European Network of
Transmission System Operators
for Electricity

COORDINATED SECURITY ANALYSIS DATA EXCHANGE SPECIFICATION

2022-02-16

SOC APPROVED
VERSION 2.0

Copyright notice:

This document is maintained by the ENTSO-E CIM EG. Comments or remarks are to be provided at cim@entsoe.eu

NOTE CONCERNING WORDING USED IN THIS DOCUMENT

The force of the following words is modified by the requirement level of the document in which they are used.

- SHALL: This word, or the terms “REQUIRED” or “MUST”, means that the definition is an absolute requirement of the specification.
- SHALL NOT: This phrase, or the phrase “MUST NOT”, means that the definition is an absolute prohibition of the specification.
- SHOULD: This word, or the adjective “RECOMMENDED”, means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase “NOT RECOMMENDED”, means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- MAY: This word, or the adjective “OPTIONAL”, means that an item is truly optional.

33

Revision History

Version	Release	Date	Paragraph	Comments
1	0	2021-04-21		Approved by SOC.
2	0	2022-02-16		The specification was enriched with the following extensions and related profiles: • Equipment Reliability (Including energy areas and roles related to network codes, Direct Current related to DC Poles for Corridors). The content of this profile will be integrated in the EQ profile of CGMES. • Steady State Instruction • System Integrity Protection Schemes (SIPS) as part of the Remedial Action profile • Power Transfer Corridors (PTC) as part of Equipment Reliability profile. • Availability plan • Generation and Load Shift Keys (Time phase, contingency induced balance, variation of losses) • Security limits as part of Equipment Reliability Approved by SOC.

CONTENTS

List of figures

List of tables

1 Scope

The Coordinated Security Analysis (CSA) data exchange specification describes the data exchanges for the CSA process. The CSA is a critical business process based on CSAm (as per SOGL article 75) to ensure the security of supply within the European electricity grid. The CSA data exchange specification also includes the regional operational security coordination per CCR (as per SOGL Article 76) as well as the Inter-RSC and inter-CCR Coordination (required by the SOGL article 75 and 76).

The CSA process is relying on input data from TSOs that are shared to the RSCs to perform remedial action optimisation for a CCR and in cooperation with the other CCRs. A common data specification shall ensure that each of the functions handling and storing any of the assessed data, will do it in an equally secure and adequate manner.

The CSA data exchange specification aims at defining a common data format to lower the IT implementation cost and enable interoperability for the TSOs and RSCs. It aims at making it possible for software vendors to develop an IT application for TSOs and RSCs that allow them to exchange information for the CSA process.

This document defines a structured way of exchanging the following data:

- Available remedial action
- Assessed element
- Contingency
- SIPS configuration
- Security limits
- Generation and Load Shift Key (GLSK)
- Power Transfer Corridor (PTC)
- Steady State Instructions Remedial action schedule (to exchange proposed, accepted/rejected, activated remedial action)
- Security analysis result
- Impact Assessment Matrix

For the next release of the specification, the CSA data exchange project group will continue enriching it with the following items:

- CSA methodology amendment
- Regional operational security coordination methodologies per CCR and input from respective RSC implementation projects

The following is out of scope of this specification:

- The reporting and the monitoring of the CSA (pursuant to SOGL article 17)
- The Probabilistic Risk Assessment (pursuant to Article 44(4) of CSAm)
- The redispatching and countertrading cost sharing (in accordance with CACM Article 74(7))

2 References

2.1 Legal references

- Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation (SOGL);
- Commission Regulation (EU) 2015/1222 of 24 July 2015 establishing a guideline on capacity allocation and congestion management (CACM);
- All TSOs' proposal for a methodology for coordinating operational security analysis in accordance with Article 75 of Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation (CSA methodology);

- Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity)

2.2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- IEC 61970-301:2021 Energy management system application program interface (EMS-API) - Part 301: Common information model (CIM) base;
- IEC 61970-600-1:2021 Energy management system application program interface (EMS-API) - Part 600-1: Common Grid Model Exchange Standard (CGMES) - Structure and rules;
- IEC 61970-600-2:2021 Energy management system application program interface (EMS-API) - Part 600-2: Common Grid Model Exchange Standard (CGMES) - Exchange profiles specification;
- IEC TS 61970-600-1:2017 Energy management system application program interface (EMS-API) - Part 600-1: Common Grid Model Exchange Specification (CGMES) - Structure and rules;
- IEC TS 61970-600-2:2017 Energy management system application program interface (EMS-API) - Part 600-2: Common Grid Model Exchange Specification (CGMES) - Exchange profiles specification;
- IEC 61968-11:2013 Application integration at electric utilities - System interfaces for distribution management - Part 11: Common information model (CIM) extensions for distribution

2.3 Specification documents references

The following specification documents, in whole or in part, are referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- ENTSO-E Assessed element profile specification;
- ENTSO-E Availability plan profile specification;
- ENTSO-E Contingency profile specification;
- ENTSO-E Equipment reliability specification;
- ENTSO-E Generation and Load Shift Key profile specification;
- ENTSO-E Impact assessment matrix profile specification;
- ENTSO-E Remedial action profile specification;
- ENTSO-E Remedial action schedule profile specification;
- ENTSO-E Security analysis result profile specification;
- ENTSO-E Steady State Instructions profile specification;
- ENTSO-E Metadata and Header profile specification;

2.4 Other references

- The Harmonised Electricity Market Role Model;
- Report on Inter-RSC and Inter-CCR Coordination for Coordinated Regional Security Analyses V1.2
- CSA Coordination Function – Business Requirements Specification v1.0
- CSA Input Data Consistency Function – Business Requirements Specification v1.0
- CSA Data Classification v1.0
- CGM-RSC Users Group - Business Requirements Specification v1.0
- CGMES profiling user guide v1.0.

3 Terms and definitions

3.1 Agreed remedial action

Agreed remedial action means a cross-border relevant remedial action for which TSOs in a region agreed to implement or any other remedial action for which TSOs have agreed that it does not need to be coordinated.

[SOURCE: CSAm art. 2.1.19]

3.2 Assessed element

Assessed element is a network element for which the electrical state is evaluated in the regional or cross-regional process and which value is expected to fulfil regional rules function of the operational security limits.

Where necessary, for defining the regional or cross-regional rules for ensuring the system security, assessed elements can be subdivided into two sub-classes – secured elements and scanned elements.

[SOURCE: 2019 Inter-RSC report, BRS CAS consistency function, 4.1]

3.3 Availability plan

A given availability schedule with a given status and cause that include multiple equipment that need to follow the same scheduling periods

[SOURCE: CSA project group]

3.4 Available remedial action

Available remedial action is a remedial action which is available to solve identified constraints. It includes the needed technical and cost information.

[SOURCE: 2019 Inter-RSC report]

All available cross border relevant remedial actions (XRAs) according to CSAm and can include more.

3.5 Capacity Calculation Region

Capacity Calculation Region (CCR) means the geographic area in which coordinated capacity calculation is applied.

[SOURCE: CACM art.2.3]

3.6 Common Grid Model (CGM)

Common Grid Model (CGM) means a Union-wide data set agreed between various TSOs describing the main characteristic of the power system (generation, loads and grid topology) and rules for changing these characteristics during the coordinated capacity calculation process.

[SOURCE: CACM art.2.2]

3.7 Constraint

Constraint means a situation in which there is a need to prepare and activate a remedial action in order to respect operational security limits.

[SOURCE: SOGL art.3.2.2]

3.8 Contingency

Contingency means the identified and possible or already occurred fault of an element, including not only the transmission system elements, but also significant grid users and distribution network elements if relevant for the transmission system operational security.

[SOURCE: CACM art.2.10]

3.9 Contingency analysis

Contingency analysis means a computer-based simulation of contingencies from the contingency list.

[SOURCE: SOGL art.3.2.27]

3.10 Contingency list

Contingency list means the list of contingencies to be simulated in order to test the compliance with the operational security limits.

[SOURCE: SOGL art.3.2.4]

3.11 Countertrading

Countertrading means a cross zonal exchange initiated by system operators between two bidding zones to relieve physical congestion.

[SOURCE: Reg 2019/943 art.2.27]

3.12 Critical Network Element

Critical network element means a network element either within a bidding zone or between bidding zones taken into account in the capacity calculation process, limiting the amount of power that can be exchanged.

[SOURCE: Reg 2019/943 art.2.69]

3.13 Cross-border relevant network element' (XNE)

Cross-border relevant network element' (XNE) means a network element identified as cross border relevant and on which operational security violations need to be managed in a coordinated way.

[SOURCE: ACER Decision on CSAM: Annex I art 2.1.8]

3.14 Cross-border relevant remedial action (XRA)

Cross-border relevant remedial action (XRA) means a remedial action identified as cross border relevant and needs to be applied in a coordinated way.

