European Network of
Transmission System Operators
for Electricity

entsoe

INCIDENT CLASSIFICATION SCALE METHODOLOGY

15 December 2025

From: Working Group Incident Classification Scale

ENTSO-E Mission Statement

ENTSO-E, the European Network of Transmission System Operators for Electricity, **is the association of the European transmission system operators** (TSOs). The **40 member TSOs, representing 36 countries**, are responsible for the secure and coordinated operation of Europe's electricity system, the **largest interconnected electrical grid in the world**.

Before ENTSO-E was established in 2009, there was a long history of cooperation among European transmission operators, dating back to the creation of the electrical synchronous areas and interconnections which were established in the 1950s.

In its present form, ENTSO-E was founded to fulfil the common mission of the European TSO community: to power our society. At its core, European consumers rely upon a secure and efficient electricity system. Our electricity transmission grid, and its secure operation, is the backbone of the power system, thereby supporting the vitality of our society. ENTSO-E was created **to ensure the efficiency and security of the pan-European interconnected power system** across all time frames within the internal energy market and its extension to the interconnected countries.

ENTSO-E is working to secure a carbon-neutral future. The transition is a shared political objective throughout the continent and necessitates a much more electrified economy where sustainable, efficient and secure electricity becomes even more important. **Our Vision: "a power system for a carbon-neutral Europe"*** shows that this is within our reach, but additional work is necessary to make it a reality.

In its Strategic Roadmap presented in 2024, ENTSO-E has organised its activities around two interlinked pillars, reflecting this dual role:

- "Prepare for the future" to organise a power system for a carbon-neutral Europe; and
- "Manage the present" to ensure a secure and efficient power system for Europe.

ENTSO-E is ready to meet the ambitions of Net Zero, the challenges of today and those of the future for the benefit of consumers, by working together with all stakeholders and policymakers.

* https://vision.entsoe.eu/

Table of Contents

Glossary

AC	Alternating Current
ACER	European Union Agency for the Cooperation of Energy Regulators
ALFC	Annual Load-Frequency Control
CE	Continental Europe
EAS	ENTSO-E Awareness System
ENTSO-E	European Network of Transmission System Operators for Electricity
FCR	Frequency containment reserves
FRR	Frequency restoration reserves
HVAC	High voltage alternating current
HVDC	High voltage direct current
ICS	Incident Classification Scale
ICSM	Incident Classification Scale Methodology
ICS criterion	The threshold(s) that define the scale and type of an incident
ICS incident	A situation where one or multiple ICS criteria have been violated
IE/NI	Ireland / Northern Ireland
kV	Kilovolt
mHz	Millihertz
MW	Megawatt
NRA	National Regulatory Authority
OS	Operational security indicators relevant to operational security
OPS	Operational security indicators relevant to operational planning
pu	Per unit
RIAR	Regional Incident and Analysis Reporting
RCC	Regional Coordination Centre
RfG	Regulation (EU) 2016/631
RR	Replacement reserves
SOGL	Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation
SOC	System Operations Committee
SPOC	Single Point of Contact
TSO	Transmission System Operator
WG ICS	Working Group Incident Classification Scale

ICS Criteria

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

1 Introduction

The Incident Classification Scale (ICS) Methodology (hereinafter the 'Methodology') has originally been developed in accordance with Article 8(3) of Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009, which has since been replaced by Article 30 of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast), to fulfil the objectives and the security indicator requirements laid out in Article 15 of Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation (SOGL). The definitions and concepts in this Methodology are in line with the SOGL, Articles 15 and 18 in particular, and are extended further to describe the real-time situation of the TSOs' systems. For example, this Methodology defines duration thresholds for voltage violations as they have not been set in the SOGL. This allows categorisation of voltage violations based on severity.

Article 30(1)(i) of Regulation (EU) 2019/943 sets the obligation for ENTSO-E to adopt common network operation tools to ensure coordination of network operation in normal and emergency conditions, including a common incident classification scale. Article 15(2) of the SOGL sets the obligation on transmission system operators (TSOs) of each European Union Member State to provide ENTSO-E with the necessary data and information for the preparation of an annual report based on the Incident Classification Scale and the operational security indicators, and on ENTSO-E to publish the annual report.

The Incident Classification Scale annual report aims to:

- provide an overview of the operational security indicators specified in Article 15(3) of SOGL;
- identify any improvements, which are necessary in order to support sustainable and long-term operational security;
- identify any improvements to network operation tools required to maintain operational security and related to real-time operation and operational planning to support TSOs in their task provided in Article 55(e) of the SOGL; and
- provide explanations of the reasons for incidents at the operational security ranking scales 2 and 3 as per the ICS adopted by ENTSO for Electricity; those explanations shall be based on an investigation of the incidents by TSOs, the process of which shall be set out in this Methodology.

The Methodology also lays out the procedure for the investigation incidents on scale 2 and 3, covering initiation, establishment, objectives and deliverables of the ICS Expert Panel for the investigation to prevent future incidents and the improvement of the resilience of the European electricity system.

Last, it should be noted that an ICS incident includes all individual ICS criteria violations during the incident. An ICS incident is classified according to the criterion that has the highest priority.

2 Definitions

1) For the purpose of this Methodology, the definitions provided for in Article 2 of Regulation (EU) 2019/943, Article 2 of Regulation (EU) 2017/1485 (SOGL), Article 2 of Regulation (EU) 2016/631, Article 2 of Commission Regulation (EU) 2016/1388 and Article 2 of Regulation (EU) 2016/1447, shall apply.

2) In addition, the following definitions shall apply:

   a) 'Initiating event' means the first event that results in one or more violations of ICS criteria.

   b) 'Isolated system' means an electricity system that is not synchronously connected to another synchronous area.

   c) 'Working Group Incident Classification Scale' or 'WG ICS' means the group formed by ENTSO-E for the purposes of this Methodology, and responsible to perform the tasks specified for the group as described in Chapters 7 and 8.

3 The Incident Classification Scale

The Incident Classification Scale (ICS) consists of five (5) scales (below scale, scale 0, 1, 2 and 3) ranging from minor incidents to major incidents. The scales are defined within the meaning of the system states in Article 18 of the SOGL. The scales and criteria are described in detail in Chapter 5. In general, the scales and corresponding system states are:

- Below Scale[1] for minor incidents; the system remains in normal state;
- Scale 0 for noteworthy minor incidents, the system remains in normal state;
- Scale 1 for significant incidents; contingency from the contingency list has been detected; the system is in alert state;
- Scale 2 for extensive incidents; violation of operational security limit, probability of simultaneous impact on multiple TSOs; the system is in emergency state;
- Scale 3 for major incident in the control area of one or multiple TSOs; the system is in blackout state.

Each scale has a set of ICS criteria that define operational thresholds on, for example, frequency and voltage, that must be met or the ICS criteria is violated and the system state changed accordingly. Furthermore, each ICS criterion has a priority as shown in Table 1 with a number from 1 to 31, where 1 denotes the highest priority and 31 the lowest priority. When an ICS incident meets several criteria, the incident is classified according to the criterion that has the highest priority. All criteria violations shall be reported by TSOs to allow for the factual evaluation of the ICS incident.

