Progetti in corso:

ISO/IEC JTC 1/SC 7	ISO/IEC 15026-2:2011 - Systems and software engineering - Systems and software assurance -- Part 2: Assurance case. Specifica i requisiti minimi per la struttura e il contenuto di un Assurance Case per migliorare la coerenza e la comparabilità degli Assurance Case e per facilitare le comunicazioni delle parti interessate, le decisioni d'ingegneria e altri Assurance Case. Secondo questo documento ISO "*An assurance case includes a top-level claim for a property of a system or product (or set of claims), systematic argumentation regarding this claim, and the evidence and explicit assumptions that underly this argumentation. Arguing through multiple levels of subordinate claims, this structured argumentation connects the top-level claim to the evidence and assumptions*". ISO/IEC CD 15026-3 Systems and software engineering -- Systems and software assurance -- Part 3:2015 System Integrity levels. Si riferisce ai livelli d'integrità dell'Assurance Case e include i requisiti relativi al loro utilizzo con e senza un Assurance Case. Secondo questo documento ISO "*A software integrity level denotes a range of values of a software property necessary to maintain system risks within tolerable limits*".
ISO/IEC JTC 1/SC 27	ISO/IEC 27021:2017 Information technology -- Security techniques -- Competence requirements for information security management systems professionals ISO/IEC/IEE 15026-1:2019: Systems and software engineering -- Systems and software assurance -- Part 1: Concepts and vocabulary ISO/IEC 15026-2:2011 Systems and software engineering — Systems and software assurance — Part 2: Assurance case ISO/IEC NP 20004: Information technology - Security techniques - Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405. Si riferisce a un problema differente e più urgente associato all'uso pratico dei Common Criteria, ossia la relazione tra i processi di sviluppo e di valutazione con l'analisi dei potenziali attacchi. E' legato all'iniziativa CAPEC. ISO/IEC TS 19608: 2018 Guidance for developing security and privacy functional requirements based on ISO/IEC 15408 ISO/IEC TS 19249: 2017 Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls

5.1.5 International Society of Automation (ISA)

ISA è un'organizzazione globale no-profit che sviluppa standard per l'industria, certifica i professionisti di settore, offre istruzione e formazione, pubblica libri e articoli tecnici, ospita convegni e fiere per i professionisti dell'automazione.
La cybersecurity per l'industria è diversa dalle altre aree. Nell'automazione industriale la priorità è mantenere l'impianto in funzione garantendo, laddove possibile, integrità e riservatezza (AIC - availability,

integrity and confidentiality) mentre nelle altre aree la priorità è la protezione dei dati (CIA - confidentiality, integrity, availability).

URL	https://www.isa.org/
Country of HQ location **Geographic Scope**	US International
Type	Industry (not for profit)

I membri ISA pagano una tassa regolare (annuale o biennale), in base al loro tipo di appartenenza, al fine di ottenere i benefici ISA come l'accesso alle informazioni tecniche e alle risorse per lo sviluppo professionale.

Risultati più rilevanti:

Standards	**ANSI/ISA 62443** (formerly **ISA-99**) - **Security for industrial automation and control systems** - è una serie di standard, report tecnici e relative informazioni che definiscono le procedure per l'implementazione di sistemi sicuri di automazione e controllo industriale (IACS). La presente guida si applica a tutte le parti interessate che attuano o gestiscono l'IACS. Tutti gli standard ISA-62443 e i report tecnici sono organizzati in quattro categorie generali denominate *General*, *Policies and Procedures*, *System and Component*.
INDUSTRIAL CYBERSECURITY STANDARDS	ANSI/ISA-62443-4-2-2018, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components. ANSI/ISA-62443-4-1-2018, Security for industrial automation and control systems, Part 4-1: Product security development life-cycle requirements. Definisce un **secure development life-cycle (SSDLC)** allo scopo di realizzare e mantenere prodotti software sicuri. Questo ciclo di vita comprende la definizione dei requisiti di sicurezza, la progettazione sicura, l'implementazione sicura (incluse le linee guida di codifica), la verifica e la convalida, la gestione dei difetti di sicurezza, la gestione delle patch e la fine del ciclo di vita del prodotto. Tali requisiti possono essere applicati a processi nuovi o esistenti per sviluppare, mantenere e dismettere hardware, software o firmware per prodotti nuovi o esistenti. Tali requisiti si rivolgono allo sviluppatore e al manutentore del prodotto, ma non agli addetti all'integrazione né all'utente finale del prodotto. ANSI/ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 CSV, Security for industrial automation and control systems, Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2015+AMD1:2017 CSV, IDT). ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security levels. Questo standard definisce i requisiti di sicurezza che sono raggruppati in sette categorie: 1) Controllo degli accessi, 2) Controllo dell'utilizzo, 3) Integrità dei dati, 4) Riservatezza dei dati, 5) Limitazione dei flussi di dati, 6) Risposta tempestiva a un evento e 7) Disponibilità delle risorse di rete. Ogni categoria comprende una mappatura dei requisiti per garantire un adeguato livello di sicurezza.