[SOURCE: CSAm art.2.1.12]

3.15 Curative remedial action

Curative remedial action means a remedial action that is the result of an operational planning process and is activated straight subsequent to the occurrence of the respective contingency for compliance with the (N-1) criterion, taking into account transitory admissible overloads and their accepted duration.

[SOURCE: CSAm art.2.1.24]

3.16 Exceptional contingency

Exceptional contingency means the simultaneous occurrence of multiple contingencies with a common cause.

[SOURCE: SOGL art.3.2.39]

3.17 External contingency

External contingency means a contingency outside the TSO's control area and excluding interconnectors, with an influence factor higher than the contingency influence threshold.

[SOURCE: SOGL art.3.2.24]

3.18 Generation Shift Key

A method of translating a net position change of a given bidding zone into estimated specific injection increases or decreases in the common grid model

[SOURCE: CACM art.2.12]

3.19 Identified constraint

Identified constraint is a couple of elements composed by one or more assessed elements and the contingency leading to a violation of an operational security limit or a function of this operational security limit.

3.20 Impact assessment

Impact assessment determines the impact of changes of a grid model on each TSO's grid and assesses whether this impact qualifies as so significant that the respective TSO is deemed "impacted" by the change.

3.21 Individual Grid Model (IGM)

Individual Grid Model (IGM) means a data set describing power system characteristics (generation, load and grid topology) and related rules to change these characteristics during the coordinated security analysis process, prepared by the responsible TSOs, to be merged with other individual grid model components in order to create the common grid model.

[SOURCE: CACM art.2.1]

3.22 Individual action

Individual action is an action that is one of the single remedial actions as defined in Article 22 of the SO Regulation.

[SOURCE: CSAm art.14.2]

3.23 Internal contingency

Internal contingency means a contingency within the TSO's control area, including interconnectors.

[SOURCE: SOGL art.3.2.23]

3.24 Load Shift Key

It constitutes a list specifying those load that shall contribute to the shift in order to take into account the contribution of generators connected to lower voltage levels (implicitly contained in the load figures of the nodes connected to the EHV grid).[SOURCE: Coordinated Capacity Calculation IG v1.0]

3.25 N-situation

N-situation means the situation where no transmission system element is unavailable due to occurrence of a contingency.

[SOURCE: SOGL art.3.2.3]

3.26 N-1 situation

N-1 situation means the situation in the transmission system in which one contingency from the contingency list occurred.

[SOURCE: SOGL art.3.2.15]

3.27 Normal state

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.

[SOURCE: SOGL art.3.2.5]

3.28 Ordinary contingency

Ordinary contingency means the occurrence of a contingency of a single branch or injection.

[SOURCE: SOGL art.3.2.54]

3.29 Operational security analysis

Operational security analysis means the entire scope of the computer based, manual and automatic activities performed in order to assess the operational security of the transmission system and to evaluate the remedial actions needed to maintain operational security.

[SOURCE: SOGL art.3.2.50]

3.30 Out of range contingency

Out of range contingency means the simultaneous occurrence of multiple contingencies without a common cause, or a loss of power generating modules with a total loss of generation capacity exceeding the reference incident.

[SOURCE: SOGL art.3.2.55]

3.31 Overlapping zone

A collection of all the overlapping cross border assessed elements which have the same sets of impacted and impacting regions.

[SOURCE: CSA data exchange project group]

3.32 Power transfer corridor (PTC)

A power transfer corridor is defined as a set of circuits (transmission lines or transformers) separating two portions of the power system, or a subset of circuits exposed to a substantial portion of the transmission exchange between two parts of the system.

[SOURCE: CSA data exchange project group]

3.33 Preventive remedial action

Preventive remedial action means a remedial action that is the result of an operational planning process and needs to be activated prior to the investigated timeframe for compliance with the (N-1) criterion.

[SOURCE: CSAm art.2.1.18]

3.34 Proposed remedial action

Proposed remedial action is a remedial action proposed by RSC after remedial action optimization. RSC coordinates proposed remedial actions with affected TSOs for intra-CCR and with affected TSOs and RSC for cross-CCR.

3.35 Remedial action

Remedial action means any measure applied by a TSO or several TSOs, manually or automatically, in order to maintain operational security.

[SOURCE: CACM art.2.13]

3.36 Remedial action configuration

Remedial action configuration means a configuration containing the grid state alteration and the availability that is sent by the TSO and from which remedial actions can be derived.

3.37 Remedial action influence factor

Remedial action influence factor means a flow deviation on a XNEC resulting from the application of a remedial action, normalised by the permanent admissible loading on the associated XNE.

[SOURCE: CSAm art.2.1.11]

3.38 Regional Security Coordinator (RSC)

Regional Security Coordinator (RSC) means the entity or entities, owned or controlled by TSOs, in one or more capacity calculation regions performing tasks related to TSO regional coordination.

[SOURCE: SOGL art.3.2.89]

3.39 Restoring remedial action

Restoring remedial action means a remedial action that is activated subsequent to the occurrence of an alert state for returning the transmission system into normal state again.

[SOURCE: CSAm art.2.1.13]

3.40 Scanned element

Scanned element is an assessed element on which the electrical state (at least flows) shall be computed and shall be subject to an observation rule during the regional security analysis process. Such observation rule can be for example avoiding the increase of a constraint or avoiding the creation of a constraint on this element, as a result of the design of remedial actions needed to relieve violations on the secured elements. A scanned element within a CCR can be any element of any CCR (irrespective of any potential qualification as XNE by one or more CCRs).

3.41 Secured element

Secured element is an assessed element on which remedial actions needed to relief these violations shall be identified, when violations of an operational security limit are identified during the regional or cross-regional security analysis. Each secured element within a CCR is an XNE.

3.42 System (integrity) protection scheme

System integrity protection scheme[1] is an automatic protection system designed to detect abnormal or predetermined system conditions and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability. Such actions may include changes in demand, generation or system configuration to maintain system stability, acceptable voltage or power flows.[2]

[SOURCE: North American Electric Reliability Corporation glossary]

Note: SOGL art.37 defines tasks to TSOs which use Special Protection Schemes

4 Abbreviated terms

CCR	Capacity Calculation Region
CGMES	Common Grid Model Exchange Standard
CIM	Common Information Model (electricity)
CSA	Coordinated Security Analysis
CSAm	Coordinated Security Analysis Methodology
EIC	Energy Identification Codes
ENTSO-E	European Network of Transmission System Operators for Electricity
HVDC	High Voltage Direct Current
IEC	The International Electrotechnical Commission
MAS	Model Authority Set
mRID	CIM Master Resource Identifier

[1] The system protection scheme (SPS) can be called system integrity protection schemes (SIPS) in some CCRs (e.g. Nordic CCR)

[2] North American Electric Reliability Corporation glossary

MTU	Market Time Unit
OCL	Object Constraint Language
OPC	Outage Planning Coordination
OWL	Web Ontology Language
RAO	Remedial Action Optimization
RCC	Regional Coordination Centres
RDF	Resource Description Framework
RDFS	RDF Schema
RefHour	Reference Hour
RSC	Regional Security Coordinator
SHACL	Shapes Constraint Language
SOC	ENTSO-E System Operations Committee
SOGL	System Operations Guideline
SIPS	System Integrity Protection Scheme
STA	Short Term Adequacy
TSO	Transmission System Operator
UCTE DEF	Union for the Coordination of the Transmission of Electricity Data Exchange Format
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
XML	Extensible Markup Language
XNE	Cross-border relevant Network Element
XRA	Cross-border relevant Remedial Action
XSD	XML Schema Definition

5 Coordinated security analysis business process

5.1 Overview

The coordinated security analysis data exchange specification defines the data exchange format for the coordinated security analysis. It covers both Inter-RSC coordination and coordinated regional security analysis (for day ahead and intraday, and for different CCR).

Inter-RSC Coordination is required by SOGL for RSCs when performing their tasks defined in SOGL (Art 77 to 81) at CCR level. CSA methodology (CSAm) developed pursuant to SOGL Article 75 provides a set of requirements for TSOs and RSCs, aimed at defining what is the content and objectives of this inter-RSC coordination. The adopted version of CSAm also emphasizes the inter-CCR coordination aspects.

The regional and cross-regional day-ahead process major steps and timings are defined in the CSAm Article 33. The process is divided in four phases.

- **Preparation - until T0:** This corresponds to the preparation of the SOs' IGMs and of all relevant information (updates of available remedial actions, contingencies, …)

- **Coordination Run 1 – from T0 to T2:** From T0 to T1 (at max) the process until the CGM is available (for 24 hours of next day). From CGM availability (max at T1) to T2:

all the phases of regional and cross regional security analyses (contingency analysis, remedial action optimization, coordination) and its possible loops.