Table 1 Incident Classification Scale

Below scale Minor incident		**Scale 0** Noteworthy minor incident		**Scale 1** Significant incident		**Scale 2** Extensive incident		**Scale 3** Major incident	
Priority	*Criterion name (short code)*	*Priority*	*Criterion name (short code)*	*Priority*	*Criterion name (short code)*	*Priority*	*Criterion name (short code)*	*Priority*	*Criterion name (short code)*
		#20	Incidents on load (L0)	#11	Incidents on load (L1)	#2	Incidents on load (L2)	#1	Blackout (OB3)
#28	Incidents leading to frequency degradation (FBS)	#21	Incidents leading to frequency degradation (F0)	#12	Incidents leading to frequency degradation (F1)	#3	Incidents leading to frequency degradation (F2)		
		#22	Incidents on network elements (T0)	#13	Incidents on network elements (T1)	#4	Incidents on network elements (T2)		
#29	Incidents on power generating facilities (GBS)	#23	Incidents on power generating facilities (G0)	#14	Incidents on power generating facilities (G1)	#5	Incidents on power generating facilities (G2)		
				#15	N-1 violations (ON1)	#6	N-1 violations (ON2)		
		#24	Separation from the Grid (RS0)	#16	Separation from the Grid (RS1)	#7	Separation from the Grid (RS2)		
#30	Violation of standards on Voltage (OVBS)	#25	Violation of standards on Voltage (OV0)	#17	Violation of standards on Voltage (OV1)	#8	Violation of standards on Voltage (OV2)		
		#26	Reduction of reserve capacity (RRC0)	#18	Reduction of reserve capacity (RRC1)	#9	Reduction of reserve capacity (RRC2)		
#31	Loss of tools, means and facilities (LTBS)	#27	Loss of tools, means and facilities (LT0)	#19	Loss of tools, means and facilities (LT1)	#10	Loss of tools, means and facilities (LT2)		

[1] Remark: The 'Below Scale' level has been added in this methodology for completeness to record incidents that are needed to calculate the operational security indicators relevant to operational security pursuant to Article 15 of the SOGL. These incidents are considered minor local incidents. The 'Below Scale' classification is used for reporting of violations of standards of voltage, incidents on power generating facilities and incidents leading to frequency degradation. For all other criteria the ICS scales 0, 1, 2 and 3 are sufficient for calculating the operational security indicators.

3.1 Differences in system states between the ICS and the ENTSO-E Awareness System

TSOs continuously report any change in the real-time status of the system state (normal, alert, emergency, blackout or restoration) in the ENTSO-E Awareness System (EAS). The EAS is focused on the real-time system state and security standards to support operational responses or information exchange between TSOs. ICS focuses on post-incident reporting, analysis and classification of system states where additional data and time is available.

As the EAS is used in real-time, the system state is determined using only the information available at the time. Under certain circumstances, this can result in discrepancies between the system state declared in EAS and the factual classification of an incident during the TSOs' reporting.

4 General provisions

1) During the ICS reporting process described in Section 8.1, the following shall apply:
   a) each TSO shall nominate a single point of contact (SPOC) to the Working Group ICS. The SPOC is responsible for:
      - reporting the ICS incidents in accordance with this Methodology;
      - responding to Working Group ICS inquiries regarding their reported incidents; and
      - validating the data of its TSO in the annual reporting process as described in Section 4.1.
   b) the incidents shall be reported in case the effect(s) or initiating event(s) occur in the network with an operating voltage of 220 kV or higher. In addition, incidents in the networks with operating voltage levels below 220 kV when relevant for maintaining operational security shall be reported in accordance with Article 15(3) of the SOGL.
   c) each TSO shall establish its own internal processes to facilitate the ICS reporting;
   d) the common data reported for each ICS incident are listed in Annex I of this Methodology. Additional data may be requested during the investigation of scale 2 and scale 3 incidents, as described in Chapter 7.
   e) each TSO shall report ICS criteria violations as they are experienced in their own control area. In case an initiating event triggers ICS criteria violations in the control area of multiple TSOs, these TSOs shall report them as they were experienced within their own control area. However, in this case, the TSOs must coordinate their reporting to avoid double reporting.
   f) frequency deviations are reported by one or two TSOs per synchronous area, specified in Chapter 5.3 on incidents leading to frequency degradation.
2) Following the synchronisation of the Baltic TSOs with the Continental Europe (CE) Synchronous Area (SA), the ICS criteria for CE SA will apply to them.

5 Definitions of ICS criteria

In this Chapter, the criteria for the classification of each incident are determined (ICS criteria).

5.1 Blackout (OB)

An incident is classified as a blackout (OB) incident when at least one of the following conditions is fulfilled in accordance with Article 18(4) of the SOGL:

- loss of more than 50 % of load (compared to the pre-incident load) in the concerned TSO's control area; or
- total absence of voltage for at least three minutes in the concerned TSO's control area, leading to the triggering of restoration plans.

When any of the conditions above is fulfilled, the TSO's electricity system is in blackout state. Blackout is always a scale 3 (OB3) incident.

Exceptions

For isolated systems, the system is in blackout in case of loss of more than 70 % of load (compared to the pre-incident load) at the time of the incident or total shut down.

5.2 Incidents on load (L)

Disconnection of load (compared to the pre-incident load) with duration of at least 3 minutes is classified as an incident on load (L) in case one of the following conditions are fulfilled:

- disconnection due to tripped transmission system elements;
- activation of system defence plan measures (automatic low frequency and low voltage demand disconnection); or
- manual disconnection of load or activation of controlled load reduction for adequacy.

Exceptions:

The following exceptions apply for the description of the criterion above:

- disconnection of load less than 100 MW and below 5 % of the pre-incident load is not reported; and
- manual disconnections of load that participate in the interruptible load services are not reported.

Table 2 Thresholds by scale for incidents on load. L denotes the measured loss of load.

	CE	Nordic	IRE/NI	Isolated systems
Scale 0 L0	$L \leq 1$ % loss of load in a TSO's control area			1 % < $L \leq 5$ % loss of load in a TSO's control area
Scale 1 L1	1 % < $L \leq 10$ % loss of load in a TSO's control area			5 % < $L \leq 15$ % loss of load in a TSO's control area
Scale 2 L2	10 % < $L \leq 50$ % loss of load in a TSO's control area			15 % < $L \leq 70$ % loss of load in a TSO's control area
Scale 3				

5.3 Incidents leading to frequency degradation (F)

An incident is classified according to this criterion in case the frequency deviation reaches the thresholds defined in Table 3. The thresholds for scale 0 are specified in accordance with Article 18(1)(b) of SOGL, the thresholds for scale 1 in accordance with Article 18(2)(c) of SOGL and the thresholds for scale 2 in accordance with Article 18(3)(b) of SOGL.

For each synchronous area, the frequency deviations are reported by the synchronous area monitor appointed by the applicable synchronous area operational agreement, which is concluded in accordance with Article 133(1) of the SOGL.

For scale 2, the 'time to recover frequency' in SOGL is used for IE/NI. The 'time to recover frequency' is not specified in SOGL for Nordic and Continental Europe (CE). Therefore, the values from Section 4.2.3 of the Nordic System Operation Agreement – Annex Load-Frequency Control & Reserves[2] are used for the Nordic scale 2 thresholds. For CE, the Frequency Containment Reserve (FCR) full activation time in Annex V of the SOGL is used for the scale 2 duration threshold.

In case a frequency violation exceeds the frequency and time thresholds of multiple scales ('below scale', 0, 1 or 2), the criteria violation is classified as the highest violated scale.

Table 3 Thresholds by scale for incidents leading to frequency degradation. Δf denotes the measured frequency deviation in millihertz, and t the measured duration.

