Associazione Italiana Strumentisti

ISA Italy Section

«LE DIMENSIONI DELLA SICUREZZA INDUSTRIALE»
I percorsi della sicurezza industriale dagli standard ISA/IEC 62443 ai temi della cybersecurity

Milano, 30 Maggio 2018

Auditorio TECNIMONT

Le dimensioni della sicurezza industriale

ReD OPEN BICOCCA RESEARCH GROUP
Responsibility and Design in OPEN ecosystems

1998-2018 20 UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA VENTESIMO ANNIVERSARIO

Massimo V.A. Manzari
Change Management Designer
Co-Founder ReD Open Bicocca Research Group

massimo@massimomanzari.it

I fondamentali....

Immagine tratta da : Current Standards Landscape for Smart Manufacturing System - NIST
http://dx.doi.org/10.6028/NIST.IR.8107

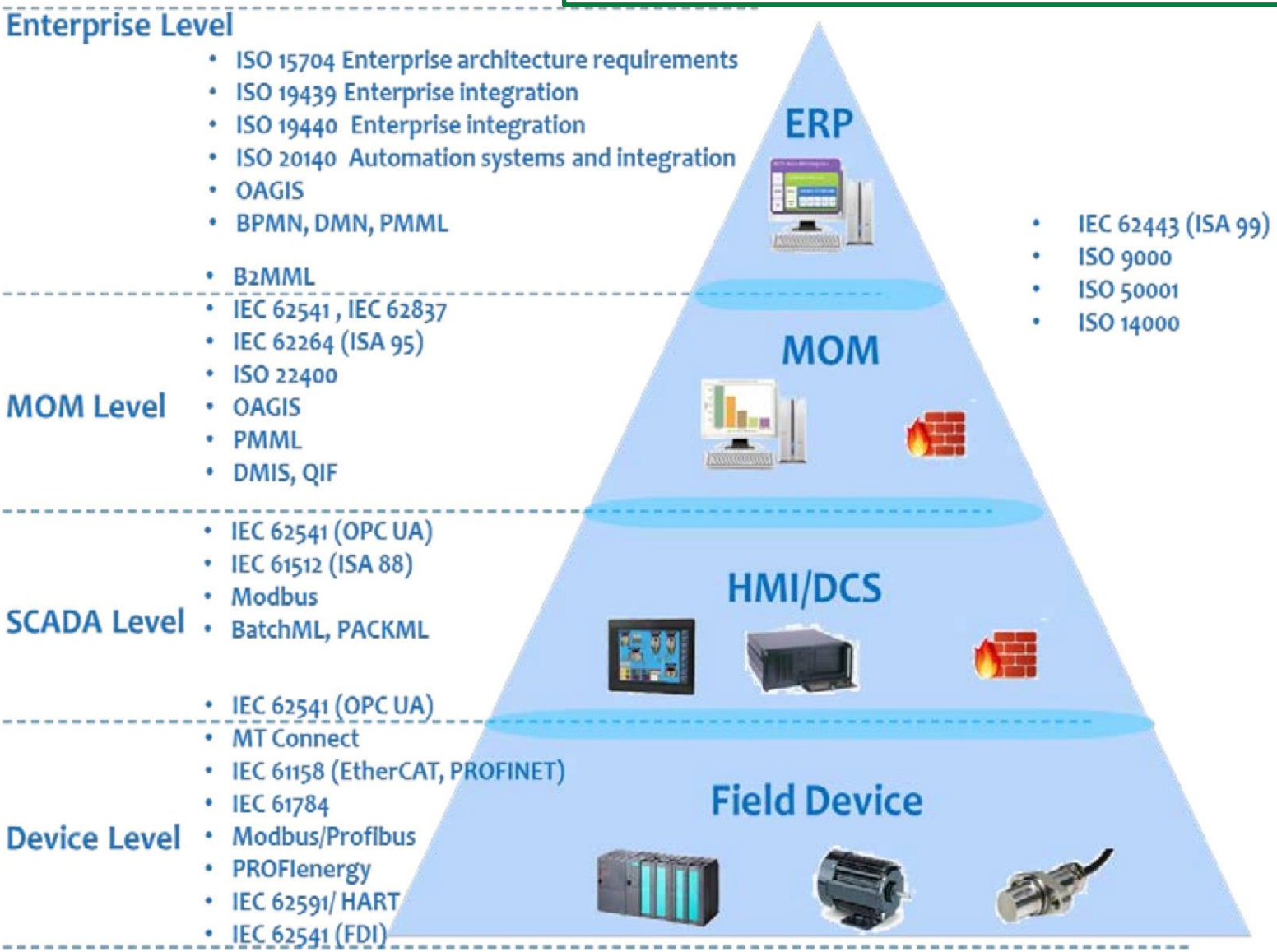
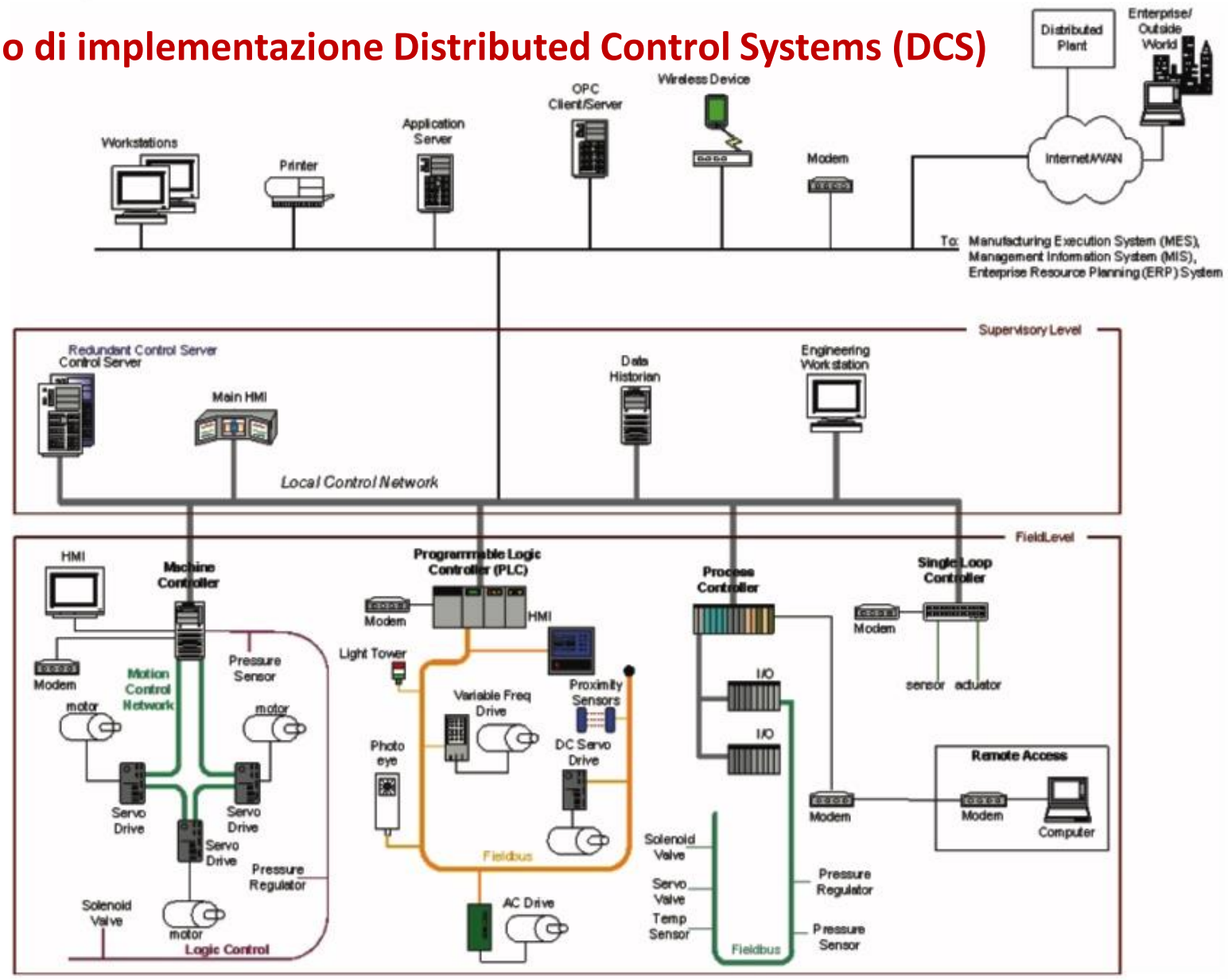


Figure 5: Standards aligned to the ISA95 model

Esempio di implementazione Distributed Control Systems (DCS)



Source: Stouffer, Keith; Joe Falco; Karen Scarfone; ***Guide to Industrial Control Systems (ICS) Security***, Special Publication 800-82, NIST, USA, 2013, figure 2.7. Reprinted courtesy of the National Institute of Standards and Technology, US Department of Commerce. Not copyrightable in the United States.