- **Coordination Run 2 – from T2 to T4:** From T2 to T3 (at max) the process until an updated CGM is available (for 24 hours of next day); this CGM includes all agreed preventive remedial actions; other information is also updated and shared (agreed curative remedial actions, new forecasts, any other changes to the inputs). From CGM availability (max at T3) to T4: all the phases of regional and cross-regional security analyses (contingency analysis, remedial action optimization, coordination) and its possible loops.

- **Final Validation – from T4 to T5.**

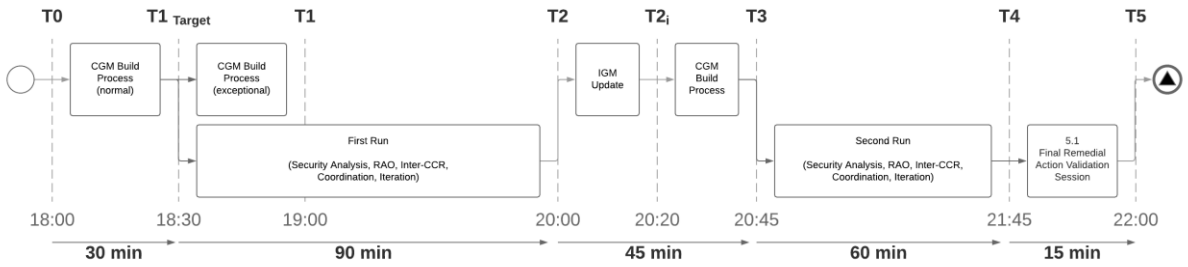

Figure 1 – Main steps on regional and cross-regional day-ahead process

Each coordination run includes the building of a CGM model, a regional security analysis and remedial action optimization with an inter-RSC and inter-CCR coordination.

The second coordination run is performed to evaluate the combined effects of all remedial actions preliminary agreed in the first one and to improve/correct where necessary. This second coordination run may also benefit of more recent forecast updates.

For intraday process, steps and timings are described below

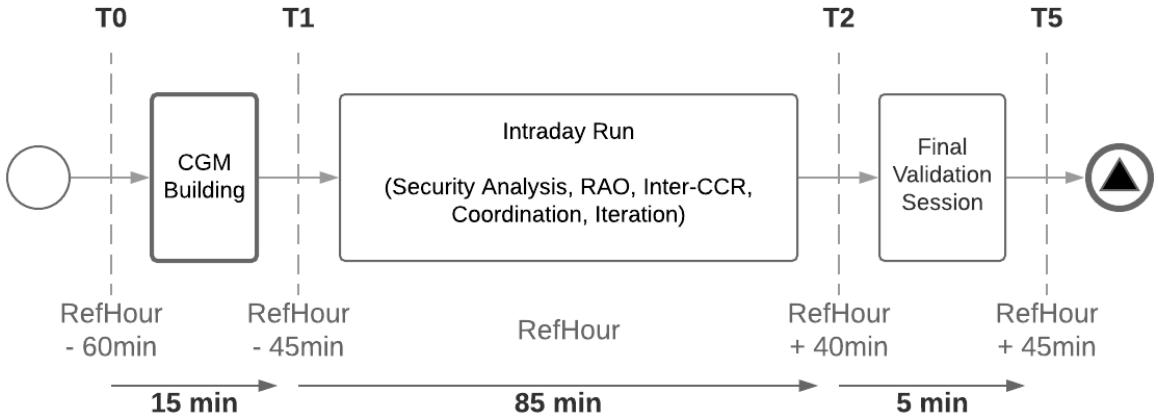

Figure 2 - Intraday process, steps and timings

- **Until RefHour - 60min:** The IGMs are made available for the following hours, at least from RefHour +1 until RefHour +9 (and preferably until end of the day).

- **From RefHour - 60min to RefHour - 45min:** The CGM is made available.
- **From RefHour - 45min To RefHour + 40min:** The regional and cross-regional process are executed.
- **From RefHour + 40min To RefHour + 45min:** The intraday final validation is executed.

5.2 Use cases

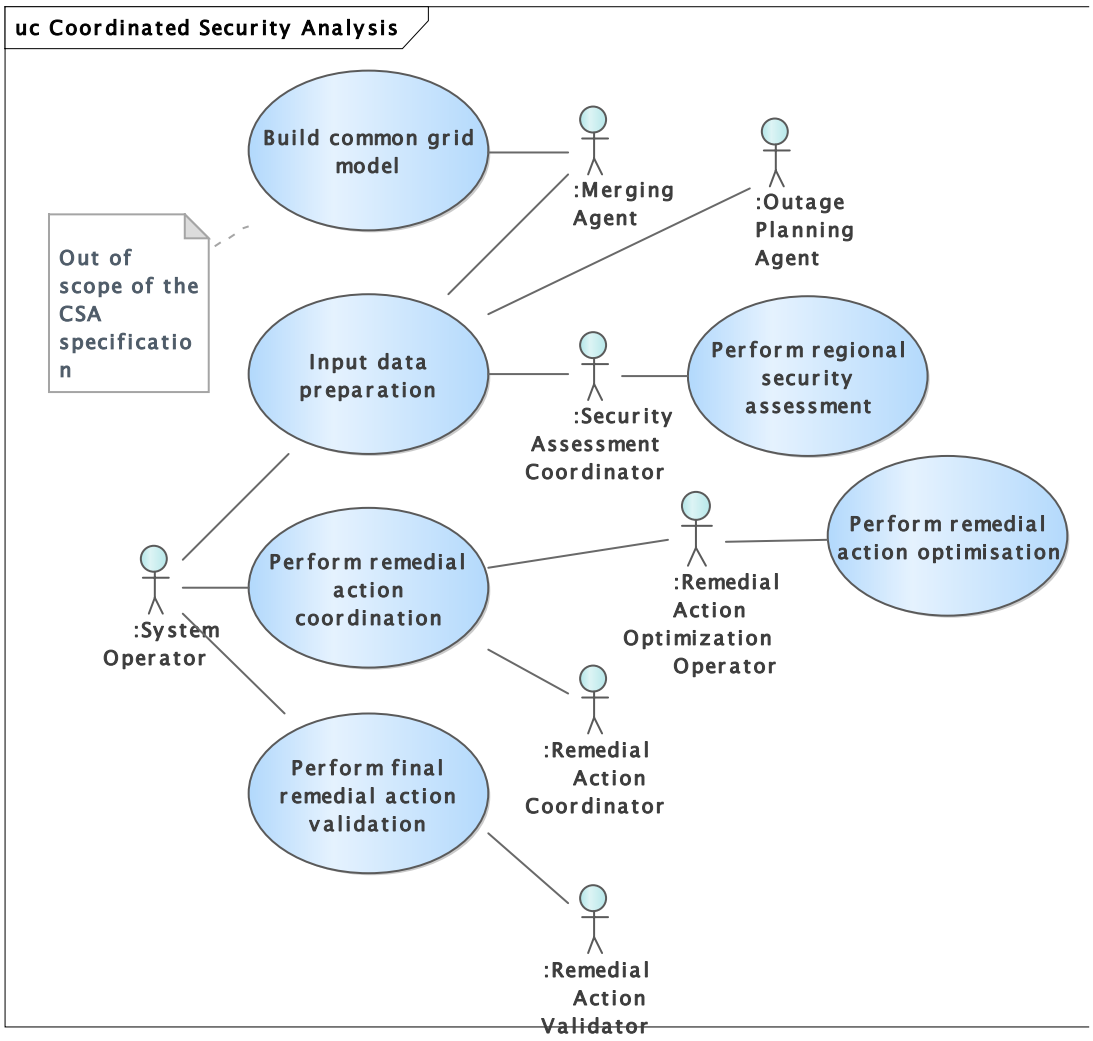

Figure 3 - Use Cases

463 Table 1 gives a list of roles involved in the CSA business process.

464 **Table 1 - Role labels and descriptions**

Role Label	Role Description
Merging Agent	The Merging Agent is responsible to gather the IGMs from SOs and build the CGM. The Merging Agent provides the CGM to the security assessment coordinator, who uses it as an input to perform the security analysis.
Outage Planning Agent	Outage Planning Agent provides the availability plan to the security assessment coordinator who uses this in case a remedial action would be the cancellation or shortening of an outage plan.
System Operator	Within CSA business process, SO provides most of the needed inputs to perform the security analysis. This role also participates in the remedial action coordination agreeing or rejecting the remedial actions.
Security Assessment Coordinator	The Security Assessment Coordinator is in charge of performing the security assessment against contingencies in order to identify potential congestions in the grid and propose to the SO a set of remedial actions to solve the found issues.
Remedial Action Optimization Operator	Remedial Action Optimization Operator performs the remedial action optimization on the basis of security assessment result before RAO and available remedial actions
Remedial Action Coordinator	The Remedial Action Coordinator main task is to get the agreement on all proposed remedial actions identified by the remedial action optimization step and potentially any additional remedial actions specifically requested by a SO.
Remedial Action Validator	The main activity of the Remedial Action Validator during the final validation session is to review unresolved relevant identified constraints (on assessed elements), discuss/find possible follow-up activities by TSOs and RSCs and deliver the conclusions.

