Club 27001

Présentation de la norme

CEI 62443

Contexte de la norme

L'association ISA (International Society of Automation) est une association américaine à portée mondiale fondée en 1945 sans but lucratif qui regroupe près de 40.000 membres.

Elle développe des standards, certifie des professionnels, fournit des cours, publie des articles techniques, organise des conférences pour les professionnels de l'automatisation.

Son comité ISA99 est un groupe de travail ouvert de plus de 500 membres sur l’aspect cyber-sécurité.

Contexte de la norme

Contexte – France

L’association ISA France est le chapitre français de l'association ISA

Liens :

- Site ISA France : http://www.isa-france.org/.
- Wiki ISA 99 international http://isa99.isa.org,
- Wiki en français de l'ISA99 : http://www.standards-isa.fr/isa99

Sources de la présentation

- Le wiki de la commission ISA99 de l'association ISA,
- Les informations et lettres de l'association ISA France,
- Les travaux menés par le CLUSIF (cybersécurité des systèmes industriels, par où commencer ?),
- Les sources ouvertes sur le sujet.

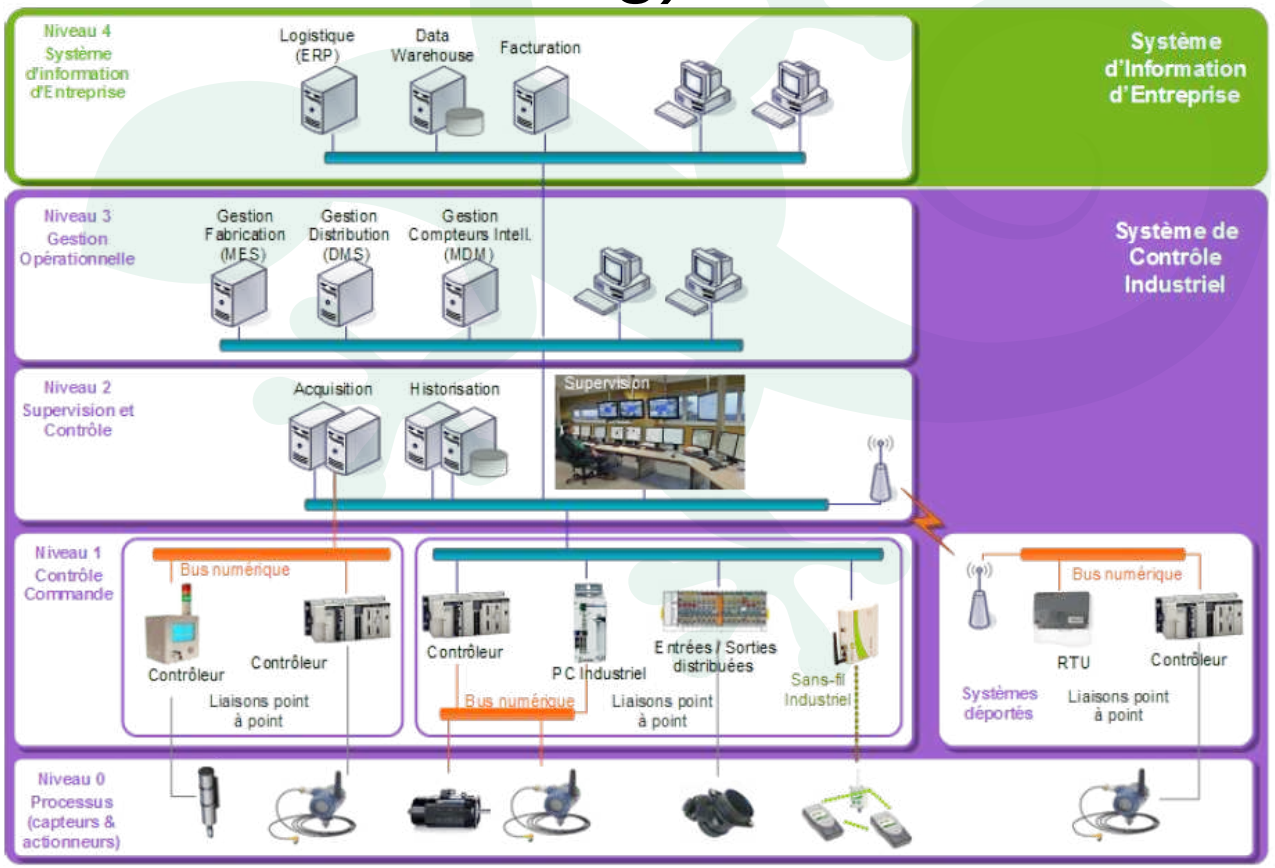
Raisons de la norme

Présentation de Jean-Pierre HAUET au FIC 2010 :

- La cyber-sécurité est un sous ensemble de la sécurité fonctionnelle (ou sûreté de fonctionnement), correspondant à la protection contre un certain type d'agressions externes,
- La sécurité fonctionnelle se fonde actuellement sur la norme CEI 61508 et sur ses dérivées,
- Cette norme impose l'analyse du système face aux agressions internes et externes.
- Elle introduit la notionde Safety Integrity Level (SIL 1 à 4) comme un indicateur et mesure de la sécurité fonctionnelle,
- Au moment de sa conception, les cyber-attaques étaient du second ordre (isolement et technologies spécifiques des systèmes de contrôle)

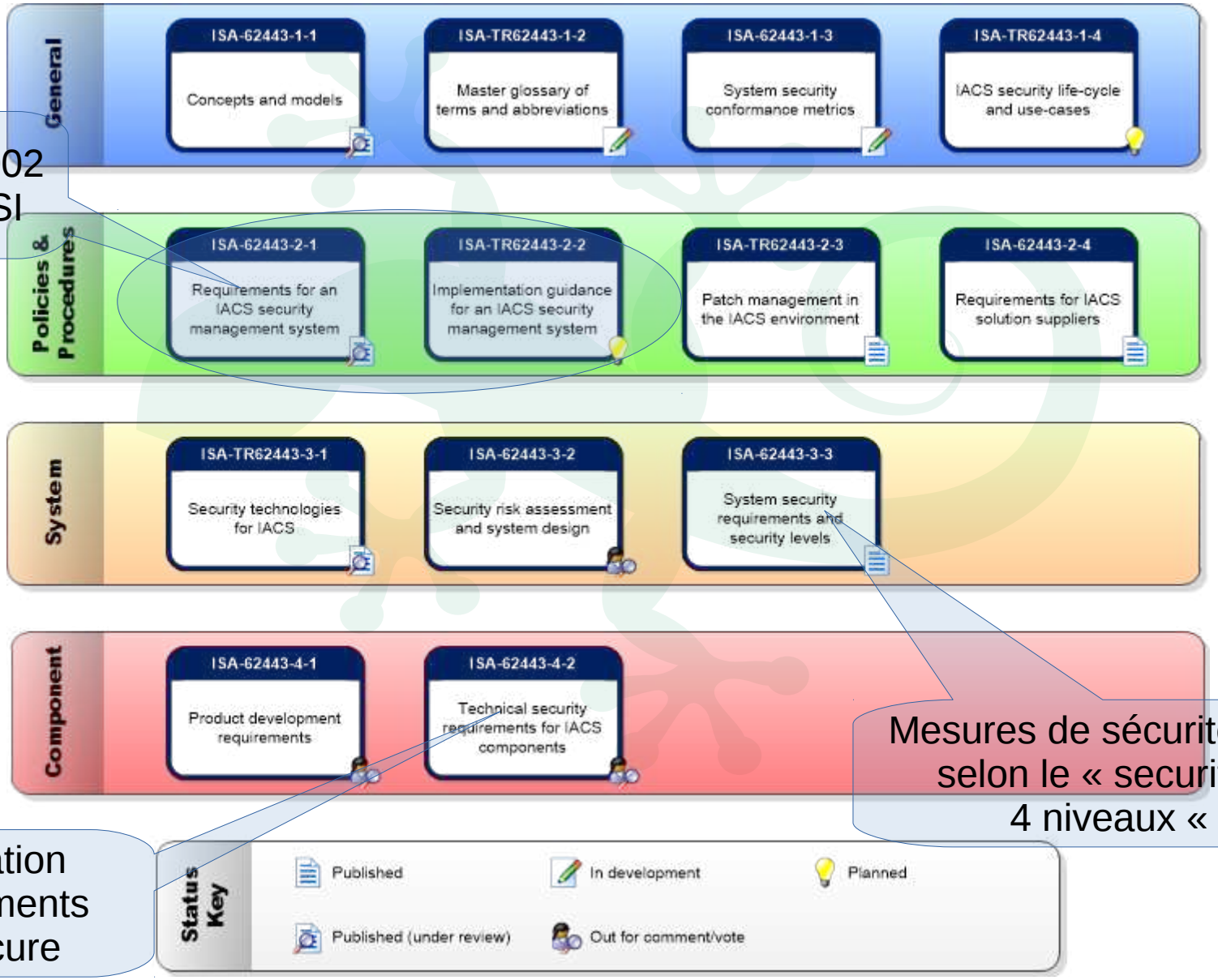
Raison de la norme

SII versus SIG, pyramide CIM (Computer Integrated Manufacturing)



Déclinaison de la pyramide CIM (source : Thierry Cornu)

