICS methodology is simple to grasp for each TSO while also being uncomplicated to report.

This Master's Thesis aims to provide a solution to improve the current ICS procedures in the way it is reported, analysed and visualised. The current incident classification scale material will be analysed and 6 TSOs involved in the ICS group or reporting are interviewed in order to acquire first hand experience from persons that have been involved with ICS for a longer time.

The thesis is constructed followingly:

- Chapter 2 defines the terms and concepts needed to analyse the incident classification scale and to suggest improvements. Furthermore, research in the field is detailed;
- Chapter 3 describes the available research material and the used methods to complete the aims of this thesis;
- Chapter 4 examines the current state of the incident classification scale methodology and the annual report;
- Chapter 5 elaborates and suggests improvements to the incident classification scale;
- Chapter 6 summarises the thesis.

2 Theoretical background

The Pan-European power grid is an enormous power transmission network, that requires cooperation between numerous operators to be kept in balance. This chapter defines the key concepts and definitions needed to grasp the theories behind power system security. This includes defining and disturbances, faults and their causes which may or may not affect the security of a power system. Section 2.1 describes power system security, stability and reliability, Section 2.2 describes disturbances and faults in the power system and their causes, Section 2.4 details situations that affect the power system but are not caused by faults, and lastly, Section 2.5 cover actions made to recover from incidents that have affected the system security.

2.1 Power system security, stability and reliability

The incident classification scale was created to improve the operational security in the Pan-European power grid. Power system security is a wide subject, that includes both real-time operation as well as short and long-term planning and is closely related to power system reliability and security. This thesis will define these concepts by using the Online Electrotechnical Vocabulary [9], published by the International Electrotechnical Commission. The definitions, differences and similarities will be further discussed by making use of an article by the IEEE and CIGRE Joint Task Force, published in the IEEE Transactions on Power Systems Journal in 2004 [10].

The International Electrotechnical Commission defines *security* [in a power system] in its Online Electrotechnical Vocabulary as [9]:

> [the] ability of an electric power system to operate in such a way that credible events do not give rise to loss of load, stresses of system components beyond their ratings, bus voltages or system frequency outside tolerances, instability, voltage collapse, or cascading[.]

In other words, power system security describes how well a (power) system can withstand potential disturbances without interrupting the customers' supply of power. An essential part of power system security is contingency analysis. Contingency analysis means to identify contingencies, i.e. credible events, that could happen in a power system. With the credible events identified, grid operators can plan and install countermeasures to make the system resistant to these contingencies or to prevent them from happening in the first place, and thus operate a power system with greater stability.

Power system stability is defined by the IEC [9] as:

> [the] ability of an electric power system to regain or to retain a steady-state condition, characterized by the synchronous operation of the generators and a steady acceptable quality of the electricity supply, after a disturbance due, for example, to variation of power or impedance[.]

Power system stability means explicitly the ability of a power system to keep or return to its stable state after a disturbance. The IEEE and CIGRE Joint Task Force [10] divides power system stability further into three categories: rotor-angle, frequency and voltage stability, as seen in Figure 1. These categories describe the main variables that characterize the physical nature of the instability. The categories are further divided according to the size of the disturbance, small and large, and the affected timespan, short and long-term.

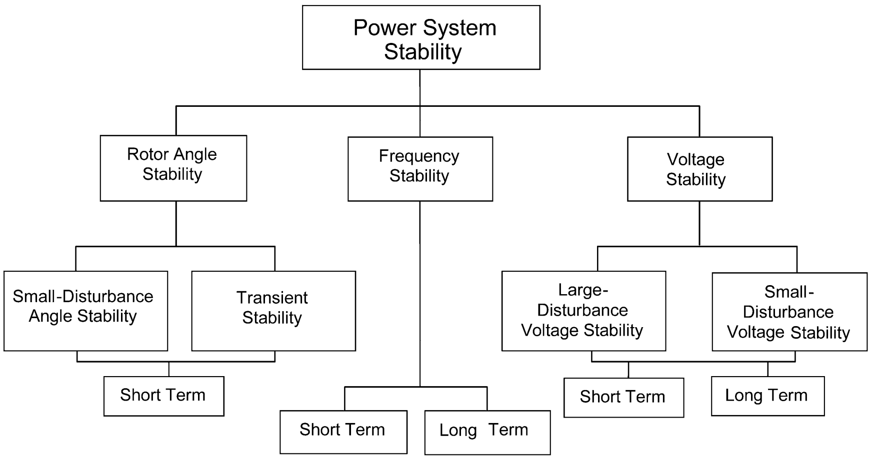

Figure 1: The stability categories as defined by the IEEE and CIGRE Joint Task Force in 2004 [10].

Power system reliability is defined by the IEC [9] as:

> [the] probability that an electric power system can perform a required function under given conditions for a given time interval.
>
> Note 1 Reliability quantifies the ability of an electric power system to supply adequate electric service on a nearly continuous basis with few interruptions over an extended period of time.
>
> Note 2 Reliability is the overall objective in electric power system design and operation.

Power system reliability is thereby defined by its connection to the observed time interval, as it measures the probability of the grid is providing an adequate supply of electricity during that observed time. It can, for example, be measured as the percentage of hours a certain part of or the power grid was able to deliver the necessary amount of energy. Furthermore, the main target of every grid owner is to make it as reliably as possible.

Ultimately, according to the IEEE and CIGRE Task Force [10], the differences between power system security, stability and reliability epitomize to three distinct features. First, while the main objective of a power system is to make it as reliable as possible, it can only be reliable if the system can be kept in a secure operating condition, preferably continuously. In a secure state, the system can retain its stability whilst being capable of coping with any contingencies that could upset it. A stable operating condition does not always guarantee the operating conditions to be secure.

Second, different systems may share the same level of stability even though they do not share the same level of security. The reason is that a disturbance, of the same size and nature, may have entirely different consequences.

Last, security and stability are time-dependent measures, which assess the state of the power system at a certain point of time. However, reliability evaluates to which degree a system has delivered an adequate supply of energy during a specified timespan.

2.2 Disturbances and faults in the power system

There are multiple kinds of events that may affect the security of a power system. When analysing events that have disturbed the system state, it is common to group related events together. A series of related events is called a *disturbance*. This thesis will use the IEC definition of a disturbance. The IEC Electropedia defines a disturbance (in an electric power system) as:

> outages, forced or unintended disconnection, or failed re-connection as a result of faults in the electric power system [9]

The Nordic and Baltic TSOs have formed a subgroup named DISTAC under Regional Group Nordic in ENTSO-E. The groups history begins already in 1964 and they produce an annual report about the Nordic and Baltic grid disturbances with the latest report from 2017 [11]. Their definitions have been tried and tested during a long time and are well suited for analysing disturbance related incidents in the power grid. The only difference between the IEC and DISTAC definitions of a disturbance, is that DISTAC specifies further to only include disturbances that involve a circuit breaker operating due to a fault in the power system [12]. However, the difference is trivial as all faults in the electric power system involves a circuit breaker switching.

The concept of a disturbance revolves greatly around the notion of a fault. IEC defines fault [of an item] in their Electropedia as:

> [the] inability to perform as required, due to an internal state [9]

A disturbance is always initiated by a fault. Furthermore, a fault may induce additional faults with or without outages, as illustrated in Figure 2. It is important to note, that an outage does not necessarily mean the interruption of power supply for an end-user, even though an outage is explicitly defined as "[an] interruption in supply of electric power" [9], because the end-user may be supplied with power through an alternative route.

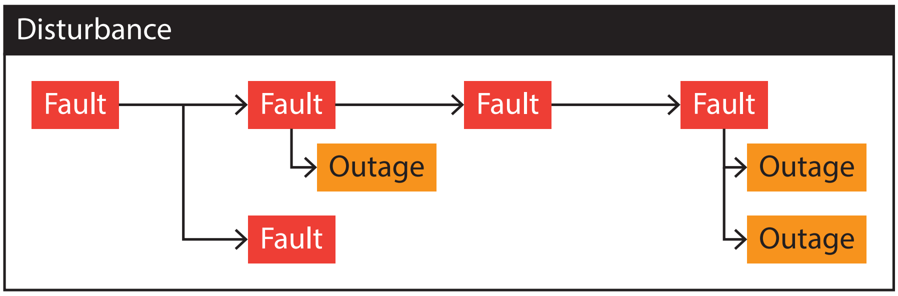

Figure 2: An example of a disturbance. The disturbance begins with a fault, which results in additional faults and outages. This means that a fault may have a fault as its cause and another fault as its consequence. It should be noted, that an outage does not necessarily mean the interruption of power supply for an end-user as the end-user may be supplied with power through an alternative route.

2.3 The cause of faults

An important aspect of disturbance analysis is investigating the causes and consequences of the disturbances and their related faults. As the DISTAC group is specialised in grid disturbance statistics [11], it makes sense to use their way of categorising fault causes. The DISTAC group has categorised fault causes in 7 different categories: lightning, other environmental causes, external influences, operation and maintenance, other and unknown.

In this thesis, these categories are simplified together into one category: technical and operational faults. However, technical and operational faults are not the only kinds of faults that may disturb the operational security. Technical and operational faults do not include faults caused off nominal parameters and/or exceeding of regulated norms and standards, that is system faults, nor latent faults. By categorising fault causes into these three groups, technical and operational faults, system faults and latent faults, as shown in Figure 3, we can describe all the kinds of events that may threaten the power system security.

Chapter 2.3.1 describes technical and operational faults, and system faults and latent faults are defined in Chapter 2.3.2 and Chapter 2.3.3, respectively.

2.3.1 Technical and operational faults

Technical faults are, as the word depicts, caused by technical errors. They originate directly from the item with the fault, for example in the form of faulty relay settings or as neglected maintenance, or are directly affecting it, for example by a lightning strike, a falling tree, a short-circuit or other technical faults. This thesis derives a definition of a technical fault from the IEC definition [9] of a fault, and defines a technical fault as:

> the inability to perform as required, due to a technical error.

Operational faults need to be extracted into a separate entity from the operation and maintenance, that is defined by DISTAC [12]. The DISTAC group includes

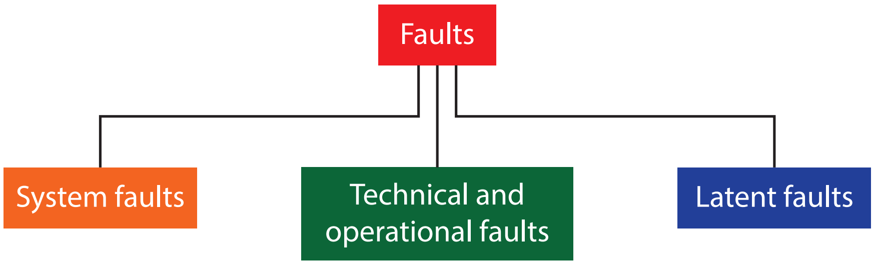

Figure 3: Faults can be divided into three main groups depending on what the fault was caused by: technical and operational faults, system faults and latent faults. These categories let us assess every event that may threaten the security of a power system.

the following causes in operation and maintenance: "Lack of monitoring, fault in settings, fault in connection plan, fault in relay plan, incorrect operation, fault in documentation, human fault" [12]. When maintenance causes are excluded, operational causes include lack of monitoring, incorrect operation, and can shortly be described as temporary faults caused by erroneous human action. Human error is defined in the IEC Electropedia [9] as "[a] discrepancy between the human action taken or omitted, and that intended or required" [9]. This thesis derives a definition of an operational fault from the above sources into the following:

> [the] inability to perform as required, due to a temporary human error.

We can consider this definition compatible with the definitions used by the DISTAC group [12] as it is simply an extension of them.

2.3.2 System faults

The categories mentioned in the Chapter 2.3 above do not include faults caused by abnormal operating conditions in the power system. Abnormal operating conditions can be caused, for example, by a drop in generation or load which, in turn, may cause too high or low frequencies or voltages. Disturbances caused by abnormal operating conditions are called system disturbances. The official IEC definition of a system disturbance [9] is:

> unplanned sudden change in electric power system operating condition that causes widespread power quality problems or interruptions
>
> Note 1 [...] A system disturbance can be initiated by a fault in the transmission system, a trip of a generation unit, loss of load, or any combination thereof. System disturbance can lead to abnormal ranges of frequency or voltage, loss of power system stability or cascading outages of power transmission circuits and as well widespread interruption of customer load.

The IEC definition only covers disturbances and not individual faults. In the scope of this work, we need to define faults caused by abnormal operating conditions. Therefore, this thesis will propose to define the concept of a *system fault*.

A *system fault* is defined in this thesis as:

> the inability of an item to perform its intended function due to off nominal parameters and/or exceeding of regulated norms and standards.

In other words, a system fault is a fault due to out of normal operating conditions. Examples of out of normal operating conditions are too high or low frequencies or voltage levels or power oscillations. Even though the the violation of electrical standards causes an item to trip, the item behaves as it was intended. The key element in a system fault is, that the normal operating conditions have been violated and that the trip is actually the intended action.

2.3.3 Latent faults

A latent fault is better described as a fault that does not affect the current stability of a power system, but does decrease the level of its security. A latent fault is a fault that goes undetected as it occurs, but surfaces as another fault aggravates the situation. The IEC Electropedia defines a latent fault [9] as:

> fault that has not become apparent.

A great example of this is a N-1 situation. The N-1 principle is a design rule, which aims to assure the system can handle one of the probable contingencies without disrupting the stability of the system [13, p. 66—67]. In recent times, the principle has been extended to also cover N-X situations. A N-1 situation may occur when one of several parallel transmission lines trip and the load carried by the tripped line has to be carried by the remaining lines. However, if the power demand increases further, the thermal capacity of the remaining lines may be exceeded and cause them to trip.

Additional examples of a latent fault could be loss of tools in the control room and a reduction of the available reserve capacity. Latent faults that are successfully compensated for, without aggravating the situation, are not reported.

2.4 No fault situations

The security of a power system can be affected by situations not involving a fault at all. Because the ICS report includes these events, the concept of a no fault situation needs to be defined. This thesis defines a no fault situation as:

> an outage or limitation without a fault.

Examples of no fault situations are sudden limitations of HVDC links due to temperatures or intentional islanding. Furthermore, this definition does not conflict with any of the other definitions in this thesis.

2.5 Remedial action

As faults in the power system can never be completely prevented, there must be some kinds of actions to mitigate their effect. A widely used term for an action, that is aimed to bring a system back to a normal state, is remedial action. However, this term is not defined in the IEC Electropedia. The ENTSO-E Network Code on Operational Security [13] describes remedial actions as "[...] any measures applied by a TSO in order to maintain Operational Security". In this thesis, remedial action is defined as:

> an action that is intended to restore a system partly or fully back to a stable state.

Remedial actions can be either manual and automatic operations and include, for example, load or generation shedding, increasing of generation or load, islanding, i.e. separating a part of the grid from the rest of it, disconnecting faults from the grid.

Manual remedial actions are conducted by the operating personnel in the control centers, while automatic remedial actions are pre-programmed schemes that operate depending on the local or system-wide operating conditions. The automatic remedial actions are often described as remedial action schemes, or RAS. Another terms that are often used interchangeably with RAS are SIPS and SPS. SIPS stands for system integrity protection system, and SPS stands for either system protection scheme or special protection scheme. Furthermore, these terms may have different meanings depending on where in the world these are used [14, 15, 16, 17]. Therefore, it would be beneficial to distinct these terms from each other.

This thesis categorises remedial actions according to the nature of its activation method, that is manual or automatic. Furthermore, automatic remedial actions are divided according to whether a circuit breaker has switched or not. If a circuit breaker does not operate, it is called an automatic remedial action by a system control scheme, or automatic SCS in short. Examples of these remedial actions are increasing/decreasing of power flow in HVDC links or the automatic generation or load changes in power plants. If a circuit breaker switches, it is called an automatic remedial action by a system protection scheme, or automatic SPS in short. Automatic SPS are, for example, load shedding or separating the grid into islands. However, this thesis classifies all conducted remedial actions, manual and automatic, as the same because the type of means used to recover from an instability do not matter significantly.

Another term associated with remedial actions is restoration state. Restoration state is the fifth operational state a transmission system can be categorised as during a disturbance, with the four first being normal, alert and emergency state and blackout [7, 8]. SOGL describes the restoration state as follows:

> A transmission system shall be in the restoration state when a TSO, being in the emergency or blackout state, has started to activate measures of its restoration plan [7].