465 Table 2 gives a list of use cases for the CSA business process.

466 **Table 2 - CSA use cases**

Use case label	Roles involved	Action descriptions and assertions
Input data preparation	SO, Merging Agent, Outage Planning Agent, Security Assessment Coordinator	In order to allow the representation of the grid as well as the proper assessment of its security and the identification of potential effective and efficient remedial actions for the mitigation of identified constraints, the SO shall provide the list of assessed elements, contingencies, remedial action (including SIPS) and equipment reliability (e.g. Power transfer Corridor, reliability limits, etc) and Steady State Instructions. Optionally Generation and Load Shift keys can be provided. SO shall provide as well its IGM to the Merging Agent, who builds the CGM as input to the CSA process. Outage Planning Agent provides the availability plan. Finally, the security assessment coordinator performs a business check on all the received data.
Build common grid model	Merging Agent	Merging agent builds the CGM as the comprehensive aggregation and calculation on

		the basis of the IGMs and some relevant additional input data (e.g. boundary information reference data); this is out of the scope of this document and part of the CGM Building Process.
Perform regional security assessment	Security Assessment Coordinator	The Security Assessment Coordinator performs the security assessment against contingencies in order to identify potential congestions in the grid. This security assessment is run according to rules defined in the CCR Article 76 methodology (at least flows and potentially other aspects of security).
Perform remedial action optimization	Remedial Action Optimization Operator	The Remedial Action Optimization Operator performs the remedial action optimization to select the most suitable remedial actions to operate the network efficiently while ensuring security of supply.
Perform remedial action coordination	SO, Remedial Action Optimization Operator, Remedial Action Coordinator.	The Remedial Action Coordination is divided in two steps. The first step consists on managing the Inter-CCR interactions. The purpose is to apply rules (According to CSAm Art. 27) to address the cross-impacts between CCRs on the overlapping zones. In the second step, the impact assessment of all proposed and adjusted remedial actions is performed. This impact assessment consists of identifying the affected SOs for each remedial action, based on the rules defined in the CCR Article 76 methodology (qualitative and/or quantitative rules) and rules for inter-CCR impact (these rules will be defined according to the amendment of CSAm Article 27).
Perform final remedial action validation	Remedial Action Validator, SO	The main activity during the final validation session is to review unresolved relevant identified constraints (on assessed elements), discuss/find possible follow-up activities by SO and Remedial Action Validator and record the conclusions. Remedial Action Validator shall provide the results and decisions to the SO.

467
468

5.3 Sequence diagram

Next figure shows a sequence diagram with the inputs of the CSA data exchange process.

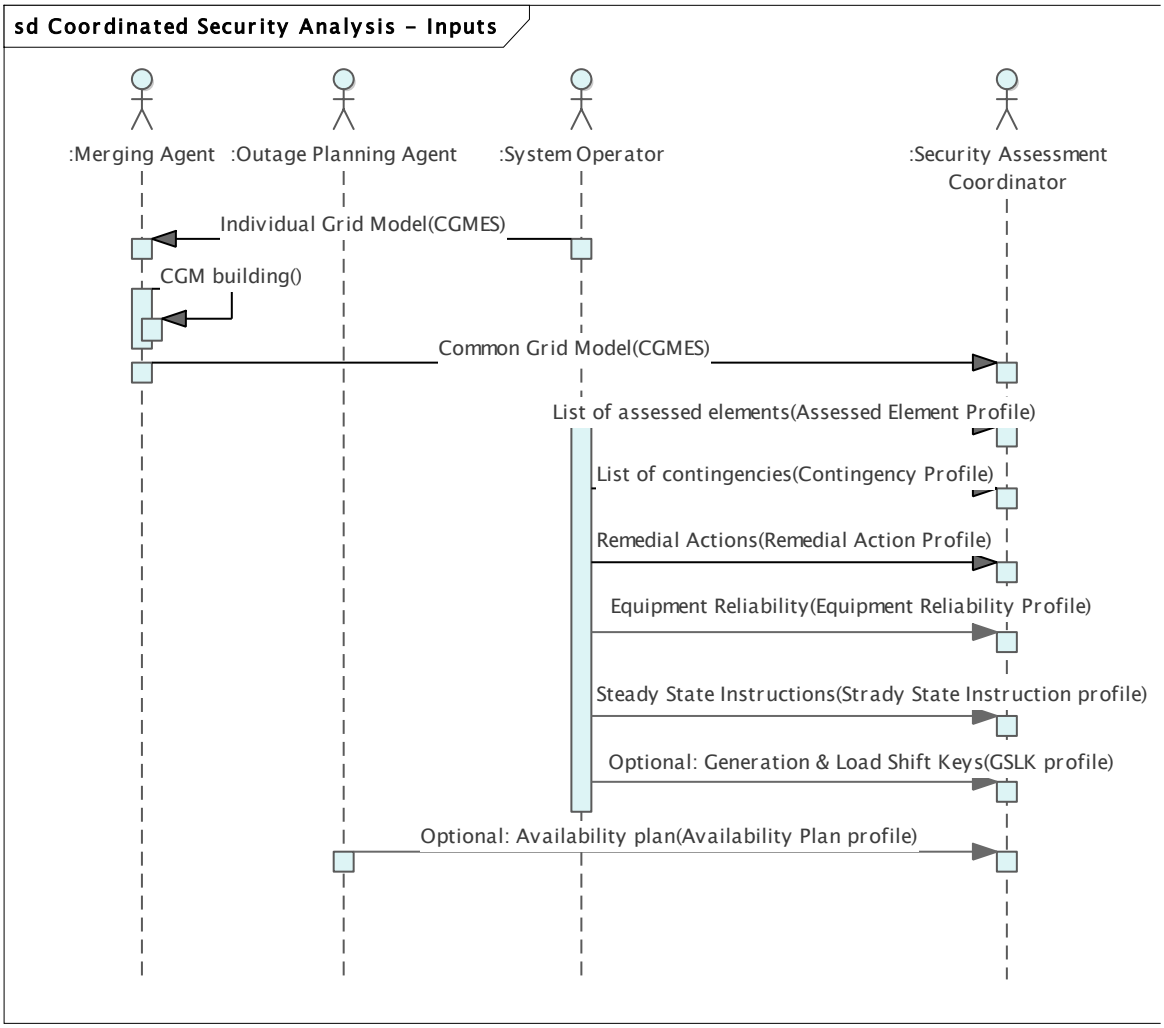

Figure 4 – CSA inputs Sequence diagram

First of all, the process starts with the submission of the Individual Grid Model from each SO to the Merging Agent. Please notice that each IGM is composed by at least four profiles (e.g. Equipment, Topology, Steady State Hypothesis and State Variables). The frequency of submission of these profiles is different. In the case of equipment and topology and their boundaries have to be submitted when there are equipment or topology changes. For steady state hypothesis and state variables, they will have to be submitted per market time unit (e.g. 1 hour or 15 min resolution). Merging Agent merges all the IGMs and provides the CGM to the Security Assessment Coordinator.

The System Operator provides the list of assessed elements, contingencies, remedial actions, equipment reliability, steady state instructions and optionally, the GLSK. Outage planning agent provides the availability plan which is an output of the OPC process.

