ETSI GS ISI 006 V1.1.1 (2019-02)

GROUP SPECIFICATION

Information Security Indicators (ISI);
An ISI-driven Measurement and
Event Management Architecture (IMA) and CSlang - A common ISI Semantics Specification Language

Disclaimer

The present document has been produced and approved by the Information Security Indicators (ISI) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGS/ISI-006

Keywords

cyber-defence, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Information Security Indicators (ISI).

The present document is included in a series of 9 ISI 00N specifications. These 9 specifications are the following (see figure 0 summarizing how the various concept is involved in event detection and interactions between all parts):

- ETSI GS ISI 001-1 [1] addressing (together with its associated guide ETSI GS ISI 001-2 [2]) information security indicators, meant to measure application and effectiveness of preventative measures.

- ETSI GS ISI 002 [3] addressing the underlying event classification model and the associated taxonomy.

- ETSI GS ISI 003 [i.1] addressing the key issue of assessing an organization's maturity level regarding overall event detection (technology/process/ people) in order to weigh event detection results.

- ETSI GS ISI 004 [i.2] addressing demonstration through examples how to produce indicators and how to detect the related events with various means and methods (with a classification of the main categories of use cases/symptoms).

- ETSI GS ISI 005 [i.3] addressing ways to produce security events and to test the effectiveness of existing detection means within organization (for major types of events), which is a more detailed and a more case by case approach than ETSI GS ISI 003 one [i.1] and which can therefore complement it.

- **ETSI GS ISI 006 (the present document) addressing another engineering part of the series, complementing ETSI GS ISI 004 [i.2] and focusing on the design of a cybersecurity language to model threat intelligence information and enable detection tools interoperability.**

- ETSI GS ISI 007 [i.6] addressing comprehensive guidelines to build and operate a secured SOC, especially regarding the architectural aspects, in a context where SOCs are often real control towers within organizations.

- ETSI GS ISI 008 [i.7] addressing and explaining how to make SIEM a whole approach which is truly integrated within an overall organization-wide and not only IT-oriented cyber defence.

Figure 0 summarizes the various concepts involved in event detection and the interactions between the specifications.

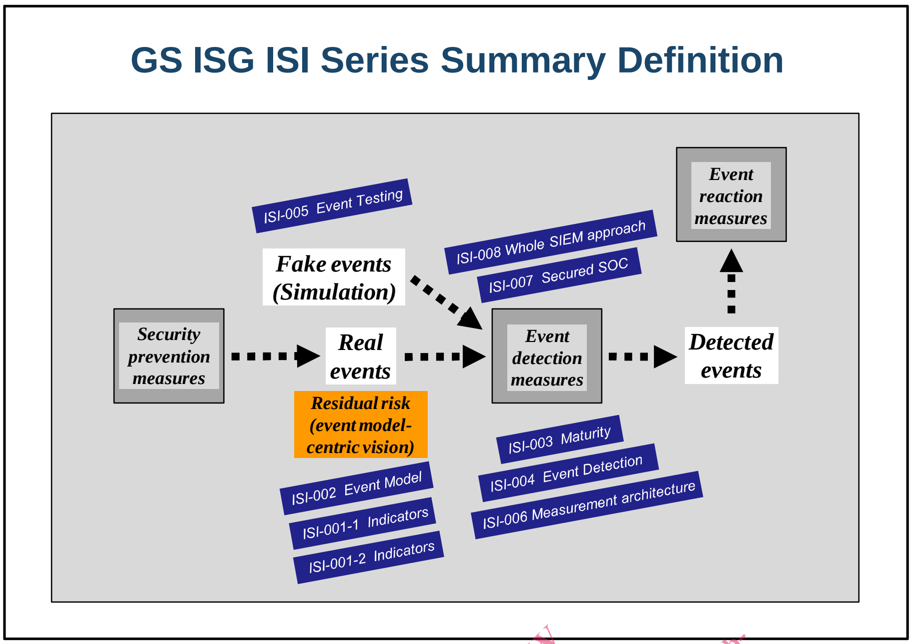

Figure 0: Positioning the 9 GS ISI against the 3 main security measures

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document proposes an ISI Measurement Architecture (IMA) for the management of security events captured and contained by the *ISI Data Lake (IDL)* and which comprises raw data enriched by methods derived from ML Algorithms of the AI domain.