The restoration state starts when the first remedial action is applied and ends when the system is back in a safe operating state, as shown in Figure 4. However, the restoration state is only entered if the system is in the emergency or blackout state. When the system is in the restoration state, the objective of all activities shall be to restore normal operating conditions in the power system [7, p. 6].

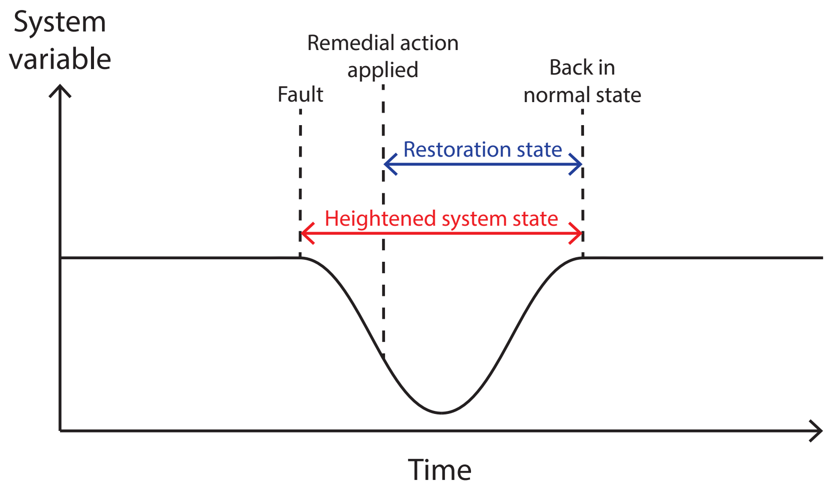

Figure 4: Remedial action is the response applied to counter the negative effects of an incident in the power system. The time from the beginning of the first remedial action until the system has returned to a stable operating state is called the restoration time, as defined in the SOGL [7]. It should be noted, that the state after the incident is not necessarily the same as the state before it.

3 Research material and methods

The main material used in this thesis is the current version of the incident classification scale methodology of 2018 [8], the produced ICS annual report of the statistical year 2017 [18] and the legislation that drove the creation of ICS [6, 7, 19]. Furthermore, the incident classification scale is compared to and reviewed with other academic and regulatory sources. For example, definitions used in this thesis are based on IEC [9] and definitions made by the DISTAC subgroup [12] in ENTSO-E, and European concepts are compared with concepts used by the North American Electric Reliability Corporation NERC [15] and the Australian Energy Market Operator AEMO [20].

Another important source of information are 6 interviews conducted with TSOs that are involved in the ICS. The participating TSOs were AST from Latvia, Energinet from Denmark, Fingrid Oyj from Finland, IPTO from Greece, RTE from France and Statnett from Norway. The interview questions and their answers are presented in Appendix A.

The methods used in this thesis are as follows. First, the current incident classification scale is reviewed. The review inspects its four step incident classification scale, operational security indicators, defined reporting procedures and the latest ICS annual report. Second, interviews made with six TSOs involved in the ICS methodology and reporting will be analysed. This analyse will be the cornerstone to find which improvements are most necessary to enhance the reporting, storing and visualising of the ICS data.

Last, each improvement suggestion is evaluated by the following criteria:

- the reasons for implementing the improvement;
- the necessary changes to be made if the improvement is implemented;
- the difficultness of implementing the improvement;
- the benefits of implementing the improvement.

4 The current state of the incident classification scale

The incident classification scale is written by the ICS subgroup and has been under development since 2013. The latest revision was accepted by the System Operations Committee (SOC) 11 April 2018 [8]. The main objective of the incident classification scale methodology is to secure a sustainable and long-term operational security and present its current state in the Pan-European power grid. The task has been divided further into smaller tasks, according to EU Regulation No 714/2009 [6] and the SOGL [7]. The ICS methodology [8] defines them in short as:

- provide an overview of the operational security indicators related to operational security and planning;
- identify improvements in general and improvements to network tools to support a sustainable and long-term operational security in both real-time operation and operational planning;
- explain the reasons behind scale 2 and 3 incidents;
- deliver an annual report based on the incident classification scale.

The ICS Methodology adopts these goals by defining an incident classification scale and security indicators, which describe the system state for further evaluation. Furthermore, it imposes reporting procedures needed to produce an annual report about the operational security in the Pan-European power grid.

Section 4.1 reviews the incident classification scale and its incident categories, Section 4.2 examines the operational security indicators, Section 4.4 evaluates the graphical aspects of the latest ICS report from 2017 [18], Section 4.5 summarises the key points from the conducted interviews with 6 representants from TSOs involved in ICS and Section 4.6 summarises this chapter and describes the most significant improvement suggestions.

4.1 The incident classification scale

The incident classification scale methodology defines a 4 step scale that evaluates the system state at a certain time according to 10 criteria. The system state steps are named normal, alert, emergency and blackout state and their gravity is described with a number from 0 to 3, with normal being level 0 and blackout being 3, as shown in Figure 5. The number of affected TSOs during an incident plays a significant role when determining the gravity of an incident.

Classifying systems and situations has been a common practice in many different situations. For example, the triage system used in medical care and crisis situations assesses which patients need care the most so that the medical personnel can aim their care towards those that need it the most [21, 22]. A medical triage system was used for the first time in the early 1800s. The triage system used in rescue

Scale 0 **Normal** Local incidents	Scale 1 **Alert** wide area incidents	Scale 2 **Emergency** extensive incidents	Scale 3 **Blackout** major incidents
System is within electrical norms and standards and can withstand a contingency without violating them nor the N-criteria. Affects one TSO.	System is within electrical norms and standards, but can not withstand a contingency without violating them. Affects neighbouring TSOs.	Electrical norms and standards are violated. Affects multiple TSOs	Part or all of the transmission system operations have been terminated.

Figure 5: The 4 step scale used in the incident classification scale. incident classification scale matrix and its notes, as presented in the ICS methodology [8]. The system state steps are named normal, alert, emergency and blackout state and their gravity is described by a number from 0 to 3, with normal being level 0 and blackout being 3. The gravity depends greatly on how many TSOs are affected during the incident.

situations is quite similar to the ICS. They both aim to correct what has gone wrong, give a brief yet concise description about the current situation and notify external actors, like authorities or in our case neighbouring TSOs, that their help may potentially be needed. Furthermore, they use the same colors to convey the perception of seriousness to the reader, as can be seen in Figure 7.

The choice of using these colors is a natural, as they are often depicted to portray appropriate emotion to the viewer [23]. Red is often used to convey anger or danger while green can be used to express good taste and happiness [24]. However, the emotional feeling is greatly affected by the readers cultural background. Yellow, for example, expresses envy and jealousy in Germany while it portrays death in Mexico. Additionally, 8 % of all men and 0.5 % of all women in Northern Europe suffer from a varying degree of red-green color blindness, which makes separating some colors from each other extra difficult for them [25]. Despite that, the colors used in the ICS table would not make the categories difficult to distinguish from each other even if it looks peculiar, as seen in Figure 6. Therefore, it is important to choose colors wisely when visualising data or any other pieces of information in order to present the information correctly to everyone. Color is a difficult yet powerful tool in information visualisation. The pioneer of information design, Edward Tufte, recommends to not use colors for a friendlier user experience [26, p. 183].

Other examples can be found in the world of business and software development, when one considers which features are more critical than others in order to produce a product that would fulfil customer requirements [27, 28]. ICS differs from these examples by the fact that it is used for statistics and evaluates therefore the events after they have happened, while the medical triage system is used in present time. Nevertheless, the ICS can and is being used in real-time and the system that uses it in real time is called the ENTSO-E Awareness System, or EAS in short [29]. The ICS and EAS may however have discrepancies when assessing the system state, because the available data in real-time is not as extensive as the data available later on, as mentioned in the ICS methodology [8].

As mentioned above, the system states used in the ICS are named normal, alert,

Figure 6: An example of how color blindness affects the currently used colors in the incident classification scale. First from top shows how it looks with normal color sight, the second presents how the colors look if the viewer has deuteranopia (red-green color blindness) and the last demonstrates how the colors look for a person with tritanopia (blue-yellow color blindness).

emergency and blackout state. They also have official definitions specified in the SOGL [7], which are opened below.

Normal state means "a situation in which the system is within operational security limits in the N-situation and after the occurrence of any contingency from the contingency list, taking into account the effect of the available remedial actions" [7]. What this effectively means, is that a system is in a normal state when it can withstand one disturbance or other kind of event without violating any electrical standards or norms nor the N-1 principle. This aligns well with established perceptions of power system stability and security in academic writings [10, 1].

Alert state describes a "system state in which the system is within operational security limits, but a contingency from the contingency list has been detected and in case of its occurrence the available remedial actions are not sufficient to keep the normal state" [7]. The alert state is somewhat identical to the normal state, except for that it can not handle another contingency without endangering the system stability, therefore breaking the N-1 rule. Multiple TSOs are also involved in the incident.

Emergency state means "the system state in which one or more operational security limits are violated" [7]. When a system enters emergency state, the risk of the state being further aggravated is dangerously high. Therefore, TSOs need to activate all countermeasures to restore the system back to normal operating conditions in order to avoid a blackout. When a TSO activates its first remedial action when in the emergency state, the system also enters the restoration state, as described in Chapter 2.5 and the SOGL [7]. The restoration state is therefore a state

Table 1: The stability criteria used in the incident classification scale [8]. Each criteria has one or more thresholds, which determine the severity of the incident with 0 being the least severe and 3 being the most. They are all consequences of some kind of event in the power system. Therefore, ICS can be said to be consequence-oriented.

Short code	Description
L	Incidents on load
G	Incidents on generation
F	Incidents on frequency degradation
T	Incidents on transmission system elements
ON	N and N-1 violations
RS	Separation from the grid
LT	Loss of tools and facilities
OV	Violation of standards on voltage
RRC	Reduction of reserve capacity
OB	Blackout

that is applied parallel to the severity state.

Blackout state "means the system state in which the operation of part or all of the transmission system is terminated; " [7]. Operating a system in a blackout state is very difficult even for skilled TSOs, because the system has already lost over half of the load and therefore also a lot of the kinetic energy that backs up the frequency. The risk of escalating the blackout into the whole area is high, and the TSOs need to start planning a black start of the whole area. The process of bringing a power system back to its full operating power is a very difficult task, as it requires careful increasing of both generation and load in order to avoid another blackout.

Usage of these terms has not been registered outside the Pan-European power system scope. Stability thresholds are however important to every synchronous power system and need to be set so its operators can operate it securely. The closest version of the incident classification scale used in the Pan-European power system is found in Australia and enforced by the Australian Energy Market Operator, AEMO [20]. They define a set of conditions that need to apply if a their power system is classified as being in a *satisfactory operating state*. Additionally, AEMO defines a set of extra conditions that need to apply in order to the system being in a *reliable operating state* or a *secure operating state*. However, there is no mention of what a state that is not satisfactory is called.

The criteria for a satisfactory system state in Australia can be compared to the 10 criteria used in the incident classification scale. The major difference between the Australian system and the European is the 4 step scale in the ICS that gives a magnitude to each criteria. For example, if the frequency threshold of a stable operating state is violated, ICS rates it as a frequency violation of scale 0 to 3. The stability criteria used in the ICS are presented in Table 1.

These categories are common values used when evaluating power system security [1]. They are all consequences of some kind of event in the power system. Therefore, ICS can be said to be consequence-oriented, as also portrayed in the TSO interviews in Section 4.5. However, the blackout criteria stands out from the rest of the criteria, because it is also defined as a system state. The blackout criteria is triggered if a system has lost more than 50 % of its demand or if no voltage has been present in a system for more than three minutes. One improvement suggestion would be to remove the blackout category and implement the blackout thresholds in the other categories. Another noteworthy fact is that every criteria does not have thresholds for every system state. For example, incidents on load (L) and separation of grid (RS) only have a threshold for alert and emergency state. The visualisation of the ICS table does portray this to the reader, as can be seen in Figure 7. Nonetheless, it could be portrayed better by aligning each criteria on its own row, as seen in Appendix D Figure D1.

The incident classification scale defines one set of extra rules, when regarding the system states and the security criteria. These rules become relevant when an incident affects several criteria at the same time. ICS has specified that "[w]hen an incident meets several criteria, the incident is classified according to the criterion that has the highest priority" [8], as shown in Figure 7. Therefore, ICS has numbered each scale of each criterion with a priority number ranging from 1 to 25 to help the reporter to determine what to report. This leads to some uncertainties when reporting the ICS data, as explained in Section 4.3.

In the end, a four step scale for assessing the system state works well when power system security needs to be evaluated in a brief yet comprehensive manner. It gives a quick overview of the power system stability, and when each TSO in the Pan-European synchronous areas can see the operating state of the other TSOs in real-time (with the help of the European Awareness System), they can take needed precautions if they notice that a neighbouring TSO system state is declining. Nonetheless, it contains some clarity issues that have made understanding the ICS and its reporting difficult. This statement is supported by the six interviews with TSOs that are involved in ICS. The interviews are reviewed in more detail in Section 4.5.

4.2 The security indicators used in the incident classification scale

The incident classification scale contains a set of operational security indicators, that are defined and enforced by the SOGL [7]. The aim of these indicators is to survey the operational security by measuring variables that affect it, namely the system state and faults, disturbances and other incidents that cause these system state violations. The measurements involve either counting the number of occurrences of a violation or contingency happening, the number of minutes a violation has lasted in a year, or a combination of them both. Furthermore, additional security indicators can and should be implemented if a need for them is deemed necessary.

As mentioned, these indicators have to be measured and reported in the ICS annual report according to the regulation. Therefore, it is necessary that the definitions and reporting procedures are compatible with them. Fortunately, the current ICS criterions are compatible with the enforced security indicators, as can be seen in

Scale 0 Anomaly		Scale 1 Noteworthy incident		Scale 2 Extensive incidents		Scale 3 Wide area incident or major incident / 1 TSO	
Priority / Short definition (Criterion short code)		**Priority - Short definition (Criterion short code)**		**Priority - Short definition (Criterion short code)**		**Priority - Short definition (Criterion short code)**	
#20	Incidents leading to frequency degradation (F0)	**#11**	Incidents on load (L1)	**#2**	Incidents on load (L2)	**#1**	Blackout (OB3)
#21	Incidents on transmission network elements (T0)	**#12**	Incidents leading to frequency degradation (F1)	**#3**	Incidents leading to frequency degradation (F2)		
#22	Incidents on power generating facilities (G0)	**#13**	Incidents on transmission network elements (T1)	**#4**	Incidents on transmission network elements (T2)		
#23	Violation of standards on voltage (OV0)	**#14**	Incidents on power generating facilities (G1)	**#5**	Incidents on power generating facilities (G2)		
#24	Reduction of reserve capacity (RRC0)	**#15**	N-1 violation (ON1)	**#6**	N violation (ON2)		
#25	Loss of tools and facilities (LT0)	**#16**	Separation from the grid (RS1)	**#7**	Separation from the grid (RS2)		
		#17	Violation of standards on voltage (OV1)	**#8**	Violation of standards on voltage (OV2)		
		#18	Reduction of reserve capacity (RRC1)	**#9**	Reduction of reserve capacity (RRC2)		
		#19	Loss of tools and facilities (LT1)	**#10**	Loss of tools and facilities (LT2)		

The priority of each criterion is shown in table 1 with a number from 1 to 25, where 1 marks the criterion with highest priority and 25 marks the criterion with lowest priority. **When an incident meets several criteria, the incident is classified according to the criterion that has the highest priority.**

Figure 7: The incident classification scale matrix and its notes, as presented in the ICS methodology [8]. Incidents are categorized into 4 scales ranging from 0 to 3, each describing the current state of the power system i.e. normal, alert, emergency and blackout state. System state assessment is further divided into 10 types of criteria. Furthermore, each criterion has a priority number ranging from 1 to 25. It should be noted, that each type of incident does not have a borderline scale assigned to it. For example, an N-1 violation only affects the state at the incident scales 1 and 2, and blackout is the single category at scale 3.

Table 2. However, the present reporting procedure of only reporting the incident with the highest priority does make measuring these security indicators more difficult, as mentioned in Section 4.1. One massive event would undoubtedly violate multiple security criteria, which would make it necessary to include all that data into one single line of data, and therefore increase the number of columns needed to report a single incident according to the incident classification scale.