Une famille de normes

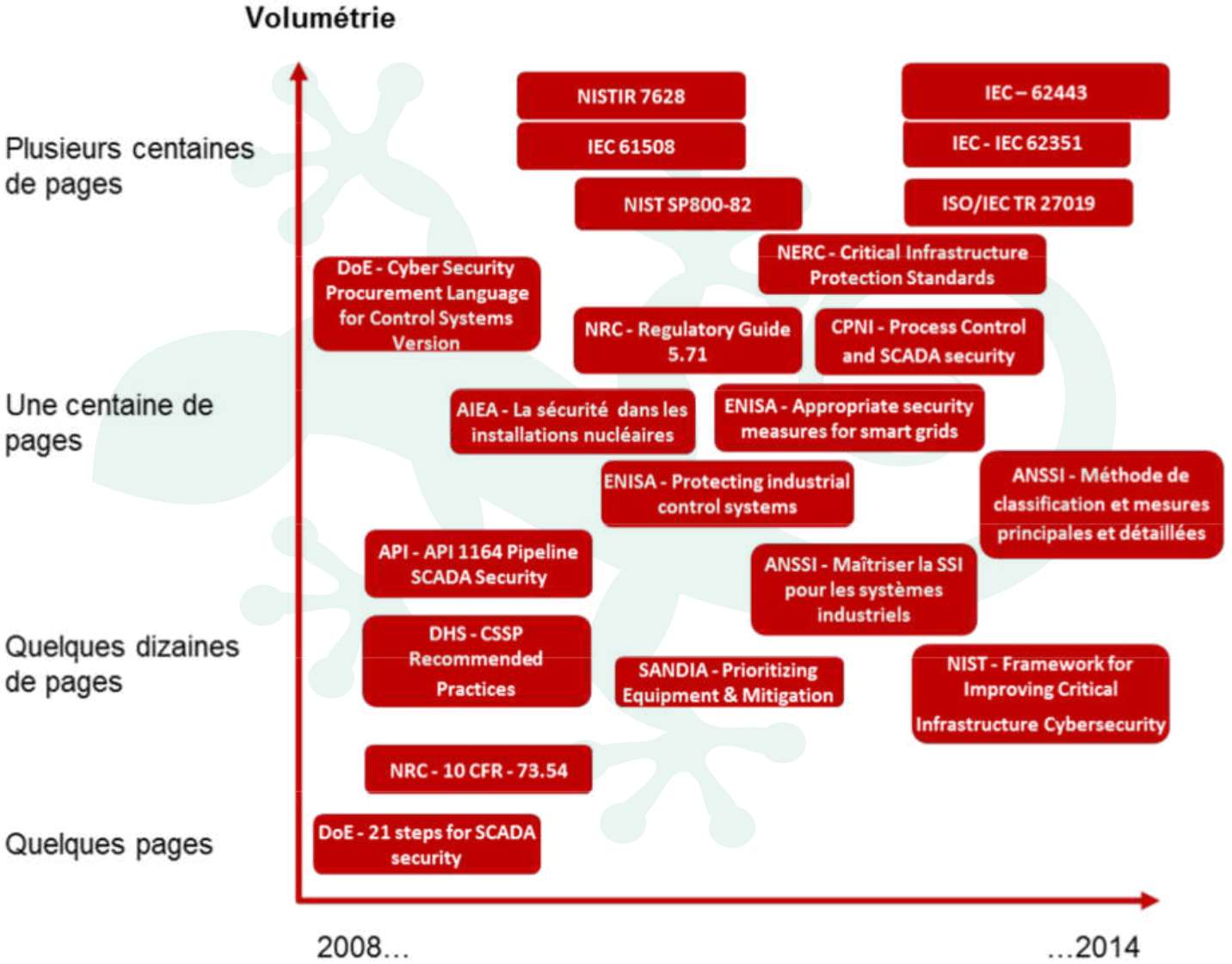


27001 – 27002
IACS / SMSI

Mesures de sécurité adaptées,
selon le « security level »
4 niveaux « SL »

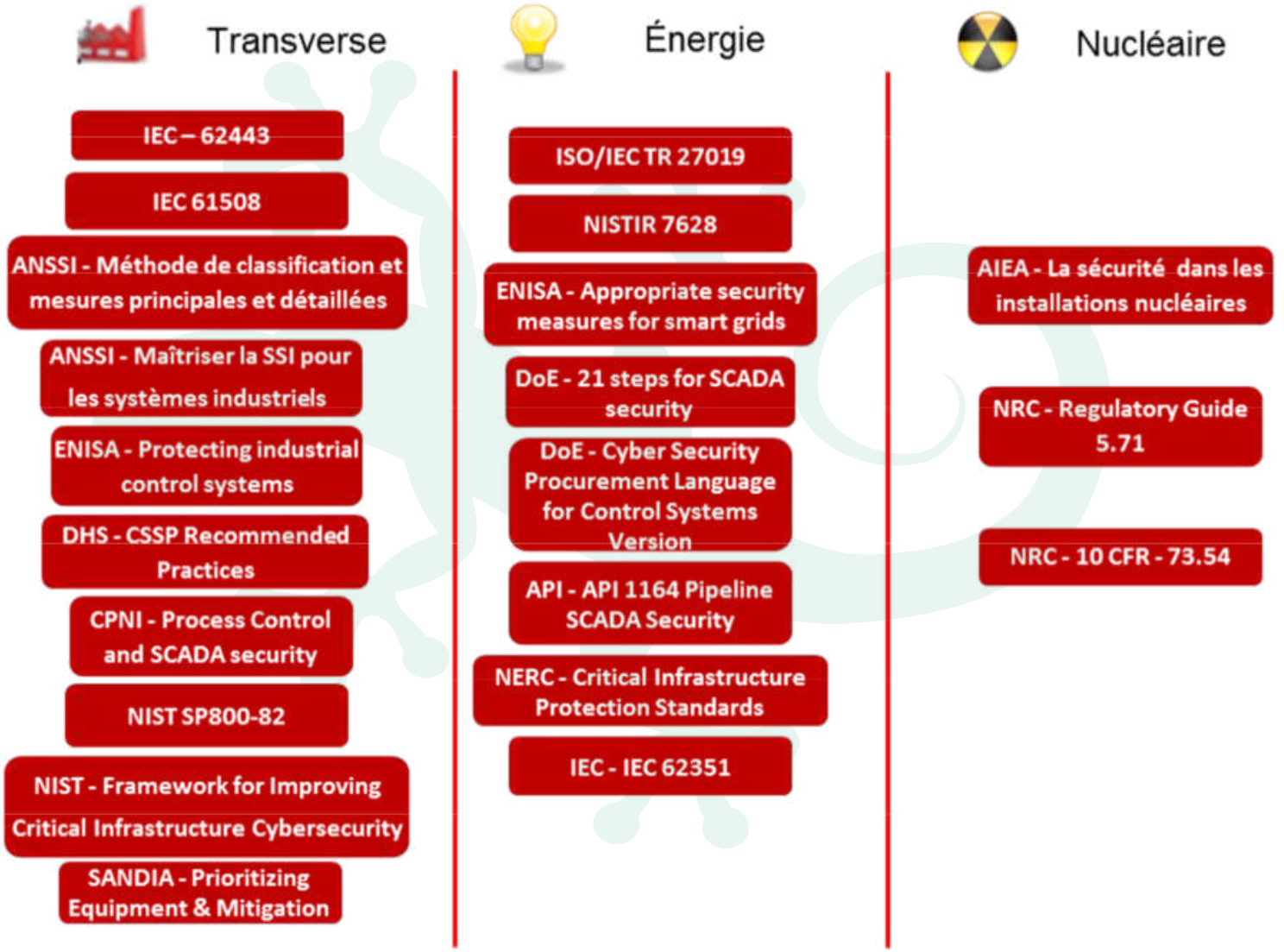
Certification
d'équipements
ISA Secure

Positionnement 62443 / Volumétrie



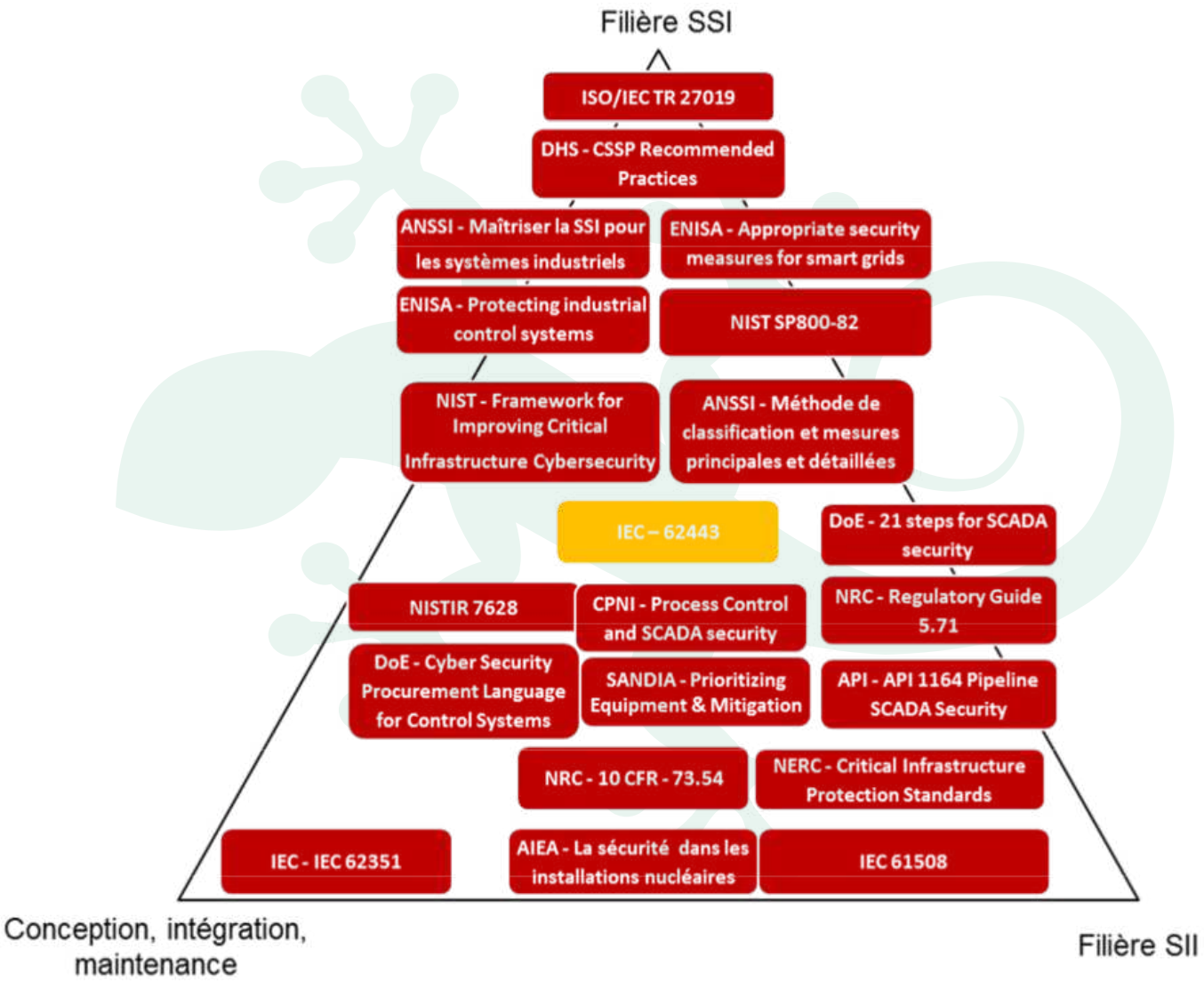
Source CLUSIF – Groupe de travail SCADA

Positionnement 62443 / Origine



Source CLUSIF – Groupe de travail SCADA

Positionnement 62443 / Public



Source CLUSIF – Groupe de travail SCADA

Parallèle avec l'ISO2700x

IEC 62443 : vers une définition holistique des niveaux de sécurité

La philosophie de la norme IEC 62443 (ISA99) relative à la cybersécurité des installations industrielles, repose sur deux approches complémentaires :

- d'une part, une analyse des mesures de nature organisationnelle (les « policies and procedures »), à mener selon les principes des normes ISO 27001 et 27002, adaptées et retranscrites dans le cadre du standard IEC 62433-2-1 (révision en cours de finalisation) et complétées par l'IEC 62443-2-4 dans le cas des intégrateurs et fournisseurs de service ;
- d'autre part, des règles techniques, définies dans le standard IEC 62443-3-3 (norme publiée) permettant de définir de façon objective, grâce à une centaine de critères, les niveaux de sécurité (SL allant de 0 à 4) que l'on peut accorder à une installation donnée au regard de chaque exigence essentielle définie par la norme (FR 1 à FR7).

