Summary

1. PURPOSE AND SCOPE OF THE CERTIFICATION AGREEMENT 2

2. REFERENCE DOCUMENT 3

3. GENERAL 4
3.1. Applicability 4
3.2. Impartiality 5
3.3. Confidentiality and information in the public domain 6
3.4. Records 7
3.5. Complaints and appeals 7
3.6. Use of trade marks and certificates 8
3.7. Changes to the certification process and regulatory updates 8
3.8. Obligations of the applicant 9

4. APPLICATION FOR CERTIFICATION 10

5. CERTIFICATION PROCEDURE 10

6. NONCONFORMITIES 12

7. SUSPENSION, WITHDRAWAL AND RESTORATION OF CERTIFICATION 13
7.1 Suspension 13
7.2 Suspension requested by the customer 13
7.3 Withdrawal 13
7.4 Penalties 13
7.5 Management of disputes and jurisdiction 14

8. CERTIFICATE CHANGES AND ADDITIONS 15

9. DURATION OF ISSUED CERTIFICATES 16

1. PURPOSE AND SCOPE OF THE CERTIFICATION AGREEMENT

A.C.&E. SRL, hereinafter referred to as A.C.&E., provides testing and certification services to support the conformity of machinery and industrial plants.
A.C.&E. wishes to offer its skills, consistent operation and impartiality as a certification body for customers manufacturing IOT and IIOT in accordance with the ISA SECURE procedure. A.C.&E. guarantees the quality of the results provided and service reliability, complying with the criteria of impartiality, professional ethics, efficiency and effectiveness, as the product certification also involves the end clients using the certified products, government authorities and non-governmental organisations.
A.C.&E. has decided to adopt a Management System complying with standard ISO/IEC 17065:2012 and the additional requirements specified by the Accreditation body PJLab for implementing a certification procedure for products, equipment/machinery, in accordance with IEC 62443-4-1 and 4-2 for cyber security and which comply with one or more of the standards listed in Annex 1 “Regulations”.

A.C.&E. has drafted this certification agreement for the provision of the activities relating to its customers’ purpose of certification.
This contract, which details the responsibilities of A.C.&E. and the responsibilities of the customer, is signed by both parties.

2. REFERENCE DOCUMENTS

This agreement is subject to the following Regulations/Directives:

STANDARD	ED	TITLE
IEC 62443-4-1	1:2018	Secure product development lifecycle requirements.
SDLA	3.0.0	Security Development Lifecycle Assurance (SDLA) Certification The SDLA certifies compliance to the ISA/IEC 62443-4-1 standard.
IEC 62443-4-2	2:2019	Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components
ICSA	1.0.0	IIoT Component Security Assurance (ICSA) Product certification for IIoT Components.
CSA	1.0.0	Component Security Assurance (CSA) Certification

All information on the scope and procedure is also verified before each activity by the website of ISA SECURE and IEC:

IEC 62443-4-1 : https://isasecure.org/certification/iec-62443-sdla-certification

IEC 62443-4-2 : https://isasecure.org/certification/iec-62443-icsa-certification

3. GENERAL

3.1. Applicability

This regulation applies to control system supplier security development lifecycle processes called ISASecure® SDLA certification (Security Development Lifecycle Assurance), embedded devices, as well as software applications, host devices and network devices , as defined in the standard [IEC 62443-4-2], IIoT devices and IIoT gateways.

The regulations does not apply to:
- Devices falling under the scope of IEC 61508
- Household devices falling under the scope of Directive 2014/53/UE

3.2. Impartiality

A.C.&E. has organised and structured specific roles, responsibilities and activities to guarantee the impartiality and absence of conflicts of interest between the certification activities and the other activities performed within the company. All internal and external staff involved in certification activities, including the staff of the impartiality safeguard committee, have undersigned a code of ethics and a letter of appointment, in which their own role is specified.

All staff working in certification activities at A.C.&E., from the proposal to document management, to inspections and reviews and the issue of the certification, are employees or personnel with a regular contract of employment, and their salaries are linked to national contractual forms and do not depend on the number of certifications issued.