4.3 The reporting rules and procedures of the incident classification scale

The incident classification scale methodology describes the process of how and what each TSO should report their data [8, p. 21–22]. This includes general rules applied to the reporting, its process and timeline and an additional section about how to

Table 2: The operational security indicators used in the incident classification scale and their associated ICS counterpart. Most of them have an ICS criterion for a secure operating state is covered, however, N violations and loss of tools and facilities are not explicitly mentioned. Furthermore, some of the security indicators measure the performance of the TSO dependent contingency lists. OS abbreviations stand for security indicators relevant for operational security and OPS stand for security indicators relevant to operational planning, as presented in Chapter 3 in the ICS methodology [8, p. 18–19].

Security indicators	Associated ICS counterpart
OS-A	T violations
OS-B	G violations
OS-C	L violations
OS-D	All emergency and alert state incidents
OS-E	RRC violations
OS-F	OV violations
OS-G	F violations
OS-H	RS violations
OS-I	OB violations
OPS-A	All ordinary contingencies (TSO dependent)
OPS-B	As OPS-A
OPS-C	All exceptional contingencies (TSO dependent)
OPS-D	As OPS-D
OPS-E	RRC violations

perform the deeper analysis of each incident that reaches a criteria of scale 2 or above.

In short, the rules specify that each TSO should report the required ICS data quarterly and that it should be delivered by a predefined contact called SPOC (single-point of contact). The reported data should include all incidents with a scale 0 or above and that have occurred in the 220 kV power grid or above and the SPOC is also responsible for replying to inquiries about the data and to validate its correctness. This practice seems simple yet robust enough and encourages creating efficient routines to provide legitimate data.

Each reported incident contains 22 values of common data [8, p. 26–27], which is reported regardless of the violation category. Depending of the type of violation, a subset of 15 more values is reported. Furthermore, there is a clause that says that all related incidents should be aggregated into one incident and that the aggregated incident should be labelled as according to the incident with the highest priority, as mentioned in Section 4.1 in Figure 7. However, the clause does not say whether the additional data should be submitted per each type of violation or only be the criteria with the highest priority. By only reporting the criteria with the highest priority, the SPOC could potentially only report the details of the highest criteria and disregard the other incidents, causing data loss. Therefore, the logical way of

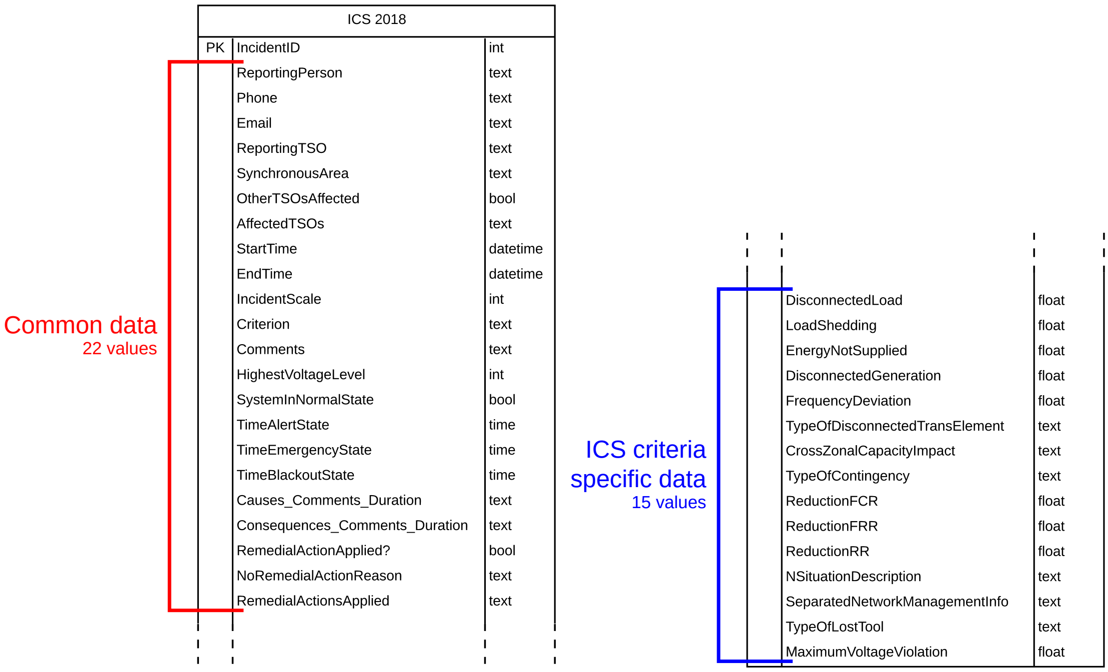

Figure 8: The database model of the current incident classification scale reporting. It contains 22 values that should be reported no matter what kind of event has disturbed the power system security, and another 15 values that should be filled in selectively depending on what kind of event has happened.

aggregating an incident would be to merge all the details of each individual incidents into an aggregated incident. This should not be a problem, because the additional details that have to be reported depending on which ICS criteria has been met do not conflict with each other too much, as can be seen in Table 3. Nevertheless, conflicts may and will happen due to the nature of the power system, entailing that the SPOC has to decide which details are more important the others. The common data for each related incident, containing information about the start time, voltage level and so on, still has to be aggregated somehow and the SPOC has to manage to do it correctly. Therefore, it is debatable whether the practice of merging a series of related incidents into one big event according to the incident with the highest priority is beneficial. Aggregating events is still an extra step that personnel with an already high workload could manage without.

This issue surfaces again when an incident involves several TSOs [8, p. 22]. Because each involved TSO has reported their side of the incident in their own grid, those need to be merged again into one event containing the details of them all. This process has the same drawbacks as described above. The only difference is that it involves multiple TSOs and thus increasing the workload and involved persons.

Fortunately, this improvement only relies on finding the common denominators and then building an improved data model accordingly. One kind of improvement to this issue is suggested in Section 5.

As mentioned earlier, each incident that reaches a criteria of scale 2 or above has

Specific data to be reported depending on ICS criteria	ICS criteria									
	T	L	G	F	RS	ON	OV	RRC	LT	OB
An estimate of disconnected load (MW)	-	X	-	X	-	-	-	-	-	X
Load shedding (MW)	-	-	-	-	X	-	-	-	-	-
Energy not supplied (MWh)	-	X	X	-	-	-	-	-	-	X
An estimate of disconnected generation (MW)	-	X	X	X	X	-	-	-	-	-
An estimate of frequency deviation (mHz)	-	X	X	X	-	-	-	-	-	-
Type of disconnected transmission system element(s)	X	-	-	-	-	-	-	-	-	-
Estimated impact on cross zonal capacity in both directions between bidding zones (MW)	X	-	-	-	-	-	-	-	-	-
Type of contingency (for disconnection of the transmission network element): ordinary, eceptional, out-of-range	X	-	-	-	-	-	-	-	-	-
FCR capacity reduction (MW)	-	-	-	-	-	-	-	X	-	-
FRR capacity reduction (MW), separated by aFRR and mFRR	-	-	-	-	-	-	-	X	-	-
RR capacity reduction (MW)	-	-	-	-	-	-	-	X	-	-
Descrition of the N or N-1 situation	-	-	-	-	-	X	-	-	-	-
Information about the management of the separated network	-	-	-	-	X	-	-	-	-	-
Type of tool lost	-	-	-	-	-	-	-	-	X	-
Maximum voltage violation	-	-	-	-	-	-	X	-	-	-
Number of additional values to report	3	4	3	3	3	1	1	3	1	2

Table 3: The additional data to be reported depending on which ICS criteria is reported. An *X* expresses that the value is reported. The sparseness of the table illustrates well that the additional columns are very specific to which criteria is reported. An improvement suggestion is presented in Section 5.

to be analysed further and presented in the ICS annual report [8, p.23–24]. To the reporting procedures include the forming of an expert panel that will conduct the investigation and informing the regulatory authorities of each affected TSO and the Agency for the Cooperation of Energy Regulators (ACER). The expert panel has to be led by an expert from a TSO not affected by the incident in order to assure neutrality in the matter. However, if the scale 2 or 3 incident occurs in an isolated network like Great Britain, the investigation is conducted internally. The regulators still have to be informed about the investigation.

The expert group's investigation task begins with collecting information about the incident. This data includes information about system conditions before and after the incident along with applied remedial actions and the sequence of all the individual events. It should be noted, that all this data would be directly available if the ICS data would not be aggregated into the incident with the highest priority. Furthermore, the expert group shall collect real-time snapshots and measurements from SCADA and PMU equipment. After the expert group has collected all the required data and finished their investigation, it has to prepare a final report about the incident with explanations of why and how it happened and recommendations to how to prevent the incident from happening again.

4.4 The ICS annual report

The latest annual report about the incident classification scale is from year 2017 and contains data from all of ENTSO-E's full members [18]. It is divided into a chapter about the global overview, a chapter about the security indicators, one chapter each about all the synchronous areas in the Pan-European power system individually and ends with a conclusion. This contains all the information that the SOGL [7] has specified. Because this thesis aims to improve visualisation of ICS data, this section will focus on reviewing the graphical aspects of the annual report as a whole, and presenting some improved visualisations in Section 5.6.

The ICS annual report of 2017 contains 75 figures in total, of which 69 are column charts, 4 are pie charts and 2 are map charts. They convey the intended information to the viewer, but there are some issues with them. First of all, they miss titles and axis labels which makes the reader wonder what the figures contain in the first place. Fortunately, the figures have captions. Second, the chosen colors for all figures except the map charts use a color palette of green and blue colors, which are not ordered according to their gradient from green to blue or the opposite. A good example of this is Figure 4 in the ICS annual report 2017 [18, p. 9]. This makes it extremely hard to associate which synchronous areas belong to which part of the pie chart. A good improvement to this figure would be to apply a gradient of gray for the pie pieces or, if color is chosen to be used, colors that can be distinguished better from each other. In case colors of different hues are chosen, it is recommended to choose the colors so that color blind viewers can see the difference between them, as mentioned in Section 4.1.

The best figures in the ICS annual report of 2017 are definitively the map charts, as they portray much more detail than, for example, a pie chart, to the reader instantly. Therefore, another improvement suggestion would be to use more map charts.

4.5 TSO interview conclusions

In order to acquire first hand information about the incident classification scale, its methodology and the processes surrounding it, an interview was conducted with 6 TSOs involved in implementing and/or reporting it. The participating TSOs were AST from Latvia, Energinet from Denmark, Fingrid Oyj from Finland, IPTO from Greece, RTE from France and Statnett from Norway. The interview questions and their answers are presented in Appendix A. The questions were divided into four categories: personal details, the current state of the ICS methodology, the current state of ICS reporting and analysing and other questions.

The personal detail questions were aimed to learn about the professional background of the interviewee and for which department the interviewee worked for at his or hers company, in order to evaluate if that affected the answers in the other categories. The represented departments represented by the interviewed persons were maintenance, system operations and its development, fault analysis and security of supply. This entails that views from multiple departments are represented and that the answers will not be one sided. Furthermore, the six interviewed persons had a combined total of 30 years of experience about the incident classification scale. Five of them were members in the ICS subgroup and one was the TSO's single-point of contact person (SPOC), that is the person reporting the ICS data.

Regarding the current state of the incident classification scale, the interviewees were of the same opinion that operational security is clearly represented in it because it is made according to the SOGL [7] requirements. However, one TSO pointed out that operational security is very tricky to analyse without a network model and that the ICS is good at measuring the system impact and should be used to that. The main purposes of the ICS were according to the interviewed persons to share experiences and build a better and more secure power system in cooperation, along with analysing the collected data to provide improvement recommendations and having a common tool that can scale the measured system impact. The most important parts of the ICS were said to be the definitions, that is the terms, thresholds of the ICS criteria and the reporting rules and procedures. Other important aspects of the ICS was that TSOs are able to study incidents impacting multiple TSOs and the applied remedial actions. Opinions about needed improvements were also given. Many said, that the definitions should be specified more and that they should make use of standardized terms and norms, as it would help TSOs report their data better. Unfortunately, TSOs tend to not report data they can not correctly collect. Furthermore, remedial actions should be included better in the methodology and reporting. One interviewee wanted to make ICS fault-oriented in order to increase the synergy benefits with already existing reporting, that is the ENTSO-E HVAC and HVDC reports made by the DISTAC subgroup [11, 30].

The reporting processes of the ICS data varied greatly between the interviewees. Some spent a couple of hours each month while one person spent about 50 hours in a year. Most of them also needed to do an unnecessary amount of manual work and contact other departments in order to acquire the needed data for the ICS report, which further increased their own and other people's workload. The most tasking issue in reporting the ICS data was that it implied doing double or even triple amount of work, because ICS is not the only report that require data. Furthermore, ICS requires the data in a different format than other reports and data needs to be thereby compiled into an additional format.

The quality of the reported data was also concerning, because some companies do not report N-1 violations even if though they have many. Furthermore, the methodology has changed multiple times since its creation making historical data less correct. The SOGL has also ruled that the ICS annual report should contain suggestions for improving the operational security. However, those have not been included yet because there has not been any scale 2 or 3 incidents in the Pan-European synchronous grids. TSOs do still have their internal processes to improve their systems. The recent change of analysing the ICS per TSO along with the overview of each synchronous area was welcome. Nevertheless, if more analysis would be implemented into the ICS annual report, it would probably delay the publishing of it more because it is a very bureaucratic process that needs an approval from multiple instances.

When asked about any benefits from the ICS, the interviewees answered that the internal processes towards ENTSO-E and cooperation with other TSOs had improved. To gain more benefits, ICS should define how to aggregate incidents and monitor which TSOs aided with what kinds of remedial actions. This would require PMU measurements at cross-border lines and generation areas and thereby allow a detailed analysis of the incidents.

The other questions asked whether the interviewees hade seen other reports related to the ICS report, their opinion about the ENTSO-E Awareness System (EAS) and ENTSO-E's Transparency Platform and whether they thought that the 4 step incident classification scale system state number should be a floating-point number. They are aimed primarily to find out potential synergy effects with already existing projects globally and in Europe particularly, and to determine whether one of the improvement suggestions would be supported by the interviewees. Other existing reports that tangent the ICS report or could supplement to its value were ENTSO-E reports, for example the HVAC and HVDC reports made by the DISTAC subgroup [11, 30] and reports made by other TSOs. Reports made by other TSOs may not be public, though.

Concerning the EAS, all interviewees recognised that it is compatible with the ICS because they have been made according to the same principles. Nevertheless, there could be more cooperation between these two groups if an issue needs another opinion or point of view. The idea of including ICS data in the ENTSO-E Transparency Platform was not supported, because the Transparency Platform contains only market relevant data. The last question about adding a decimal to the incident classification scale number was supported if it would improve reporting quality.

To summarise the interviews, each TSO representative felt that the ICS complies with the rules enforced in the SOGL [7]. However, terms and procedures should be clarified and defined better to increase the data quality, the data format should be converted to a fault-oriented format and the reporting of the ICS data should be improved to decrease the workload.

4.6 Summary of the current state of the incident classification scale

As a summary, the incident classification scale categorises well each kind of incident that could potentially upset normal operating conditions and in the worst case cause a blackout. It defines a 4 step scale that evaluates the system state at a certain time according to 10 criteria, along with security indicators to measure the operational security and reporting rules and procedures to help TSOs report the needed data. However, the ICS definitions are sometimes unclear and the reporting procedures take a lot of time to complete by many TSOs.

Chapter 5 presents improvement suggestions that would unite ICS more with already existing reporting and also make the reporting process more streamlined by removing the extra aggregation step of merging related incidents into one line of data. Furthermore, additional improvements about storing and visualisation is presented.

5 Improving the incident classification scale

This chapter evaluates the improvement areas of the incident classification scale. It evaluates each improvement suggestion according to the following steps:

- the issue in the current state and the solution in short;
- the gains and losses of implementing the improvement;
- the necessary changes to be made if the improvement is implemented;
- the difficultness of implementing the improvement;

The improvement areas are divided into three categories: improvements to the incident classification scale, improvements to data storing and improvements to data visualisation. Chapter **??** analyses the improvement areas to the incident classification scale methodology, Chapter **??** inspects different data storing solutions and Chapter **??** considers various visualisation approaches.

5.1 Stop aggregating individual incidents into one incident

In the current state, each related incident is merged into a single event before being reported to the ICS system. Aggregating all related events into one single event is an immense problem that introduces unnecessary loss of details of every reported incident, while also introducing additional steps of work that could easily be avoided, as described in Chapter 4.

The loss of data occurs every time any single incident is merged with another because in the current state, every incident has 22 values of common data 15 values of category specific data and they are simple overwritten by the incident with the highest priority, as is mentioned in Section 4.3.