Next figure shows a sequence diagram of the CSA data exchange process

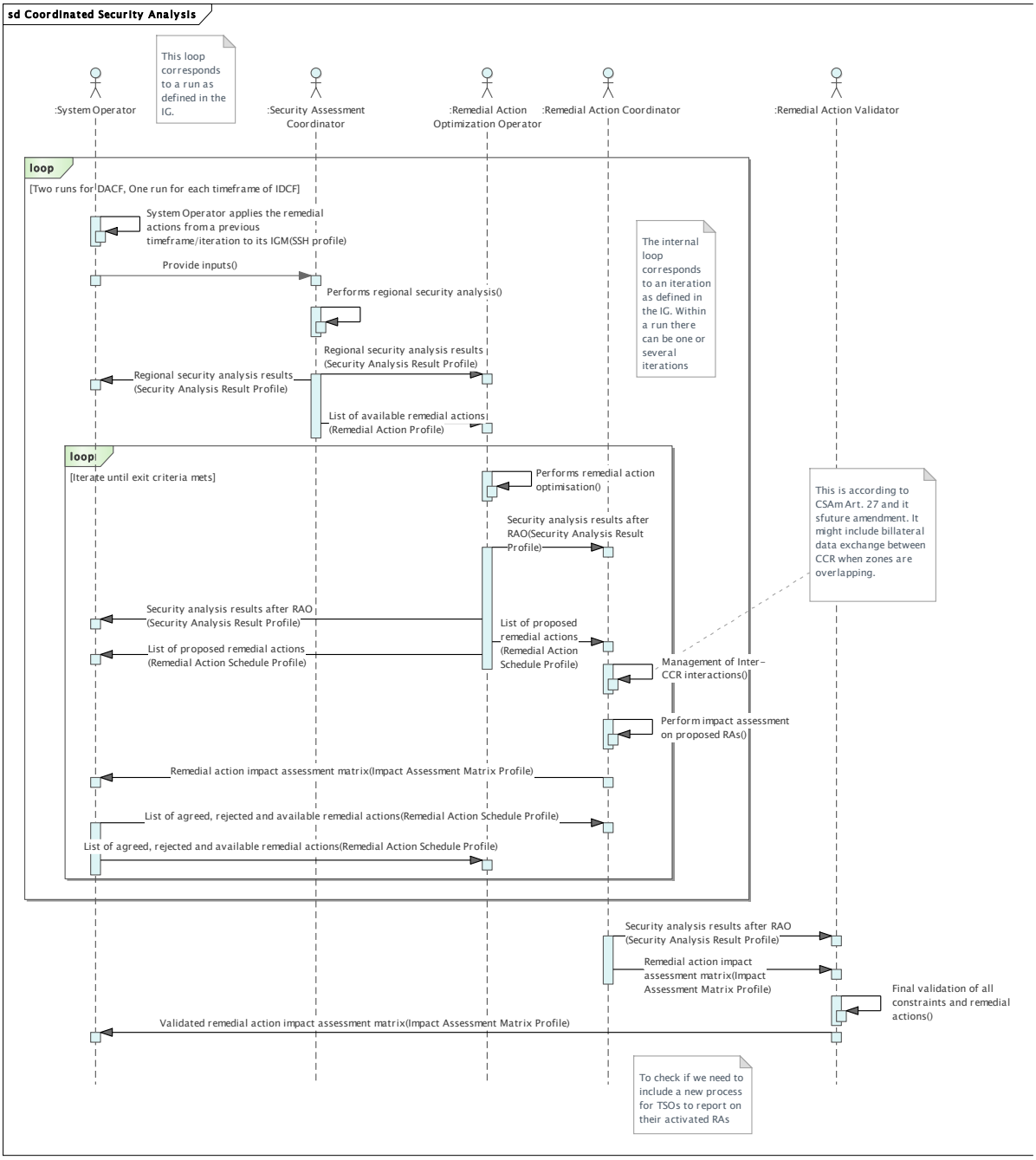

Figure 5 - CSA general sequence diagram

With all the inputs, Security Assessment Coordinator runs the regional security analysis. Basically, the security assessment allows to identify potential congestions in the grid. The result of this contingency analysis contains the identified limit violations in both base case (N situation) and considering contingencies (N-1, N-2 situation). Apart from the violations, Security Assessment Coordinator also provides the available remedial actions to the Remedial Action Optimization Operator. The available remedial actions are the remedial actions which are available to solve identified constraints.

The remedial action optimization is performed for each Capacity Coordination Region. As a result of the optimisation, the security analysis after RAO and a list of proposed remedial actions are delivered to both System Operator and Remedial Action Coordinator.

After that, Remedial Action Coordinator addresses the inter-CCR interactions which consists in addressing the cross-impacts between CCRs on the overlapping zones. Just after the CCR interactions, remedial action coordinator performs the impact assessment on the proposed remedial actions. The outcome of this process is the impact assessment matrix. The main purpose of the matrix is to identify the affected SOs for each remedial action. The impact assessment matrix is delivered to the SOs. Each SO shall agree or reject each remedial action by which it is impacted. If a SO rejects a remedial action, it shall provide the reasoning and (optionally) suggest alternative new available remedial actions or modified available remedial actions. Both optimization and coordination are repeated during several iterations until an exit criterion meets. The exit criteria can be, for instance, when all the identified constraints have been solved with the agreed remedial actions, or time limit is reached.

The big loop is also defined as run. In Day-Ahead there will be two runs and in Intraday only one. Basically, for the day ahead, the process is repeated twice.

After coordination, a final remedial action validation session is performed by the remedial action validator which receives from remedial action optimization operator the security analysis results and the impact assessment matrix. The main activity during the Final Validation Session is to review unresolved relevant identified constraints (on assessed elements) and discuss or find possible follow-up activities by SOs and Remedial Action Validator. Finally, the validated impact assessment matrix is delivered to the System Operator and the process finishes.

5.4 State diagrams

5.4.1 Remedial action state diagram

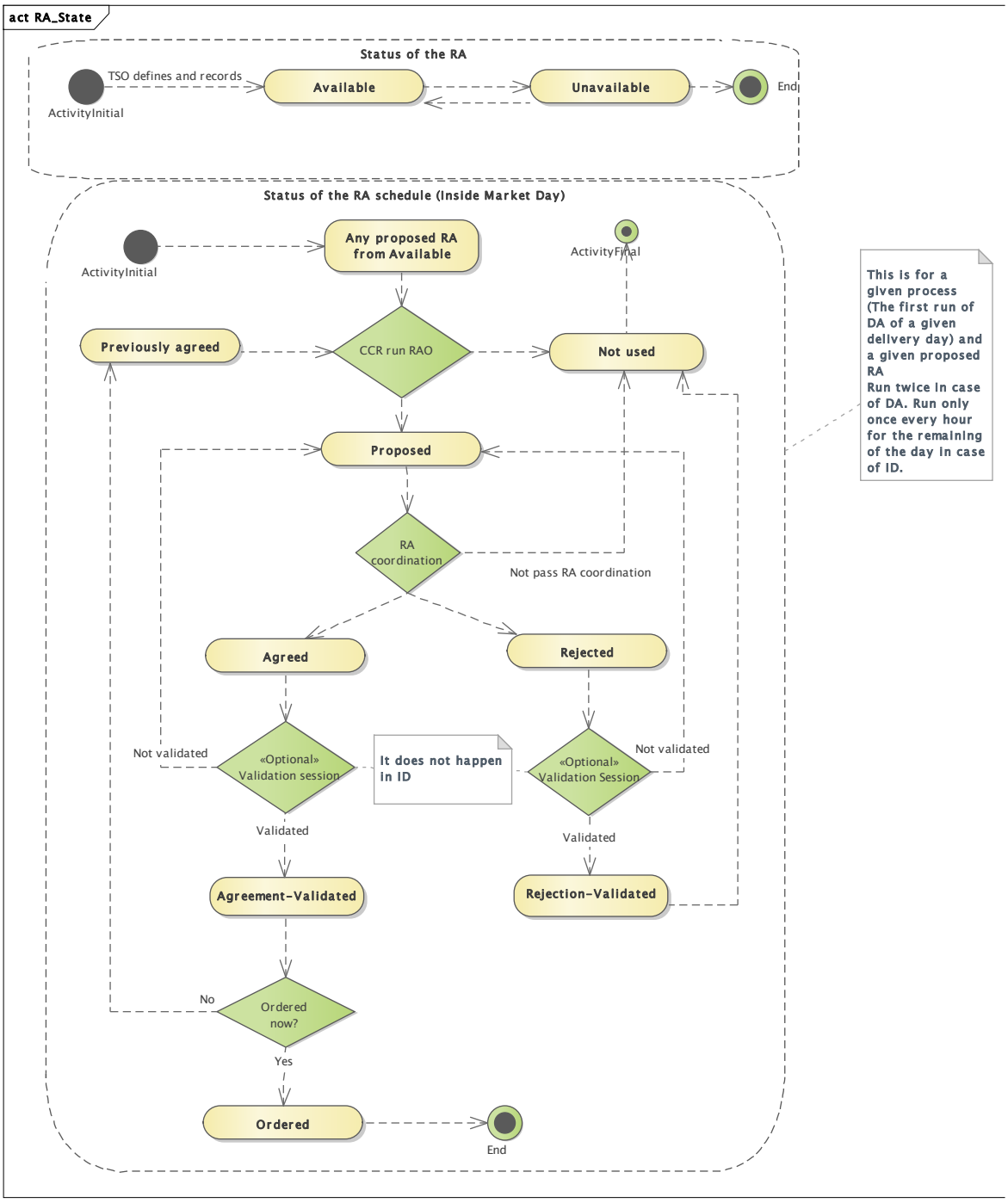

Figure 6 - Remedial action state diagram

System operator can define a set of remedial actions in the system. Once defined, an remedial action can be considered as available, in this case the remedial action can be taken into account when running the CSA process or unavailable in case that an remedial action cannot be used. In case that a remedial action is not needed anymore, once it is disabled, then it can be archived for tracking and historic purposes.