Le standard IEC 62443-3-3 applicable aux systèmes, et son extension l'IEC 62443-4-2 applicable aux composants de ces systèmes, constituent une avancée majeure dans le domaine de l'évaluation de la cybersécurité des installations industrielles car ils prennent en considération les spécificités du monde industriel et propose une approche technique rationnelle pour mener les évaluations.

Cependant, aux côtés de l'approche technique, l'approche organisationnelle héritée de l'ISO 27000, reste qualitative. Ceci fait que, si les cotations SL0, SL1…SL4 que l'on peut accorder à un système prennent bien en compte les qualités intrinsèques du système (c'est-à-dire sa « capability »), elles n'intègrent pas toutes les données particulières à son exploitation dans un environnement donné.

Parallèle avec l'ISO2700x et avenir

Afin de remédier à cette situation, un nouveau groupe de travail, animé par Pierre Kobes (Siemens) et Lee Neitzel (Wurldtech), l'ISA99-WG3-TG3, a été constitué. Son objectif est de mettre au point une approche holistique afin de parvenir à une notion de « niveau de protection » intégrant l'ensemble des aspects à prendre en considération.

Pour ce faire, la notion de niveau de protection s'appuierait sur le concept de « niveau de maturité (Maturity level) », introduit dans l'IEC 62443-1-1 (Revision) et précisé dans l'IEC 62443-4-2. Ce concept est dérivé de celui de maturité logicielle (Maturity Level ou CMMI) introduit il y a une trentaine d'années par le Carnegie Mellon Institute dans le domaine du développement des logiciels et communément utilisé dans l'industrie. Dans le cas de la cybersécurité, il s'agirait de caractériser la maitrise des intervenants dans la mise en œuvre des différentes pratiques permettant de construire la cybersécurité (figure 1).

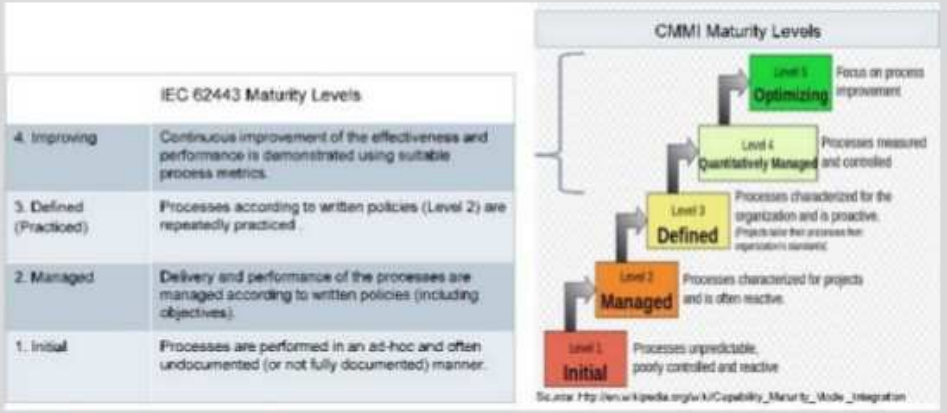


Figure 1 : Maturity levels et CMMI – Source : ISA

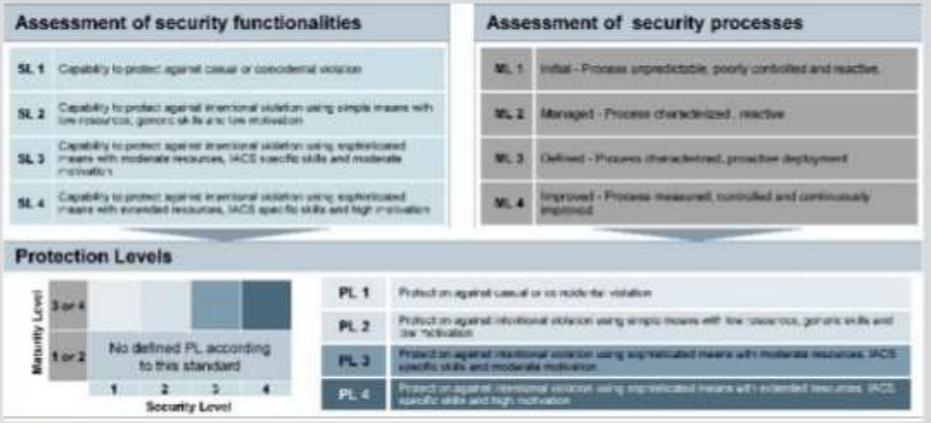


Figure 2 : Combinaison des Security levels et des Maturity levels pour définir les Protection levels – Source : ISA.

Partant de là, disposant des Security levels (SLs) afférant à un système et du Maturilty levels (ML) afférant à l'organisation qui en est responsable, il semble possible de combiner les deux afin de définir un niveau de protection (PL ou Protection level) d'une installation.

Ceci est l'idée générale et elle nous semble intéressante. Mais le groupe démarre tout juste ses travaux et il y a encore du chemin afin que cette approche ne devienne un standard, approuvé et documenté.

Jean-Pierre Hauet – jean-pierre@hauet.com

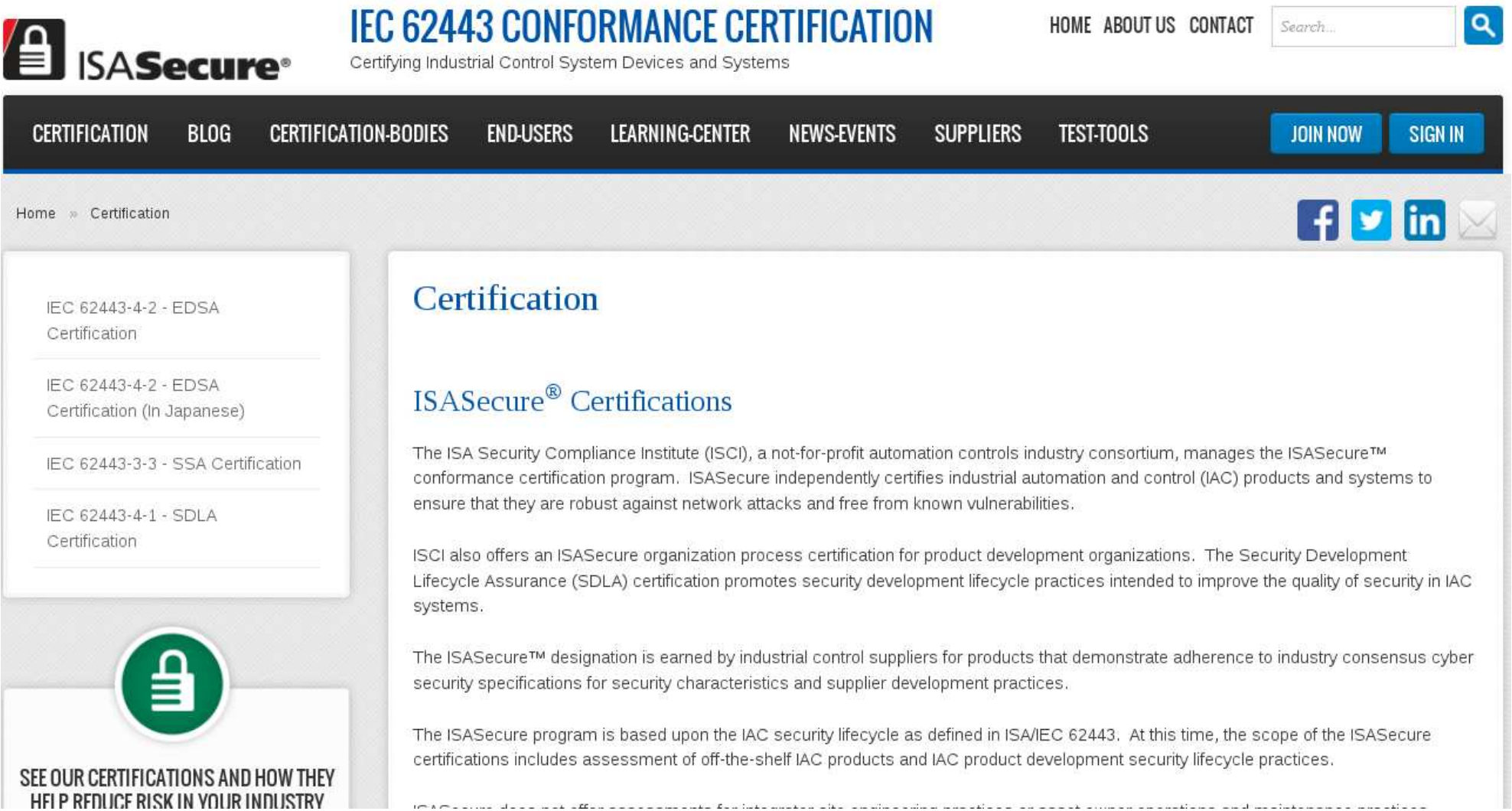
62443 pragmatique

Présentation

ISA-Secure

EDSA

ISA Secure
Certification de systèmes



ISA Secure versus ANSSI

La cybersécurité des systèmes de contrôle : comparaison entre les approches ISA/IEC et ANSSI

L'ISA a été pionnière en formalisant une approche graduée de cyber-sécurisation des systèmes numériques industriels, basée sur le concept de niveau de sécurité qui est noté en abrégé « SL » (Security Level) dans les documents constitutifs de le standard ISA99, aujourd'hui repris par la CEI en tant que norme IEC 62443.