	CE	Nordic	IRE/NI	Isolated systems
Below Scale FBS	50 mHz < Δf for 0 < $t \leq$ 5 min. **OR** 100 mHz < Δf for 0 < $t \leq$ 2 min.	100 mHz < Δf for 0 < $t \leq$ 5 min. **OR** 250 mHz < Δf for 0 < $t \leq$ 2 min.	200 mHz < Δf for 0 < $t \leq$ 5 min. **OR** 250 mHz < Δf for 0 < $t \leq$ 3 min.	100 mHz < Δf for 0 < $t \leq$ 7 min. **OR** 250 mHz < Δf for 0 < $t \leq$ 3 min.
Scale 0 F0	50 mHz < Δf for 5 < $t \leq$ 15 min. **OR** 100 mHz < Δf for 2 < $t \leq$ 5 min.	100 mHz < Δf for 5 < $t \leq$ 15 min. **OR** 250 mHz < Δf for 2 < $t \leq$ 5 min.	200 mHz < Δf for 5 < $t \leq$ 15 min. **OR** 250 mHz < Δf for 3 < $t \leq$ 10 min.	100 mHz < Δf for 7 < $t \leq$ 20 min. **OR** 250 mHz < Δf for 3 < $t \leq$ 10 min.
Scale 1 F1	50 mHz < Δf for t > 15 min. **OR** 100 mHz < Δf for t > 5 min.	100 mHz < Δf for t > 15 min. **OR** 250 mHz < Δf for t > 5 min.	200 mHz < Δf for t > 15 min. **OR** 250 mHz < Δf for t > 10 min.	100 mHz < Δf for t > 15 min. **OR** 250 mHz < Δf for t > 10 min.
Scale 2 F2	200 mHz < Δf for t > 30 sec.	500 mHz < Δf for t > 1 min. **OR** F > 1000 mHz	500 mHz < Δf for t > 1 min.	500 mHz < Δf for t > 1 min.
Scale 3				

[2] Nordic System Operation Agreement (SOA) – Annex Load-Frequency Control & Reserves (LFCR) (entsoe.eu)

5.4 Incidents on network elements (T)

Disconnection of a transmission system element that is part of an alternating current (AC) network with an operating voltage of **220 kV or higher** and in a network with **operating voltage levels below 220 kV when relevant for maintaining operational security,** pursuant to Article 15(3) of the SOGL. Furthermore, disconnection of high voltage direct current (HVDC) elements is included. The disconnection is reported in the event of:

- unplanned disconnection (due to, for example, human and asset safety, faults, or malicious attacks) in cases where there is no time for security analysis and/or activation of remedial actions; or
- (automatic) disconnection by a protection device;

For transmission system element(s) not capable of automatic reconnection, disconnection is deemed to be final if reconnection has not occurred after 3 minutes.

Additionally, an incident on a high-voltage direct current (HVDC) system is reported in the event of:

- reduction or change of HVDC flow by protection or control devices; or
- reduction or change of HVDC flow resulting in the N-1 criterion not being fulfilled or the degradation of operational security standards (voltage or frequency);

when the reduction or change of flow through HVDC systems between (a)synchronous areas exceed the thresholds presented in Table 5. In case multiple HVDC interconnectors experience a change of flow within a sliding window of 15 minutes, the sum of changes for each interconnector shall be considered. If the thresholds are different on each side of the HVDC systems, the lowest threshold value of the (a)synchronous areas shall be used to classify the incident.

In the event of disconnection of a tie-line or a link between more than one TSO (including HVDC), only the TSO in whose control area the initiating event was in should report to avoid double reporting.

Exceptions

No reporting is required in case:

- planned manual disconnection of the AC transmission system element(s);
- disconnection of transmission lines where successful automatic re-closure has occurred and no other ICS criteria threshold is reached; or
- planned manual disconnection or change of flows of HVDC interconnectors.

Table 4 Thresholds by scale for incidents on transmission system elements

	CE	Nordic	IRE/NI	Isolated systems
Scale 0 T0	Disconnection of: • transmission system element(s); • tie-line; or • HVDC system.			
Scale 1 T1	Disconnection of: • transmission system element(s); • tie-line; or • HVDC system, that results in the N-1 criterion[3] to not be fulfilled, even after the activation of remedial action(s) pursuant to Article 20 of the SOGL.			
Scale 2 T2	Disconnection of: • transmission system element(s), or • tie-line, or • HVDC system in case, as a consequence of the disconnection, there is at least one violation of a TSO's operational security limits, defined in accordance with Article 25 of SOGL, that propagates a scale 1, 2 or 3 incident to an interconnected TSO.			
Scale 3				

Table 5 Thresholds for change of power flow for HVDC interconnectors between (a)synchronous areas.

	CE	Nordic	IRE/NI	Isolated systems
Scale 0 T0				
Scale 1 T1	$1500 < P \leq 3000$ MW	$1500 < P \leq 3000$ MW	$500 < P \leq 800$ MW	*Not applicable*
Scale 2 T2	$P > 3000$ MW	$P > 3000$ MW	$P > 800$ MW	*Not applicable*
Scale 3				

[3] Taking into account the derogations pursuant to Article 35(4) and 35(5) of the SOGL.

5.5 Incidents on power generating facilities (G)

An incident is classified as an incident on power generating facilities (G) when generation is reduced or disconnected within one TSO's control area and reaches the thresholds defined in the Table 6. Disconnection or reduction of power generating facilities is reported in case of:

- unexpected reduction of generation (no time for security analysis and/or activation of remedial actions) within 15 minutes;
- disconnection of power generating facility connected to network; or
- the sum of disconnected and reduced power generating facilities within 15 minutes exceeds the thresholds presented in Table 6.

The 'Below Scale' incidents on generating facilities (GBS) are used to calculate the operational security indicators relevant to operational security OS-B pursuant to Article 15(3)(b) of the SOGL. The incidents should only include tripped generation units and are compiled by WG ICS from the Unavailability of Production and Generation Units data of the ENTSO-E Transparency Platform[4]. Therefore, TSOs are not required to include the GBS events in their reporting process described in Chapter 8.

Table 6 Thresholds by scale for incidents on power generating facilities. P denotes the magnitude of the lost generation power.

	CE	Nordic	IRE/NI	Isolated systems
Below Scale GBS	100 < *P* ≤ 600 MW	100 < *P* ≤ 600 MW	100 < *P* ≤ 200 MW	>100 to biggest unit in the system
Scale 0 G0	600 < *P* ≤ 1500 MW	600 < *P* ≤ 1500 MW	200 < *P* ≤ 500 MW	Biggest unit in the system
Scale 1 G1	1500 < *P* ≤ 3000 MW	1500 < *P* ≤ 3000 MW	500 < *P* ≤ 800 MW	Larger than the biggest unit in the system
Scale 2 G2	3000 MW < *P*	3000 MW < *P*	800 MW < *P*	Power plant with the biggest unit in the system
Scale 3				

[4] Unavailability of Production and Generation Units (transparency.entsoe.eu). WG ICS is not responsible for the data quality within the Transparency Platform

5.6 N and N-1 violations (ON)

The'(N-1) criterion' is defined pursuant to Article 3(14) of the SOGL.

Exceptions:

Pursuant to Article 35(4) of the SOGL, a TSO shall not be required to comply with the (N-1) criterion in the following situations:

a) during switching sequences;
b) during the time period required to prepare and activate remedial actions.

Furthermore, unless a Member State determines otherwise a TSO shall not be required to comply with the (N-1) criterion as long as there are only local consequences within the TSO's control area in accordance with Article 35(5) of the SOGL.

(N-1) situations due to voltage violations are covered in Section 5.9.

Table 7 Thresholds by scale for N-1 violations (ON1) and N violations (ON2).

	CE	Nordic	IE/NI	Isolated systems
Scale 0				
Scale 1 ON1	N-1 criterion is not fulfilled, even after the activation of remedial action(s) pursuant to Article 20 of the SOGL. or N-1 criterion is not fulfilled and can't be restored within the limits set for transitory admissible overloads of transmission system elements			
Scale 2 ON2	At least one operational security limit is violated and propagates a scale 1, 2 or 3 incident to an interconnected TSO.			
Scale 3				

5.7 Separation from the grid (RS)

An incident is classified according to this criterion in case of a system incident leading to a situation where a synchronous area is split into one or more synchronous regions, as referred to in Article 3(11) of the Regulation 2017/2196 on establishing a network code on electricity emergency and restoration ('Network code on emergency and restoration'). The classification criteria of a separation of grid incident are presented in Table 8. Each separation should be counted as a separate violation of any of these criteria.