Immagine tratta da : Current Standards Landscape for Smart Manufacturing System - NIST http://dx.doi.org/10.6028/NIST.IR.8107

Per approfondire …

Setting the Standard for Automation™

ISA
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709
E-MAIL info@isa.org
www.isa.org

The 62443 Series of Standards

Industrial Automation and Control Systems Security

Introduction

The 62443 series of standards have been developed jointly by the ISA99 committee and IEC Technical Committee 65 Working Group 10 (TC65WG10) to address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS). The ISA versions of the standards and reports in the series have names of the form "ISA-63443-x-y", while the IEC versions appear as "IEC 62443-x-y." The ISA and IEC versions of each document are released as closely together as possible.

Scope

The concept of industrial automation and control systems electronic security is applied in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries. Manufacturing and control systems include, but are not limited to:

- hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems.
- associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Series Goal

The goal in applying the 62443 series is to improve the safety, availability, integrity and confidentiality of components or systems used for industrial automation and control, and to provide criteria for procuring and implementing secure industrial automation and control systems. Conformance with the requirements of the 62443 series is intended to improve electronic security and help identify and address vulnerabilities, reducing the risk of compromising confidential information or causing degradation or failure of the equipment (hardware and software) of processes under control.

The content of the series is directed towards those responsible for specifying, designing, developing, implementing, or managing industrial automation and control systems. This information also applies to users, system integrators, security practitioners, and control systems manufacturers and vendors.

A series of standards, being developed by 2 groups:

- ISA99 Committee → ANSI/ISA-62443
- IEC TC65/WG10 → IEC 62443

With guidance and consultation from:

- ISO/IEC JTC1/SC27 → ISO/IEC 2700x

The documents in the 62443 series are shown in Figure 1.

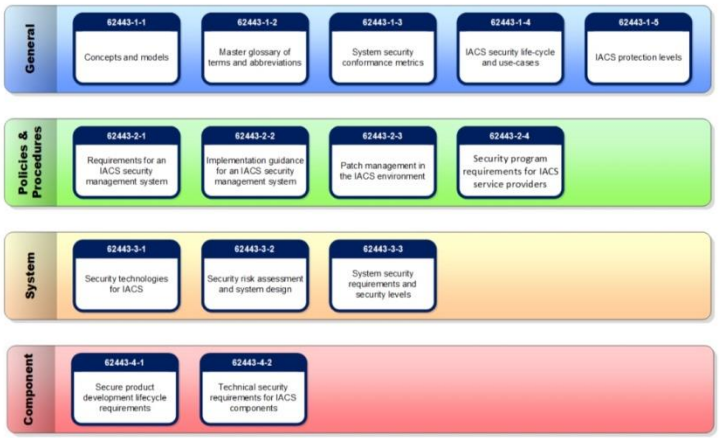


Figure 1 – 62443 Documents

Revised: February 2018

http://isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf

The IERC definition states that IoT is "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.".

http://www.internet-of-things-research.eu

Le dimensioni globali del fenomeno

Table 1: Smart Manufacturing and other manufacturing paradigms[1, 2, 3, 4, 5 and 6]

Smart Manufacturing Characteristics	Other Manufacturing Paradigms	Enabling Technology
• Digitization of every part of a manufacturing enterprise with interoperability and enhanced productivity • Connected devices and distributed intelligence for real time control and flexible production of small batch products • Collaborative supply chain management with fast responsiveness to market changes and supplying chain disruption • Integrated and optimal decision making for energy and resource efficiency • Advanced sensors and big data analytics through product lifecycle to achieve fast innovation cycle	**Lean Manufacturing** - Emphasis on utilizing a set of "tools" that assist in the identification and steady elimination of all kinds of waste in a manufacturing system[1]	Process leveling; work flow optimization; real-time monitoring and visualization
	Flexible Manufacturing - utilizing an integrated system of manufacturing machine modules and material handling equipment under computer control to produce products with changed volume, process and types[2]	Modularized design; interoperability; service oriented architecture
	Sustainable Manufacturing - creating products with minimal negative environmental impacts while conserving energy and natural resources and enhancing human safety[3].	Advance materials; sustainable processes metrics and measurement, monitoring and control
	Digital Manufacturing - using digital technology through product lifecycle to improve product, process, and enterprise performance and reduce the time and cost of manufacturing[4].	3D modeling; model based engineering; product lifecycle management
	Cloud Manufacturing – - a form of decentralized and networked manufacturing based on cloud computing and service-oriented architecture (SOA)[5].	Cloud Computing, IoT, virtualization, service-oriented technologies, and advanced data analytics
	Intelligent Manufacturing - implementing artificial intelligence based intelligent production that can automatically adapt to changing environments and varying proc ess requirements, with minimal intervention from human[6].	Artificial intelligence ; Advanced Sensing and control; optimization; knowledge management
	Holonic Manufacturing - applying agents to a dynamic and decentralized manufacturing process, so that changes can be made dynamically and continuously[7].	Multi-agent systems; decentralized control; model based reasoning and planning
	Agile Manufacturing - utilizing effective processes, tools, and training to enable manufacturing systems to respond quickly to customer needs and market changes while still controlling costs and quality[8].	Collaborative engineering, supply chain management, product life cycle management