Ce type d'approche est devenu un dénominateur commun dans le domaine des SI industriels et a été adopté par d'autres standards publiés depuis : dans le nucléaire (IEC 62645, NRC 5.71, AIEA NSS#17), dans d'autres référentiels de l'industrie (NIST 800-82 r2 en cours de finalisation) et par l'ANSSI dans deux documents essentiels : « *Méthode de classification et principales mesures* » et « *Mesures détaillées* » publiés en janvier 2014. Les grands groupes industriels qui ont initié des programmes de cybersécurité retiennent également ce type d'approche, souvent en déclinant l'un ou l'autre des référentiels.

Face à cette multiplication des référentiels, les équipementiers (actionneurs, automates, supervision…) et les intégrateurs s'inquiètent de savoir si ces approches sont compatibles entre elles et notamment avec les exigences françaises éditées par l'ANSSI. Plusieurs constructeurs d'automates ont étudié de près les exigences ANSSI pour les comparer à celles de l'ISA/CEI mais les résultats restent confidentiels. ISA-France et le groupe de travail SCADA du CLUSIF ont donc décidé de réaliser une étude similaire pour la partager publiquement : c'est l'objet du présent article qui traite des niveaux et critères de classification, avant de se pencher précisément sur la comparaison de certaines exigences.

Source ISA Flash N° 56

ISA Secure versus ANSSI

Les principales différences entre les deux approches

Affectation des systèmes à des classes (ANSSI) ou à des SL (ISA/CEI)

Une méthode d'affectation à une classe est suggérée dans le document de l'ANSSI et est conforme à l'esprit « High-level risk analysis »[4] de l'ISA/CEI, à savoir une prise en compte à la fois de l'impact en cas de cyber-attaque réussie (sur les personnes, les biens, l'activité économique et l'environnement) et d'une estimation de sa probabilité sur la base d'un modèle prenant en compte les type de systèmes, la connectivité, l'accessibilité et le type d'attaquants.

Pour l'ANSSI comme pour l'ISA/CEI, l'approche est aujourd'hui plutôt qualitative, guidée par des scénarios. L'ISA/CEI mentionne (annexe A de 62443-3-3) qu'avec l'augmentation des connaissances et des modèles mathématiques sur les attaques, risques et les incidents, on peut espérer à terme avoir des modèles plus quantitatifs, basés sur des approches statistiques.

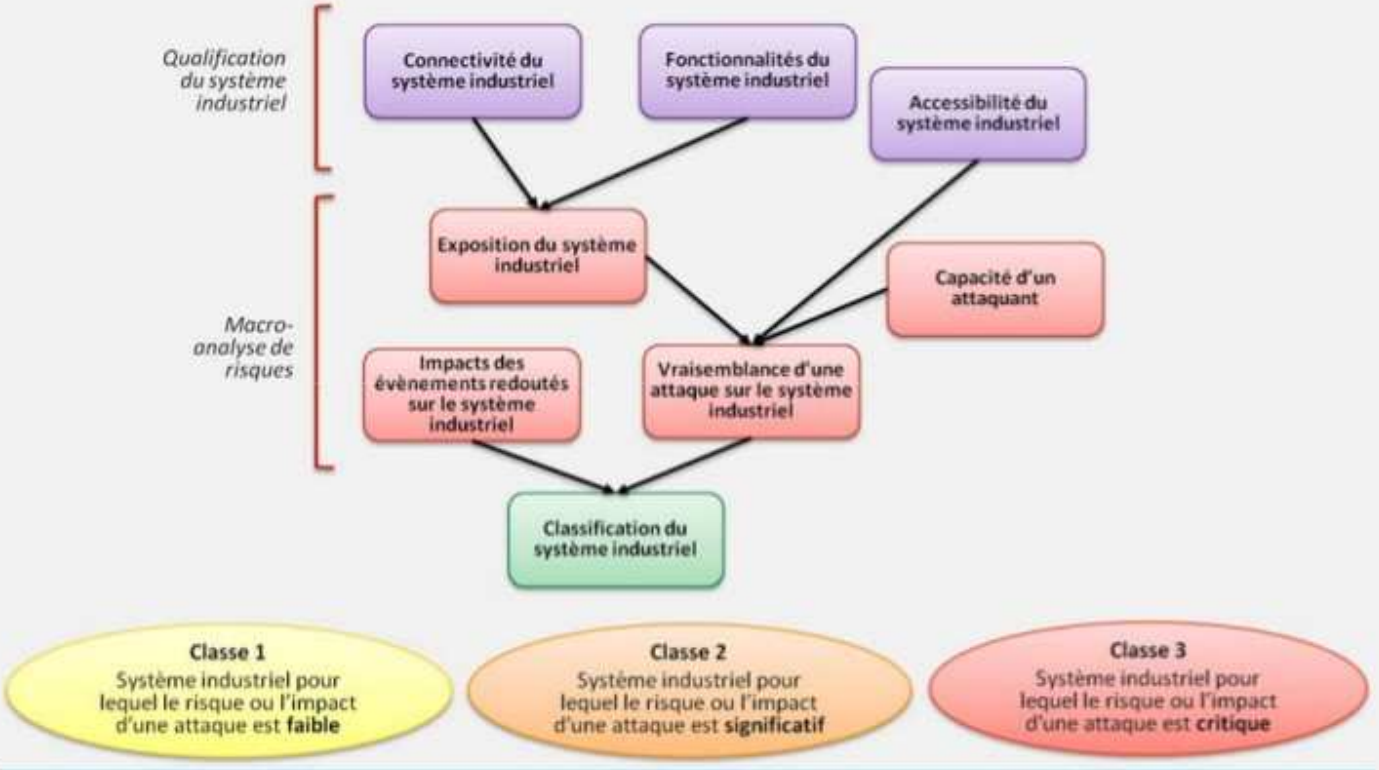
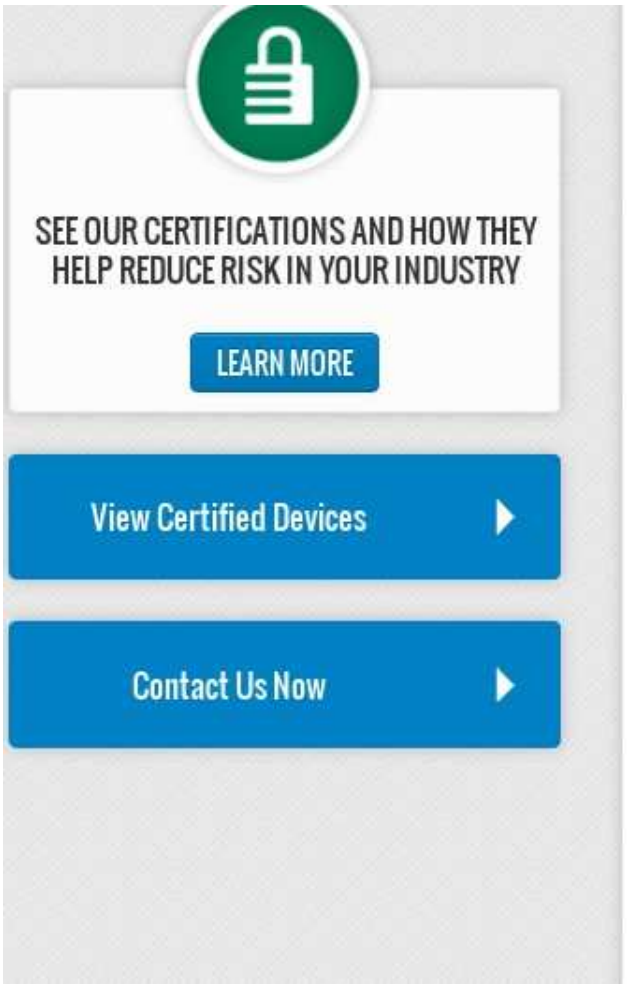


Figure 1 : Logique d'affectation à une classe selon l'ANSSI.

ISA Secure
Certification de systèmes



The ISASecure™ designation is earned by industrial control suppliers for products that demonstrate adheren security specifications for security characteristics and supplier development practices.

The ISASecure program is based upon the IAC security lifecycle as defined in ISA/IEC 62443. At this time, th certifications includes assessment of off-the-shelf IAC products and IAC product development security lifecy

ISASecure does not offer assessments for integrator site engineering practices or asset owner operations ar ISASecure certifies off-the-shelf systems; not the site engineered / deployed systems.

ISCI offers three certifications with four security assurance levels (SAL) in alignment with ISA/IEC 62443.