Furthermore, A.C.&E. performs its activities avoiding and preventing conflicts of interest, maintaining a position of non-subjection to the specific interests of others of any kind which could interfere in any way with the results of their activities. The staff are aware of the need to notify any potential conflicts of interest that may arise to the Management.

The Management has analysed the risk of compromising its own impartiality; the assessment, and any identification, is performed continuously - and at least once a year during the Management Review - also involving the staff and encouraging them to report any suspicious or hazardous situation they may directly become aware of.

For any impartiality risks identified also following the actions of other persons or external bodies or organisations, A.C.&E. implements suitable actions for managing the potential impact on its performance, either by eliminating or minimising the source or monitoring the risk, and documents how this risk was managed: if, for example, a risk of impartiality due to staff relations is identified, this could be managed by assigning the staff to a different task. The Management undertakes to inform all operating staff of the principle of impartiality, and demands that this be applied: each person is required to undersign the Code of Ethics and the Letter of Appointment.

It is underlined that A.C.&E. and its internal or external staff shall not:

- be the designer, manufacturer, installer, distributor or maintenance engineer of the certified product;
- offer or provide advice to their customers (see point 3.2);
- offer or provide internal audit services for their

customers.

Without prejudice to the following:

the possibility to exchange information (e.g., explanations of results or clarifications of requirements) between A.C.&E. and its customers.

Staff who have provided advice for a given product shall not be used to review or take decisions relating to the certification of that product for a period of no less than three years.

The organisational structure of A.C.& E. excludes the risk of conflicts and/or interference between A.C.& E s.r.l. and the certification activities of A.C.& E., implementing the same methods, i.e., by undersigning the code of ethics, letters of appointment and meetings.

Furthermore, the activities of A.C.&E. are not marketed or proposed as linked to the activities of an organisation that provides consulting services.

3.3. Confidentiality and information in the public domain

A.C.&E. guarantees confidentiality of the information obtained during the conduct of its activities, in accordance with the provisions of current privacy legislation (– Decreto Legislativo 51/2018). The guarantee of confidentiality is included as a contractual clause in the certification agreement, in which A.C.&E. indicates the information it intends to make public to the customer.
As regards the protection of confidential information, A.C.&E. has defined the following security measures required to eliminate or reduce any data protection risks.
An IT Systems Administrator has been appointed at A.C.&E. and assigns authorisation credentials to each appointed person that consist of:
the appointed person's personal ID code
a password known only to the appointed person
The IT network has an authorisation system that enables access to and processing of data, according to the authorisation profile of the person accessing the system.
In order to guarantee the integrity of the data against the risk of destruction, damage or loss of data due to external intrusions or viruses, the Systems Administrator has established the software protections to be adopted. The software or hardware systems used to obtain an acceptable security standard are upgraded automatically by the server connected to the Internet.
Every user shall adopt conduct to reduce the risk of attacks on the company IT system through viruses or any other aggressive software, and is bound to monitor the regular operation and periodic upgrading of the software installed.
The Systems Administrator has given specific instructions on data storage, recovery and elimination and/or destruction where required.
Data recovery is checked every six months by the Systems Administrator using the specific module, and evidence of this is provided during the Management Review.
Documents with significant contents or documents considered confidential are not sent by e-mail or fax without the prior written authorisation of the customer. The documents are sent by UPLOAD WITH ZIPPED FILES WITH PASSWORD (see Operating Instruction).

Hard copies of deeds and documents containing personal data, and particularly sensitive or legal data, assigned to the data processors to perform their related tasks, are monitored and stored by the appointed persons until their return in a manner that prevents access thereto by unauthorised persons, and are returned at the end of the assigned operations.
Documents containing sensitive and legal data are kept in places that are continuously monitored by the company staff.
A.C.&E. shall inform the Customer, or any data subjects, of the information they are obliged to provide by law, or the use of confidential information where contractually authorised, unless they are prohibited by law from informing them.
If information concerning the customer is obtained from other sources, it shall be kept confidential between the customer and A.C.& E., which in any case shall not reveal the source to the customer, unless other such agreements are made with the party providing the information.

3.4. Records

All records are kept for 13 years to demonstrate that all certification process requirements have been effectively met. The information transmission system developed by A.C.&E. ensures that confidentiality is maintained.