Immagine tratta da : Current Standards Landscape for Smart Manufacturing System - NIST http://dx.doi.org/10.6028/NIST.IR.8107

Current Standards Landscape for Smart Manufacturing Systems – NIST 2016

Le dimensioni globali del fenomeno

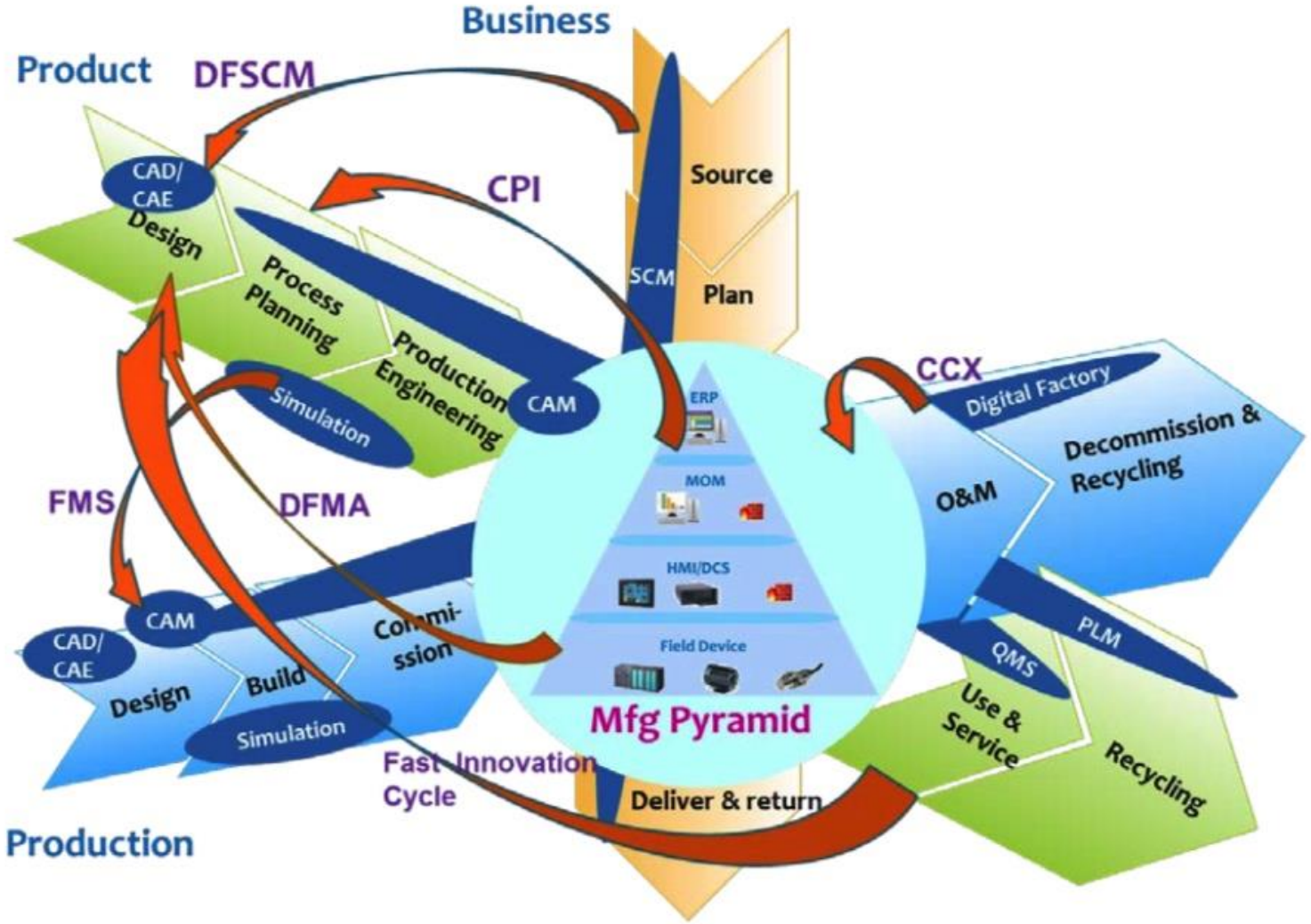


Figure 1. Smart Manufacturing Ecosystem

Current Standards Landscape for Smart Manufacturing Systems

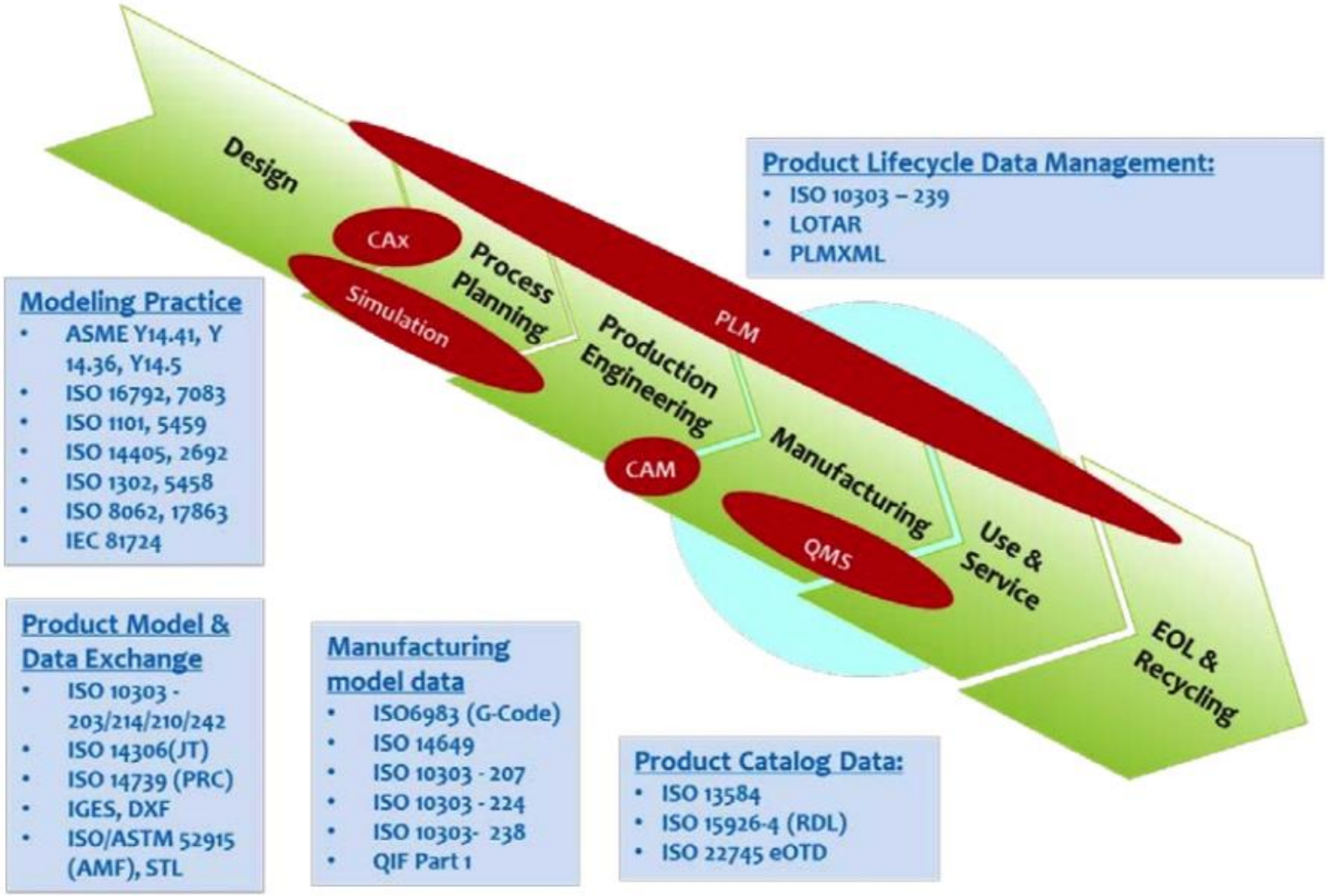


Figure 2. Standards along the Product Lifecycle

Immagine tratta da : Current Standards Landscape for Smart Manufacturing System - NIST http://dx.doi.org/10.6028/NIST.IR.8107

Le dimensioni globali del fenomeno

Health and Safety Executive

Home | News | Guidance | About you | About HSE | Contact HS

HSE » About HSE » Inside HSE

Rate this page ☆☆☆☆☆ Share Free updates

Inside HSE

+ How we work
+ Annual and other reports

Inside HSE

Our mission is to prevent death, injury and ill health in Great Britain's

Introduction

Cyber security is a term used to define measures taken to protect Industrial Automation and Control Systems (IACS) against threats to security through accidental circumstances, actions or events, or through deliberate attack. The threats can originate from the internet, corporate networks, maintenance activities, software upgrades, and unauthorised access etc. with the potential to result in incidents with major health, safety or environmental consequences.