The benefits of implementing this improvement would be a decreased workload for reporting persons. Furthermore, the reporting procedure would probably become even more simple because the TSO databases already contain each of these events in them and the data could be sent to the ICS group directly. Additionally, reporting all the incidents creates automatically a storyline for the event series. If an expert group has to perform an investigation of an scale 2 or 3 incident, they will therefore have all the required data available immediately. The factual report mentioned in the ICS methodology [8] could theoretically be generated automatically. Moreover, reporting persons will quickly be accustomated to the reporting procedures and transparency and cooperation between each TSO will increase.

It should be noted, that even if all this information is gathered, it does not have to be publicly presented in the annual report. The additional information as a result of this improvement could provide valuable information if analysed and presented at least internally. The data could be used to analyse, for example, how many of the scale 0 incidents escalated into scale 1 or 2 incidents or if there are any relationships between some categories.

This improvement would only require adding one column to the data model, namely incident ID, to indicate which event series the incident belongs to. The existing rule of only regarding the incident with the highest priority can still be used, however it would be used only after all of the individual incidents have been reported. Furthermore, if all data is stored, one could test different ways of aggregating related incidents to find the technique that works best.

The difficulty of implementing this improvement is minimal, as it requires adding one value to the data that is already reported, and the existing aggregation rules can be reused. Modern databases should be able to handle the increased amount of data, which is minimal when compared to the amount of data TSOs are collecting constantly.

5.2 Making the incident classification fault-oriented

The most significant issue in reporting the incident classification scale data is that the definitions are unclear and that TSOs omit events that they do not know how to report, as mentioned in Section 4.3. Because the ICS is consequence-oriented, it is straightforward to fit it into the disturbance model with a cause, fault and a consequence, as illustrated in Figure 9, because all the incident categories can be assigned as a consequence. However, a consequence can also function as a cause and trigger other faults. The cause, fault and consequence circle may be triggered multiple times and it may be difficult to actually find the consequence that should be reported to the ICS. Therefore, it is quite problematic to report only consequences.

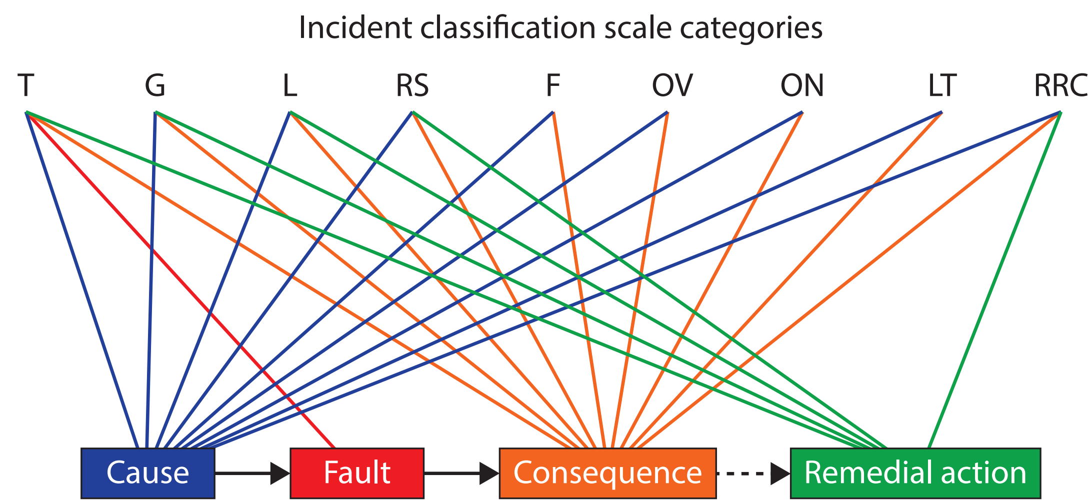

Figure 9: The way the incident classification scale categories fit into the cause, fault and consequence concept. The ICS category abbreviations are presented in Table 1

ICS is also the only report in ENTSO-E that is consequence-oriented, which makes collecting data to it an additional workload. The DISTAC group in ENTSO-E does however publish a fault-oriented HVAC grid disturbance report [11]. Furthermore, the same group also publish an outage-oriented HVDC report [30]. The perk of these reports are that they have been reported for a long time and have a tried and tested definitions and reporting methods, with the roots set in the 1960s [11]. By establishing a common foundation for reporting, we are able to do achieve a more efficient reporting, gather data with better quality and thus spend more time analysing the data in different ways and obtain more results. The common denominator between these reports is the fault. The next step is then to create a data model that can store all the different fault scenarios that can upset a power system.

The created model and its compatibility with the ICS, HVAC and HVDC report is presented in Figure 10. The categories in it are technical and operational faults, system faults, latent faults, no faults and remedial actions. They were chosen by evaluating all the different kinds of events that could potentially cause out of normal operating conditions, as can be seen in Appendix C in Figure C1 on the right side of the event column. The theoretical definitions can be read in Section 2.2. Furthermore, remedial actions were inserted because they are essential in bringing the system back into a stable operating state and because the it was one of the improvement suggestions, as presented in Section 4.5.

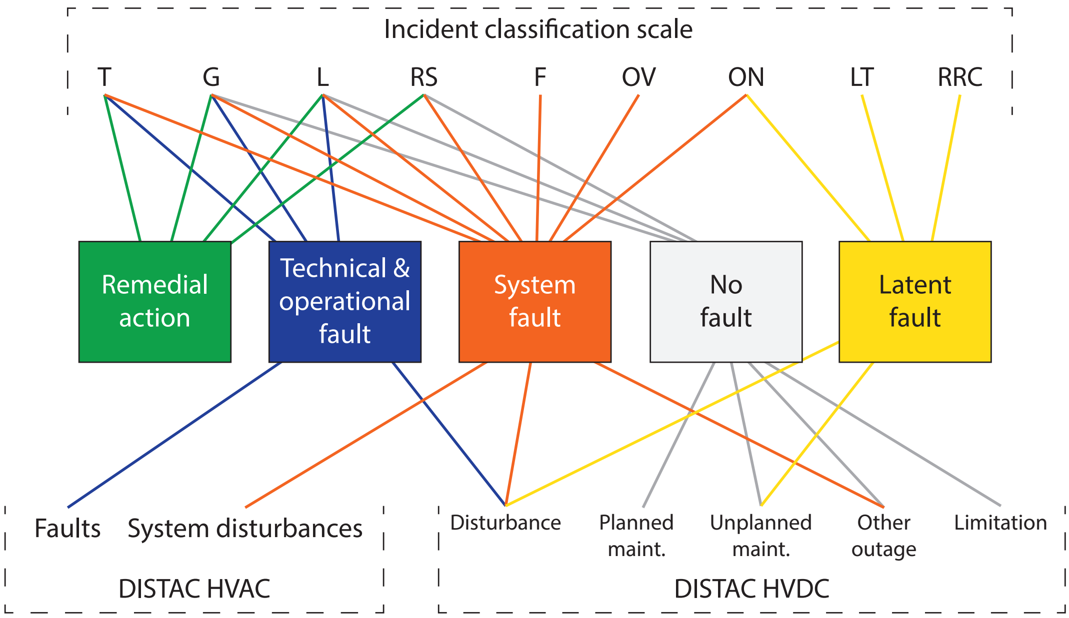

Figure 10: How the consequence-oriented incident classification scale categories, the fault-oriented HVAC report [11], produced by ENTSO-E's DISTAC group, and the outage-oriented HVDC report [30], also produced by ENTSO-E's DISTAC group, align with with the cause, fault, consequence and remedial action model.

The values in this data model are presented in Figure 11. This table is suitable for all the event types, that is technical and operational faults, system faults, latent faults, no faults and remedial actions. With this data model, we have decreased the table width from 37 columns to 15. The data model is missing a column for the scale value because when all individual incidents are reported and the values are correct, the system should be able to calculate the system scale automatically. This results in yet another benefit, that the SPOCs do not need to calculate the scales themselves. The SPOCs only need to take care of reporting the data correctly, and the system will take care of the rest.

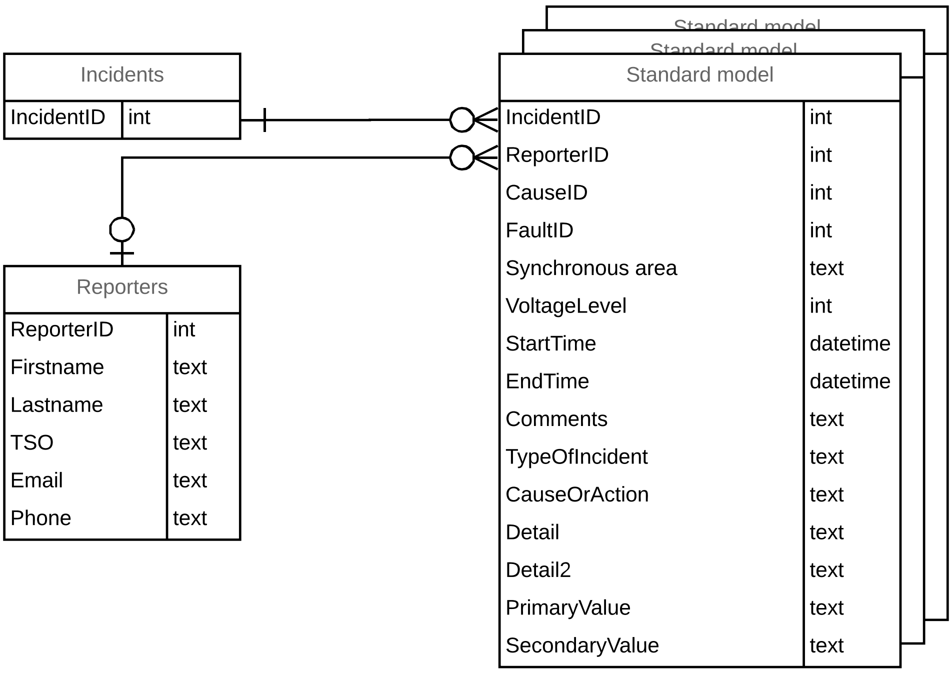

Figure 11: The data model of a fault-oriented table. This table is suitable for all the event types, that is technical and operational faults, system faults, latent faults, no faults and remedial actions. With this data model, we have decreased the table width from 37 columns to 15. Each data model has an IncidentID identification, which is meant to mark which events belong together. Furthermore, each reporter has an own user profile in order to avoid putting unnecessary and repeated information into the reported data. The usage of this data model is described in Appendix C.

The impact of this change is immense and implementing it may be difficult, because all tools and reporting practices need to be repurposed to work in a fault-oriented way. However, the benefits do outweigh the negative aspects. The persons responsible for reporting would have a system specifically designed for reporting these incidents, and it is very easy to divide the workload of, for example, reporting of remedial actions and technical and operational faults to separate experts if a TSO wants to. And lastly, double and triple reporting the same data to many different reports made by ENTSO-E would not be done anymore.

5.3 Add support for floating-point numbers for some incident classification scale categories

Aggregating smaller incidents into bigger incidents has been a difficult task in the ICS, especially because all individual events have been aggregated into one single event. However, this changes if the improvement in Section 5.1 would be implemented. Automatic calculation of the incident scale, mentioned in Section 5.2, would also introduce flexibility to the system. It would therefore be necessary to introduce rules to how ICS categories should behave when multiple of them happen in a small enough timeframe. These rules are presented in Table 4.

The aggregation rules are written from the ICS category criterions, which means that they are fully compatible with the other improvements in this chapter. Furthermore, these will make automating the ICS scale calculation easier, which is mentioned in Section 5.2.

5.4 Remove blackout from the incident classification scale categories

The blackout category is present as both a system state as well as an ICS category in the ICS methodology of 2018 [8], as can be seen in Figure 7. The blackout criteria is triggered if a system has lost more than 50 % of its demand or if no voltage has been present in a system for more than three minutes.

Therefore, this thesis will suggest to remove the blackout criteria from the ICS categories and move the criteria into violation of voltage (OV) and incidents on load (L). This improvement would be a minor yet easy upgrade, that would make the ICS categories more coherent. An implemented version of this is shown in Appendix D.

5.5 Redesign the incident classification scale table used in the incident classification scale methodology 2018

Table 1 in the incident classification scale methodology from 2018 presents the incident classification scales used at the moment in the ICS. It is a nice and compact table, but unfortunately it is hard to find anything from it because it is not clear whether a category can be found in a column or not. Therefore, the incident categories should be listed on the leftmost column so the reader can quickly find which categories the table contains.

The table can be further improved by indicating which categories have the appropriate system scale defined for them and which do not. By only filling in the cells that have a corresponding ICS category and a defined system scale threshold, the viewer can instantly see which categories have which thresholds defined. An improved version of the ICS table is presented in Appendix D in Figure D1.

Furthermore, one of these tables should be done for each synchronous area, because then the thresholds can be written directly into the table. This would make it easier for new people to see which categories have which scales and what the

Table 4: The aggregation rules for the incident classification scale categories. Only G, L and RRC incidents can be aggregated into a bigger event of the same kind, because the rest of the ICS categories depend on other circumstances to increase in magnitude. For example, separation of grid (RS) needs to affect other TSOs, while multiple incidents on generation can simply be summed together.

ICS category	Aggregation rule
G	Interpolate the scale linearly between the threshold limits. For example, a generation loss of 900 MW in the Nordic synchronous area would result in a G0.7. When calculating G incidents together, they are simply summed together.
L	Interpolate the scale linearly between the threshold limits. As the G incidents, but with the L incident thresholds.
F	No aggregation
T	Escalates to a scale 1 incident if an ON incident is reported during the T incident. Escalates to a scale 2 incident if at least one of the TSO's operational security limits are violated or if a neighbouring TSOs report remedial actions
ON	Escalates to a scale 2 incident if neighbouring TSOs report any incidents during the ON incident.
RS	Escalates to a scale 2 incident if the separated grid has a load above 1500 MW and a neighbouring TSO also reports an RS incident from the same separated grid.
OV	Escalates to a scale 2 incident if a neighbouring TSO also reports an OV incident.
RRC	Interpolate the scale linearly between the threshold limits. As the G incidents, but with the RRC incident thresholds.
LT	Escalates to a scale 1 incident if a neighbouring TSO reports any incidents during the LT incident. However, only if the neighbouring TSO's incident was caused by the LT incident.

thresholds for them are. The ICS table for the Nordic synchronous area is presented in Appendix D in Figure D2.

Lastly, these tables can be used even if they have the priorities removed and the suggestions in this thesis are not implemented, because the the rows are ordered in the same order.

5.6 Improving visualisation in the annual report to convey information to the reader better

As mentioned in Section 4.4, the ICS annual report contains a lot of figures that show data to the reader. This section will suggest some improvements to portray the contained data in a more compact and clearer way. The main suggestions is to not use colors of similar hue and in a mixed order. This makes it hard for the reader to find which data is presented where in the chart and which parts are associated with the other parts. A better solution is to use grayscales or single color gradients, which are suitable for color blind people too.

Furthermore, the human eye is always trying to compare the pictures presented to it by nature. Therefore, it is recommended to place the data in such way on the canvas that it is easy to compare with other objects. For example, by putting similar data beside each other and by grouping similar objects together.

Figure 15, 12, 13 and 14 present improved ways of showing the data presented in the ICS annual report from 2017. The original figures from the ICS annual report from 2017 can be found in Appendix B.