3.5. Complaints and appeals

A.C.&E. considers and manages complaints and appeals as nonconformities.
Within 8 days of receipt of complaints and appeals, the Technical Secretariat shall notify the customer that they are processing the complaint or appeal. The Technical Secretariat gathers and processes all the related information, analysing the causes and any corrective actions, as it is familiar with the certification procedures, but never intervenes in the assessment of or decision on the certification. Where directly involved in a complaint, the complaint is managed by the CTO.
After assessing the complaint or appeal, A.C.&E. informs the complainant in writing of the outcome and conclusion of the complaint or appeal process. In the case of recourse to a corrective action to solve the complaint or appeal, A.C.&E. implements these actions.

3.6. Use of trade marks and certificates

Refer to document ITA_MOD03-PG02-REGULATION ON THE USE OF THE LOGO for the use of trade marks and certificates.

3.7. Changes to the certification process and regulatory updates

If the certification procedures introduces new requirements (e.g. issue of a new standard) or some requirements (e.g. standard) are subject to revision, and these have an effect on the customer, the CTO reviews the new requirements and establishes the related actions needed to guarantee conformity, which must be implemented by the customers. The Technical Secretariat notifies these changes to the customers and the related actions required to ensure conformity with the requirements laid down in the certification procedure. A.C.&E. checks that the changes have been implemented by the customers within 6 months following notification.

In addition to “external” changes affecting the customer, A.C.&E. has taken into consideration other “internal” changes coming directly from the customer (e.g. new technologies, new sites, etc.). Also in these cases, the CTO reviews the new requirements and establishes the related actions to assess the conformity with the requirements laid down in the certification procedure. The Technical Secretariat notifies the customer of the related actions required, which must be implemented. A.C.&E. checks that the changes have been implemented by the customers within 6 months following notification.

The actions undertaken by A.C.&E. to check the changes that affect the certification are:

- assessment (paragraph 7.4)
- review (paragraph 7.5)
- decision (paragraph 7.6)
- issue of official certification documentation subjected to revision (paragraph 7.7) to extend or reduce the scope of the certification;
- issue of certification documentation on surveillance activities subjected to revision;
- the change or updating of the list (paragraph 7.8)

The decision to not exclude one of the above-described activities must be minuted (e.g., if a certification requirement which is not a product requirement changes, it may not be necessary to perform any assessment, review or decision)

3.8. Obligations of the applicant

The customer must:

a) always meet the certification requirements which, including product requirements and any appropriate amendments notified by A.C.&E. must always be implemented;

b) ensure that the certified product continues to meet the product requirements specified in the standards or other regulatory documents identified in the certification procedure.

c) allow:

1) the performance of the assessment and surveillance (where required), also making available the documentation and records, providing access to relevant equipment, the site/s, area/s, staff and subcontractors of the customer;

2) the investigation of complaints;

d) make declarations on the certification that are consistent with the actual scope of the certification

e) not use its product certification in a manner that could discredit A.C.&E. or make any declarations concerning their product certification which A.C.&E. may consider misleading or unauthorised;

f) under suspension, withdrawal or expiry of the certification, stop using all the advertising material containing any reference to this and take actions as required in the certification procedure (e.g. return the certification documents) and adopt any other measure requested;

g) if they provide copies of the certification documents to others, the documents must be reproduced in their entirety;

h) in referring to their product certification in communication means such as documents, leaflets or advertising material, comply with the provisions of the certification logo regulation of A.C.& E.;

i) comply with any requirement that may be provided for in the certification procedure relating to the use of conformity marks and product information;

j) keep records of all complaints submitted that they are aware of, concerning conformity with the certification requirements and make these records available to A.C.&E. when requested, and

1) take appropriate actions with reference to these complaints and any defects reported in the products which could affect the conformity with the certification requirements,
2) document the actions undertaken;

k) promptly inform A.C.& E., of any changes which may affect their ability to meet the certification requirements.

These changes may be:

- the legal, commercial, organisational status or ownership;
- the organisation and management (e.g. the persons who hold key management positions, take decisions or technical staff);
- contact details and production sites;
- major changes to the quality management system.