Exceptions:

Planned islanding, used for example as a remedial action or being a result of maintenance, is not considered as an RS incident. This criterion does not apply to isolated systems. DC interconnections are not considered for this criterion.

Table 8 Thresholds by scale for separation from the grid. *L* denotes the latest calculated load in the separated region before it splits from the system.

	CE	Nordic	IRE/NI
Scale 0 RS0	Separation of a part of the transmission system from the synchronous area, involving one or more TSOs, in case the separated region has a load between 1 % < *L* ≤ 5% of total load in the synchronous area before the incident.		
Scale 1 RS1	Separation from the grid, involving one TSO, in case the separated region has a load *L* > 5 % of total load in the synchronous area before the incident.		
Scale 2 RS2	Separation from the grid involving more than one TSO in case the separated region has a load *L* > 5 % of total load in the synchronous area before the incident.		
Scale 3			

5.8 Loss of tools, means and facilities (LT)

This ICS criterion is violated in case a TSO experiences the loss of real time-tools, means and facilities. The following items shall be monitored, as specified in Article 24(1) of the SOGL:

- facilities for monitoring the system state of the transmission system, including state estimation applications and facilities for load-frequency control (for example, ENTSO-E Awareness System (EAS));
- means to control the switching of circuit breakers, coupler circuit breakers, transformer tap changers and other equipment which control transmission system elements;
- means to communicate with the control rooms of other TSOs and Regional Coordination Centres (RCCs);
- tools for operational security analysis; and
- tools and communication means necessary for TSOs to facilitate cross-border market operations.

A backup tool, mean or facility must be able to fully take over the functionality of the main solution.

Table 9 Thresholds by scale for loss of tools, means and facilities.

	CE	Nordic	IRE/NI	Isolated systems
Below scale LTBS	Loss of any tool, mean or facility for more than 30 minutes without consequences for other TSO(s).			
Scale 0 LT0	Loss of any tool, mean or facility, both main and backup solution, for more than 30 minutes without consequences for other TSO(s).			
Scale 1 LT1	Loss of any tool, mean or facility for more than 30 minutes and with consequences for other TSO(s) while the backup system(s) are being used.			
Scale 2 LT2	Loss of any tool, mean or facility, **including backup solution (if exists)**, for more than 30 minutes and with consequences for other TSO(s).			
Scale 3				

5.9 Violation of standards on voltage (OV)

Violation of standards on voltage are reported when in steady-state a connection point, as defined in Article 2(15) of Commission Regulation (EU) 2016/631, to the transmission system is operated outside the voltage ranges defined in Article 27 of the SOGL considering the time ranges and thresholds defined in Table 10 and 11. In addition to the legal requirement, TSO-to-TSO tie-lines are reported based on the time ranges and thresholds for connection points.

For isolated systems, the violation of standards on voltage is reported when a node of the transmission system is operated at voltage exceeding the pre-incident voltage level by ±10 % for more than 15 minutes.

The 'Below Scale' data are used to report the remaining voltage violation incidents necessary to calculate the operational security indicators OS-F1 and OS-F2. These events are not included in the Scale 0, 1 and 2 incidents and therefore need to be reported separately as part of the ICS monthly TSO data collection process.

In case a voltage violation exceeds the voltage and time thresholds of multiple scales ('below scale', 0, 1 or 2), the criteria violation is classified as the highest violated scale.

Table 10 Voltage and time ranges at the connection point between > 110 kV and ≤ 300 kV. *U* denotes the measured voltage in per unit, and *t* the measured duration.

	CE	Nordic	IRE/NI	Isolated system
Below Scale OVBS	*U* ≤ 0,90 pu, for *t* ≥ 5 min. **OR** 1,118 pu ≤ *U* for *t* ≥ 5 min.	1,05 pu ≤ *U*, for *t* ≥ 5 min.		
Scale 0 OV0	*U* ≤ 0,90 pu, for *t* ≥ 15 min. **OR** 1,118 pu ≤ *U* for *t* ≥ 15 min.	1,05 pu ≤ *U*, for *t* ≥ 15 min.		
Scale 1 OV1	*U* ≤ 0,85 pu, for *t* ≥ 30 seconds **OR** *U* ≤ 0,90 pu, for *t* ≥ 60 min. **OR** 1,118 pu ≤ *U*, for *t* ≥ 60 min. **OR** 1,15 pu ≤ *U*, for *t* ≥ 30 seconds	*U* ≤ 0,90 pu, for *t* ≥ 30 seconds **OR** 1,05 pu ≤ *U*, for *t* ≥ 60 min. **OR** 1,10 pu ≤ *U*, for *t* ≥ 30 seconds	*U* ≤ 0,90 pu, for *t* ≥ 30 seconds **OR** 1,10 pu ≤ *U*, for *t* ≥ 30 seconds	Voltage exceeding pre-incident voltage level by ±10 % for more than 15 minutes
	without consequences for neighbouring TSO			
Scale 2 OV2	Same as Scale 1 but with consequences on at least one neighbouring TSO			
Scale 3				

Table 11 Voltage and time ranges at the connection point above 300 kV. *U* denotes the measured voltage in per unit, and *t* the measured duration.

	CE	Nordic	IRE/NI	Isolated system
Below Scale OVBS	*U* ≤ 0,90 pu, for *t* ≥ 5 min. **OR** 1,05 pu ≤ *U*, for *t* ≥ 5 min.	1,05 pu ≤ *U*, for *t* ≥ 5 min.		
Scale 0 OV0	*U* ≤ 0,90 pu, for *t* ≥ 15 min. **OR** 1,05 pu ≤ *U*, for *t* ≥ 15 min.	1,05 < *U* ≤ 1,10 pu, for *t* ≥ 15 min.		
Scale 1 OV1	*U* ≤ 0,85 pu, for *t* ≥ 30 seconds **OR** *U* ≤ 0,90 pu, for *t* ≥ 60 min. **OR** 1,05 pu ≤ *U*, for *t* ≥ 60 min. **OR** 1,10 pu ≤ *U*, for *t* ≥ 30 seconds	U ≤ 0,90 pu, for *t* ≥ 30 seconds **OR** 1,05 pu ≤ *U*, for *t* ≥ 60 min. **OR** 1,10 pu ≤ *U*, for *t* ≥ 30 seconds	*U* ≤ 0,90 pu, for *t* ≥ 30 seconds **OR** 1,05 pu ≤ *U*, for *t* ≥ 30 seconds	Voltage exceeding pre-incident voltage level by ±10 % for more than 15 minutes
	without consequences for neighbouring TSO			
Scale 2 OV2	Same as Scale 1 but with consequences on at least one neighbouring TSO			
Scale 3				

5.10 Reduction of reserve capacity (RRC)

An incident is classified by the percentage reduction of reserve capacity in a TSO's control area as defined in Table 11. The reduction is compared to the target amount of reserve for each TSO and for each type of reserve (FCR, FRR and RR) for the given timeframe.

The reduction of reserve capacity is calculated using the minimum reporting time which is according to each TSOs scheduling resolutions of power generating facilities. The scheduling resolutions can vary per TSO between 5 and 30 minutes and the reduction of reserve capacity is in relation to the pre-fault levels.

Exceptions:

Activated energy bids are not considered as reduction of reserve capacity.

Table 12 Thresholds by scale for reduction of reserve capacity

	CE	Nordic	IRE/NI	Isolated systems
Scale 0 RRC0	More than 20 % reduction with a duration less than or equal to 30 minutes and there are no means to compensate for that reduction in real-time system operation			
Scale 1 RRC1	More than 20 % reduction with a duration of more than 30 minutes and there are no means to compensate for that reduction in real-time system operation			
Scale 2 RRC2	Reserve capacity unavailable more than 30 minutes and there are no means to compensate for that reduction in real-time system operation			
Scale 3				

6 Operational security indicators

The calculation of operational security indicators listed in Articles 15(3) and 15(4) of the SOGL is based on all the incidents reported on scales 0 to 3. In addition, the ICS annual report shall show each indicator for each TSO.