By means of the IDL sets of raw data should be typed, categorized and enriched in a unique manner for which formal Set and Graph Manipulation (S/G M) Theories and Techniques are applied. The ML-based classification mechanism uses a-priori learned information of a so-called *ISI-type matrix* containing the tuple pairs of ISI query tuple and the associated typed target tuple.

The dynamics of automation and control systems is modelled by *data<n-tuple>space* with the basic operations of *publishing, subscribing, etc. in order to manage ISI events* (i.e. formally events are graph edges of the intended semantics) that occur in Industrial Automation and Control [i.9] or other Ultra Large-Scale Systems [i.20]. The *ISI Data Lake (IDL)* functions as an *asynchronous memory* managing multiple security events at same time.

The compound IMA/IDL approach of the present document is based on theories of manipulation of sets and graphs combined with ML algorithms where appropriate. The latter applies pattern recognition measures for the purpose of enriching, i.e. filtering the raw ISI data representations of <n-tuples> from the IDL.

The notation *CSlang* is given in an operational style that supports the definition of Abstract Data Types (ADT), ML pattern matrices and ISI events. Since *CSlang* is intentionally not defined by a full formal grammar it is thus to be considered as a semiformal approach. Nevertheless it is intended to provide basic **schemes of comprehension** that deal with properties, e.g. the semantics of a concrete *ISI Signature* using types with variables, that are called sorts and operations with constraints that define the constraints respectively the invariants (axioms) of a type.

Cyber Security and Incident Event Management is an upcoming issue that is currently handled by several Standardization Committees and Industrial Specification Groups working on ISI classification and Cyber Security Evaluation. Other standardization activities such as Incident response management of the ISO/IEC SC27 have recently started. By this and other issues of complex security and safety evaluation and incident responses a need of more formality has been identified. Thus many project ToRs have raised the need to put more resources on approaches based on formal semantics and ontologies. Consequently the present document proposes an advanced standard of a common semantics specification approach that is able to fill the identified formality gap.

1 Scope

The present document provides a common interaction semantics model called ISI Measurement Architecture (IMA) based on formal approaches that are partially leaned from **Set and Graph Theories**, such as [i.8] and [i.16], etc. Graph Theory is the semantics background to reason by simulation, using appropriate tools. Between both, i.e. a foreground ontological specification and a background graph semantics pattern - a structure-preserving relationship should exist.

The given approach of the present document is meant among other things to support the incident reaction operation analysis performed by the staff of SOCs, in order to decide reasonably on observed security events and related measures. More specifically all stakeholders (CISOs, IT security managers, Designers, Programmers, etc.) get on hand a Common *ISI Semantics* Specification Language (called *CSlang*) which enables stakeholders to communicate in a common unique way to each other based on graph semantics. *CSlang* is designed to be a dialect of the **Common Logics(CL)** defined by the ISO/IEC SC32 Committee on Data Interchange in the international standard IS 24707 that share a uniform semantics based on *Traditional First Order Logics with Equality (TFOL)* according to [i.17] and [4].

The present document is structured as follows (after clauses 2 and 3 respectively dedicated to references and definition of terms, symbols and abbreviations):

- **Clause 4** describes models and methods of the ISI Measurement Architecture, including the challenge of transforming ISIs into knowledge about incidents.
- **Clause 5** invents advanced Common Logics (CL) concepts of the ISI Semantics Specification Language - CSlang.
- **Annex A** presents the Proof of Concepts (PoC) by aligning ontology specifications to graph specifications of the two levels of Semantics Approach.
- **Annex B** presents mathematical basic definitions of graph manipulation theory.
- **Annex C** documents authors and contributors.
- **Annex D** documents applied bibliography of semantic.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS ISI 001-1: "Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture".