4. APPLICATION FOR CERTIFICATION

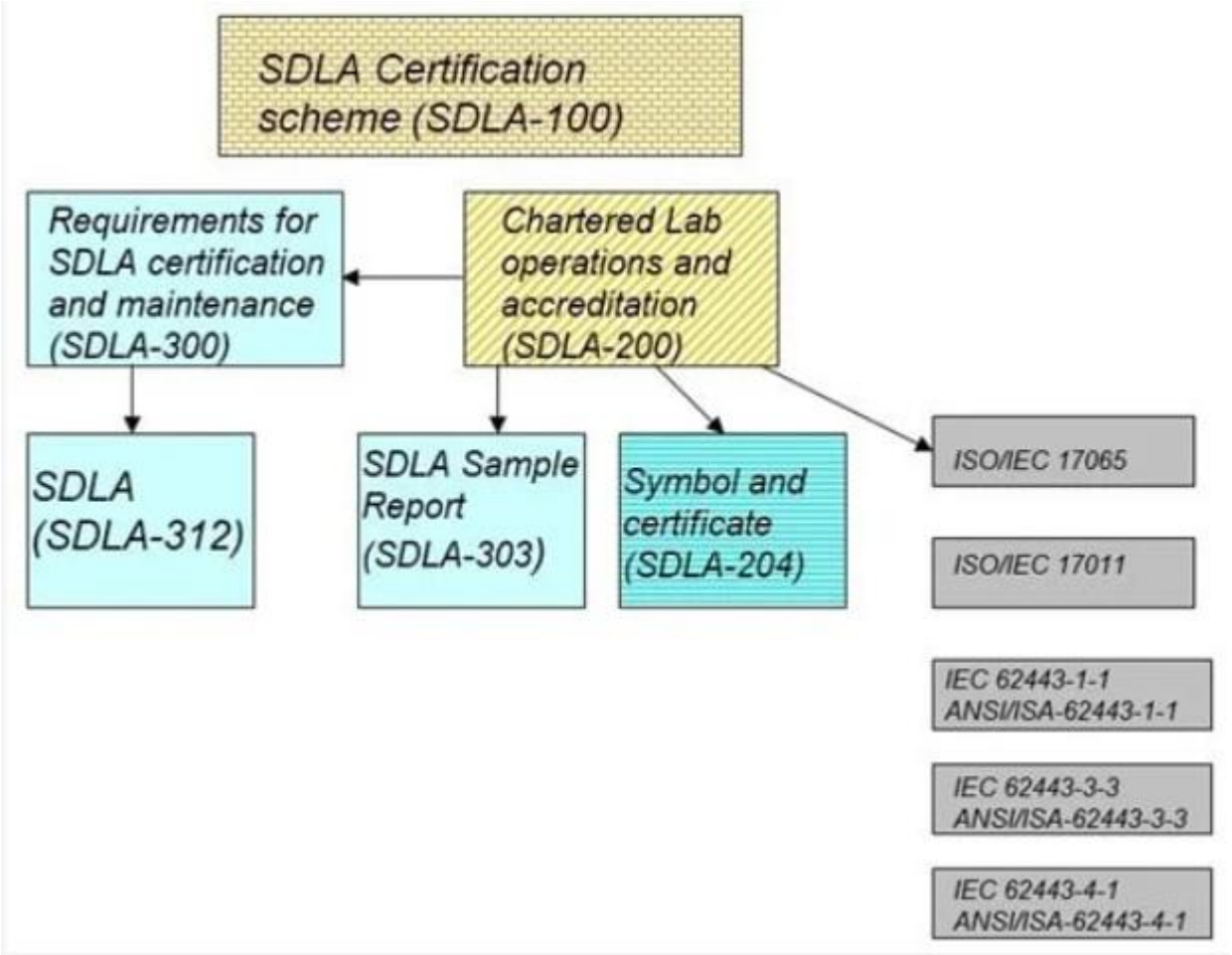
The customer completes the file “IT_MOD01-PG02_DOMANDA” available on the website ac-e.webflow.io/ and forwards the application to the Technical Secretariat (areatecnica@ac-e.com), returning it signed along with this agreement.
If the application is reviewed, the latter will be revised, updated and then signed.