6.1 Operational security indicators relevant to operational security

Operational security indicators relevant to operational security are listed in Article 15(3) of the SOGL. The calculation rules for the operational security indicators relevant to operational security are provided in Table 13.

Table 13 Operational security indicators relevant to operational security

Security indicator	Name of the indicator and SOGL reference	Calculation rules	Reference
OS-A	Number of tripped transmission system elements per year per TSO - SOGL Article 15(3)(a)	Add up the number of transmission system elements tripped reported for all the incidents on scale 0, 1, 2 and 3.	Section 5.4 Incidents on network elements.
OS-B	Number of tripped power generation facilities per year per TSO - SOGL Article 15(3)(b)	Add up the number of power generation facilities tripped reported for all the incidents on the 'Below Scale' and scale 0, 1, 2 and 3. The number of tripped generation facilities collected for the 'Below Scale' category will be taken from the transparency platform.	Section 5.5 Incidents on power generating facilities
OS-C	Energy not supplied due to unscheduled disconnection of demand facilities per year per TSO - SOGL Article 15(3)(c)	Add up the energy not supplied reported for all incidents on scale 0, 1, 2 and 3 due to unscheduled disconnection of demand facilities.	Reported for incidents on power generating facilities (G), Section 5.5.
OS-D1	Time duration of being in alert and emergency states per year per TSO - SOGL Article 15(3)(d)	Add up the time in alert and emergency states reported for all incidents on scale 0, 1, 2 and 3.	No particular reference. Alert and emergency state duration is reported for all incidents.
OS-D2	Number of instances of being in alert and emergency states per year per TSO - SOGL Article 15(3)(d)	Add up the number of incidents on scale 0,1, 2 and 3 in case alert or emergency state was reported.	No particular reference. Alert and emergency state duration is reported for all incidents.

OS-E1	Time duration within which there was a lack of reserve identified per year per TSO - SOGL Article 15(3)(e)	Add up the duration of incidents reported under the criteria RRC0, RRC1 and RRC2; and the duration of all other incidents on scale 0, 1, 2 and 3 in case the reduction of reserve capacity is reported.	Section 5.10 Reduction of reserve capacity.
OS-E2	Number of incidents for which there was a lack of reserve identified per year per TSO - SOGL Article 15(3)(e)	Add up the number of incidents reported under the criteria RRC0, RRC1 and RRC2; and the number of all other incidents on scale 0, 1, 2 and 3 in case the reduction of reserve capacity is reported.	Section 5.10 Reduction of reserve capacity.
OS-F1	Time duration of voltage deviations exceeding the ranges from tables 1 and 2 of SOGL Annex II per year per TSO - SOGL Article 15(3)(f)	Add up the duration of incidents reported under the criteria OV 'Below Scale' and Scale OV0, OV1 and OV2; and add up the duration of all other incidents on the 'Below Scale', scale 0, 1, 2 and 3 in case voltage deviations are reported which exceed the ranges from SOGL Annex II.	Section 5.9 Violation of standards on voltage.
OS-F2	Number of voltage deviations exceeding the ranges from tables 1 and 2 of SOGL Annex II per year per TSO - SOGL Article 15(3)(f)	Add up the number of incidents reported under the criteria OV 'Below Scale' and scale OV0, OV1 and OV2; and add up the duration of all other incidents on the 'Below Scale', scale 0, 1, 2 and 3 in case voltage deviations are reported which exceed the ranges from SOGL Annex II.	Section 5.9 Violation of standards on voltage.
OS-G1	Number of minutes outside the standard frequency range per year per synchronous area - SOGL Article 15(3)(g)	Add up the number of minutes outside the standard frequency range.	Provided by the Annual Load-Frequency Control reporting pursuant to Article 16 of the SOGL.
OS-G2	Number of minutes outside the 50% of maximum steady state frequency deviation per year per synchronous area - SOGL Article 15(3)(g)	Add up the number of minutes outside the 50% of maximum steady-state frequency deviation.	Provided by the Annual Load-Frequency Control reporting pursuant to Article 16 of the SOGL.
OS-H	Number of system-split separations or local blackout states per year – SOGL Article 15(3)(h)	Add up the number of incidents reported under the criteria RS1 and RS2.	Section 5.7 Separation from the grid.

OS-I	Number of blackouts involving two or more TSOs per year - SOGL Article 15(3)(i)	Add up the number of incidents reported under the criteria OB3, in case two or more TSOs are involved.	Section 5.1 Blackout (OB).

6.2 Operational security indicators relevant to operational planning

Operational security indicators relevant to operational planning are listed in Article 15(4) of the SOGL. The calculation rules for the operational security indicators relevant to operational planning are provided in Table 14.

Table 14 Operational security indicators relevant to operational planning

Abbreviation	Name of the indicator and SOGL reference	Calculation rules
OPS-A	Number of incidents in which an incident contained in the contingency list led to a degradation of the system operation state - SOGL Article 15(4)(a).	Add up the number of incidents on scale 0, 1, 2 and 3 in case degradation of system operation state is reported and in case the cause of the incident is a contingency from contingency list.
OPS-B	Number of the incidents counted by indicator OPS-A (incidents in which an incident contained in the contingency list led to a degradation of the system operation state), in which a degradation of system operation conditions occurred as a result of unexpected discrepancies from load or generation forecasts - SOGL Article 15(4)(b).	Add up the number of incidents counted by indicator OPS-A in case unexpected discrepancies from load and generation forecasts were reported as the cause of the incident.
OPS-C	Number of incidents in which there was a degradation in system operation conditions due to an exceptional contingency - SOGL Article 15(4)(c).	Add up the number of incidents on scale 0, 1, 2 and 3 in case degradation of system operation state is reported and in case the cause of the incident is an exceptional contingency.
OPS-D	Number of the incidents counted by indicator OPS-C (incidents in which there was a degradation in system operation conditions due to an exceptional contingency), in which a degradation of system operation conditions occurred as a result of unexpected discrepancies from load or generation forecasts - SOGL Article 15(4)(d).	Add up the number of incidents counted by indicator OPS-C in case unexpected discrepancies from load and generation forecasts were reported as the cause of the incident.

OPS-E	Number of incidents leading to a degradation in system operation conditions due to lack of active power reserves - SOGL Article 15(4)(e).	Add up the number of incidents on scale 0, 1, 2 and 3 in case lack of active power reserves was reported as the cause of the incident.

7 Procedure for the investigation of scale 2 and scale 3 incidents

1. The objective of ICS incident investigations is the prevention of future incidents and the improvement of the resilience of the European electricity system. The investigation shall be conducted impartially and should not intend to allocate responsibility or liability to any party.
2. For each scale 2 and 3 incident, a detailed report shall be prepared explaining the reasons for the incident and based on ICS Expert Panel investigation. The report is prepared by an ICS Expert Panel consisting of representatives from each TSO affected by the incident, the leader of the expert panel from a TSO not affected by the incident, relevant RCC(s) and a WG ICS representative. Regulatory authorities and ACER are included in the expert panel upon their request.
3. Pursuant to Article 1(2) of the Regional Coordination Centre Post-Operation and Post-Disturbances Analysis and Reporting Methodology (hereinafter the "RIAR Methodology)", an "RCC Investigation Subgroup" shall be created within the Expert Panel if the RCC Investigation Threshold, defined in Article 5(1) of the RIAR Methodology, is met. In accordance with Article 3(1) of the same methodology, each RCC shall appoint an RCC SPOC and shall communicate this to Working Group ICS via email. Working Group ICS will update the RCC SPOC list on an annual basis.
4. All documents made public by the ICS Expert Panel and the RCC Investigation Subgroup are published on ENTSO-E's website.
5. The timeline and process flow is illustrated in Annex 3.