- Notify HSE
- FAQs
- Legislation
- Subscribe

Real people video

More about how we work

Appendix 1: Process for the Management of Cyber Security on IACS

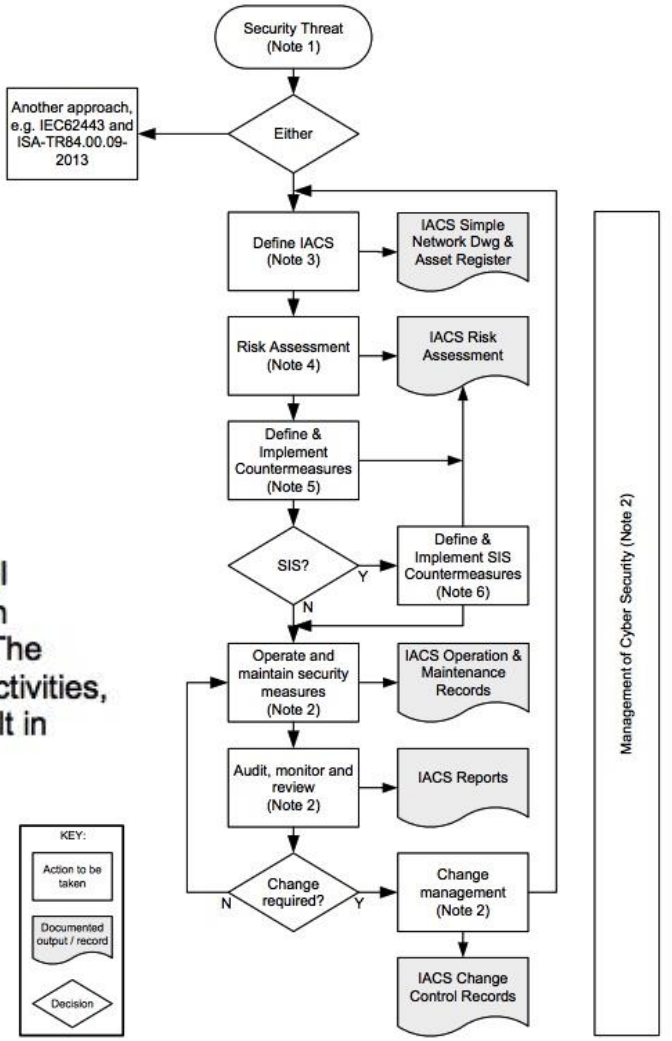


Figure 1: Process for Management of Cyber Security on IACS

http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

Le dimensioni globali del fenomeno

NIST Releases Version 1.1 of its Popular Cybersecurity Framework

April 16, 2018

GAITHERSBURG, Md.—The U.S. Commerce Department's National Institute of Standards and Technology (NIST) has released version 1.1 of its popular Framework for Improving Critical Infrastructure Cybersecurity, more widely known as the Cybersecurity Framework.

"Cybersecurity is critical for national and economic security," said Secretary of Commerce Wilbur Ross. "The voluntary NIST Cybersecurity Framework should be every company's first line of defense. Adopting version 1.1 is a must do for all CEO's."

Credit: N. Hanacek/NIST

MEDIA CONTACT

Jennifer Huergo
jennifer.huergo@nist.gov
(301) 975-6343

ORGANIZATIONS

Information Technology Laboratory
Applied Cybersecurity Division
Cybersecurity and Privacy Applications Group