[2] ETSI GS ISI 001-2: "Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1".

[3] ETSI GS ISI 002: "Information Security Indicators (ISI); Event Model A security event classification model and taxonomy".

[4] ISO/IEC 24707: "Information Technology - Common Logic - A Framework for a Family of Logic-based Languages".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS ISI 003: "Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection".

[i.2] ETSI GS ISI 004: "Information Security Indicators (ISI); Guidelines for event detection implementation".

[i.3] ETSI GS ISI 005: "Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness".

[i.4] ISO 27035-2:2016: "Information technology - Security techniques - Information security incident management -- Part 2: Guidelines to plan and prepare for incident response".

[i.5] Directive (EU) 2016/1148 of The European Parliament and of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

[i.6] ETSI GS ISI 007: "Information Security Indicators (ISI); Guidelines for building and operating a secured Security Operations Center (SOC)".

[i.7] ETSI GS ISI 008: "Information Security Indicators (ISI); Description of an Overall Organization-wide Security Information and Event Management (SIEM) Approach".

[i.8] Peter D.Mosses(Ed.): "CASL Reference Manual", LNCS2960 Springer.

[i.9] IEC 62443-series: "Security for industrial automation and control systems".

[i.10] ISO/IEC 19086-2: "Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric model".

[i.11] OPC Foundation (07-19-2017): "OPC UA Companion Standard for Sercos".

NOTE: Available at https://opcfoundation.org.

[i.12] BSI.Bund: "Sicherheitsanalyse Open Platform Communications Unified Architecture (OPC UA)".

NOTE: Available at https://www.bsi.bund.de/DE/Publikationen/Studien/OPCUA/OPCUA_node.html.

[i.13] Wolfgang Ertel: "Grundkurs Künstliche Intelligenz - Computational Intelligence", 4. Auflage 2016, Springer Vieweg Verlag; ISBN 978-3-658-13548-5.

[i.14] Roberto Bruni, Andrea Corradini, Ugo Montanari, Universität Pisa, Italy: "Modelling a Service and Session Calculus with Hierarchical Graph Transformation".

[i.15] Claudia Ermel, Jens Richter, Jan deMeer: "Regelgestützte Modellierung von Anwender-Szenarien Kritischer Infrastrukturen für Analyse und Ausbildung" GI/ACM Regionalgruppe Berlin-Brandenburg, 22-11-2013.

[i.16] J.M.Spivey: "The Z-Notation - A Reference Model", C.A.R. Hoare Series Editor, Prentice Hall 1989.

[i.17] Jan de Meer et al.: "Introduction into Algebraic Specification based on the Language ACT ONE", Computer Networks - International Journal of Distributed Informatique, Vol.23, No.5, North Holland 1992.

[i.18] Axel Rennoch et al.: "Security Indicators Quick Reference Card".

NOTE: Available at https://cdn1.scrvt.com/fokus/e492943d2f291a76/4905070bb7ea30262ddf855393d14e21/SQC_Download_Etsi_isiQRC1.pdf.

[i.19] Dan Pilone: "UML2.0 - Taschenbibliothek", 2006 O'Reilly media.

[i.20] CMU SEI(June 2006) Pitsburg: "Ultra Large-scale Systems - The SW Challenge of the Future", Bill Pollak Chief Editor, created in performance of FG Contract FA8721-05-C-003, Linda Northorp ULS Study-lead.

NOTE: Available at https://insights.sei.cmu.edu/saturn/ultra-large-scale-systems/.