7.1 Scale 2 or scale 3 incident reporting, and classification

1. It should be noted that the scale 2 or 3 incident reporting process is an additional reporting task to the ICS Annual Reporting process.
2. TSOs shall report all incidents in their own control area that are suspected to be classified as scale 2 or scale 3 incidents in accordance with the Methodology to WG ICS and neighbouring TSOs.
3. The TSO shall report the suspected scale 2 or 3 incident immediately when possible and not later than one week after the start of a suspected scale 2 incident, or in case of a suspected scale 3 incident, immediately when possible and not later than three business days.
4. The TSO shall additionally report preliminary data of the incident to WG ICS to support the preliminary classification. The preliminary data shall be reported within the timeframes defined in paragraph 7.1(3).
5. The preliminary data shall contain at least:
    a. time of the incident;
    b. affected TSOs;
    c. a list of violated ICS criteria and related data as per Annex 1; and
    d. short explanation of the incident, its causes and consequences.

6. WG ICS shall classify the ICS incident according to this Methodology within five days following the receipt of the preliminary data from the TSO.
    a. If the preliminary data indicate undoubtedly that the incident did not meet any scale 2 or 3 criteria, the procedure for investigation stops here.
    b. In case the preliminary data is not sufficient to classify the incident, WG ICS shall contact the TSO SPOC for additional information about the incident.
7. Pursuant to Article 3(3) of the RIAR Methodology, WG ICS shall ask the RCC SPOCs to nominate a main and substitute RCC member in case the incident involved two or more TSOs. WG ICS and the RCC members shall jointly verify if the RCC Investigation Threshold was met in accordance with Article 4(2) of the RIAR Methodology.
8. If the incident meets any scale 2 or scale 3 criteria, WG ICS shall inform ENTSO-E about the incident and shall nominate 1 or 2 members to participate in the Expert Panel before the first meeting. ENTSO-E shall nominate the convener to chair the incoming ICS Expert Panel.
9. TSOs affected by the scale 2 and scale 3 incidents shall inform their national regulatory authority (NRA) before the investigation is launched as required by Article 15(5) of the SOGL.
10. ENTSO-E shall inform RCC SPOCs and ACER about the upcoming investigation in due time before it is launched and not later than 1 week before the first meeting of the expert panel. NRAs and ACER may nominate members to participate in the ICS Expert Panel.
11. When a scale 2 incident affects only one TSO, the first ICS Expert Panel meeting is conducted as usually. If in this meeting, it is undoubtedly confirmed that the incident affected only one TSO, the investigation proceeds as an internal investigation led by the affected TSO. The original Expert Panel members may, at their request, continue to participate in the investigation as members. The reports of the internal investigation shall be shared with ENTSO-E, the TSOs, RCCs, ACER, NRAs and the impacted DSOs. The internal reports shall follow the timeline set for the ICS Expert Panel reports.

7.2 ICS Expert Panel formation

1. The ICS Expert Panel conducts the scale 2 or scale 3 incident investigation. The expert panel shall consist of the following members:
    a. **The convener of the expert panel**: ENTSO-E shall nominate an expert from a TSO not affected by the incident as the leader of the expert panel to ensure neutrality of the investigation;
    b. **Expert panel members**: each TSO affected by the scale 2 or scale 3 incident shall appoint an expert to represent the TSO in the expert panel. Furthermore, at least two members from TSOs not impacted by the incident shall be included in the expert panel;
    c. **RCC members**: At least one RCC member if the RCC Investigation Threshold was met based on the preliminary data in accordance with Article 5 of the RIAR Methodology. In addition, at least one RCC member from an RCC whose region was not affected by the incident shall be included. In the event that all RCCs were affected, all RCCs shall agree on the RCC members that participate in the ICS Expert Panel;
    d. **WG ICS representative**: WG ICS shall nominate 1 or 2 representative(s) from the group to ensure that the procedure for the investigation of scale 2 and scale 3 incidents is followed;

e. Representatives of the regulatory authorities and ACER as nominated per their request; and

f. Depending on the nature of the incident and its impact on distribution grids, the ICS Expert Panel may decide to invite technical experts from the DSO(s) in the affected area(s) to participate to the investigation, provided that they comply with the requirements of Article 35 of Directive (EU) 2019/944, and/or experts from the EU DSO Entity. In the latter case, the representative shall be employed by a DSO complying with the requirement of Article 35 of Directive (EU) 2019/944 or by the EU DSO Entity secretariat.

2. The parties entitled to nominate members to the ICS Expert Panel according to paragraph 1 shall nominate their representatives within one week after the preliminary classification of the incident by the WG ICS. Such nominations shall be notified via mail without delay to ENTSO-E for the first ICS Expert Panel meeting to be convened.

3. After the nomination of the Expert Panel members, the convener of the ICS Expert Panel shall convene the first ICS Expert Panel meeting within two weeks after the nominations are complete, or within one week from an incident of scale 3.

4. If a reported incident affects two or more TSOs, the WG ICS shall classify the incident according to the Methodology and invite all RCC members to verify whether the RCC Investigation Threshold was met. More specifically, pursuant to Article 1(2) of the RIAR Methodology, an "RCC Investigation Subgroup" shall be created within the Expert Panel if the RCC Investigation Threshold, defined in Article 5(1) of the RIAR Methodology, is met. In accordance with Article 3(1) of the same methodology, each RCC shall appoint an RCC SPOC and shall communicate this to WG ICS via email. WG ICS will update the RCC SPOC list on an annual basis.

7.3 Timeline for investigating scale 2 and scale 3 incidents

1. The ICS Expert Panel investigation has the following timeline:

   i. by six months after the end of the incident, the ICS Expert Panel shall publish an ICS Factual Report that will provide the factual basis for the final report;

   ii. by twelve months after the end of the incident, the ICS Expert Panel shall publish an ICS Final Report on the investigation of the incident;

2. In the event the TSOs affected by the incident receive urgent inquiries from their regulatory authorities or external stakeholders regarding the incident, the ICS Expert Panel may decide to accelerate the incident investigation.

7.4 Data Collection

1. To perform the relevant analysis of the incident, the ICS Expert Panel shall require the data reported by the affected TSOs, RCCs, DSOs, SGUs or third parties within the scope of SOGL, and depending on the type of the incident, additional data necessary for the investigation.

2. In case the ICS Expert Panel requires additional data and information for the investigation, the ICS Expert Panel shall request this additional data directly from the relevant TSOs, RCCs, DSOs, SGUs or third parties within the scope of SOGL with a written request. Examples of the data that can be requested by the ICS Expert Panel are listed in Annex I and II.

3. Collected data regarding the incident from relevant TSOs, RCCs, DSOs, SGUs or third parties within the scope of SO GL shall be shared between the ICS Expert Panel and the RCC Investigation Subgroup.
4. The recipients (relevant TSOs, RCCs, DSOs, SGUs or third parties within the scope of SOGL) of the written request shall, as soon as possible and within 14 calendar days of the receipt of the written request, provide the data and information in accordance with the request of the expert panel.
    a. In case the request for a dataset is unclear, the recipient shall seek clarification from the Expert Panel within 3 business days after receiving the request. The ICS Expert Panel shall clarify the request as needed.
    b. In case a specific dataset cannot be provided withing the indicated time period, the recipient of the data request shall explain the underlying reasons for the delay to the ICS Expert Panel, which may decide to extend the time period for data provision.
    c. In case the specific dataset cannot be provided, whether in full or in part, the recipient of the data request shall within 7 calendar days explain the underlying reasons to the ICS Expert Panel, which may decide to adjust or withdraw the request.
5. If, during the course of the investigation, additional information and/or data not specified in this methodology or requested by the Expert Panel, becomes available to the Panel, the Expert Panel shall assess its relevance to the investigation. If deemed relevant the Expert Panel shall consider it in preparing the factual and/or final reports.