RELATED LINKS

FACT SHEET: Cybersecurity Framework Version 1.1

https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

Le dimensioni globali del fenomeno

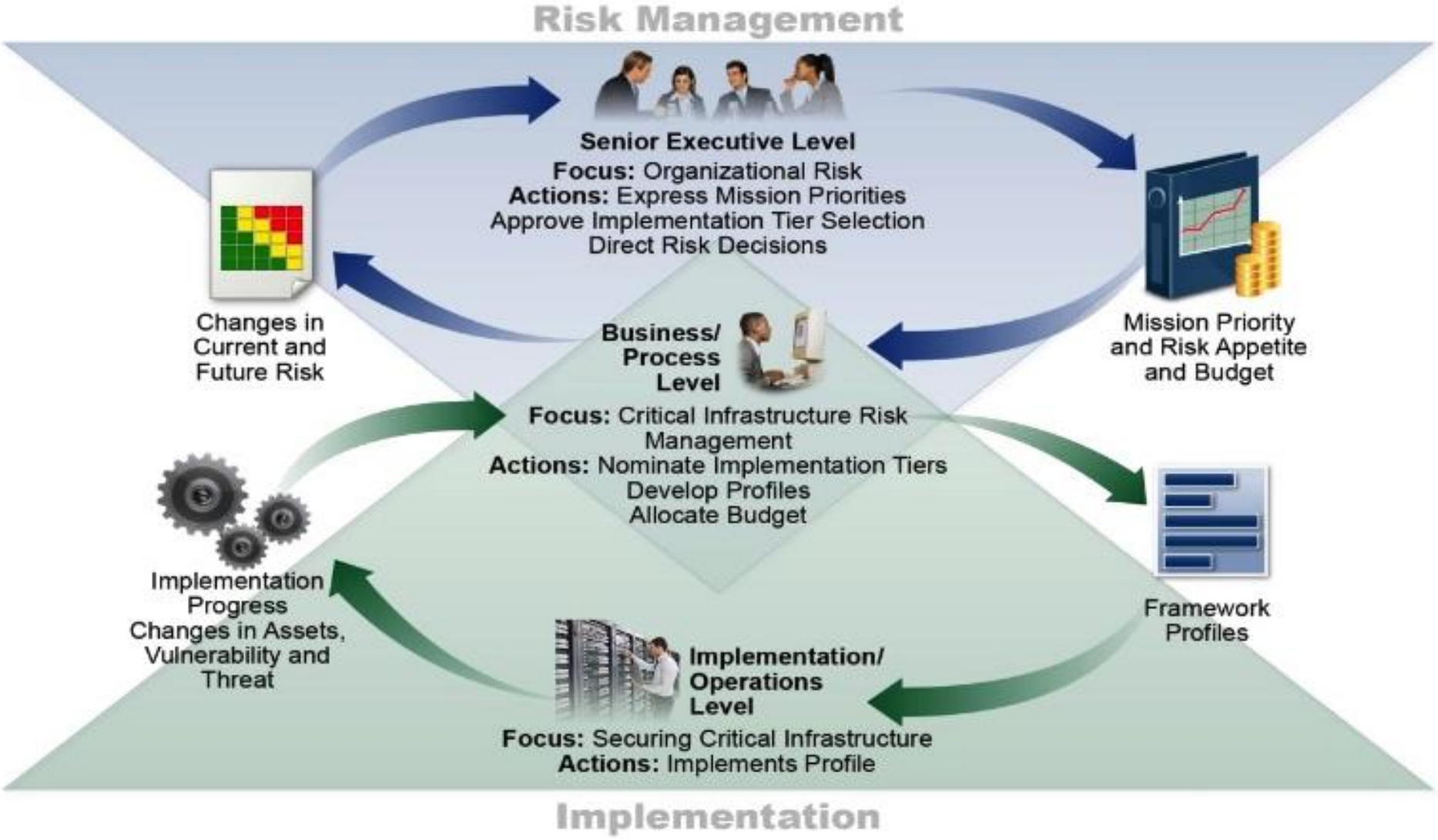


Figure 2: Notional Information and Decision Flows within an Organization

Immagine tratta da: Framework for Improving Critical Infrastructure Cybersecurity - Version 1.1

National Institute of Standards and Technology https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Le dimensioni globali del fenomeno

From:
Framework for Improving Critical Infrastructure Cybersecurity - Version 1.1
National Institute of Standards and Technology https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