All available remedial actions can be used for the remedial action optimization process which will choose the most appropriate remedial actions to solve the different issues in the scenario. These remedial actions are denominated as proposed remedial action.

Just after the remedial action optimisation process is finished, remedial action coordination starts. If the remedial action does not pass the coordination, then it becomes available again. If it passes the coordination, the remedial action can be agreed or rejected. These two states must be validated during the validation session. If they are not finally validated, they become available again.

In case that a rejected remedial action is agreed, then it becomes proposed and could be used again as an input for the remedial action optimisation process. On the other hand, for the agreed remedial actions that are validated they can be activated now or in a later stage. In case that an remedial action is not activated now, then it becomes a previously agreed remedial action. If it is activated now, then the remedial action changes its status to activated and the process finishes.

5.4.2 Contingency category diagram

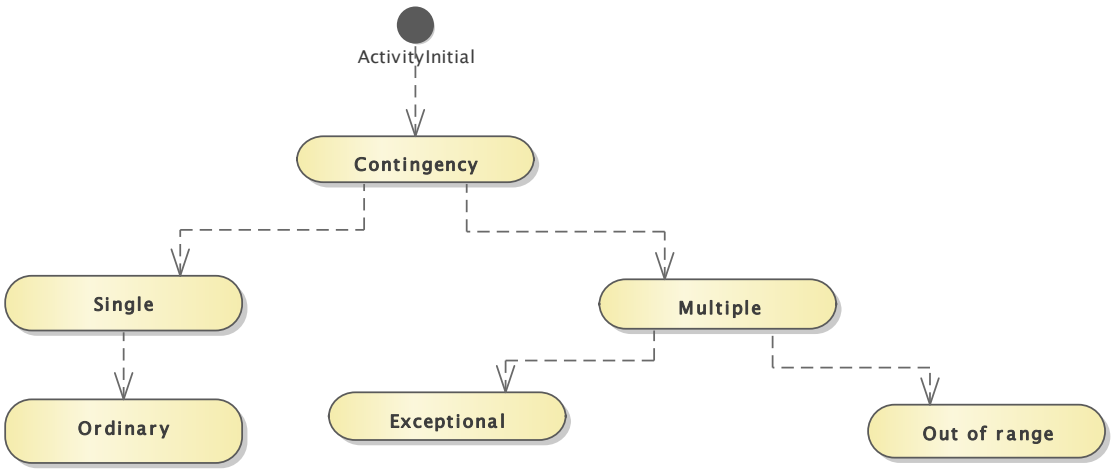

Figure 7 - Contingency category diagram

We can have single and multiple contingencies. A single contingency can contain a single contingency element (often referred to as n-1 contingencies) and a multiple contingency can contain several contingency elements (n-x).

Within the single group of contingencies, we only have ordinary contingencies. An ordinary contingency means the occurrence of a contingency of a single branch or injection

Within the multiple groups of contingencies, we have exceptional contingencies which means the simultaneous occurrence of multiple contingencies with a common cause, and out of range contingencies which means the simultaneous occurrence of multiple contingencies without a common cause, or a loss of power generating modules with a total loss of generation capacity exceeding the reference incident

5.4.3 Network element category diagram

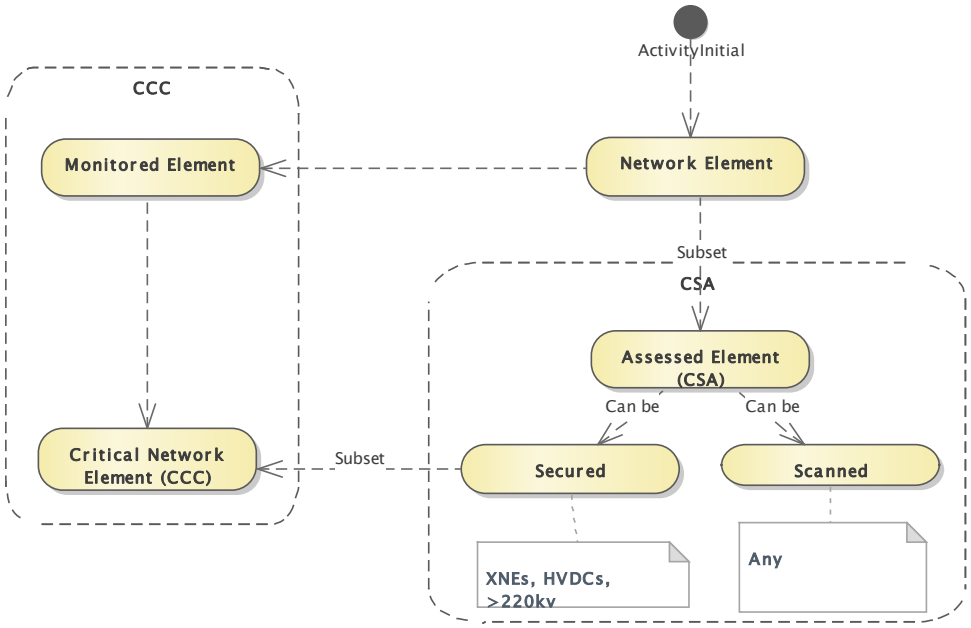

Figure 8 – Network element category diagram

Any network element could be an assessed element in CSA. The assessed elements can be secured or scanned. A Secured element is an Assessed Element on which remedial actions needed to relief these violations shall be identified, when violations of an operational security

limit are identified during the regional or cross-regional security analysis. A secured element could be a cross network element, HVDC lines or lines over 220 KV.
A scanned is an Assessed Element on which the electrical state (at least flows) shall be computed and shall be subject to an observation rule during the regional security analysis process. Such observation rule can be for example avoiding the increase of a constraint or avoiding the creation of a constraint on this element, as a result of the design of remedial actions needed to relieve violations on the secured elements. A scanned element could be any gird element.
A critical network element is a network element monitored during the coordinated capacity calculation process. Critical network elements are a subset of the secured elements.

5.5 Other diagrams

5.5.1 System Integrity Protection Schemes (SIPS) overview

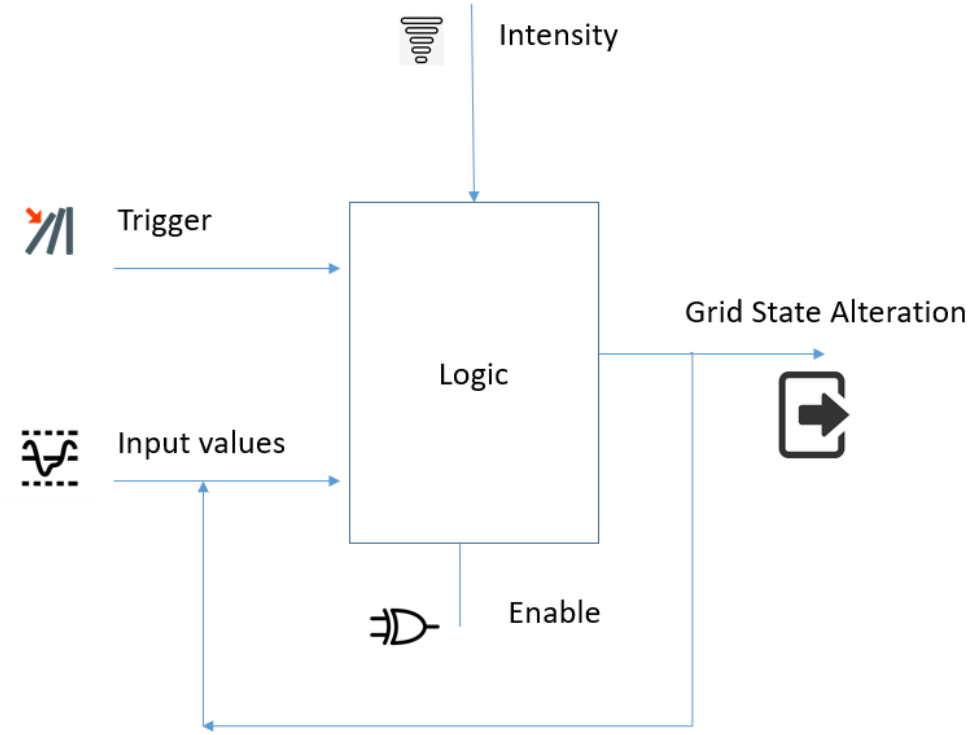

Figure 9 - SIPS overview

System Integrity Protection Schemes (SIPS) / Remedial Action Schemes (RAS) are often applied by TSOs to utilize the transmission capacity beyond conventional N-1 considerations. This is done while still maintaining reliability of supply, for example by relieving overloaded lines through immediate disconnection of generator units when lines are disconnected by their protective relay equipment. Other schemes are also in use, such as emergency power on HVDC links, load shedding and network splitting. Without modelling SIPS or RAS unrealistic congestion/overload will be reported by the power flow simulation tools.