7.5 Factual Report

1. After collecting the data, the ICS Expert Panel shall prepare the **ICS Factual Report**, which provides at least:
    a. the description of the system conditions right before the incident;
    b. the description of the system conditions after the incident;
    c. activated remedial actions and measures from system defence plan; and
    d. the sequence of events, including the description of all violations of operational security limits and other consequences of the incident.
    e. the preliminary analysis on the causes of the incident, which shall be of provisional nature and subject to amendments in the final report;
    f. description of the data collected;
    g. measures already taken by impacted system operators; and
    h. planned next steps.
2. Each TSO that provided information shall approve the factual correctness of their information contained in the report, before the expert panel proceeds with performing further analysis and preparing the final report.

7.6 Final Report

1. The ICS Expert Panel shall prepare the ICS **Final Report**, which shall include at least:
    a. the identification and analysis of the causes of the incident;

b. the evaluation of the activated remedial actions and measures from system defence plan;

c. the evaluation of the actions of TSO employees in charge of real-time operation of the transmission system;

d. the description of the functioning of the transmission system element(s);

e. the conclusions and the explanations of the reasons for the incident;

f. the recommendations based on the conclusions of the investigation in order to avoid similar incidents in the future; and

g. the conclusions of the RCC Investigation shall be added as a dedicated chapter of the ICS Final Report. The dedicated RCC Investigation chapter shall be reviewed by the ICS Expert Panel, to ensure alignment, before being added to the ICS Final Report.

8 Annual report

Pursuant to Article 15(1) of SOGL, ENTSO-E shall publish each year by 30 September on their website an annual report on operational security indicators described in Chapter 6.

8.1 Annual reporting process and timeline

1) The reporting period for ICS annual reports is one calendar year. Each TSO shall report the incidents occurring between 1 January and 31 December. When an ICS incident begins in one calendar year and ends in another calendar year, the incident is included in the ICS annual report for the year in which the incident began.

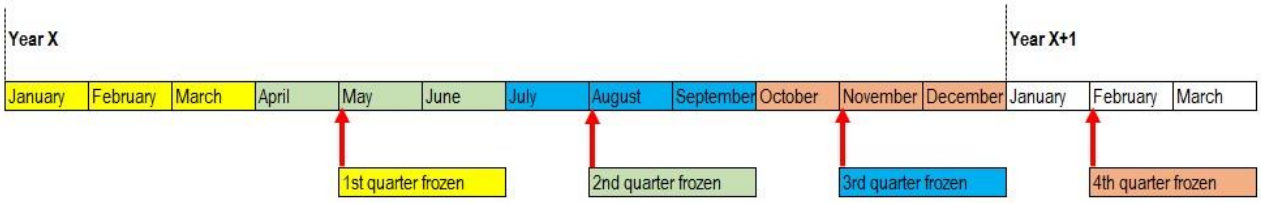
2) **Each TSO shall report an incident classified in accordance with the ICS criteria, as defined in Chapter 5 of this Methodology, at the latest by the end of the month following the month in which the incident began**. The members of Working Group Incident Classification Scale (WG ICS) analyse the ICS incidents reported by the TSOs and freezes the database of incidents after the end of each quarter of the year:

   – ICS incidents occurring from 1 January to 31 March are reported by 1 May;

   – ICS incidents occurring from 1 April to 30 June are reported by 1 August;

   – ICS incidents occurring from 1 July to 30 September are reported by 1 November; and

   – ICS incidents occurring from 1 October to 31 December are reported by 1 February on the following year.



3) TSOs may modify the data after the above deadlines subject to the approval of the WG ICS.

4) According to Article 16(2) of the SOGL, each TSO shall provide the necessary data and information by 1 March for the preparation of the annual reports based on the ICS. The ICS report will be published each year by 30th September.

5) Each TSO shall report the consumption and the total circuit length in their control area. The consumption is reported for the whole calendar year (from 1 January to 31 December) and refers to the electricity consumption in the area of a TSO corresponding to the coverage area of the reported ICS incidents. The circuit length is measured at the end of the calendar year. Circuit length is defined in the ENTSO-E Grid Disturbance Definitions for the Power System Above 100 kV[5].

6) After all the data needed for the ICS annual report have been provided, the annual report shall be prepared with the following steps:

   1. The reported ICS data is frozen on 1 March pursuant to Article 16(2) of the SOGL. All TSOs should have delivered the necessary data and information for the preparation of the annual reports based on the incident classification scale;

[5] *ENTSO-E Grid Disturbance Definitions for the Power System Above 100 kV (eepublicdownloads.azureedge.net)*

2. WG ICS prepares the annual report, including calculation of the operational security indicators, analysis of the incidents, and retrieving the explanations of the reasons for scale 2 and scale 3 incidents, from the respective ICS Expert Panel;
3. Validation of reported data and contents of the annual report by each ICS SPOC;
4. Review of the draft report by relevant Steering Groups under the System Operation Committee (SOC);
5. SOC review of the report;
6. Finalisation of the report by WG ICS;
7. SOC approval of the final report; and
8. Publication of the final annual report by 30 September each year.

8.2 Content of the annual report

The annual report includes at least the following information:

- operational security indicators listed in Articles 15(3) and 15(4) of SOGL and calculated according to Chapter 6;
- statistical overview on all reported incidents on scale 0, 1, 2 and 3;
- analysis on the incidents for scale 1 and above;
- identification of any improvements, which are necessary to support sustainable and long-term operational security; and
- explanations of the reasons for incidents on scales 2 and 3 based on the investigation carried out according to Chapter 7.

Annex 1 Data to be reported for recorded ICS incidents

Table 15 shows what data shall be reported for each incident. *X* denotes a mandatory field to report on the left row for the ICS criteria in the top column heading. *C* denotes that the field is calculated from other given fields. The ICS criteria short codes are explained in the Glossary.

Table 15 Mandatory data to be reported for each ICS incident.

	OB3	L2	L1	L0	F2	F1	F0	FBS	T2	T1	T0	G2	G1	G0	GBS	ON2	ON1	RS2	RS1	RS0	OV2	OV1	OV0	OVBS	RRC2	RRC1	RRC0	LT2	LT1	LT0
Incident ID	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
TSO	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Synchronous area	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
Start time of the incident	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
End time of the incident	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Duration (h:mm)	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
Scale	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
ICS criterion	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Highest voltage level affected by the incident									X	X	X										X	X	X	X						
Incident on a tie line, yes/no									X	X	X					X	X				X	X	X	X						
Incident on a HVDC system, yes/no									X	X	X					X	X				X	X	X	X						
Cause of incident	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Choose a type of contingency for reported element	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Comments on the causes of the incident																														
Preventive remedial actions applied																X	X													
Comments on the preventive remedial actions applied																														
Curative remedial actions applied									X	X						X	X													
Comments on the curative remedial actions applied									X	X																				
Reason for not applying remedial actions																														
Number of tripped network elements									X	X	X																			
Type(s) of disconnected network elements									X	X	X																			
An estimate of disconnected load, MW	X	X	X	X																										
Load in a TSO's control area before incident, MW	X	X	X	X														X	X	X										
Energy not supplied due to unscheduled disconnection of demand facilities, MWh	X	X	X	X																										
Load shedding, MW	X	X	X																											
Split synchronised regions load, MW																		X	X	X										
An estimate of disconnected generation, MW												X	X	X	X															
Number of tripped power generation facilities												X	X	X	X															
Maximum/minimum measured voltage, pu																					X	X	X	X						
Maximum frequency deviation, mHz					X	X	X	X																						
Time in alert state (h:mm)		X	X		X	X			X	X		X	X			X	X	X	X		X	X			X	X		X	X	
Time in emergency state (h:mm)		X			X				X			X				X		X			X				X			X		
Time in blackout state (h:mm)	X																													
Time in restoration state (h:mm)	X	X	X		X				X			X				X		X	X	X	X				X			X		
FCR capacity reduction, MW																									X	X	X			
FRRa capacity reduction, MW																									X	X	X			
FRRm capacity reduction, MW																									X	X	X			
RR capacity reduction, MW																									X	X	X			
FCR capacity before the incident, MW																									X	X	X			
FRRa capacity before the incident, MW																									X	X	X			
FRRm capacity before the incident, MW																									X	X	X			
RR capacity before the incident, MW																									X	X	X			
Type of lost TSO tool, mean or facility																												X	X	X
List of affected TSOs (please separate the TSOs by commas, NO if no TSO affected)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Number of other TSOs affected (besides the reporting TSO)	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
Description of the N or N-1 situation (network elements affected, identification of out-of-range contingencies, etc.)									X	X						X	X													
Information about the management of the separated network																		X	X											
Additional information about the incident																														