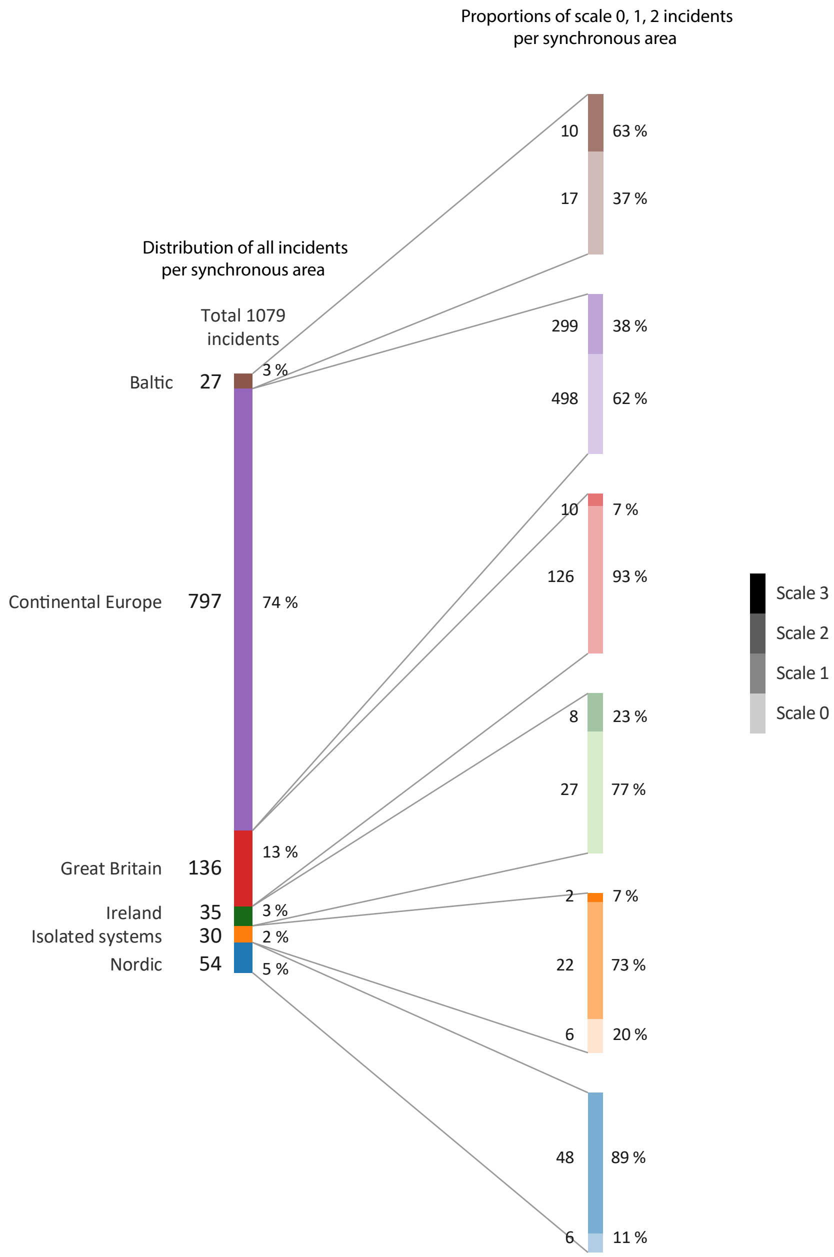

Figure 12: An improved version of Figures 3–5 from the ICS annual report of 2017 [18]. The original figures presented the number of incidents per synchronous area, their percentage distribution per synchronous area and finally compared the scale distribution inside each synchronous area with each other. The improved figure starts by turning the pie chart into a column and then plotting the number of incidents on it. Then it incorporates the percentage distribution of into the figure by plotting the smaller left bars on the right side bigger. The improved figure breaks the recommendation of not using colors in it, but if benefits outweigh the bad effects it can be done [26]. By using colors here, we can distinguish better which bar belongs to the correct synchronous area. Furthermore, the colors were checked to be suitable with color blind people. Last but not least, this figure also plots the number of incidents per scale as a bonus.

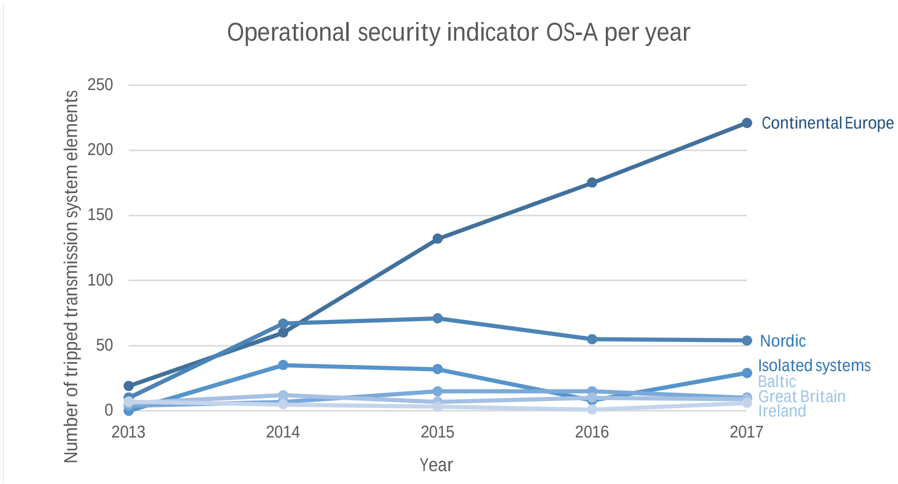

Figure 13: An improved version of Figure 17 from the ICS annual report of 2017 [18]. The original figure presented the operational security indicator OS-A per synchronous area. The synchronous areas were plotted on the x-axis and each annual value was plotted on top of it as a column chart. However, this makes it hard to compare annual values between synchronous areas. Furthermore, column charts may sometimes cause an excessive amount of chart junk. Therefore, the improved version moved the years to x-axis and plotted each synchronous area as a line on the chart area. The legend could also be removed when each line is labelled at the point it ends. This lets the reader quickly see which synchronous area has most OS-A indicators than the rest, because they are already ordered from top to bottom on the right side of the figure.

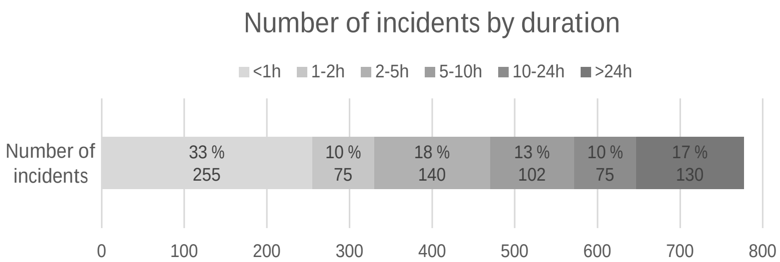

Figure 14: An improved version of Figure 25 from the ICS annual report of 2017 [18]. The original figure presented the number of incidents distributed according to its duration, with the duration category on the x-axis. The original figure worked really well, but I wanted to add more details to it in order for the reader to get as much information from it as possible. Therefore, I rotated the staples by 90 degrees and to allow the reader to see immediately the total amount of incidents in 2017. Then I coloured the duration categories in rising grayscale value with the lightest being the incidents lasting under one hour and the darkest being the incidents lasting more than 24 hours. Because darker colors indicate naturally of something more unhealthy and dangerous than lighter, this reader should automatically associate the lighter colors indicating incidents of shorter durations and darker as longer.

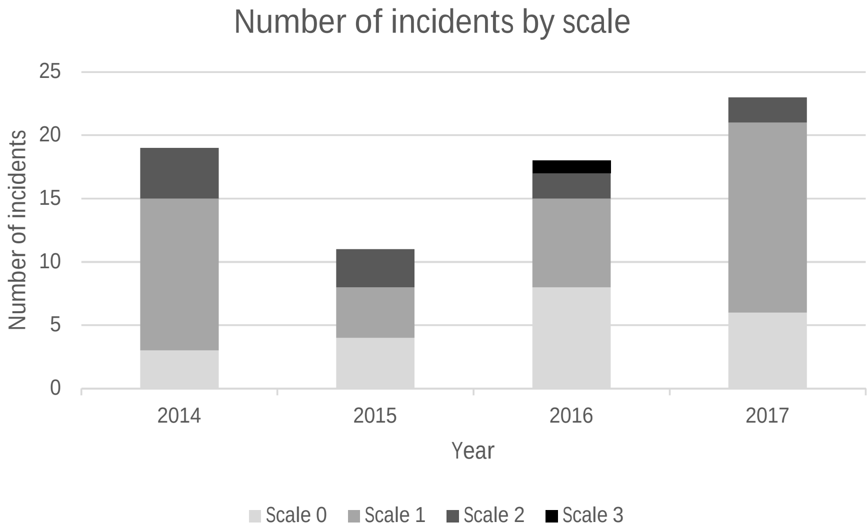

Figure 15: An improved version of Figure 75 from the ICS annual report of 2017 [18]. The original figure had the scales on the x-axis. Unfortunately, this makes it hard to compare the total number of incidents for the years 2014–2017. By plotting the years on the x-axis instead and stacking the scales on top of each other, we can present the same data as previously. Additionally, Figure 74 becomes obsolete as the improved figure shows them both at the same time.

6 Summary

This thesis has reviewed the current incident classification scale methodology and reporting procedures and suggested six different ways to improve it. The most significant improvement suggestion is to change the reporting type of ICS from a consequence-oriented to a fault-oriented way of reporting. This improvement would increase the amount of reported data significantly, but improve the data quality, by clarifying the definitions and using well known standards by the IEC and ENTSO-E's DISTAC subgroup, and decrease the workload enormously by eliminating double and even triple reporting and by making shared reporting with co-workers easier. Additionally, this thesis has defined new terms that could be used in the field more and implemented into the IEC Electropedia.

The other significant improvement suggestion is to start reporting all occurred incidents instead of aggregating them into a single incident. The benefits of this is an increase of available details and more transparency between TSOs, which will in turn also improve the cooperation between everyone.

Lastly, this thesis gives some handy information visualisation tips, improves the incident classification table among other subjects. The implementation of all these improvements will not be a quick and easy task, but will require careful planning due to the number of involved TSOs and because the reporting of the incident classification scale data is legally binding. Steps forward have to be taken, but it is important to evaluate all the possible choices before finally committing.

References

[1] K. Morison, , and P. Kundur, “Power system security assessment,” *IEEE Power and Energy Magazine*, vol. 2, pp. 30–39, Sep. 2004.

[2] ENTSO-E aisbl, “2018 Ten Year Network Development Plan.” `https://tyndp.entsoe.eu/Documents/TYNDP%20documents/TYNDP2018/consultation/Main%20Report/TYNDP2018_Executive%20Report.pdf`, 2018. [Online; accessed 09.03.2019].

[3] H. Byrd and S. Matthewman, “Lights out: the dark future of electric power.,” *New Scientist*, vol. 222, p. 26–27, May 2014.

[4] U.S.-Canada Power System Outage Task Force. and United States. , *Final report on the August 14, 2003 blackout in the United States and Canada [electronic resource] : causes and recommendations / U.S.-Canada Power System Outage Task Force*. U.S. Dept. of Energy [Washington, D.C], 2004.

[5] ENTSO-E aisbl, “ENTSO-E AT A GLANCE.” `https://docstore.entsoe.eu/Documents/Publications/ENTSO-E%20general%20publications/140925_ENTSO-E_at_a_Glance.pdf`, Sep 2014. [Online; accessed 08.01.2019].

[6] The European Parliament and The Council of the European Union, “REGULATION (EC) No 714/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity and repealing Regulation (EC) No 1228/2003.” `https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0015:0035:EN:PDF`, Jul 2009. [Online; accessed 05.01.2019].

[7] European Commission, “COMMISSION REGULATION (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation.” `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1485&from=EN`, Aug 2017. [Online; accessed 05.01.2019].

[8] Incident Classification Scale Subgroup, “INCIDENT CLASSIFICATION SCALE.” `https://docstore.entsoe.eu/Documents/SOC%20documents/Incident_Classification_Scale/180411_Incident_Classification_Scale.pdf`, Mar 2018. [Online; accessed 05.01.2019].

[9] International Electrotechnical Commission, “Electropedia: The world’s online electrotechnical vocabulary.” `http://www.electropedia.org`. [Online; accessed 05.01.2019].

[10] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, and V. Vittal, “Definition and classification of power system stability ieee/cigre joint task force on stability terms and definitions,” *IEEE Transactions on Power Systems*, vol. 19, pp. 1387–1401, Aug 2004.

[11] DISTAC subgroup, "Nordic and Baltic Grid Disturbance Statistics 2017." https://docstore.entsoe.eu/Documents/Publications/SOC/Nordic/Nordic-and-Blatic-HVAC-Disturbance-Statistics-2017.pdf. [Online; accessed 19.03.2019].

[12] DISTAC subgroup, "Guidelines for the Classification of Grid Disturbances above 100 kV." https://docstore.entsoe.eu/Documents/Publications/SOC/Nordic/HVAC_guidelines_2017_04_13.pdf, Apr 2017. [Online; accessed 18.03.2019].

[13] ENTSO-E aisbl, "Supporting Document for the Network Code on Operational Security." https://www.entsoe.eu/fileadmin/user_upload/_library/resources/OS_NC/130924-AS-NC_OS_Supporting_Document_2nd_Edition_final.pdf, Sep 2013. [Online; accessed 09.03.2019].

[14] M. Begovic, V. Madani, and D. Novosel, "System integrity protection schemes (sips)," in *2007 iREP Symposium - Bulk Power System Dynamics and Control - VII. Revitalizing Operational Reliability*, pp. 1–6, Aug 2007.

[15] The North American Electric Reliability Corporation, "Glossary of terms used in nerc reliability standards." https://www.nerc.com/files/glossary_of_terms.pdf. [Online; accessed 2.03.2019].

[16] P. M. Anderson and B. K. LeReverend, "Industry experience with special protection schemes," *IEEE Transactions on Power Systems*, vol. 11, pp. 1166–1179, Aug 1996.

[17] Y. Dong, J. Hou, J. Zhang, Y. Wang, and H. Wang, "The research, design and practice of the online special protection systems," in *12th IET International Conference on Developments in Power System Protection (DPSP 2014)*, pp. 1–4, March 2014.

[18] Incident Classification Scale Subgroup, "2017 ICS Annual Report," Sep 2017.

[19] The European Parliament and The Council of the European Union, "Energy - Market legislation." https://ec.europa.eu/energy/en/topics/markets-and-consumers/market-legislation. [Online; accessed 09.01.2019].

[20] , "Australian Energy Market Commission." https://www.aemc.gov.au/sites/default/files/2019-02/NER%20-%20v119_0.PDF, Feb 2019. [Online; accessed 08.04.2019].

[21] I. Robertson-Steel, "Evolution of triage systems," *Emerg Med J*, vol. 23, pp. 154–155, Feb 2006. 16439754[pmid].

[22] J. Nordström, F. Goerlandt, J. Sarsama, P. Leppänen, M. Nissilä, P. Ruponen, T. Lübcke, and S. Sonninen, "Vessel triage: A method for assessing and communicating the safety status of vessels in maritime distress situations," *Safety Science*, vol. 85, pp. 117–129, 06 2016.

[23] A. J. Elliot, "Color and psychological functioning: a review of theoretical and empirical work," *Front Psychol*, vol. 6, pp. 368–368, Apr 2015.

[24] M. M. Aslam, "Are you selling the right colour? a cross-cultural review of colour as a marketing cue," *Journal of Marketing Communications*, vol. 12, no. 1, pp. 15–30, 2006.

[25] "Facts About Color Blindness." `https://nei.nih.gov/health/color_blindness/facts_about`. Accessed: 08.04.2019.

[26] E. R. Tufte, *The Visual Display of Quantitative Information*. Cheshire, Conn.: Graphics Press, 2nd ed. ed., 2001.

[27] R. G. Docters, "Improving profitability through product triage," *Business Horizons*, vol. 39, no. 1, pp. 71 – 78, 1996.

[28] J. Karlsson and K. Ryan, "A cost-value approach for prioritizing requirements," *IEEE Software*, vol. 14, pp. 67–74, Sep. 1997.

[29] ENTSO-E aisbl, "Annual report 2017." `https://annualreport2017.entsoe.eu/wp-content/uploads/2018/06/ENTSO-E_Annual_Report_2017.pdf`, 2017. [Online; accessed 09.03.2019].

[30] DISTAC subgroup, "Nordic and Baltic HVDC Utilisation and Unavailability Statistics 2017." `https://docstore.entsoe.eu/Documents/Publications/SOC/Nordic/Nordic-and-Blatic-HVDC-Disturbance-Statistics-2017.pdf`. [Online; accessed 19.03.2019].

Appendices

A Interview results

This appendix contains the results from the conducted interviews. The questions are grouped into 4 parts: personal details, questions about the current state of the ICS methodology, the current state of the ICS reporting and other questions. There were a total of 6 interviews with different TSOs. Appendix A.1–A.6 presents the answers for AST, Energinet, Fingrid Oyj, IPTO, RTE and Statnett, respectively.

A.1 AS ”Augstsprieguma tīkls”, AST

This section presents the answers to the interview questions by AS ”Augstsprieguma tīkls” (AST) from Latvia. The questions are grouped into 4 parts: personal details, questions about the current state of the ICS methodology, the current state of the ICS reporting and other questions and presented in Tables A1–A4

Question	Answer
What is your name?	Anrijs Maklakovs
Which TSO do you represent and in which department do you work? What is your professional background?	AST Maintenance and health at work supervision service B.Sc in Electrical Engineering, Senior Electrical Engineer
What is your role in the ICS subgroup?	Member
How long have you been active in the ICS subgroup?	Since 2015
What have you been involved in the ICS subgroup?	I am the only TSO from the Baltics and I report and wash the Baltic data. I was involved in reviewing the incident classification scale methodology.
What are your responsibilities regarding the ICS at your TSO?	Everything
What are you personally most interested in regarding the ICS report?	The most interesting part is sharing experiences with other TSOs.