As shown in Figure 9, a SIPS is based on a logic which has inputs signals and related triggers to start the logic. Depending on the logic conditions and the intensity of the event, if the logic is enabled, the output of the SIPS will result in a grid state alteration.

The following are some examples of the objectives of system-wide protection/control schemes:

- Overload mitigation
- System separation for transient stability
- Load and generation shedding/rejection
- Under and over Voltage load shedding
- Under and over Frequency generation/load shedding
- Detection/shutdown of islanded network
- Over Frequency tripping of unloaded generators
- Improvement of power transmission to increase total transfer capability
- Improvement of system stability under the large deployment of renewable energy resources
- Maximize the capability of apparatus (the thermal limit of apparatus**).**

611 Any values described in SteadyStateHypothesisProfile (SSH) can be input values or Grid
612 State Alteration value.

6 Application profile specification

6.1 General

CSA business process relies on data exchange standards to exchange the information on the base power flow case. These are models representing IGMs and CGMs. In addition, the CSA needs information on remedial actions, assessed elements, contingencies, etc in order to complete the data needed to perform the coordinated security analysis. The additional information is supplied by the following profiles:

- Remedial action profile
- Assessed element profile
- Contingency profile
- Equipment reliability profile which includes SIPS configuration, security limits, Power Transfer Corridor
- Generation and Load Shift Key profile
- Availability plan profile
- Remedial action schedule profile
- Security analysis result profile
- Impact assessment matrix profile
- Steady state instruction profile

6.2 Compatibility with other data exchange standards

Profiles that will be used for CSA process are designed in a way that they are compatible with both CGMES v2.4 (IEC TS 61970-600-1 and -2:2017) and CGMES v3.0 (IEC 61970-600-1 and -2:2021). However, the following attention points shall be noted:

- If CGMES v2.4 is used to represent the IGM and CGM the remedial action cannot efficiently model power electronics and battery units as these objects are only available in CGMES v3.0

- The information about the operational limits is exchanged in the equipment instance data in the case of CGMES v2.4 based data exchange. Therefore, when there is a need to frequently update the information on the limits, this will require that equipment data is exchanged more frequently or that difference equipment profile shall be used to optimize the data exchange. This limitation does not occur if the IGM and CGM are using CGMES v3.0 as the operational limits is exchanged in the steady state hypothesis instance data.

- In order to achieve an optimal information exchange, it is assumed that persistent identifiers are used for the IGM and CGM objects. Applying CSA profiles as add-on to an exchange which does not rely on persistent identifiers will create a lot of overhead for the exchange eventually leading to a decreased reliability of the whole process.

The usage of UCTE DEF as a data exchange format for IGM and CGM for the purpose of CSA process is not recommended in conjunction with this set of profiles, for the following non-exhaustive list of reasons (to name a few):

- CSA profiles metadata require linkage with the IGM and CGM. UCTE DEF models are identified by file name. Therefore, an additional metadata layer must be added.

- CSA profiles require references to identifiers of the elements from IGM in order to link the remedial actions, assessed elements, etc. UCTE DEF used node codes and circuit

numbers (for interconnecting elements) in order to uniquely identify them. Therefore, if UCTE DEF is used there will be a need to maintain a list of persistent identifiers and their relationship with node names or elements names.

- CSA requires information on different operational limits that are related to the different time phases to be studied. UCTE DEF has very limited capabilities to exchange limits.

- Due to the scope of the UCTE DEF the CSA would be limited in terms of what kind of grid state alterations and remedial actions could be described and considered in the coordination process. Identification of type and modelling of the network elements that support voltage control, shunt-connected reactive devices, voltage regulation on transformers in case of regulator being modelled on the non-regulated power transformer end, will require special attention as they are not in scope of UCTE DEF and will be impossible to model without extending UCTE DEF.

- Generation capacity used as part of remedial actions should be modelled in detail due to limits handling in case of aggregated modelling.

- UCTE DEF does not separate the information related to the equipment, the information related to the operating point and it also does not cover the solution information. Data consistency changes between data exchanged with CSA profiles and UCTE DEF data will be more extensive (full model exchange), have high dependencies over mapping tables that have to be integrated in the middleware, and will not benefit from using one equipment model for multiple time stamps.

- UCTE DEF does not allow exchange of power flow solution data, therefore this report will have to be standardized (out of scope of this document) to achieve full information exchange.

- Use of replaced IGM in created CGM is not possible to trace in case of UCTE DEF, that might complicate the process of CSA data validation against the grid models and remedial action applicability.

6.3 Constraints naming convention

The naming of the rules shall not be used for machine processing. The rule names are just a string. The naming convention of the constraints is as follows.

“{rule.Type}:{rule.Standard}:{rule.Profile}:{rule.Property}:{rule.Name}”

where

rule.Type: C – for constraint; R – for requirement

rule.Standard: the number of the standard e.g. 301 for 61970-301, 456 for 61970-456, 13 for 61968-13. 61970-600 specific constraints refer to 600 although they are related to one or combination of the 61970-450 series profiles. For NC profiles, NC is used.

rule.Profile: the abbreviation of the profile, e.g. TP for Topology profile. If set to “ALL” the constraint is applicable to all IEC 61970-600 profiles.

rule.Property: for UML classes, the name of the class, for attributes and associations, the name of the class and attribute or association end, e.g. EnergyConsumer, IdentifiedObject.name, etc. If set to “NA” the property is not applicable to a specific UML element.

rule.Name: the name of the rule. It is unique for the same property.

Example: C:600:ALL:IdentifiedObject.name:stringLength

6.4 Data exchange specification constraints

This clause defines requirements and constraints that shall be fulfilled by applications that conform to this document.

- R:NC:ALL:Region:reference

  The reference to the region is normally a reference to the capacity calculation region, which is identified by “Y” EIC code of the capacity calculation region.

- R:NC:ALL:SystemOperator:reference

  The reference to the System Operator is normally identified by “X” EIC code of TSO.

6.5 Metadata

ENTSO-E agreed to extend the header and metadata definitions by IEC 61970-552 Ed2. This new header definitions rely on W3C recommendations which are used worldwide and are positively recognised by the European Commission. The new definitions of the header mainly use Provenance ontology (PROV-O), Time Ontology and Data Catalog Vocabulary (DCAT). The global new header is included in the metadata and document header specification document.

The header vocabulary contains all attributes defined in IEC 61970-552. This is done only for the purpose of having one vocabulary for header and to ensure transition for data exchanges that are using IEC 61970-552:2016 header. This specification does not use IEC 61970-552:2016 header attributes and relies only on the extended attributes.

6.5.1 Constraints

The identification of the constraints related to the metadata follows the same convention for naming of the constraints as for profile constraints.

- R:NC:ALL:wasAttributedTo:usage

  The prov:wasAttributedTo should normally be the “X” EIC code of the actor (prov:Agent).

- R:NC:ALL:version:usage

  Coordinated security analysis process requires an information about the number of iteration within a given coordination run to be exchanged as metadata. The attribute dcat:version indicates the version of the model that is serialised in the document where the header is located. Within a coordination run the underling model (the individual grid model) is not changed while in each iteration within the coordination run the model of remedial action and potentially other related models representing CSA profiles change. As the dcat:version is indicating the version of the model, e.g. remedial action, it is the attribute to be used to indicate the iteration number within a coordination run.

- R:NC:ALL:wasInfluencedBy:minimumRequirement

  The attribute prov:wasInfluencedBy indicates the dependency of a given model from another one. The following figure defines the minimum requirement for the references that need to be provided in the document header of all models that conform to CSA profiles.