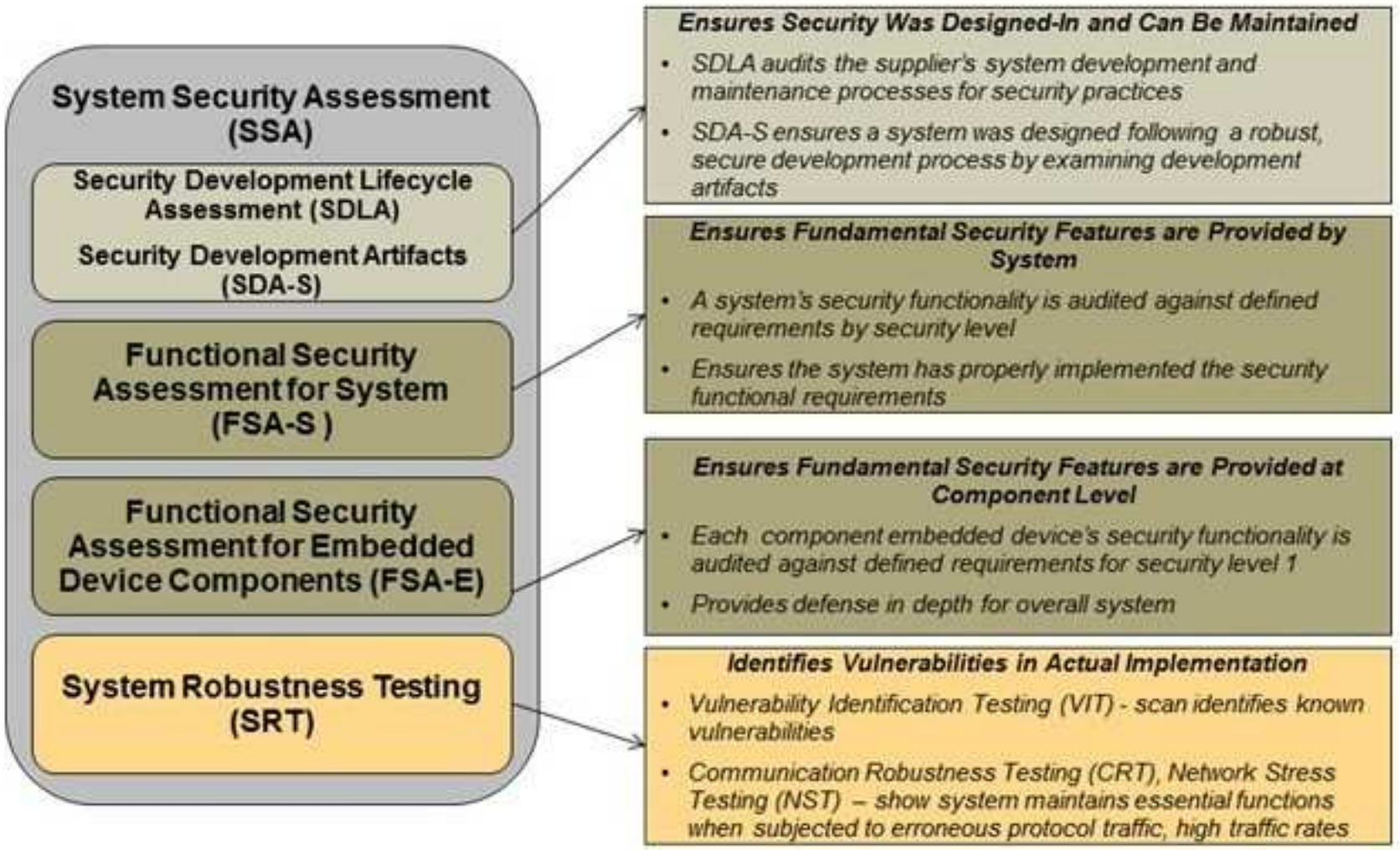
1. ISASecure Embedded Device Security Assurance (EDSA) Certification
2. ISASecure System Security Assurance (SSA) Certification
3. ISASecure Security Development Lifecycle Assurance (SDLA) Certification

The government of Japan has adopted ISASecure as part of their critical infrastructure protection scheme an lab to process certifications locally in Japan. Japanese language translations of ISASecure certification spec Japanese ISASecure Certification Scheme web pages.

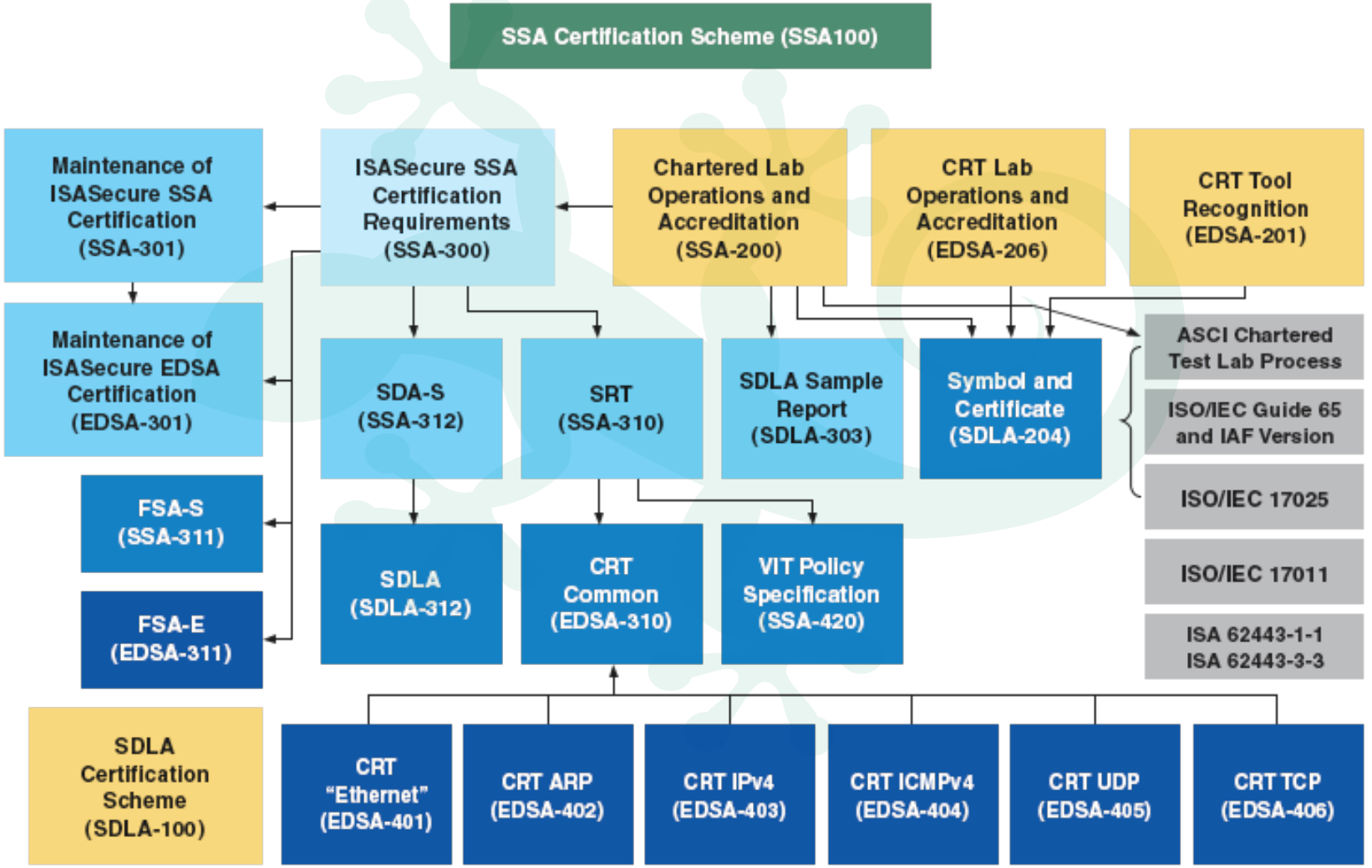
ISASecure EDSA Certification Scheme (In Japanese)

To see the complete list of certified devices, visit the ISASecure Certified Device List page.

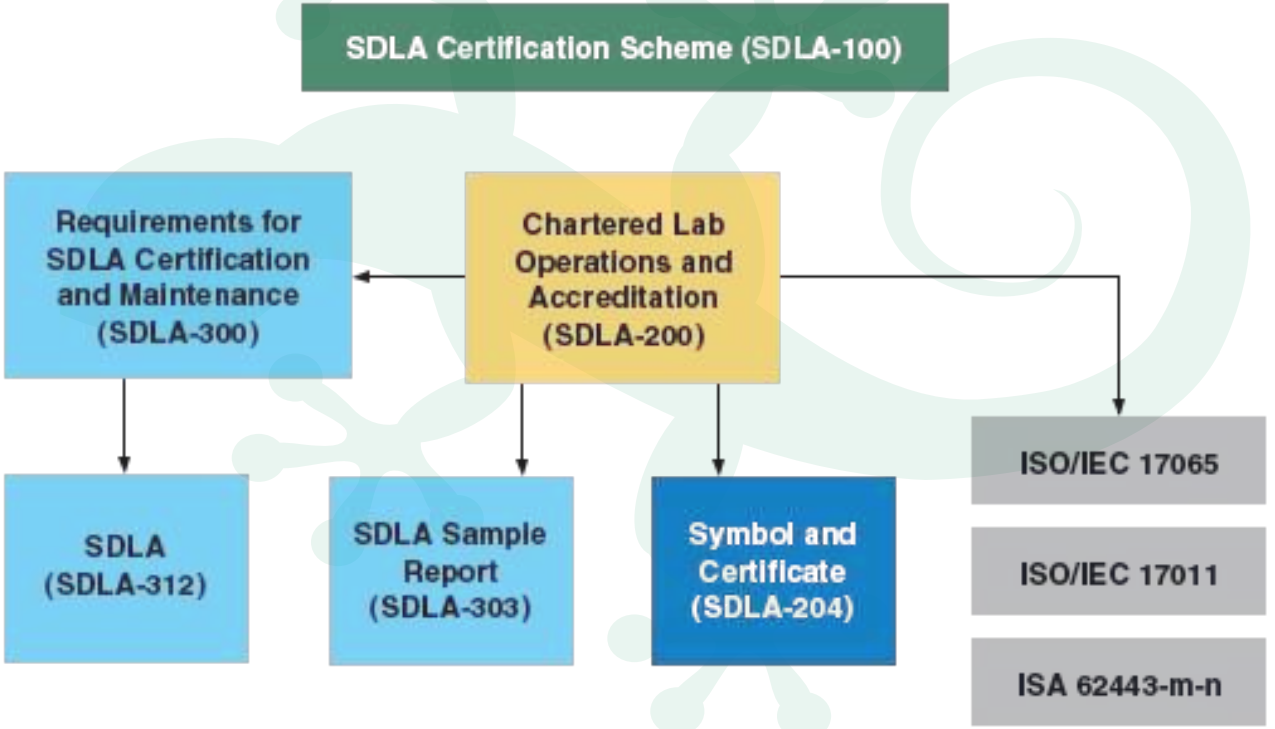
62443-3-3 – SSA
System Security Assurance