Table A1: AST’s answers to personal detail questions.

Question	Answer
What do you think is the main purpose of ICS?	Transparency. To share data and create common procedures and rules and to build a safer interconnected transmission network.
One focus area is operational security, is that clearly represented?	Yes, the idea is clearly represented. The ICS is made according to the operational security requirements defined in the SOGL.
What do you think is the most important part in the ICS methodology?	The thresholds, other things are clear, as well as the organisation. The thresholds are hard to set because the data quality depends on it. The thresholds are a bit wide for every TSO. There is also a lack of information about what should be reported on each (ICS) level.
Does the ICS methodology provide sufficient tools and definitions to accurately produce a report that fulfils its goals?	Normally, if something is unclear it is sufficient to read the latest version of the methodology to understand what to do. If you regularly participate the working group meetings you are aware of common rules, difficulties and experience of others.

Table A2: AST's answers to questions about the current state of the incident classification scale methodology.

Question	Answer
How does your reporting procedure of ICS data look like?	Once a month the data is collected into an Excel sheet and uploaded to the ICS homepage. The reported data is then washed after each quarter of a year, after which the data is considered final.
How much time does the ICS reporting take? (in hours)	Probably a couple of hours in a month. It does not take long because there are not a lot of incidents to report, about 7-8, max 10, incidents a year, and because there is no need for any specific information to report and I am experienced to do that.
How many persons does the reporting involve in your company?	Only me.
Are there any difficulties in the reporting process?	For me, no.
Does the report analyse the reported data well and present the information well to the reader?	The problem is that the methodology changes and that the data quality is lacking. The report is also a bit too wide, like comparing pears and apples. This/next report there should contain information about each TSO, like a summary. That could clear up things.
Does the report convey improvement suggestions for increasing the operational security well?	I don't know because I'm not in the highest systems operation committee and I don't know what they do with it.
Does your company get any benefits from the work done for the ICS?	The rules need to be followed. I think it's getting better, and the results will be better in the future. As said, the grid is quite stable because the grid is connected to the Russian synchronous grid. In 2025 it is planned to connect to the European synchronous area. Then the operational security could actually matter. At the moment, the HVDC and line switching stuff is reported.

Table A3: AST's answers to questions about the current state of reporting the incident classification scale data.

Question	Answer
Have you read reports by ENTSO-E or other companies that tangent the content of the ICS report?	DISTAC.
Do you think the ENTSO-E Awareness System is compatible with the ICS?	Yes.
Do you think that ICS should be incorporated to the ENTSO-E Transparency Platform?	I am not involved and aware of ENTSO-E Transparency Platform. For me, transparency is no problem.
Do you know of other reports that supplement the value of the ICS report?	EAS may have a report. The data from ICS is used to create report for performance indicators (SOGL).
Do you think that the ICS scale could be a floating-point number?	Here we have the thresholds again. Thresholds for each incident type is made according to type. There is scaling for each type and the scaling between different types. It means that incident types can't be compared directly. So, there is a lot of issue that should be salved in one report. That's the biggest challenge. If more data from incidents would be reported, the thresholds that work best could be analysed and determined. If the aggregation gives better results, I'm for it.

Table A4: AST's answers to other questions.

A.2 Energinet

This section presents the answers to the interview questions by Energinet from Denmark. The questions are grouped into 4 parts: personal details, questions about the current state of the ICS methodology, the current state of the ICS reporting and other questions and presented in Tables A5–A8

Question	Answer
What is your name?	Anders Bratløv
Which TSO do you represent and in which department do you work? What is your professional background?	Energinet, Denmark Security of Supply M.Sc. Electrical Engineering
What is your role in the ICS subgroup?	Just reporting. Single point of contact between Energinet and ICS. Collecting data and reporting to ICS.
How long have you been active in the ICS subgroup?	Since 2014
What have you been involved in the ICS subgroup?	Just reporting events from Energinet. Nothing else
What are your responsibilities regarding the ICS at your TSO?	Make sure to contact the right people internally regarding ICS reporting. Most data I collect myself
What are you personally most interested in regarding the ICS report?	Only events regarding disturbances in the transmission grid supports my normal work. Even though consequences regarding remedial actions and affects on voltage, frequency, reserves and so on are beyond my normal work. All other parts of ICS is also beyond my normal work, and require support from other departments and collecting other data than I would normally do

Table A5: Energinet's answers to personal detail questions.

Question	Answer
What do you think is the main purpose of ICS?	The purpose is to identify and relate bigger events to see the consequences on a cross-regional view and to suggest improvements. To have an overview of the whole ENTSOE area to see if the system is having more or less critical events. ICS is supposed to be consequence-oriented, but don't think the annual report reflects that.
One focus area is operational security, is that clearly represented?	I think all the categories are supporting the operational security in some way. Each category cannot stand alone to tell the whole story, but they all contribute with some information. The challenge is to pinpoint which data in each category that are market-driven, operational-driven, fault-driven and system-driven. Random mixing of the different views makes it difficult to extract the wanted conclusions and data. I think that part is important to highlight: regarding one piece of data, shall it have focus from market, operation, fault, system or other. Will be problematic to use results if someone like me reports with market-view if it should be with system-view. Both are relevant, but with different outcome
What do you think is the most important part in the ICS methodology?	The important part is not a single category, but the possibility to register the consequence of a large event which affects multiple TSO's and thus get the big picture of an event. Even though I don't think the methodology supports it well, because each TSO only report their own events, and not events that affects them from other TSO's.
Does the ICS methodology provide sufficient tools and definitions to accurately produce a report that fulfils its goals?	I think activation of system protection schemes and emergency power controls etc. should be monitored as well to provide information regarding events. The ICS does have plenty of definitions and categories. However, the definitions need to be more specific. For example, it would be easier to see whether some remedial actions, such as SPS and emergency power controls, actually support the frequency restoration. ICS is not sufficient regarding voltage-levels. In Denmark 132 kV and 150 kV is also part of transmission grid (and several HVDC links is on that voltage level), and have effect on the system

Table A6: Energinet's answers to questions about the current state of the incident classification scale methodology.

Question	Answer
How does your reporting procedure of ICS data look like?	Every quarter I report T and LT. once a year I report the other categories because they involve more internal resources to collect
How much time does the ICS reporting take? (in hours)	Difficult to answer. Typing in the report-sheet requires often 4 work days each year, but most of the data I collect regarding normal work, and how much time my colleagues use to collect data is unknown.
How many persons does the reporting involve in your company?	Primarily just me. But get some support with some categories from 5 departments
Are there any difficulties in the reporting process?	Many. I only fill in the most necessary information to reduce collecting more data. Difficult to exactly understand what to report. No real feedback regarding the reported data, and only few people are interested in it even though it is mandatory to report. Some of the categories are not reported because the data is not available.
Does the report analyse the reported data well and present the information well to the reader?	No. There are plenty of data not reported, and no way of monitoring whether the information is true. The credibility of the data suffers when some companies do not report N-1 violations even though they have many. The report is, in its current state not used for anything internally in Energinet.
Does the report convey improvement suggestions for increasing the operational security well?	No. the relevant events are improved in other ways. Incidents in the own grid are investigated internally without ICS.
Does your company get any benefits from the work done for the ICS?	No. only very few people in Energinet knows what ICS is, and the report is not used internally.

Table A7: Energinet's answers to questions about the current state of reporting the incident classification scale data.

Question	Answer
Have you read reports by ENTSO-E or other companies that tangent the content of the ICS report?	Mostly internal reports that cover some aspects from ICS. DISTAC HVAC and HVDC reports most of the relevant items regarding T incidents [from the ICS].
Do you think the ENTSO-E Awareness System is compatible with the ICS?	It should be and there would need to be more cooperation between the ICS and the EAS team. ICS should mostly be an offline report of EAS with possibility of more details to clarify the events
Do you think that ICS should be incorporated to the ENTSO-E Transparency Platform?	I haven't used the ETP so can't say.
Do you know of other reports that supplement the value of the ICS report?	DISTAC HVAC and HVDC report. Know the RGN also monitor frequency from a subgroup
Do you think that the ICS scale could be a floating-point number?	If it helps showing that many small events can be closer to result in a higher consequence, I will support the idea. But don't know if I understand the concept of floating-point number

Table A8: Energinet's answers to other questions.

A.3 Fingrid Oyj

This section presents the answers to the interview questions by Fingrid Oyj from Finland. The questions are grouped into 4 parts: personal details, questions about the current state of the ICS methodology, the current state of the ICS reporting and other questions and presented in Tables A9–A12

Question	Answer
What is your name?	Markku Piironen
Which TSO do you represent and in which department do you work? What is your professional background?	Fingrid Oyj Operation development M.Sc Electrical engineering
What is your role in the ICS subgroup?	Member
How long have you been active in the ICS subgroup?	8 years
What have you been involved in the ICS subgroup?	Developing the methodology and the annual report.
What are your responsibilities regarding the ICS at your TSO?	Reporting person from Fingrid
What are you personally most interested in regarding the ICS report?	Incidents on load and transmission system elements and incidents that affect the reserve capacity.

Table A9: Fingrid's answers to personal detail questions.

Question	Answer
What do you think is the main purpose of ICS?	To improve the operational security and energy markets, and to gather statistics about the events that affect them.
One focus area is operational security, is that clearly represented?	The security indicators are explicitly about the operational security.
What do you think is the most important part in the ICS methodology?	The definitions, that describe the criteria, and the reporting rules and procedures. There could be an internal document with more detailed definitions.
Does the ICS methodology provide sufficient tools and definitions to accurately produce a report that fulfils its goals?	The definitions should be more detailed. Frequency and voltage violations, for example, seem to be clear when you read them first, but as you report the data you notice that the measurements are not always constantly above the thresholds. So should the reporting consider 3min moving averages or something else?

Table A10: Fingrid's answers to questions about the current state of the incident classification scale methodology.

Question	Answer
How does your reporting procedure of ICS data look like?	Most of the data is quite straight forward, but some of it needs to be gathered manually. However, the thresholds are quite high and the number of events needed to gather manually therefore low. The grid is monitored internally more detailed. For example, number of minutes the frequency has crossed a certain thresholds in a week/month/year is tracked. RRC reporting is very manual, as the control room reports their findings and we collect them. The events are very rare because the threshold is 20% of the whole reserve capacity. If an incident affects a neighbouring TSO, Fingrid does not need to ask for any extra details from them because Fingrid has a system that contains the needed information.
How much time does the ICS reporting take? (in hours)	Fingrid data takes monthly with Excel 3–6 hours. Disturbances are reported very fast. The easily retrieved data is reported every month, but the more difficult data is reported every quarter to avoid disturbing other people too much.
How many persons does the reporting involve in your company?	I've been reporting alone, but recently I got a colleague that reports with me because ICS has become a legally binding.
Are there any difficulties in the reporting process?	Yes. How to get the data if it is not directly in the system? Who should note the events and who should report? There is always a risk of information loss and misinterpretation when information needs to flow between multiple people.
Does the report analyse the reported data well and present the information well to the reader?	The authorities have now demanded more information, so I suppose not. The report could be more detailed, but then again multiple instances review the report (ICS, St.G Operations, SOC, ACER), which makes the approval very long and bureaucratic. Furthermore, the methodology has been updated many times since it was created, resulting in new data not being comparable at all with the previous data. It would be good if we had the same methodology for some years now.
Does the report convey improvement suggestions for increasing the operational security well?	I don't think so. If there are scale 2 or 3 incidents, there should be. Now we had some of those incidents, but they happened in isolated systems and won't therefore help the Nordic and Central European synchronous area.
Does your company get any benefits from the work done for the ICS?	The internal responsible parties for reporting the ICS data has become clearer. TSOs could also incorporate the ICS's security indicators into their own security indicators.

Table A11: Fingrid's answers to questions about the current state of reporting the incident classification scale data.

Question	Answer
Have you read reports by ENTSO-E or other companies that tangent the content of the ICS report?	Some ENTSO-E annual reports contain a bit of the same content. Energinet and SvK, maybe Germany, have had some operational security reports. ENTSO-E winter reports could also tangent the content.
Do you think the ENTSO-E Awareness System is compatible with the ICS?	It has been recently stated, that it is not and that it does not fully have to be because the control centre's operating personnel assess the system state as they believe it to be in real-time. The consensus has been, that ICS and EAS are individual groups and may incorporate each other's definitions if they want to.
Do you think that ICS should be incorporated to the ENTSO-E Transparency Platform?	The transparency platform (TP) contains market relevant data. I wouldn't merge ICS with the TP.
Do you know of other reports that supplement the value of the ICS report?	Reports made by other TSOs are interesting. Energinet has made an interesting report about energy adequacy.
Do you think that the ICS scale could be a floating-point number?	I would rather have the scale fixed and then have a sufficient number of levels.

Table A12: Fingrid's answers to other questions.

A.4 Independent Power Transmission Operator S.A., IPTO

This section presents the answers to the interview questions by Independent Power Transmission Operator S.A. (IPTO) from Greece. The questions are grouped into 4 parts: personal details, questions about the current state of the ICS methodology, the current state of the ICS reporting and other questions and presented in Tables A13–A16

Question	Answer
What is your name?	Lefteris Grammatikopoulos
Which TSO do you represent and in which department do you work? What is your professional background?	IPTO System Operation and Control Dept. Electrical Engineer
What is your role in the ICS subgroup?	Reporting Person (SPOC) Member of ICS Subgroup
How long have you been active in the ICS subgroup?	From 2014
What have you been involved in the ICS subgroup?	Yes, on both. ICS is teamwork. After discussions and controls, the changes are approved jointly.
What are your responsibilities regarding the ICS at your TSO?	Collect data, make reports, upload files on SharePoint. Participate on ICS SG meetings.
What are you personally most interested in regarding the ICS report?	As a dispatcher, incidents are part of my work. Gives me also the possibility to work with persons from other TSOs and to exchange experience and understand better ENTSO-E SO GL.

Table A13: IPTO's answers to personal detail questions.

Question	Answer
What do you think is the main purpose of ICS?	It's a statistical tool that aims to provide an overview of Operational Security Indicators.
One focus area is operational security, is that clearly represented?	All indicators relative to F, V, G are strictly related to Op.Security. But also "loss of tools and facilities" or "reduction of RC" and others are very important, because in certain circumstances may have an important effect on Op. Security.
What do you think is the most important part in the ICS methodology?	Personally, I think that incidents with consequences in other countries and the Remedial Actions applied are the most important aspects.
Does the ICS methodology provide sufficient tools and definitions to accurately produce a report that fulfilsits goals?	ICS methodology is in continuous upgrading. The last one is in use from 2018 and I hope that it will fulfil its goals.

Table A14: IPTO's answers to questions about the current state of the incident classification scale methodology.

Question	Answer
How does your reporting procedure of ICS data look like?	
How much time does the ICS reporting take? (in hours)	1 or 2 days/month
How many persons does the reporting involve in your company?	2 persons from System Operation and Control Dept.
Are there any difficulties in the reporting process?	No, until now.
Does the report analyse the reported data well and present the information well to the reader?	When the incidents have minor consequences there is no need for further information. For large incidents (greater severity) there are other forms of reporting as defined by ENTSO-E's Network Codes.
Does the report convey improvement suggestions for increasing the operational security well?	I hope so.
Does your company get any benefits from the work done for the ICS?	It helps us to observe better the requirements of ENTSO-E and to comply with them. The Op.Security didn't change but it helped us to adopt common rules with the other TSOs.

Table A15: IPTO's answers to questions about the current state of reporting the incident classification scale data.

Question	Answer
Have you read reports by ENTSO-E or other companies that tangent the content of the ICS report?	No, but I think all reports should be compliant with SO GL.
Do you think the ENTSO-E Awareness System is compatible with the ICS?	Yes. The issue when we changed the ICS methodology was to be compatible with EAS.
Do you think that ICS should be incorporated to the ENTSO-E Transparency Platform?	I don't know. I think TP is important to provide information to market participants. ICS is different.
Do you know of other reports that supplement the value of the ICS report?	No
Do you think that the ICS scale could be a floating-point number?	I think that current ICS methodology is OK. Smaller events mean smaller impact to an LFC area and probably no influence to neighbouring countries. So they aren't so important. More important are those that could lead to cascading effects with major consequences (and affect also other countries). Currently we report these cases.