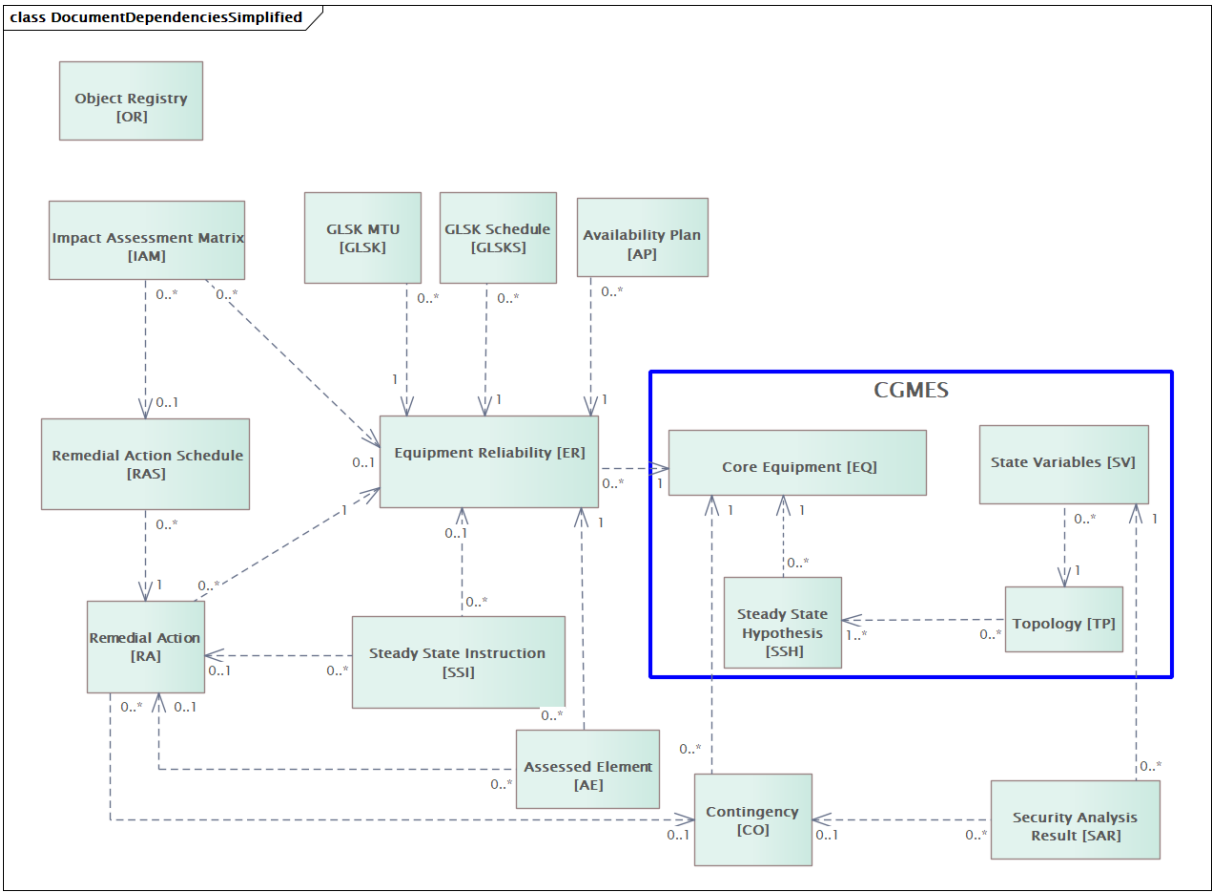

Figure 10. Document header dependencies minimum requirement

6.5.2 Reference metadata

ENTSO-E header and metadata project group is in charge of providing guidance on how to use the reference data and where it is stored. Business processes utilizing the CSA profiles should liaise with above mentioned ENTSO-E project.

The header defined for CSA profiles and included in each profile required availability of a set of reference metadata:

- accessRights: to be defined;
- accrualPeriodicity: should refer to ENTSO-E codelist;
- businessProcess: should refer to ENTSO-E codelist;
- atLocation: should refer to the ENTSO-E Central Issuing Office list of Y-EIC code;
- creator: should refer to the ENTSO-E Central Issuing Office list of X-EIC code;
- wasAttributedTo: should refer to the Central Issuing Office list of X-EIC code;
- keyword: should refer to ENTSO-E codelist;
- type: should refer to ENTSO-E codelist;
- wasGeneratedBy: to be defined.

mult.	Header attributes	Description	Assessed element	Contingency	Remedial Action	Remedial Action Schedule	Impact assesment matrix	Security analysis result	Equipment Reliability	GLSK	Availability plan	Steady instruction profile
[0..1]	md:created		N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A
[0..1]	md:modellingAuthoritySet		N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A
[0..1]	md:scenarioTime		N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A
[0..n]	md:profile		N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A
[0..n]	md:Model.DependentOn		N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A
[0..n]	md:Model.Supersedes		N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A
[0..1]	md:version		N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A
[0..1]	md:description		N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A
[0..1]	prov:generatedAtTime	The date and time when the model was serialized in the document where the header is located.	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1
[0..1]	prov:atLocation	Reference to a region or a domain for which this model is provided	N\A	N\A	N\A	N\A	Optional 0..1	N\A	N\A	N\A	N\A	N\A
[0..n]	prov:wasInfluencedBy	A reference to the model on which the model serialised in this document depends on.	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n
[0..n]	prov:hadPrimarySource	The version of the MAS from where a version of a model is originating.	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1
[0..n]	prov:wasGeneratedBy	Run. Reference to an activity or the exact business nature (process, configuration) which produced or uses the model	N\A	N\A	N\A	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	N\A	N\A	N\A	N\A
[0..n]	prov:wasAttributedTo	Sender. Reference to the agent (or service provider) from which the model originates.	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1
[0..n]	prov:wasRevisionOf	revisionNumber. When a model is updated the resulting model supersedes the models that were used as basis for the update. Hence this is a reference to the model which are superseded by this model. A model can supersede 1 or more models	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1
[0..n]	prov:specializationOf	Relates to the model. The version of the MAS that is managing the version of the model.	N\A	N\A	N\A	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	N\A	N\A	N\A	N\A
[0..1]	time:hasXSDDuration	The duration of the validity period of the model that it is serialized in the document where the header is located. It is only used in relation to the inXSDDateTimeStamp property which indicates the beginning of the validity period of the model. The end of the validity period is derived from both inXSDDateTimeStamp and hasXSDDuration	Optional 0..1	Optional 0..1	Optional 0..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1
[0..1]	time:inXSDDateTimeStamp	The date and time that this model represents, i.e. for which the model is (or was) valid. If used n relation with hasXSDDuration it indicates the beginning of the validity period.	Optional 0..1	Optional 0..1	Optional 0..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1
[0..1]	euvoc:status	Indicates the status of a skos:Concept or a skosxl:Label, or any resource related to controlled vocabulary management.	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1
[0..1]	eumd:applicationSoftware	Identifies the application software which generated this instance file	N\A	N\A	N\A	N\A	N\A	Optional 0..1	N\A	N\A	N\A	N\A
[0..n]	eumd:usedSettings	powerflow settings	N\A	N\A	N\A	N\A	N\A	Optional 0..1	N\A	N\A	N\A	N\A
[0..1]	eumd:processType	The exact business nature. Reference to Business Process configurations.	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1
[0..1]	eumd:serviceLocation	Reference to a service location (region or a domain).										
[0..1]	dcterms:description	A free-text account of the item.	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1
[0..1]	dcterms:accessRights	Information about who can access the resource or an indication of its security status	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1
[0..n]	dcterms:conformsTo	profile. An established standard to which the described resource conforms.	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n	Mandatory 1..n
[0..1]	dcterms:identifier	mRID. An unambiguous reference to the resource within a given context	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1
[0..1]	dcterms:license	A legal document under which the resource is made available.	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1
[0..1]	dcterms:rights	A statement that concerns all rights not addressed with dcterms:license or dcterms:accessRights, such as copyright statements.	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1
[0..1]	dcterms:rightsHolder	An unambiguous reference to the resource within a given context	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1
[0..1]	dcterms:type	type. The nature or genre of the resource.	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1
[0..1]	dcterms:accrualPeriodicity	The frequency at which dataset is published.	N\A	N\A	N\A	Mandatory 1..1	Mandatory 1..1		N\A	N\A	N\A	N\A
[0..1]	dcterms:creator	The entity responsible for producing the resource.	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1
[0..1]	dcat:keyword	A keyword or tag describing the resource.	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1
[0..1]	dcat:version	The version number of a resource	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1	Mandatory 1..1
[0..1]	dcat:previousVersion	The previous version of a resource in a lineage	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1
[0..1]	dcat:hasVersion	This resource has a more specific, versioned resource	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A
[0..1]	dcat:isVersionOf	The inverse of hasVersion	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A
[0..1]	dcat:hasCurrentVersion	This resource has a more specific, versioned resource with equivalent content	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1
[0..1]	adms:versionNotes	A description of changes between this version and the previous version of the resource	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1	Optional 0..1

For instance, the attribute prov:wasGeneratedBy requires a reference to an activity which produced the model or the related process. The activities are defined as reference metadata and their identifiers are referenced from the header to enable the receiving entity to retrieve the “static” (reference) information that it is not modified frequently. This approach imposes a requirement that both the sending entity and the receiving entity have access to a unique version of the reference metadata. Therefore, each business process shall define which reference metadata is used and where it is located.