Annex 2 Additional data for the investigation of scale 2 and scale 3 incidents

Because the nature of scale 2 or 3 incidents can vary greatly, the ICS Expert Panel must specify what additional data is requested for the ICS Expert Panel investigation of the incident. These data can be, for example (but not limited to):

a) ex-ante data about, for example planning, forecast and security analysis results before the incident;

b) real-time snapshots;

c) measurements from SCADA and/or equipment in substation(s) (including any recordings from the protection equipment, actions of special protection schemes, automation, Wide Area Monitoring System, etc.). The inquiry must specify which equipment or measurements are needed;

d) excerpts from operational logs for data on operators' activities;

e) information on the functioning of the equipment, transmission system elements, significant grid users;

f) information on stopping of the load-frequency control;

g) automatic actions by special protection system;

h) all automatic and manual defence actions that were executed;

i) If relevant, restoration and resynchronisation actions;

j) information about communication and timing with other TSOs, DSOs and significant grid users; and

k) other relevant measurements and data as defined by the ICS Expert Panel.

Annex 3 Timeline of the ICS Expert Panel investigation

Figure 1 describes the ICS Expert Panel investigation process diagram.

Figure 2 presents the detailed part of the ICS Expert Panel investigation from the creation of it to its conclusion. These figures form an informative part of this Methodology; in case of doubt, reference should be made to ICS Expert Panel procedure as it is described in Chapter 7.

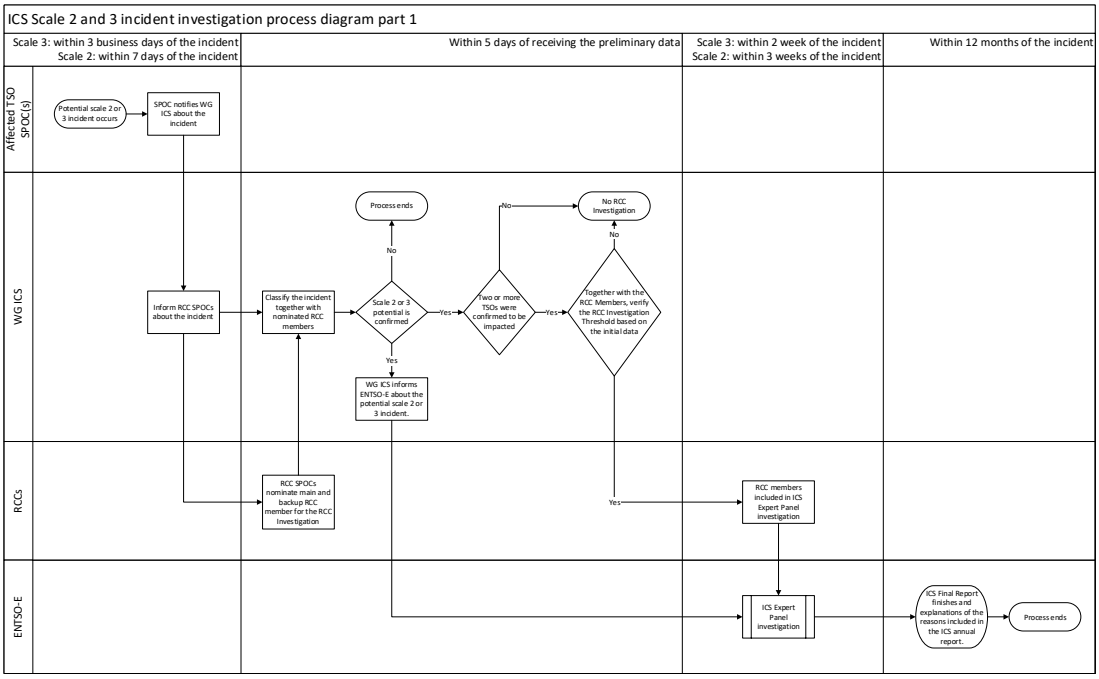


Figure 1 ICS Scale 2 and 3 incident investigation process diagram part 1

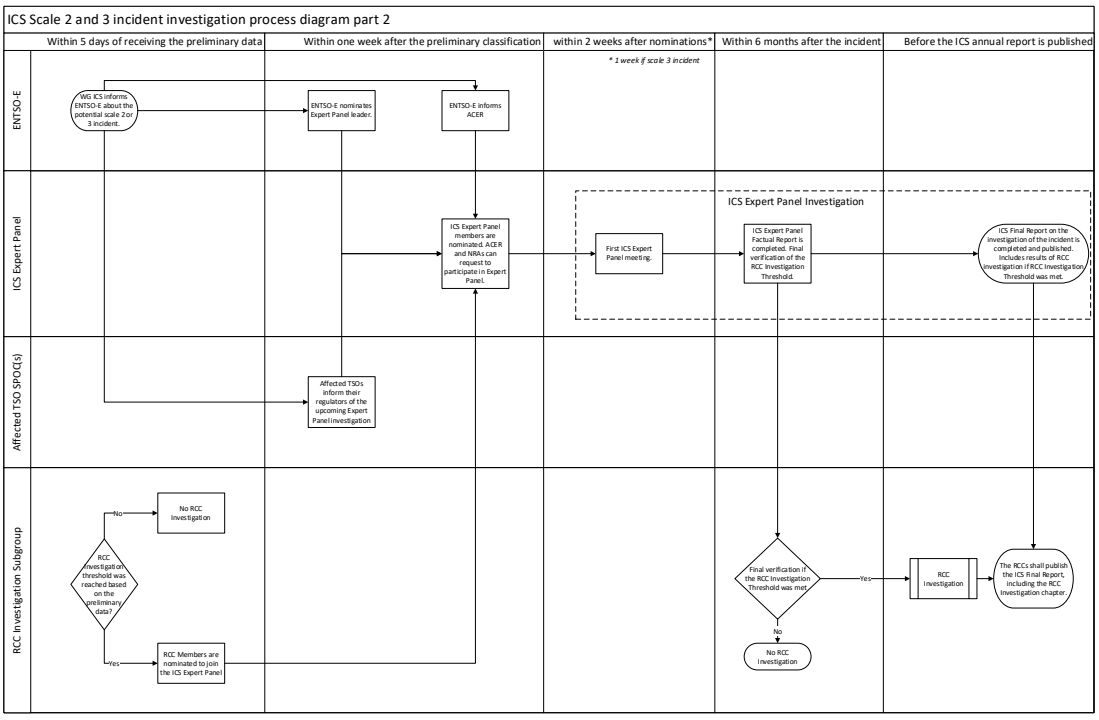


Figure 2 ICS Scale 2 and 3 incident investigation process diagram part 2