[i.21] Zohar Manna et al.: "The Logical Basis for Computer Programming - Vol. 1: Deductive Reasoning", 1985 Addison Wesley Publishing Inc.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS ISI 001-2 [2] and the following apply:

Abstract Data Type (ADT): specification of multiple sets of data, their properties and relationships among each other, in terms of sorts, operations and equations

Common Logics (CL): logic framework comprising syntax, higher order constructions and relations of a first-order modelling theory

data<n-tuple>space: structuring of the raw data space, called ISI Data Lake (IDL) by 'n-tuples', allowing processes to publish and subscribe upon

ISI Measurement Architecture (IMA): approach to enrich big dat sets, (i.e. ADTs) using methods from Graph Theory or Artificial Intelligence

OPC UA: M2M-communication-based Unified Architecture of the OPC Foundation

semantics: formal representation of system properties that provides formal reasoning on a mathematical level occasionally executable by modeling tools

3.2 Symbols

For the purposes of the present document, the symbols given in ETSI GS ISI 001-2 [2] apply.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS ISI 001-2 [2] and the following apply:

ADT	Abstract Data Type
CL	Common Logics

NOTE: See ISO/IEC 24707 [4].

CV	Continuous Variable
CSlang	Common ISI Semantics Specification Language
DOM	Data Object Model

GM	Graph Manipulation (Tool/Theory)
HMI	Human-Machine Interface
NOTE:	See IEC 62443 [i.9].
IACS	Industrial Automation and Control Systems
IDL	ISI Data Lake
IEX	Incident coming from EXternal sites
IMA	ISI Measurement Architecture
ISI	Information Security Indicators
ML	Machine Learning (Tool)
SCADA	Supervisory Control And Data Acquisition
SLA	Service Level Agreement
NOTE:	ISO/IEC 19086-2 [i.10] SLA Framework - p2 Metric Model.
STIX(TM)	Structured Threat Information eXpression
NOTE:	STIX 2.0 Draft http://stixproject.github.io/stix2.0/.
UUT	Unit Under Test
NOTE:	IEEE AutomaticTestMark-upLanguage.
XML	eXtensible Markup Language

4 ISI Measurement Architecture - Models and Methods

4.1 The Challenge of transforming ISIs into Knowledge about Incidents

4.1.0 Introduction

The present document invents an advanced ISI Measurement Architecture (IMA) by a Big Data respectively ISI enrichment scheme. The process of Big Data Enrichment is intended to be supported by semantics-based tools from the shelf such as Machine Learning (ML), Graph Manipulation (GM), Ontology Specification (OS), Data Object (DO) Modelling, etc.

Firstly it is required to have a way of defining semantics for reasoning on ISIs and secondly, it is required to simulate designed ISI/IMA models. In case of IMA a compositional approach of Graph Manipulation together with Set Theories (i.e. Abstract Data Types) have been chosen to provide a semantics platform to represent distinctive IMA models.

A given formal model is set into relationship to an Industrial Automation and Control System (IACS) model that uses ontologies. If the relationship can be designed such that it is *structure-preserving* it is called a *homomorphism*. Checking homomorphism means to prove structural relationship between a given IACS ontological model with respect to its GM-based executable semantics model.

The anticipated *Communication Model* of IMA is based on an *data<n-tuple> space* i.e. a kind of platform that manages *ISI Events* such as incidents, measurements, data logging but also attacks and failures, etc. that are handled according to the principles of a *publish-subscribe communication paradigm* applicable to all components that exchange data<n-tuples>.

In figure 1 the '*Knowledge Pyramid*' respectively '*Knowledge Graph'*, is shown, of how to transform flat raw ISI related data into expert knowledge on security incidents. This approach is based on a so-called *Type Graph* (see next paragraph) that models e.g. an ISI Enrichment/Classification Process based on machine learning methods. When the so-called *learning matrix* - comprising typical pairs of queried and targeted incident patterns - has been sufficiently trained, it can be applied to the continuous classification process of unknown/untrained input patterns from an observed Industrial Automation and Control System (IACS). The unknown patterns stem from the basic entity nodes of the raw data level of the type graph in figure 1.