Table A16: IPTO's answers to other questions.

A.5 Réseau de transport d'électricité, RTE

This section presents the answers to the interview questions by Réseau de transport d'électricité (RTE) from France. The questions are grouped into 4 parts: personal details, questions about the current state of the ICS methodology, the current state of the ICS reporting and other questions and presented in Tables A17–A20

Question	Answer
What is your name?	Caroline Pelin
Which TSO do you represent and in which department do you work? What is your professional background?	RTE (France) National System operation dispatcher in a regional control center
What is your role in the ICS subgroup?	Representing RTE
How long have you been active in the ICS subgroup?	1 month (2 meetings)
What have you been involved in the ICS subgroup?	Annual ICS report 2018 report + implementing the ACER proposals for the methodology 2019.
What are your responsibilities regarding the ICS at your TSO?	In charge of controlling and organizing reporting procedures at RTE, involving the 8 French dispatching. ICS representant in ICS subgroup.
What are you personally most interested in regarding the ICS report?	Analysing the consequences of European incidents to understand the effects on our national grid

Table A17: Réseau de transport d'électricité's (RTE) answers to personal detail questions.

Question	Answer
What do you think is the main purpose of ICS?	Providing recommendations for the TSO regarding the events of the year (what to improve, where the weak point of the system are)
One focus area is operational security, is that clearly represented?	
What do you think is the most important part in the ICS methodology?	
Does the ICS methodology provide sufficient tools and definitions to accurately produce a report that fulfils its goals?	If every TSO would report correctly the data, the methodology would be a great help. Unfortunately, many TSOs do not report all the events.

Table A18: Réseau de transport d'électricité's (RTE) answers to questions about the current state of the incident classification scale methodology.

Question	Answer
How does your reporting procedure of ICS data look like?	Reporting from 8 interlocutors in a single form check by me.
How much time does the ICS reporting take? (in hours)	Last year about 50h but we have reported only the event on the 400kV grid, this year we will report also for the 225kV so it will probably increase.
How many persons does the reporting involve in your company?	About 10 people from regional and national dispatching.
Are there any difficulties in the reporting process?	People do not necessarily understand the necessity of an European report of incidents because we already have a lot of internal reporting to analyse our own incident. My job is to explain them the goal.
Does the report analyse the reported data well and present the information well to the reader?	I think so
Does the report convey improvement suggestions for increasing the operational security well?	I only read the 2017 report and I don't think there is any big suggestions in it
Does your company get any benefits from the work done for the ICS?	

Table A19: Réseau de transport d'électricité's (RTE) answers to questions about the current state of reporting the incident classification scale data.

Question	Answer
Have you read reports by ENTSO-E or other companies that tangent the content of the ICS report?	No but I don't have time to read all ENTSO-E reports.
Do you think the ENTSO-E Awareness System is compatible with the ICS?	The two are compatible (same scale) so it could be interesting to have a stronger cooperation
Do you think that ICS should be incorporated to the ENTSO-E Transparency Platform?	I don't think so because we don't have a homogeneous reporting's quality so it could misrepresent the reality of the TSOs.
Do you know of other reports that supplement the value of the ICS report?	I don't know about it
Do you think that the ICS scale could be a floating-point number?	No opinion

Table A20: Réseau de transport d'électricité's (RTE) answers to other questions.

A.6 Statnett

This section presents the answers to the interview questions by Statnett from Norway. The questions are grouped into 4 parts: personal details, questions about the current state of the ICS methodology, the current state of the ICS reporting and other questions and presented in Tables A21–A24

Question	Answer
What is your name?	Jørn Schaug-Pettersen
Which TSO do you represent and in which department do you work? What is your professional background?	Statnett Fault analysis, about 8 persons big. Electrical engineer and computer science, B.Sc double major.
What is your role in the ICS subgroup?	With the group since the beginning and the only "original member". ICS was 32 people at most. 5-10 ppl do the main work. One task is washing the data.
How long have you been active in the ICS subgroup?	Since the beginning
What have you been involved in the ICS subgroup?	Washed all HVDC last year. This year Landsnet and Statnett.
What are your responsibilities regarding the ICS at your TSO?	Both member of ICS subgroup and the SPOC, that is the ICS single point of contact. Some TSOs divide these tasks between two persons.
What are you personally most interested in regarding the ICS report?	Since I'm working in fault analysis, I'm most interested in the faults and their causes and the consequences. Therefore, I like fault-oriented thinking with a focus area on TSO benchmarking and system impact.

Table A21: Statnett answers to personal detail questions.

Question	Answer
What do you think is the main purpose of ICS?	Have a system where you can scale the system impact. Also, do future analysis of system security. If you can measure the system impact on different incidents, you can abstract the system security. In the end, system security is the secondary task and making the security analysis is a different task. Therefore, the main task of the ICS is to register all incidents and then scale them according to the defined scale, which usually depends on the gravity of the consequence. And the gravity of the consequence depends on the background of the person who is reporting. If someone has worked with fault analysis, that person will focus on TSO benchmarking and system impact, and if someone has worked with operations planning, that person will probably focus on market impact.
One focus area is operational security, is that clearly represented?	I would not say that operational security is the focus area. Operational security is what SOGL is asking for. Operational security is very tricky to assess without a network model. ICS is very good in measuring the system impact, because that is what it is made for. It is not made for TSO benchmarking. We have other reports that do TSO benchmarking, for example, the Nordic and Baltic Grid Disturbance Statistics made by ENTSO-E's DISTAC group.
What do you think is the most important part in the ICS methodology?	I'm going to answer what is the most important part of the ISC methodology to improve. The most important improvement would be to specify the focus area of the ICS, because it includes a bit of everything at the moment. There are about 50 columns to report and none of them are clear. System impact should be more focused, and the ICS should be made compatible with current ENTSO-E HVDC and HVAC reporting because that would increase the quality of data a lot. HVAC reporting has been done for 30 years and is therefore tried and tested to be good. The ICS is consequence oriented, HVAC statistics are fault oriented and the HVDC statistics are outage oriented. The common de-nominator for them all is faults. When everything is compatible, you can just abstract the data and analyse it, with the possibility to extend the analysis even further. The HVDC statistics can be tricky to include into ICS, because they include incidents with outages but without any faults. Planned work, for example maintenance, can make a huge impact on the system. I think that the only way to become compatible with the SOGL is by making ICS fault oriented. Currently, ICS connects the cause directly to the consequence. That makes it incompatible with any existing statistics and very difficult to make statistics with. Analysis of the data, as it is clearly mentioned that it should be included in the SOGL. The scaling of incidents is also a bit too wide. Nobody knows how many scale zeros become a scale 1. Incidents on transmission system elements and N-violations are tricky to aggregate. Incidents on load and generation should be straightforward. At least one PMU measurements should be added to each incident so that the frequency during the incident could be monitored and the system impact assessed.
Does the ICS methodology provide sufficient tools and definitions to accurately produce a report that fulfils its goals?	No. There are no definitions. What is an incident? ICS should use more the IEC vocabulary 60050. However, IEC is missing some definitions. But then again, some of the missing definitions in IEC have been used within Nordel for 30 years. The Nordel definitions are used in the Nordic and Baltic Grid Disturbance reports, which is also expanding into an Europe wide grid disturbance report with over 20 TSOs joining. These definitions should be suggested to IEC. Some of the thresholds for each category and their scale level is set by system impact, and some of them are defined in SOGL. Furthermore, the point of ICS is to report the top 2% of all incidents that give the system and direct impact. I think the impact on the system should be caused by trips and it should be seen in the frequency. ICS provides one tool named the ENTSO-E Disturbance and Incident Classification Tool, or EDICT shortly. EDICT is a web tool made to collect ICS data. However, it was made by some company with specifications that were crafted in just 3 weeks. This resulted in a tool that is unusable, and why most of the ICS data is reported in an Excel sheet. The ICS web tool would primarily revolve around a functioning database with good import and export functions.

Table A22: Statnett's answers to questions about the current state of the incident classification scale methodology.

Question	Answer
How does your reporting procedure of ICS data look like?	Data is delivered 4 times a year in an Excel sheet. Then punch it manually into EDICT. Punching it manually into EDICT unnecessary double work.
How much time does the ICS reporting take? (in hours)	Depends on how accurately you do it. Normally, I extract my ICS data from the HVDC data. Sorting of incidents still has to be done manually and then every column has to be inserted into EDICT, also manually. It takes a long time to input over 50 columns, and you can't even distinct the optional columns from the compulsory. It seems very strange to do double, or even triple, reporting for TSOs with a good data system. In the end, the reporting takes too long, and it is mainly because it is too unclear.
How many persons does the reporting involve in your company?	Fault analysis department and one person. Norway has the most amount of fault reports in their database in the world. 30 000 reports already half way in March.
Are there any difficulties in the reporting process?	Answered previously.
Does the report analyse the reported data well and present the information well to the reader?	The report is more like a summary per synchronous area and doesn't tell so much. Now it is being reported per TSO. This year it's a nice spread of different incidents with some G:s some L:s etc. The presentation of this year includes both an overview of each synchronous area and a per TSO analysis. Furthermore, ACER is pushing hard on the reporting. That is also a reason to go forward with fault-oriented reporting because it gives us better means to analyse the data.
Does the report convey improvement suggestions for increasing the operational security well?	Answered above.
Does your company get any benefits from the work done for the ICS?	No. We haven't had any big incidents. In Norway, we can look at Sweden and Finland at what kind of big faults they report. However, the detail level is too low. We would need fault-oriented reporting to make a better analysis and get better benefits. We could get more benefits by defining how to aggregate incidents. For this, we need to have an accurate scale and PMU measurements, preferably per generation area. These PMU measurements would allow us to see oscillations or instability in the system, which in turn are consequences or system faults. Monitoring cross-border exchange can help analysing when we want to know how much neighbouring TSOs have helped with an incident. PMU measurements of cross-border lines and generation areas would be necessary.

Table A23: Statnett's answers to questions about the current state of reporting the incident classification scale data.

Question	Answer
Have you read reports by ENTSO-E or other companies that tangent the content of the ICS report?	No, but a lot that looks like DISTAC HVDC and HVAC. One American report by NERC existed, but the guy who did it passed away about 15 years ago. It was consequence-oriented and had about 200 incidents a year.
Do you think the ENTSO-E Awareness System is compatible with the ICS?	Most of it is. They should be more compatible. They often ask the ICS group of what they think about, for example, an incident and how it should be scaled.
Do you think that ICS should be incorporated to the ENTSO-E Transparency Platform?	No. The transparency is about showing everything, and therefore has a totally different purpose. ICS is the top 2% of the incidents, i.e. the worst incidents. Transparency platform and DISTAC should be compatible.
Do you know of other reports that supplement the value of the ICS report?	Not as we speak, but there's a lot of things that is written in the SOGL of what ICS is supposed to do. However, it can't be done with the present data, while some people think it should do it. Then info has to be retrieved from other instances. ACER wanted ICS to be everything (while it is the top 2%).
Do you think that the ICS scale could be a floating-point number?	Yes. L and G should be and only one decimal.

Table A24: Statnett's answers to other questions.

B The original figures from the incident classification scale report of 2017

This appendix presents the original figures from the incident classification scale report of 2017 [18]. The improved figures are presented in Section 5.6

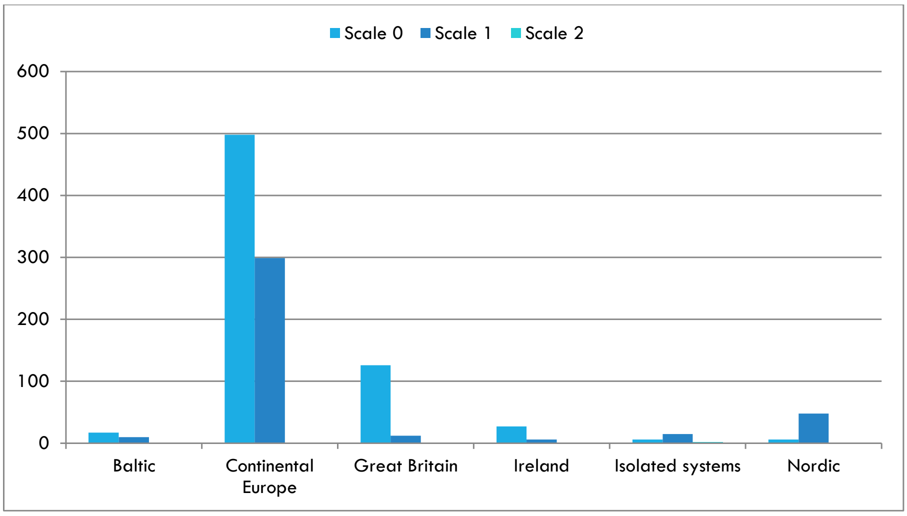

Figure 3. Number of incidents per synchronous area

Figure B1: An improved version of Figure 3 from the ICS annual report of 2017 [18].

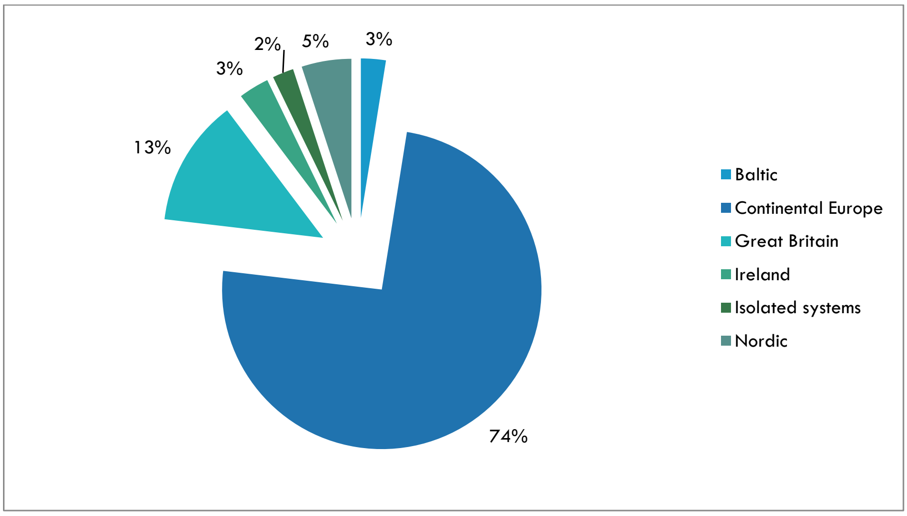

Figure 4. Distribution of incidents per synchronous area

Figure B2: An improved version of Figure 4 from the ICS annual report of 2017 [18].

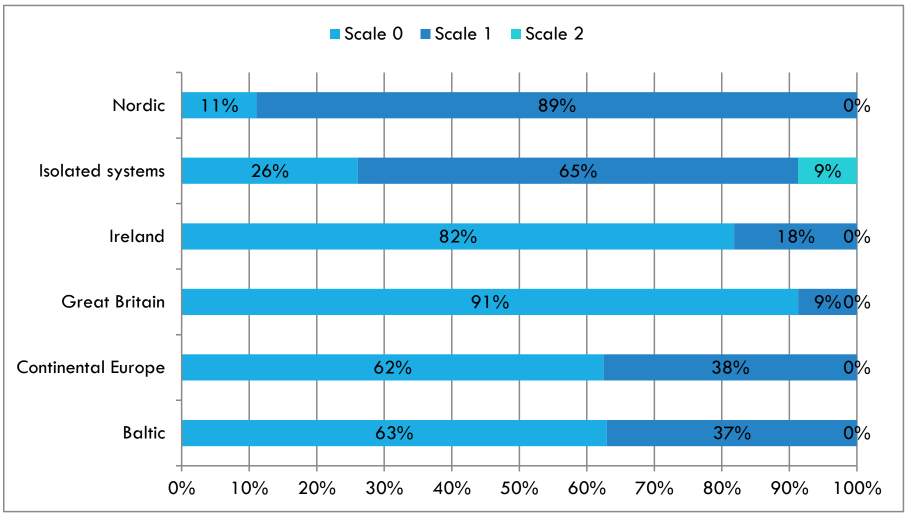

Figure 5. Proportions of scale 0, 1, and 2 incidents per synchronous area

Figure B3: An improved version of Figure 5 from the ICS annual report of 2017 [18].