5. CERTIFICATION PROCEDURE

Based on the customer's request, as per the table below, already completed in the application:

Security Development Lifecycle Assurance (SDLA) Certification (mandatory)
Component Security Assurance (CSA) Certification
IIoT Component Security Assurance (ICSA)

the following flow will be monitored:



The customer has the right to have the tests performed by a laboratory of their choice, other than that proposed by A.C.&E. The laboratory chosen by the customer shall be confirmed by A.C.&E. and in any case accredited in accordance with standard ISO 17025 and shall submit a copy of the related accreditation.

6. NONCONFORMITIES

If nonconformities arise in relation to the certification requirements during the certification procedure, the CTO examines the nonconformity and decides on the appropriate actions to be undertaken, which may be:

- the continuation of the certification under specific conditions (enhanced surveillance);
- the reduction of the scope of the certification to eliminate the non-conforming product variants;
- the suspension of the certification pending corrective actions by the customer;
- the withdrawal/non-issue of the certification.

When the actions involve the assessment, review and decision on the certification, the procedure must be repeated (including surveillance checks), having resolved a nonconformity.

7. SUSPENSION, WITHDRAWAL AND RESTORATION OF THE CERTIFICATION

7.1 Suspension

If the certification is suspended, the CTO takes this decision and the Technical Secretariat notifies the following to the customer:

- the actions required to end the suspension and restore the certification for the product(s) in compliance with the certification procedure;
- any other actions required by the certification procedure.

A.C.&E. takes into consideration the suspension or withdrawal and/or withdrawal due to failure to comply with the payments as specified in the certification agreement.

All the requirements must be implemented in order to end the suspension.

The customer shall implement the required actions within 6 months; an extension of 6 months may be granted, following which, if the actions required have not been implemented, the certification is withdrawn.

If the certification is restored following suspension, A.C.&E. implements all required changes to the official certification documents, the information to the public (list of websites), trade mark authorisations, in order to ensure that all the appropriate indications are given that the product continues to be certified. If it is reduced, A.C.&E. shall inform the public that the scope of the certification has been reduced and that this is clearly notified to the customer and is clearly specified in the certification documentation and in the information to the public.

7.2 Suspension requested by the customer

If the certification is terminated at the request of the customer, or suspended or withdrawn, A.C.&E. takes the actions specified in paragraph 4.1.3 and implements all the changes required for the official certification documents, the information to the public (list of websites), the authorisations for the use of trade marks, etc., in order to ensure that there are no indications that the product continues to be certified.

In the case of the reduction in the scope of application of the certification, A.C.&E. undertakes the actions described in paragraph 7.10, implementing all the changes required to the official documents by the certification procedure, to the information to the public (list of websites), the authorisations for the use of trade marks in order to ensure that the reduced scope of application of the certification is clearly notified to the customer and is clearly specified in the certification documentation and in the information to the public.

7.3 Withdrawal

Customers whose certification has been withdrawn in relation to a given procedure shall definitively stop using the A.C.&E. logo in all its forms and places in relation to the aforementioned procedure.

In the event of withdrawal of the certification, A.C.&E. notifies in writing that the logo may not be used in any form or place.

The customer is permitted to sell any stocks of products on which the logo has already been placed provided that these products were manufactured during the period of validity of the certification and are sold while stocks last.

7.4 Penalties

In the event of a breach of the regulation by the customers, A.C.&E. applies the following measures, in increasing order of severity:

- written warning with request to immediately adopt the corrective actions and treatments;
- in the event of the failure to implement, or inappropriate implementation of the corrective actions and/or treatments and/or the repetition of the nonconformity: suspension of the certificate for a period that is commensurate to the severity of the situation;
- in the event of non-compliance and/or repeated breach beyond the term of the suspension: withdrawal of the certification.

For each breach of the rules governing the use of logos contained in the logo use regulation, in the contract (certification agreement and regulation), the customer shall pay A.C.&E. a penalty equal two times the price of the certification

Furthermore, A.C.&E. may request compensation for any further damages caused by any matter relating to the improper use of the logo by the customer.