The anticipated ETSI GS ISI 006 (the present document) notation *CSlang - a Common (ISI Semantics) Specification Language* (as defined in clause 5) offers *semantic*, *static, dynamic and data typing specification* and modelling concepts. *Static* system properties are architectural design properties that are modelled by a so-called *Type Graph* representing architectural relations among components, devices, processes, stakeholders including humans. Dynamic system properties are behavioural design properties and are modelled by a so-called *Event Graph* representing communication relationships among data sources and targets that are interconnected by an 'ether' which is the so-called *ISI Data Lake (IDL)* that captures data representations as *data<n-tuples>*.

Finally strong Abstract Data Typing is achieved by means of a *many-sorted Algebr*a comprising data sets (SORTS), operations and functions (OPNS) on these sorts, typed variables, and *conditional equations (EQNS).* A conditional equation is the algebraic specification equivalent of a system event that comprises an event head node and an event tail node, i.e. a *pair of ordered nodes* that is represented by an directed edge of the graph.

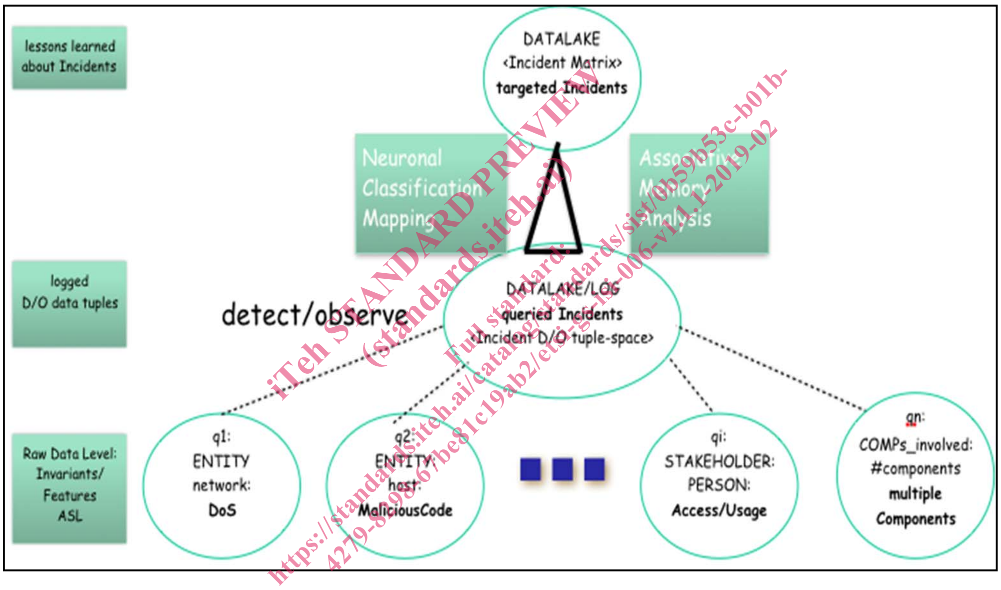
lessons learned about Incidents
DATALAKE
‹Incident Matrix›
targeted Incidents
Neuronal Classification Mapping
Associative Memory Analysis
logged D/O data tuples
detect/observe
DATALAKE/LOG
queried Incidents
‹Incident D/O tuple-space›
Raw Data Level: Invariants/ Features ASL
q1: ENTITY network: DoS
q2: ENTITY: host: MaliciousCode
qi: STAKEHOLDER: PERSON: Access/Usage
qn: COMPs_involved: #components multiple Components

Figure 1: Type Graph representing the Knowledge Pyramid

4.1.1 Providing Upfront Indicators

To be efficient, a SOC of an IACSystem, will need appropriate *Security Detection Solutions* deployed in the right place in the Customer infrastructure, including the Cloud. In order to select the right Security Detection Solutions, the CISO needs to have a good understanding of its environment and to be able to quickly identify the types of security threats he needs to fight. By helping customers to identify upfront (see figure 1) types of incidents they are likely to face and map this with the catalogue of measures that will be relevant to cover these incidents, CISOs have a strong opportunity to quickly demonstrate, e.g. by means of the suggested tool box in the present document, the right decision to be taken.