62443-3-3 – SSA System Security Assurance



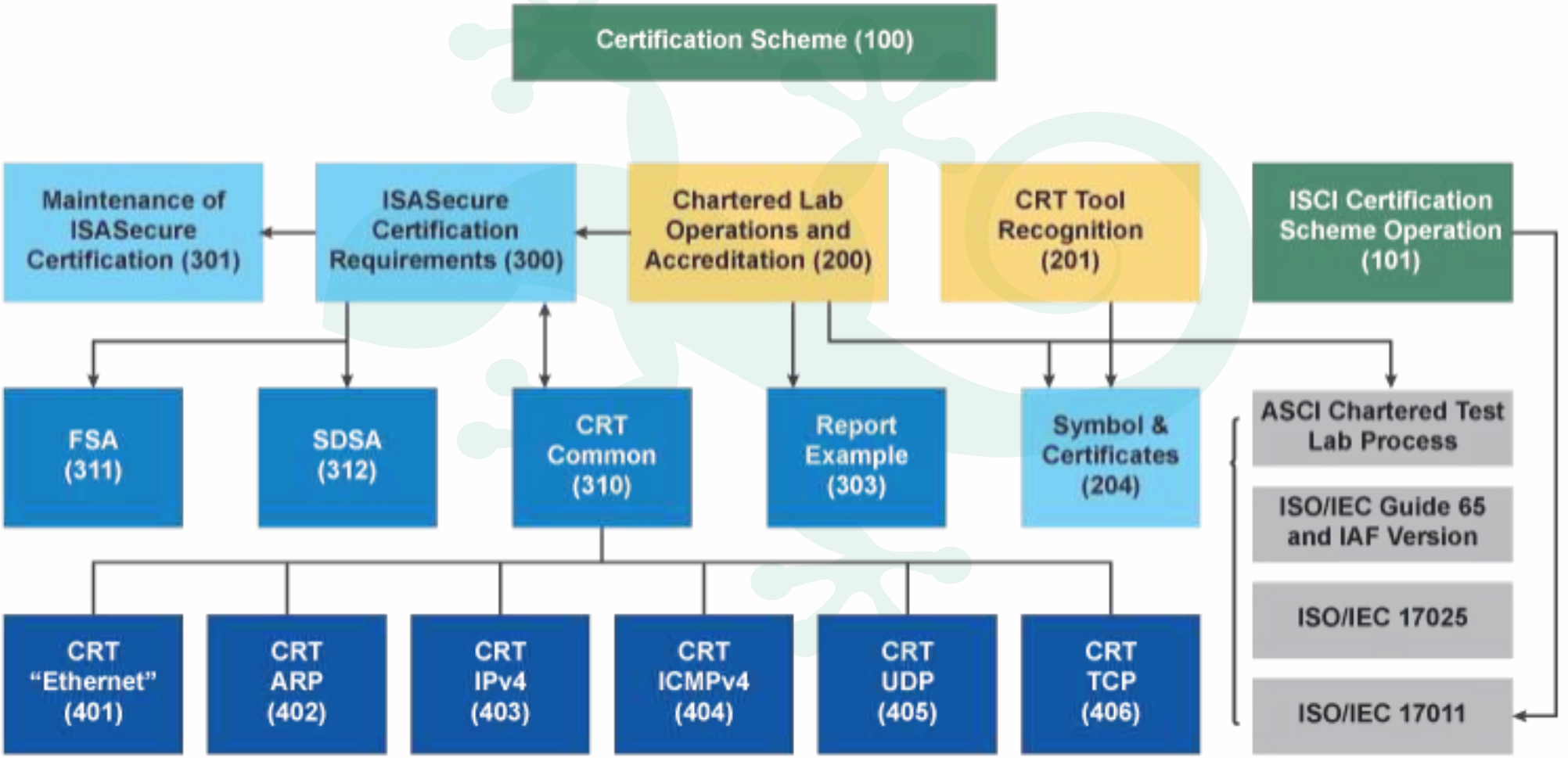
62443-3-3 SDLA Security Development Lifecycle Assurance