A.C.&E. uses all means to check and ascertain that the logo is used in compliance with the regulations, requesting the submission of documentation. If the customer refuses, A.C.&E. has the right to terminate the services contract pursuant to Art. 1453 of the “Codice Civile”. A.C.&E. reserves the right to report any abuses or incorrect uses of the logo by the customer on its website.

7.5 Management of disputes and jurisdiction

Any disputes will be referred to the jurisdiction of the Courts of Verona.

8. CERTIFICATE CHANGES AND ADDITIONS

If the certification procedures introduces new requirements (e.g. issue of a new standard) or some requirements (e.g. standard, **the product**) are subject to revision, and these have an effect on the customer, the CTO reviews the new requirements and establishes the related actions needed to guarantee conformity, which must be implemented by the customers. The Technical Secretariat notifies these changes to the customers and the related actions required to ensure conformity with the requirements laid down in the certification procedure. A.C.&E. checks that the changes have been implemented by the customers within 6 months following notification.

In addition to “external” changes affecting the customer, A.C.&E. has taken into consideration other “internal” changes coming directly from the customer (e.g. new technologies, new sites, etc.). Also in these cases, the CTO reviews the new requirements and establishes the related actions to assess the conformity with the requirements laid down in the certification procedure. The Technical Secretariat notifies the customer of the related actions required, which must be implemented. A.C.&E. checks that the changes have been implemented by the customers within 6 months following notification.

The actions undertaken by A.C.&E. to check the changes that affect the certification are:

- assessment
- review
- decision
- issue of official certification documentation subjected to revision to extend or reduce the scope of the certification;
- issue of certification documentation on surveillance activities subjected to revision;
- the change or updating of the list

The decision to not exclude one of the above-described activities must be minuted (e.g., if a certification requirement which is not a product requirement changes, it may not be necessary to perform any assessment, review or decision).

9. DURATION OF THE CERTIFICATES ISSUED

The ISASecure SDLA program complements these ISASecure certification programs that certify specific products and is therefore mandatory in order to obtain the ICSA and/or CSA certification.

The SDLA Certificate has a duration of 36 months, an organization MAY extend the expiration date for their existing 36-month certification by undergoing a recertification audit as described in ISASecure_SDL.R10.

An applicat can apply for a SDLA readiness evaluation, which is a certification with the duration of 12 months. This scheme of certification is used in case an applicant does not have a product ready for evaluation.
A certifier SHALL grant an extension to an initial SDLA certification that had been granted with 12 months to expiration, if the following criterion is met. The new certification SHALL expire at the end of the month, 36 months after the granting of the prior 12-month certification.

- All SDLA requirements that initially passed based upon an SDLA readiness evaluation have passed an SDLA full evaluation, where these evaluation types are defined in requirement ISASecure_SDL.R5 of this document. If this criterion has not been met as of the expiration date of the 12-month certification, SDLA certification SHALL expire. In this case, to regain SDLA certification, a development organization SHALL pass all requirements based upon an SDLA evaluation as defined in requirement ISASecure_SDL.R5.

In order to maintain ICSA and CSA certifications the applicant must remain in good standing under the Security maintenance audit (SMA).

Good standing under SMA for a supplier of an ICSA-certified component, formally means that SMA for the component has been conducted as required by this specification, and there are currently no open SMA nonconformities for the component.

The SMA is a process that has 3 mandatory steps:
- One year after certification: The one-year period after ICSA certification. The subject releases of this audit are the certified version of the product and its updates and upgrades, whether or not certified ; or
- Next SDLA recertification: The period from the point of ICSA certification, up to the time of the next SDLA recertification of the supplier, where the recertification applies to the SDL for which the product falls under the scope of that SDL. This option MAY be selected IF this period is between 9 months and 18 months in length. The subject releases of this SMA are the certified version of the product and its updates and upgrades, whether or not certified. This option allows SMA activities and SDLA recertification activities to be coordinated for efficiency where feasible.

All records are kept for 13 years to demonstrate that all certification process requirements have been effectively met.

Verona on _____ of_____ 20___

A.C.&E. S.r.l. **Signed** **Matteo Marconi - CEO**	**Customer:** **Signed**