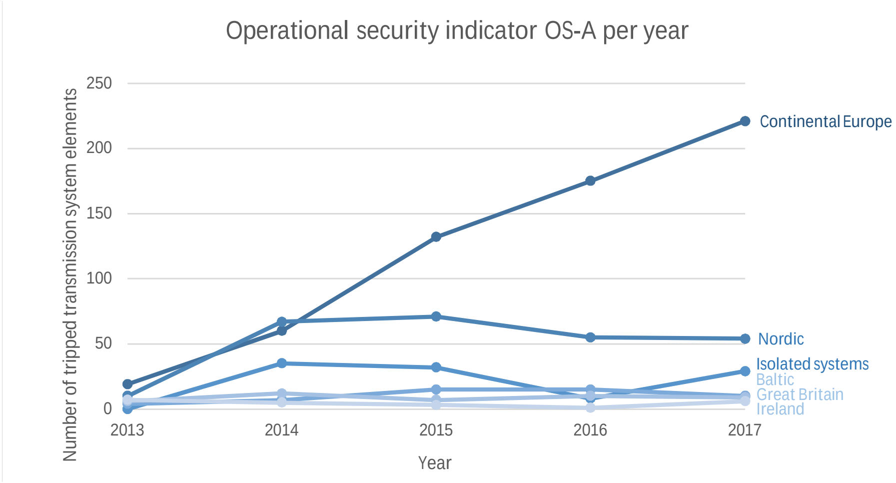

Figure B4: An improved version of Figure 17 from the ICS annual report of 2017 [18].

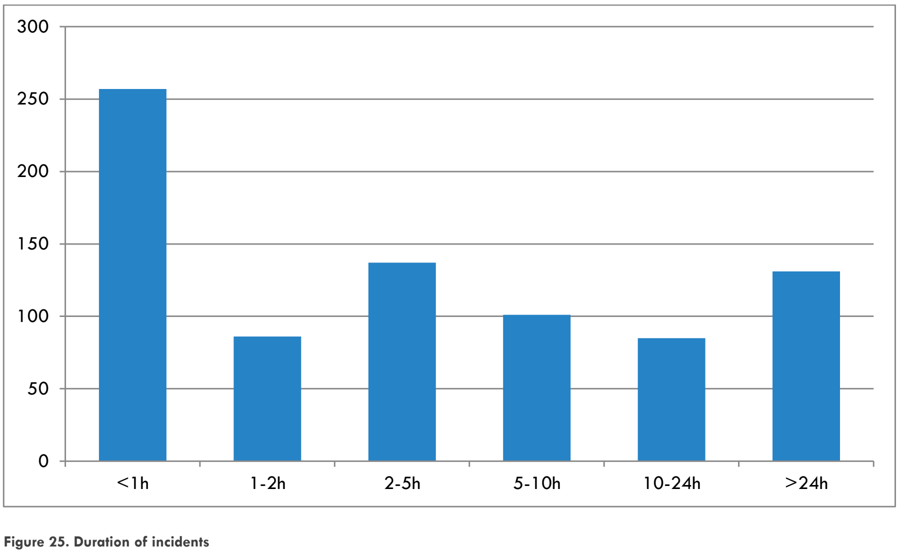

Figure B5: An improved version of Figure 25 from the ICS annual report of 2017 [18].

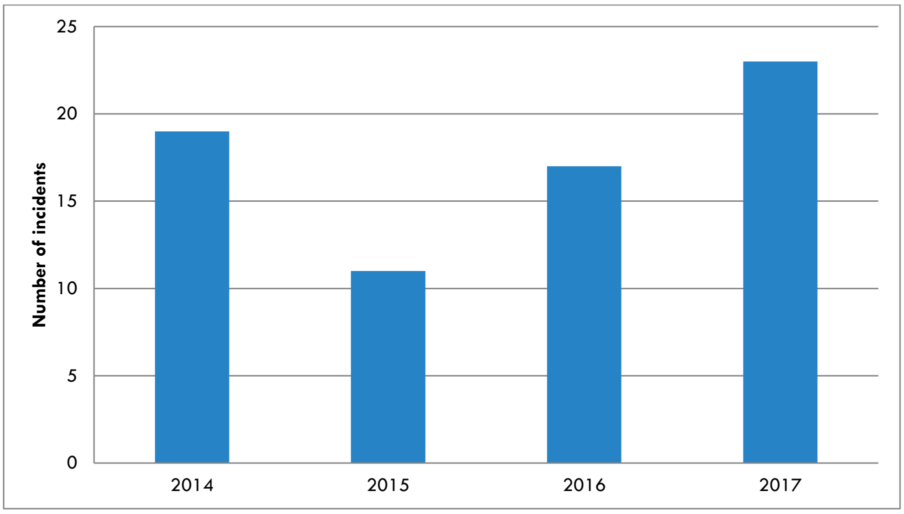

Figure 74. Incidents by scale 2014 – 2017

Figure B6: An improved version of Figure 74 from the ICS annual report of 2017 [18].

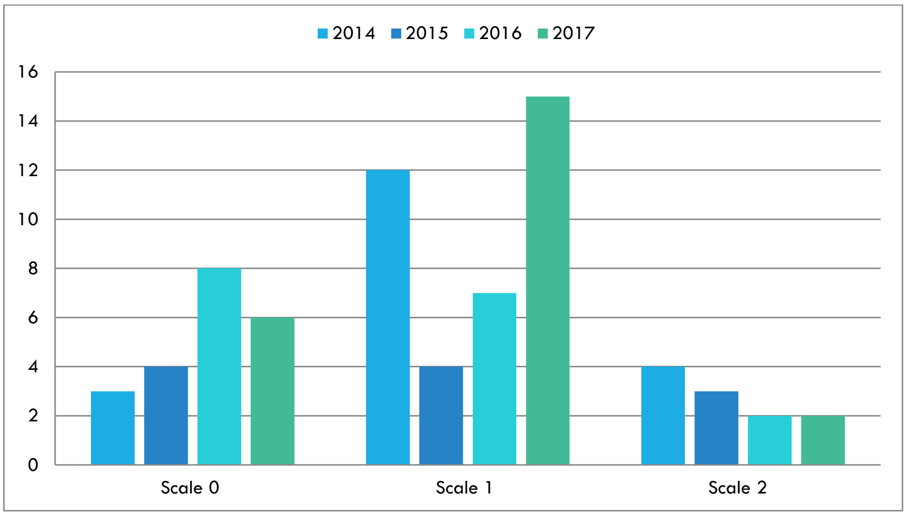

Figure 75. Incidents by scale 2014 - 2017

Figure B7: An improved version of Figure 75 from the ICS annual report of 2017 [18].

C Incident classification cheat sheet

This appendix presents the cheat sheet that can be used in connection with the incident classification scale reporting. The cheat sheet page 1 is presented in Figure C1 and page 2 in Figure C2.

Incident classification scale (ICS)

cheat sheet, page 1/2

DISTAC/CIGRE HVDC ●
EDFS/DISTAC HVAC ●
ICS/EAS HVAC & HVDC ●

Instructions

This cheat sheet is meant to teach how the reporting of one incident works. each cause of a violation or remedial action do the following:

1. Find the cause or remedial action from the “Action/cause” column.
2. File one event for each type of incident criteria that is satisfied
3. into the database corresponding to the value in the “Event” column.

The needed data can also be extracted from the data indicated in the “Data exists in” column.

ICS short codes and explanations	
L	Incidents on load
F	Incidents leading to frequency degradation
T	Incidents on transmission system elements
G	Incidents on generation
ON	N or N-1 violations
RS	Separation from grid
OV	Violation of standards on voltage
RRC	Reduction of reserve capacity
LT	Loss of tools and facilities

(2. Report each of these separately) Type of incident	(3. Into this database) Event	(1. Start here) Action/cause	Data exists in: DISTAC/CIGRE HVDC	Data exists in: EDFS/DISTAC HVAC	Data exists in: ICS/EAS HVAC & HVDC
T, G, L	Techn. and oper. faults	Environmental causes	●	●	●
		External influences	●	●	●
		Operation and maintenance	●	●	●
		Technical equipment	●	●	●
		Other	●	●	●
		Unknown	●	●	●
T, G, L, F, RS, OV, ON	System faults	High/low voltage		●	●
		High transmission on line		●	●
		High/low frequency		●	●
		High/low harmonic		●	●
		Voltage dip/swell	●	●	●
		Power oscillations		●	●
		Separation from grid			●
LT, ON, RRC	Latent faults	Loss of tools			●
		N-violation			●
		Reduction of reserve capacity	●		●
T, G, L, RS	Remedial Actions	Manual	●		●
		Automatic (SPS)			●
		Automatic (SCS)	●		●
L, G	No faults	Limitation	●		●
		Maintenance	●		
		Other outage	●		
		Separation from grid			●
		High/low generation/load			●

ICS category	Primary value	Secondary value
L	Change in load, MW	Energy not supplied, MWh
F	Change in frequency, mHz	PMU-measurement data
T	Type of transmission system element	TSO Operational security limits violated (Y/N)
G	Change in generation, MW	
ON	Number of contingencies that can lead to deviations from operational security limits	Number of vulnerable neighbouring TSOs
RS	Load of isolated system, MW	PMU-measurement data
OV	Number of substations affected	Number of TSOs affected
RRC	Change in reserve capacity, MW “FCR/aFRR/mFRR/RR”	Change in reserve capacity, % “FCR/aFRR/mFRR/RR”
LT	Number of lost tools, number/”all”	
RA	Depends on remedial action type	PMU-measurement data

When to report end time for event	
ICS category	End time
L	when RA is applied
F	when frequency is back within limits
T	when cleared
G	when RA is applied
ON	when cleared
RS	when island has been reconnected
OV	when cleared
RRC	when cleared
LT	when cleared

Figure C1: The ICS cheat sheet that can be used in connection with the incident classification scale reporting, page 1.

Incident classification scale (ICS)

cheat sheet, page 2/2

Definitions used

Referenced and/or adjusted from the IEC 60050 and ENTSO-E/DISTAC definitions

Event type	Description	Reference	Example
Fault	inability to perform as required, due to an internal state	IEC 60050	
Technical fault	The inability of an item to perform as required, due to a technical error.	Derivation of fault from IEC and DISTAC	Short-circuit, breaker failure
Operational fault	The inability of an item to perform as required, due to a temporary human error.	Derivation of fault from IEC	Incorrect or forgotten operation of equipment
System fault	The inability of an item to perform its intended function due to off nominal parameters and/or exceeding of regulated norms and standards.	Derivation of fault from IEC	High/low frequency, high/low voltage, high/low harmonics, power oscillations.
Latent fault	A fault that has not become apparent.	IEC 60050	N violation, loss of tools or facilities.
Remedial action	An action that is intended to restore a system partly or fully back to a stable state.	This thesis	Load shedding, added generation, net split.
No fault	Outage or limitation without a fault.	This thesis	Sudden limitation on a HVDC link due to temperatures, separation of grid.

Example technical or operational fault event

ReporterID	Synchronous area	Voltage level	Start time	End time	Type of incident	Action or Cause	Detail	Detail2	Primary value	Secondary value
1	Nordic	230 kV	5.3.2019 09:00	5.3.2019 18:30	T	External influence	Tree felling		Overhead line	No

Example system fault event

ReporterID	Synchronous area	Voltage level	Start time	End time	Type of incident	Action or Cause	Detail	Detail2	Primary value	Secondary value
1	Nordic	400 kV	4.3.2019 09:00	4.3.2019 09:00.15	L	Voltage dip			-400 MW	0

Example remedial action

ReporterID	Synchronous area	Voltage level	Start time	End time	Type of incident	Action or Cause	Detail	Detail2	Primary value	Secondary value
1	Nordic	230 kV	4.3.2019 09:00.15		G	Automatic (SCS)	Added generation		400	0

Figure C2: The ICS cheat sheet that can be used in connection with the incident classification scale reporting, page 2. The short codes are the same as used in the ICS methodology of 2018 [8] while the definitions are either cited from IEC 60050 [9] or derived from them in order to achieve maximum compatibility.

D Improved incident classification scale tables

This appendix presents the improved versions of the incident classification scale tables. Figure D1 presents a table that shows the overview of all incident categories and how they are scaled and Figure D2 show the table med specifically for the Nordic synchronous area.

Incident classification scale – overview

Categories	Scale 0 **Normal**	Scale 1 **Alert**	Scale 2 **Emergency**	Scale 3 **Blackout**
Incident on load L		1–10 % loss of load in TSO control area	10–50 % loss of loan in TSO control area	>50 % loss of load in TSO control area
Frequency degredation F * reported by responsible TSO	See frequency deviations from methodology	See frequency deviations from methodology	See frequency deviations from methodology	
Incident on a transmission system element T	Disconnection of a tie-line, a HVDC-system or the highest voltale element(s) in the contingency list, and			
	without additional ICS scale 0 or above consequences	a N-1 violation occurs	at least one TSO's operational security limits are violated or because of a wide area consequence on a regional or synchronous area level results in having to activate at least 1 measure of the system defence plan	
Incident on generation G	See generation loss limits from methodology	See generation loss limits from methodology	See generation loss limits from methodology	
N or N-1 violation ON		At least one contin-gency from the contin-gency list can lead to deviations from opera-tional security limits with consequences on neighbouring TSOs, even after the activation of remedial action(s)	There is at least one wide area deviation from operational security limits after the activation of remedial action(s) in N situation.	
Separation from grid RS	Involves only one TSO and at least one of the asynchronous systems has a load of		Involves more than one TSO and at least one of the asynchronous systems has a load larger than 1500 MW	
	See load limits from methodology	See load limits from methodology		
Violation of voltage standards OV	More than 30 minutes in one substation, see limits from methodology	More than 30 minutes in one TSO control area and more than one substation	More than 30 minutes in involving more than one TSO	No voltage for 3 minutes in TSO control area
Reduction of reserve capacity RRC	More than 20 % reduction for 15–30 minutes	More than 20 % reduction for more than 30 minutes	Reserve capacity un-available for more than 30 minutes	
Loss of tools and facilities LT	Loss of any tool for more than 30 minutes and without conse-quences to neigh-bouring TSOs	Loss of any tool for more than 30 minutes and with consequences to neighbouring TSOs and/or? Unplanned evacuation to the back up control room	Loss of all tools for more than 30 minutes	

Figure D1: Improved version of the incident classification table.

Incident classification scale – Nordic synchronous area

Categories	Scale 0 **Normal**	Scale 1 **Alert**	Scale 2 **Emergency**	Scale 3 **Blackout**
Incident on load L		1–10 % loss of load in TSO control area	10–50 % loss of load in TSO control area	>50 % loss of load in TSO control area
Frequency degredation F * reported by Svenska Kraftnät	100–250 mHZ deviation during 3–15 min or 250–500 mHZ deviation during 0–5 min	100–250 mHZ deviation over 15 min or 250–500 mHZ deviation over 5 min	>500 mHZ deviation	
Incident on a transmission system element T	Disconnection of a tie-line, a HVDC-system or the highest voltale element(s) in the contingency list, and			
	without additional ICS scale 0 or above consequences	a N-1 violation occurs	at least one TSO's operational security limits are violated or because of a wide area consequence on a regional or synchronous area level results in having to activate at least 1 measure of the system defence plan	
Incident on generation G	Loss of 600–1500 MW of generation	Loss of 1500–3000 MW of generation	Loss of >3000 MW of generation	
N or N-1 violation ON		At least one contin-gency from the contin-gency list can lead to deviations from opera-tional security limits with consequences on neighbouring TSOs, even after the activation of remedial action(s)	There is at least one wide area deviation from operational security limits after the activation of remedial action(s) in N situation.	
Separation from grid RS	Involves only one TSO and at least one of the asynchronous systems has a load of		Involves more than one TSO and at least one of the asynchronous systems has a load of	
	200–1500 MW	larger than 1500 MW	larger than 1500 MW	
Violation of voltage standards OV	Voltage outside range 0.90–1.05 pu for more than 30 minutes in one substation	Voltage outside range 0.90–1.05 pu for more than 30 minutes in 1+ substations in one TSO	Voltage outside range 0.90–1.05 pu for more than 30 minutes in more than one TSO for neighbouring substation	No voltage for 3 minutes in TSO control area
Reduction of reserve capacity RRC	More than 20 % reduction for 15–30 minutes	More than 20 % reduction for more than 30 minutes	Reserve capacity un-available for more than 30 minutes	
Loss of tools and and facilities LT	Loss of any tool for more than 30 minutes and without conse-quences to neigh-bouring TSOs	Loss of any tool for more than 30 minutes and with consequences to neighbouring TSOs and/or? Unplanned evacuation to the back up control room	Loss of all tools for more than 30 minutes	

Figure D2: Improved version of the incident classification table for the Nordic synchronous area.