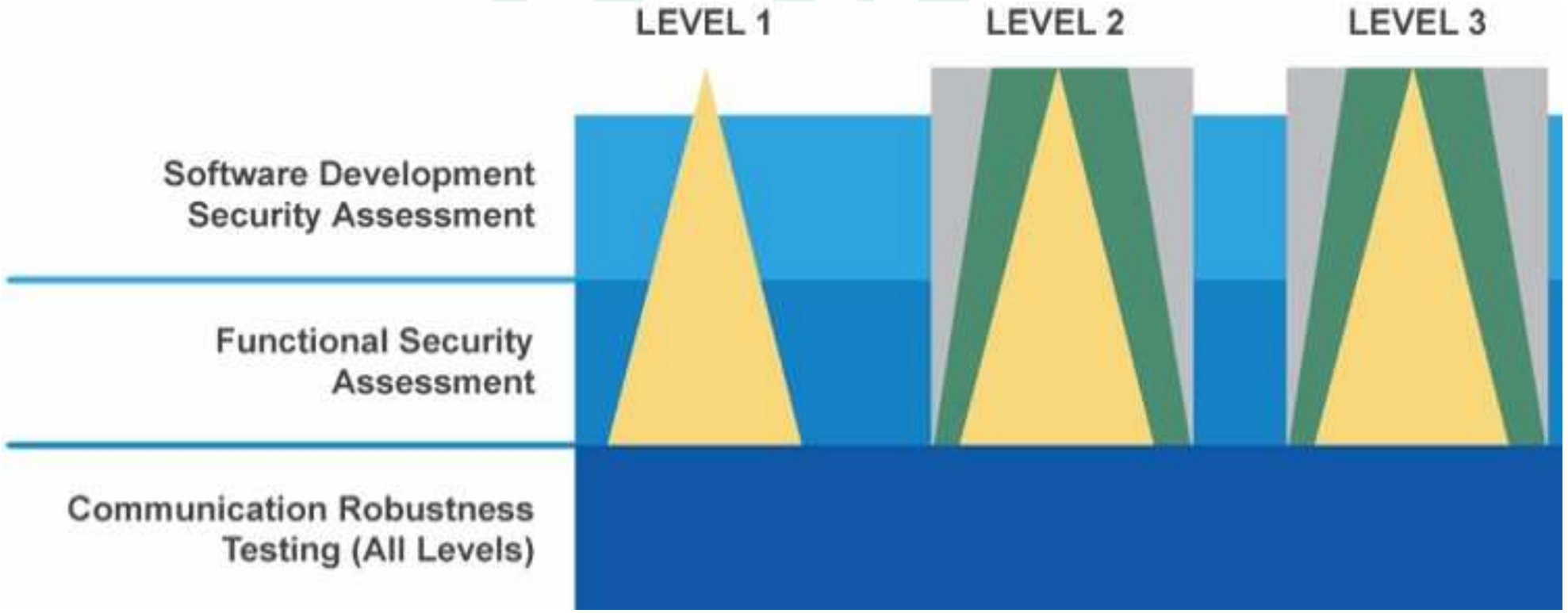
EDSA

Du concret pour la
certification des systèmes embarqués

62443-3-3 EDSA Embedded Device Security Assurance



62443-3-3 EDSA Embedded Device Security Assurance



EDSA 100 - dans le concret

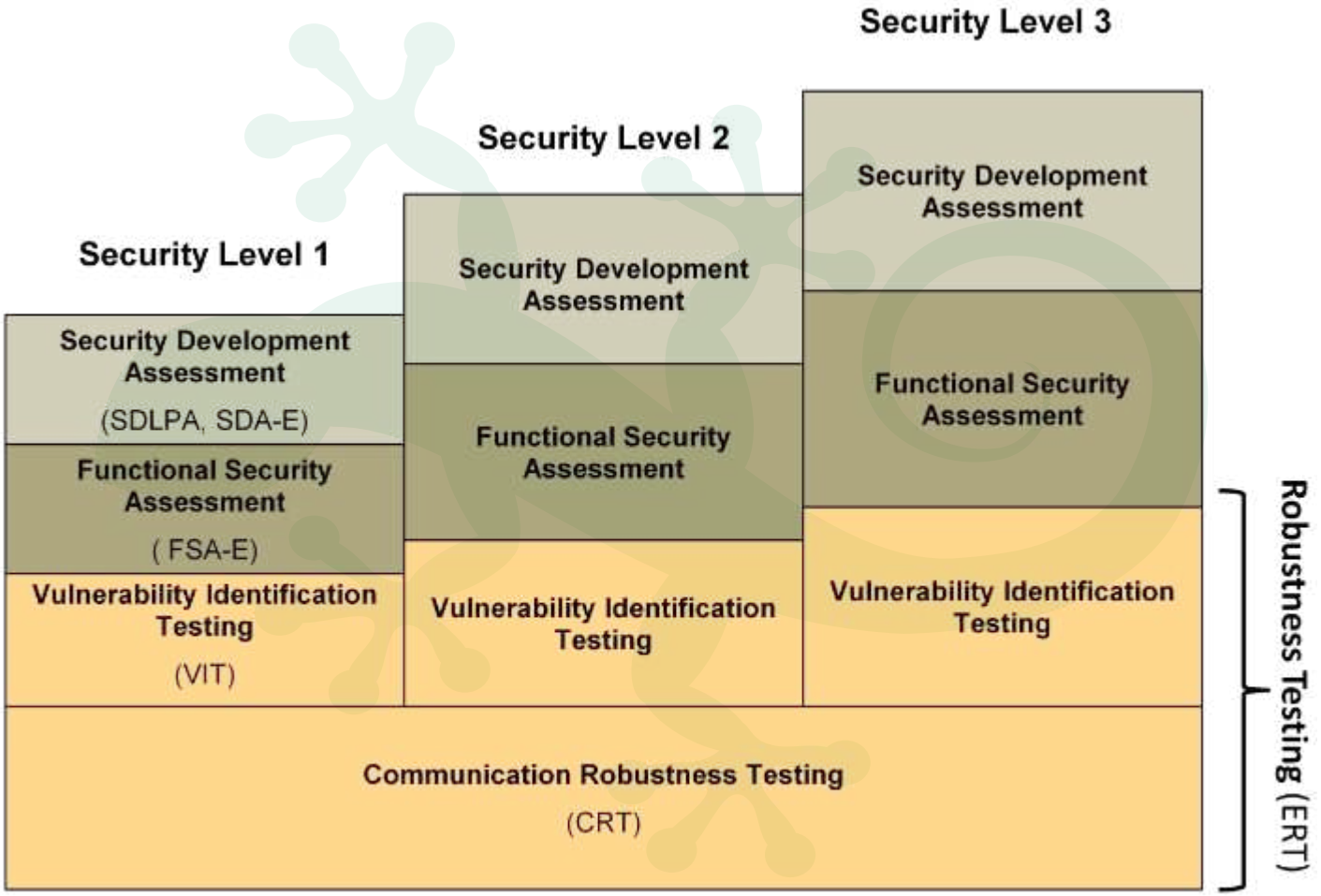


Figure 1 - Structure of ISASecure Embedded Device Certifications

EDSA 100 - dans le concret

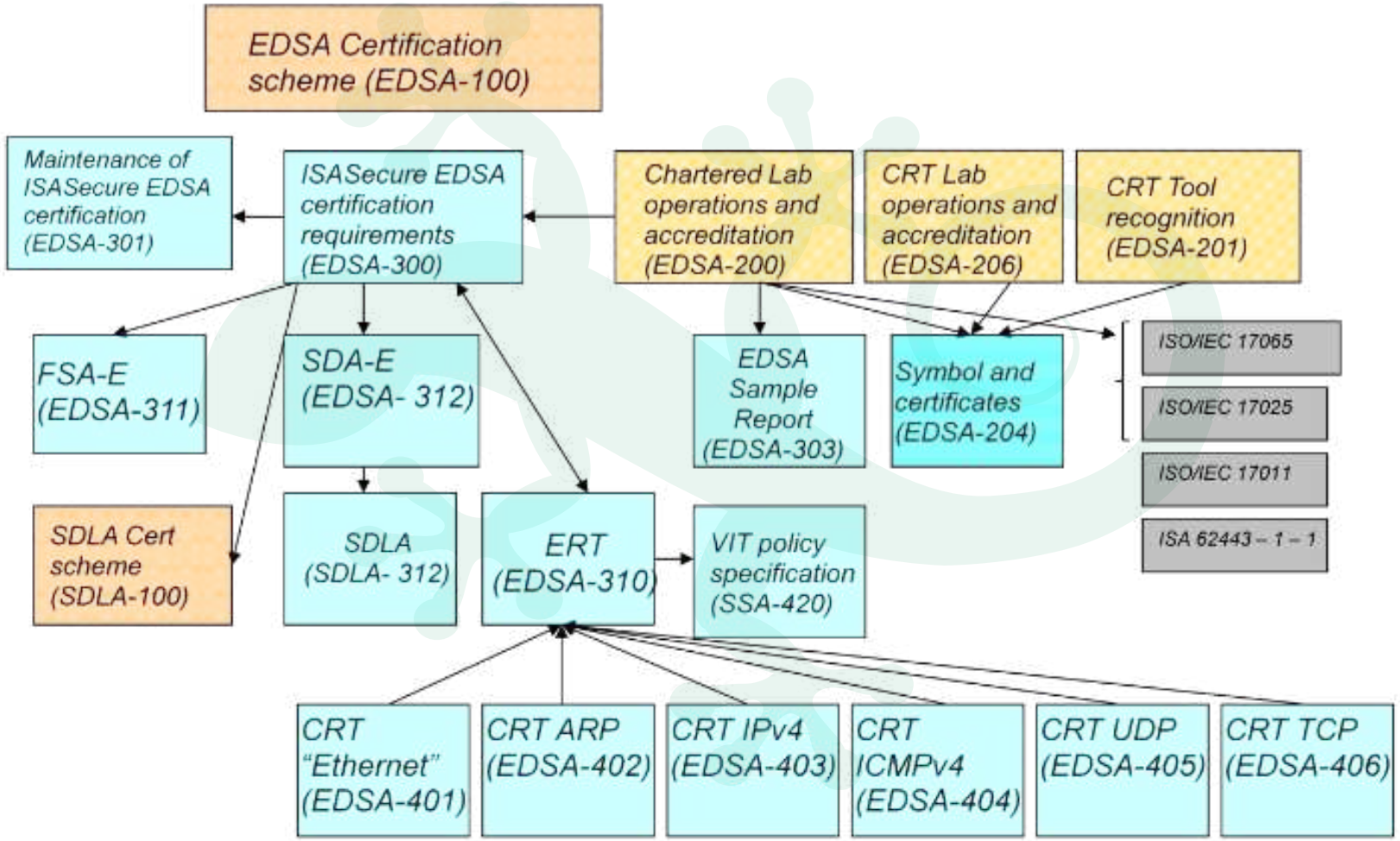


Figure 2 - ISASecure EDSA Documents

EDSA 311 - dans le concret

ASCI Automation Standards Compliance Institute

EDSA-311
ISA Security Compliance Institute - Embedded Device Security Assurance -
Functional Security Assessment (FSA)

Data Confidentiality

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure™* Level	Comments / Clarifications
FSA-DC-1	Confidentiality of Data in Transit	The IACS embedded device shall protect the confidentiality of transmitted information	FR 4.10 COMMUNICATION CONFIDENTIALITY NIST 800-53 SC-9	NA	Within a protected area physical controls may be sufficient
FSA-DC-1.1	No Clear Text in Data Transit	The IACS embedded device shall not send any data in clear text format for basic prevention of unauthorized disclosure of information during communication	FR 4.10 COMMUNICATION CONFIDENTIALITY (1) NIST 800-53 SC-9 (1)	All	If required by application and not directly supported can only be allocated if confidentiality is only needed outside the zone of the embedded controller and the communications can be limited to the zone or encrypted by a boundary device prior to leaving the zone.
FSA-DC-1.2	Cryptographic Protection for Data Confidentiality	The IACS embedded device shall employ cryptographic mechanisms to prevent unauthorized disclosure of information during communication	FR 4.10 COMMUNICATION CONFIDENTIALITY (1) NIST 800-53 SC-9 (1)	>1	If required by application and not directly supported can only be allocated if confidentiality is only needed outside the zone of the embedded controller and the communications can be limited to the zone or encrypted by a boundary device prior to leaving the zone.
FSA-DC-1.3	Cryptographic Key Management	The IACS embedded device shall provide automated support for automation of cryptographic key management	FR 4.11 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT NIST 800-53 SC-12	>2	Key generation needs to be performed using an effective random number generator. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution in accordance with defined standards
FSA-DC-2	Confidentiality of Data at Rest	The IACS embedded device shall provide measures to protect confidentiality of stored information		N/A	Can provide additional layer of security for high value data. May not apply frequently to embedded products but can protect critical information stored within an otherwise non-secured environment

EDSA 312 – SDL assesment

ASCI Automation Standards Compliance Institute

EDSA-312
ISA Security Compliance Institute - Embedded Device Security Assurance -
Software Development Security Assessment

Phase: SMP

Requirement ID	Requirement Name	Requirement Description	Source of Requirement	*ISASecure* Level[1]	Comments/Clarifications
Project Management					
SDSA-SMP-1	Security Management Plan	A security management plan, which documents the plan for ensuring that security is addressed throughout the development lifecycle, shall be created as a stand alone document or as part of another plan, unless security management is already included as part of the standard software development lifecycle.	IEC-61508-3: 6.2.1	All	
SDSA-SMP-1.1	Identification of responsibilities	The persons, departments and organizations which are responsible for carrying out and reviewing the applicable security related activities shall be documented.	IEC-61508-1: 6.2.1b	All	
SDSA-SMP-1.2	Review of security management plan	If a security management plan is created it shall be reviewed by all those who are assigned responsibility in the plan.	IEC-61508-1: 6.2.3, 6.2.4, & DO-178B: 4.2.g	All	
SDSA-SMP-1.3	Lifecycle Model	The development organization shall establish a life-cycle model to be used in the development and maintenance of the product. This model shall be documented.	IEC 61508-1: 6.2.1.c, DO-178B: 4.3 & ISO/IEC 15408-3: ALC_LCD.1.1D	All	
SDSA-SMP-1.3.1	Lifecycle Model Details	The lifecycle model shall document the transition between software lifecycle processes by specifying: (1) The inputs to the process, including feedback from other processes, (2) Any integral process activities that may be required to act on these inputs, (3) Availability of tools , methods, plans, and procedures.	DO-178B: 4.3b	All	
SDSA-SMP-1.4	Basic Security Training	All people involved in software development of a product that has security concerns shall be given basic training in good security engineering practice and the secure development process that will be used on the project. In addition, software developers shall receive detailed training on common basic causes and mitigation techniques. Testers shall receive training in security test techniques. The security management plan should document the security training plan for all those working on the software development.	CLASP: Institute security awareness program Microsoft: Stage 0: Education and awareness IEC 61508-1: 6.2.1.h	All	Engineers must understand what it takes to build and deliver secure features; not how to develop security features. These skills are currently not taught in most colleges and universities and on average most software engineers know very little about software security.
SDSA-SMP-1.5	Competence	Those involved in software development of a product that has security concerns must be competent in carrying out the tasks assigned to them.	IEC 61508-1: 6.2.1.h	All	
SDSA-SMP-1.6	Development Tools	The development organization shall identify all development tools (including versions) used to create the product and document this information.	ISO/IEC 15408-3: ALC_TAT1.1D & IEC 61508-3: 7.4.4.2	All	NOTE: Unless otherwise notified the reference ISO/IEC 15408-3 hereafter designates the 2008 version, i.e. ISO/IEC 15408-3:2008.
SDSA-SMP-1.6.1	Development Tools Options	The development organization shall document the selected implementation-dependent options of the development tools in the security management plan.	ISO/IEC 15408-3: ALC_TAT1.2D	>2	
SDSA-SMP-1.7	Revision of security management plan	The software planning process should provide a means to revise the security management plan as a project progresses.	DO-178B: 4.2e	All	
SDSA-SMP-2	Action Item Resolution	A process shall exist for ensuring that action items from review meetings are documented and tracked to closure.	IEC-61508-1: 6.2.1.g	All	

EDSA 310 – Trames de test

EDSA-310
ISA Security Compliance Institute –
Embedded Device Security Assurance –
Common requirements for communication robustness testing of IP-based protocol implementations

Version 1.7

September 2010

Requirement CRT.R61 – Reproducibility of protocol-specific robustness test failure

If the DUT fails to adequately maintain an essential service or exhibits other behavior that indicates a failure during a protocol-specific robustness test, this behavior SHALL be reproducible before the test is given a failed status.

Requirement CRT.R62 – Generation of reproducible robustness tests

A documented reproducible deterministic process (which MAY be a seeded pseudo-random process) SHALL drive basic robustness and load stress testing, so that, for a specific implementation of the software under test, these phases of the testing comprise a 100% reproducible process with no variance..

Requirement CRT.R63 – Pseudo-random seed value

When a pseudo-random test process is employed to drive robustness testing, that process SHALL be keyed by an initial seed value of at least 16 bits that SHALL be listed in the test report.

Requirement CRT.R64 – Pseudo random seed reuse

When a pseudo-random test process is employed, the test framework SHALL provide a mechanism whereby a prior seed value can be configured before the test starts, so that a re-test of unchanged software will generate the identical test sequence provided that the response sequence is unchanged.

It is the responsibility of the implementer of the protocol software in the device under test (DUT) to ensure reproducibility of responses to a duplicated test sequence; when that is not possible, the assistance in diagnosis that observable retest can provide may not be available.

The test process MAY use feedback during the test selection process, so that detected apparent anomalies in the responses of the DUT can trigger focusing of subsequent tests on those protocol aspects that appear to cause the anomalies to manifest. Thus any change or correction in the software under test may cause the attack resistance tests to diverge at points where those changes affect the DUT's responses, thereby limiting the extent to which instrumented retest can assist in diagnosis of the cause of the discovered anomalies.

9.6 Test report

9.6.1 General

A test laboratory performing protocol-specific robustness testing provides a test report that meets the following requirements. These reporting requirements are common to all protocols. Any additional reporting requirements unique to a specific protocol are discussed in the ISASecure robustness test specification for that protocol. In addition, all CRT test reports meet the common reporting requirements in Clause 7.

Requirement CRT.R65 – Report basic protocol specific robustness test information

The report for a protocol-specific robustness test shall meet all of the basic test reporting requirements in Clause 7: Requirement CRT.R20 through Requirement CRT.R28, inclusive.

EDSA 401 – Dans le coeur des tests

EDSA401 Ethernet Robustness Test Specification

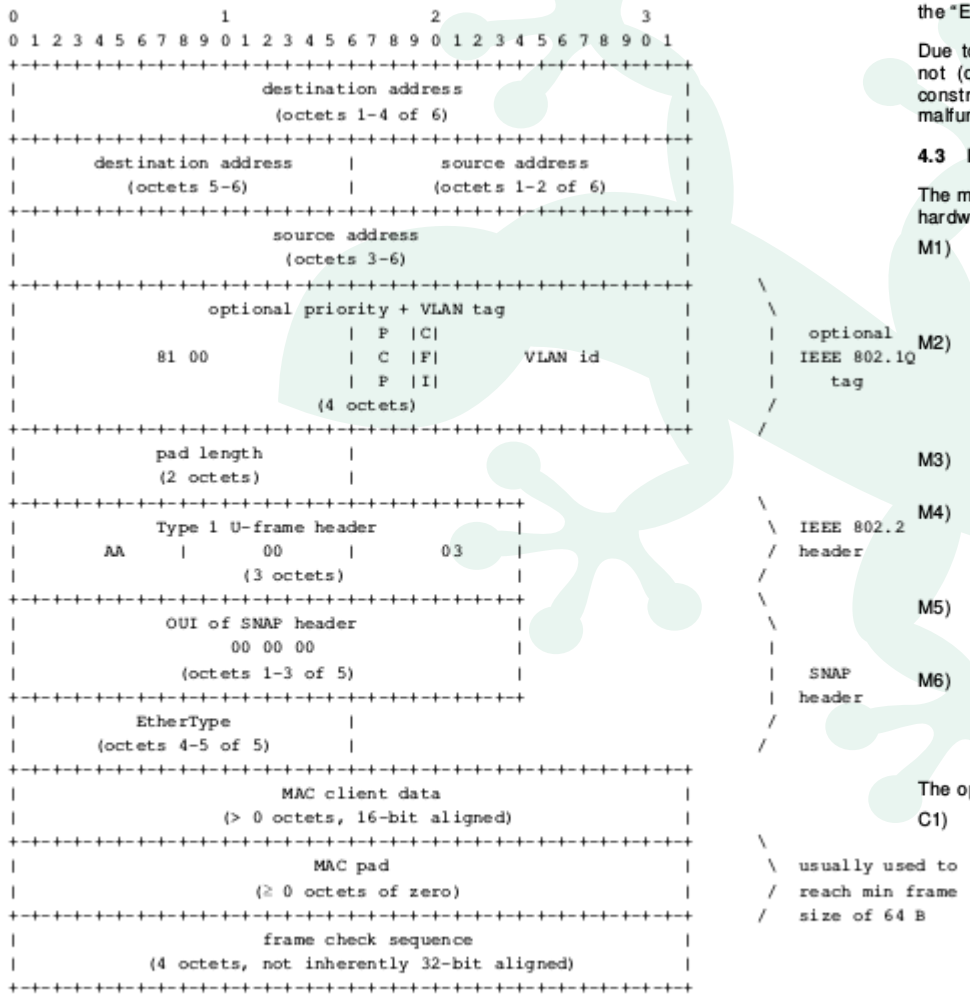


Figure 1 – IEEE 802.3 frame structure with IEEE 802.2 Type 1 and IEEE 802 SNAP

The Ethernet II frame is structured as shown in Figure 2, using a big-endian octet order. The location and structure of the optional IEEE 802.1Q VLAN/priority tag is included.

4.2.4.2 Jumbo frames

IEEE 802.3 does not support "jumbo frames" – ones whose size exceeds that permitted by the IEEE 802.3 standard – because use of such frames would create interoperability problems. However, many procurement specifications require that purchased equipment support jumbo frames. When devices have that capability, it typically is a configuration option of the device, used with the Ethernet II version of the "Ethernet" frame format. For more information see http://en.wikipedia.org/wiki/Jumbo_frame.

Due to lack of interoperability, devices that are configured to support jumbo frames and those that are not (or cannot be) usually are not permitted on the same subnet. However, an attacker is not so constrained. Therefore, while the DUT need not process jumbo frames correctly, it is not permitted to malfunction when receiving jumbo frames.

4.3 Mandatory and optional protocol features

The mandatory features of the "Ethernet" protocol that are amenable to testing using standard "Ethernet" hardware are:

M1) Each "Ethernet" frame SHALL contain at least 64 octets; frames that otherwise would contain fewer than 64 octets SHALL include a Pad field, per IEEE 802.3, 3.1.1.

NOTE 1 The Ethernet hardware of some TDs may extend automatically the size of frames less than the minimum. When that is the case, DUT testing of robustness to receipt of overly short frames (known as "runt frames") will not occur.

M2) As used by the TD to test the DUT with valid frames, the "Ethernet" frame SHALL comprise a maximum of 1518 octets when no Q-tag is present, or 1522 octets when one Q-tag is present, per IEEE 802.3, 3.1.1 and IEEE 802.1Q.

NOTE 2 This size can increase to over 15 kB when jumbo frames (4.2.4.2) are employed on Ethernet II networks. Embedded devices are not expected to use such large frames when communicating with automation control devices.

M3) As used by the TD to test the DUT with invalid frames, the "Ethernet" frame MAY exceed the maximum frame size specified in M1).

M4) The first (lsb) bit in the destination address field SHALL be used to designate the address type as either an Individual address (lsb = 0) or a Group address (lsb = 1), per IEEE 802.3, 3.2.3.b. However, the broadcast address (0xFF FF FF FF FF FF) is classified as a group address even though its first bit is zero.

M5) The "Ethernet" frame's EtherType field SHALL contain a valid value as specified at http://www.iana.org/assignments/ethernet-numbers and http:/standards.ieee.org/regauth/ethertype/eth.txt

M6) The number of pad octets required in a frame data field SHALL be computed such that the total frame size is 64 B, and shall be zero when the total frame size without pad octets is 64 B or greater.

NOTE The TD may exceed this limit when testing the DUT's ability to accept or reject very large frames.

The optional (i.e., conditionally present) features of the Ethernet II protocol are

C1) All Ethernet II frames received by a device with a destination address set to the IEEE 802 broadcast address SHALL be presented to the superior network layer.

ISA Secure – Equipements certifiés

- Description des tests très complète,
- Produit un rapport de conformité avec des tests automatiques,
- Comme PCI, des outils de test qualifiés (approche industrielle).

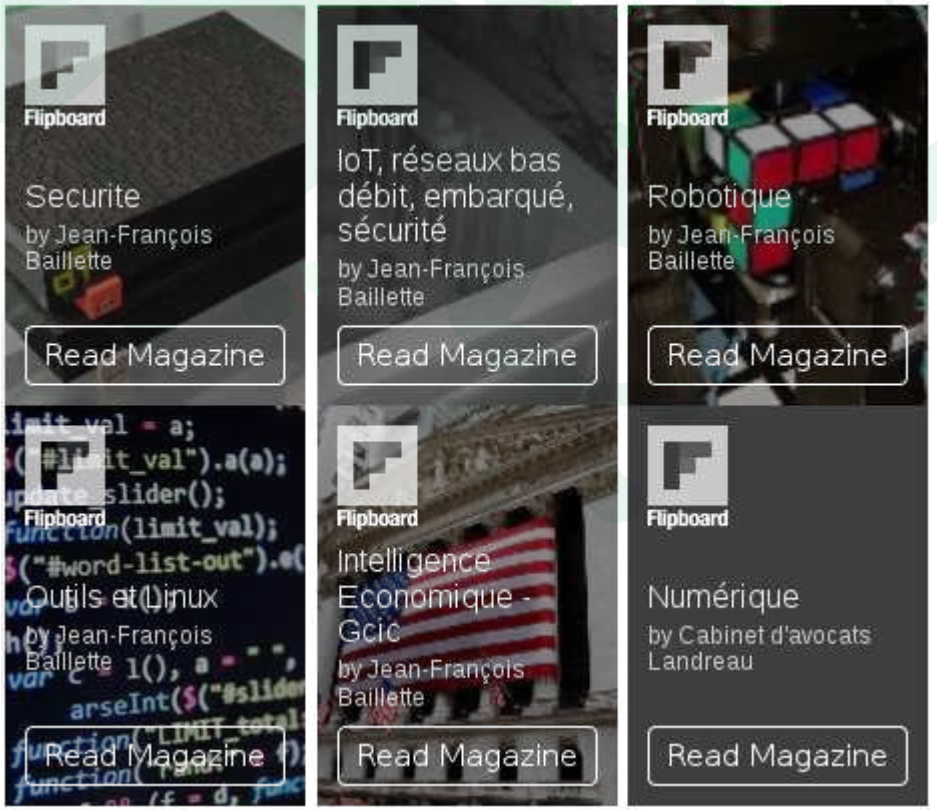
ISASecure Certified Devices

Picture	Supplier ▲	Type	Model	Version	Level	Certification Date
	Azbil Corporation	DCS Controller	Harmonas/Industrial-DEO/Harmonas-DEO system Process Controller DOPCIV (Redundant type)	R4.1	EDSA 2010.1 Level 1	12/17/2014
	Hitachi, Ltd.	DCS Controller	HISEC 04/R900E	01-08-A1	EDSA 2010.1 Level 1	7/14/2014
	Honeywell Process Solutions	Safety Manager	HPS 1009077 C001	R145.1	EDSA 2010.1 Level 1	6/6/2011
	Honeywell				EDSA	

SÉMINAIRE CAPTRONIC SÉCURITÉ IOT ET SYSTÈMES EMBARQUÉS

En partenariat avec CapTronic, nous vous proposons un séminaire de présentation des expériences et bonnes pratiques de sécurité pour la mise au point de solutions embarquées basées sur les réseaux bas débit pour objets connectés (IoT [1]).

Détail du programme et inscriptions à la journée sécurité IoT et systèmes embarqués.



jfbaillette@g-echo.fr