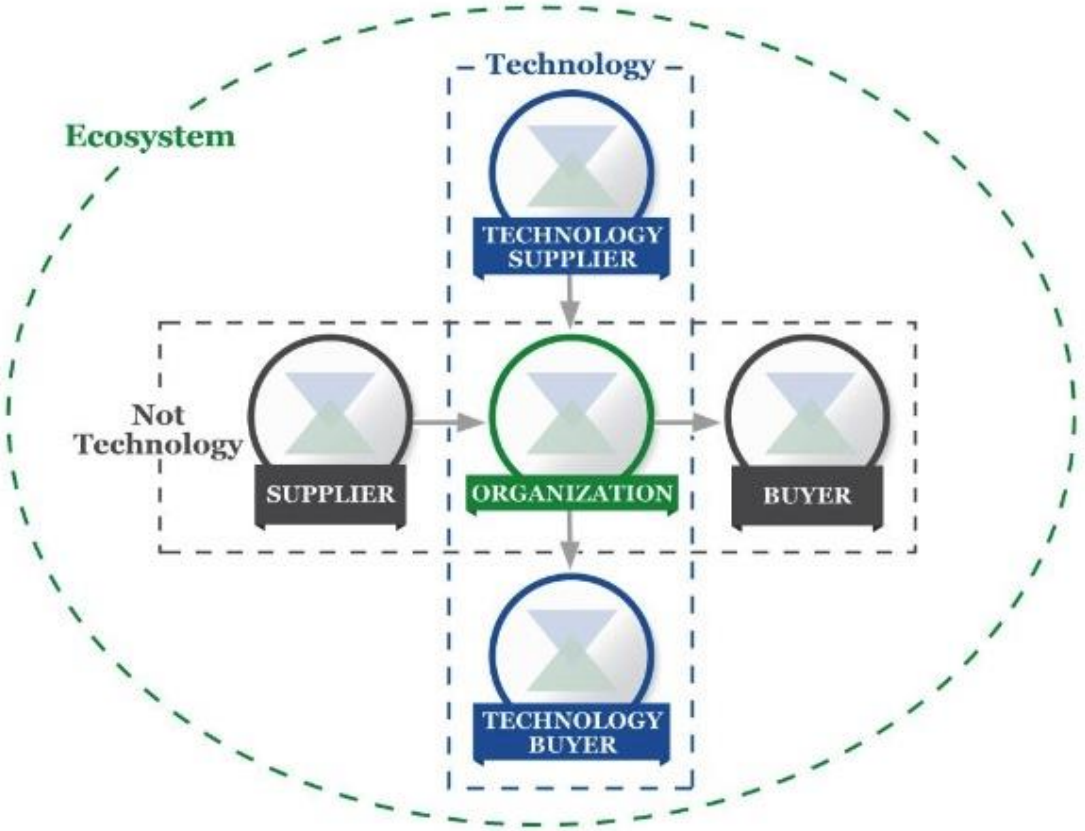


Figure 3: Cyber Supply Chain Relationships

The parties described in Figure 3 comprise an organization's cybersecurity ecosystem. These relationships highlight the crucial role of cyber SCRM in addressing cybersecurity risk in critical infrastructure and the broader digital economy. These relationships, the products and services they provide, and the risks they present should be identified and factored into the protective and detective capabilities of organizations, as well as their response and recovery protocols.

In the figure above, "Buyer" refers to the downstream people or organizations that consume a given product or service from an organization, including both for-profit and not-for-profit organizations. "Supplier" encompasses upstream product and service providers that are used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products or services provided to the Buyer. These terms are applicable for both technology-based and non-technology-based products and services.

IoT Privacy & Security Risk

NIST Privacy Engineering & Cybersecurity for IoT Programs

March 29, 2018

Intanto in Italia

http://www.sviluppoeconomico.gov.it/index.php/it/industria40

Intanto in Italia

Industria 4.0: Le tecnologie abilitanti

1. **Advanced Manufact. Solutions** — • Robot collaborativi interconnessi e rapidamente programmabili
2. **Additive Manufacturing** — • Stampanti in 3D connesse a software di sviluppo digitali
3. **Augmented Reality** — • Realtà aumentata a supporto dei processi produttivi
4. **Simulation** — • Simulazione tra macchine interconnesse per ottimizzare i processi
5. **Horizontal/ Vertical Integration** — • Integrazione informazioni lungo la catena del valore dal fornitore al consumatore
6. **Industrial Internet** — • Comunicazione multidirezionale tra processi produttivi e prodotti
7. **Cloud** — • Gestione di elevate quantità di dati su sistemi aperti
8. **Cyber-security** — • Sicurezza durante le operazioni in rete e su sistemi aperti
9. **Big Data and Analytics** — • Analisi di un' ampia base dati per ottimizzare prodotti e processi produttivi

http://www.sviluppoeconomico.gov.it/index.php/it/industria40

Intanto in Italia

http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

a protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia

CHI SIAMO | COSA FACCIAMO | CULTURA DELLA SICUREZZA | IL MONDO DELL'INTELLIGENCE | PER LE IMPRESE | DOCUMENTAZIONE | COMUNICAZIONE

Home » Gnosis » Nuovi scenari di rischio, per l'intelligence impegno strategico

Nuovi scenari di rischio, per l'intelligence impegno strategico

25 maggio 2018

Gnosis

Gnosis, rivista dell'Agenzia informazioni e sicurezza interna, nasce nel 2004 come

Presidenza del Consiglio dei Ministri

PIANO NAZIONALE
PER LA PROTEZIONE CIBERNETICA
E LA SICUREZZA INFORMATICA

Marzo 2017

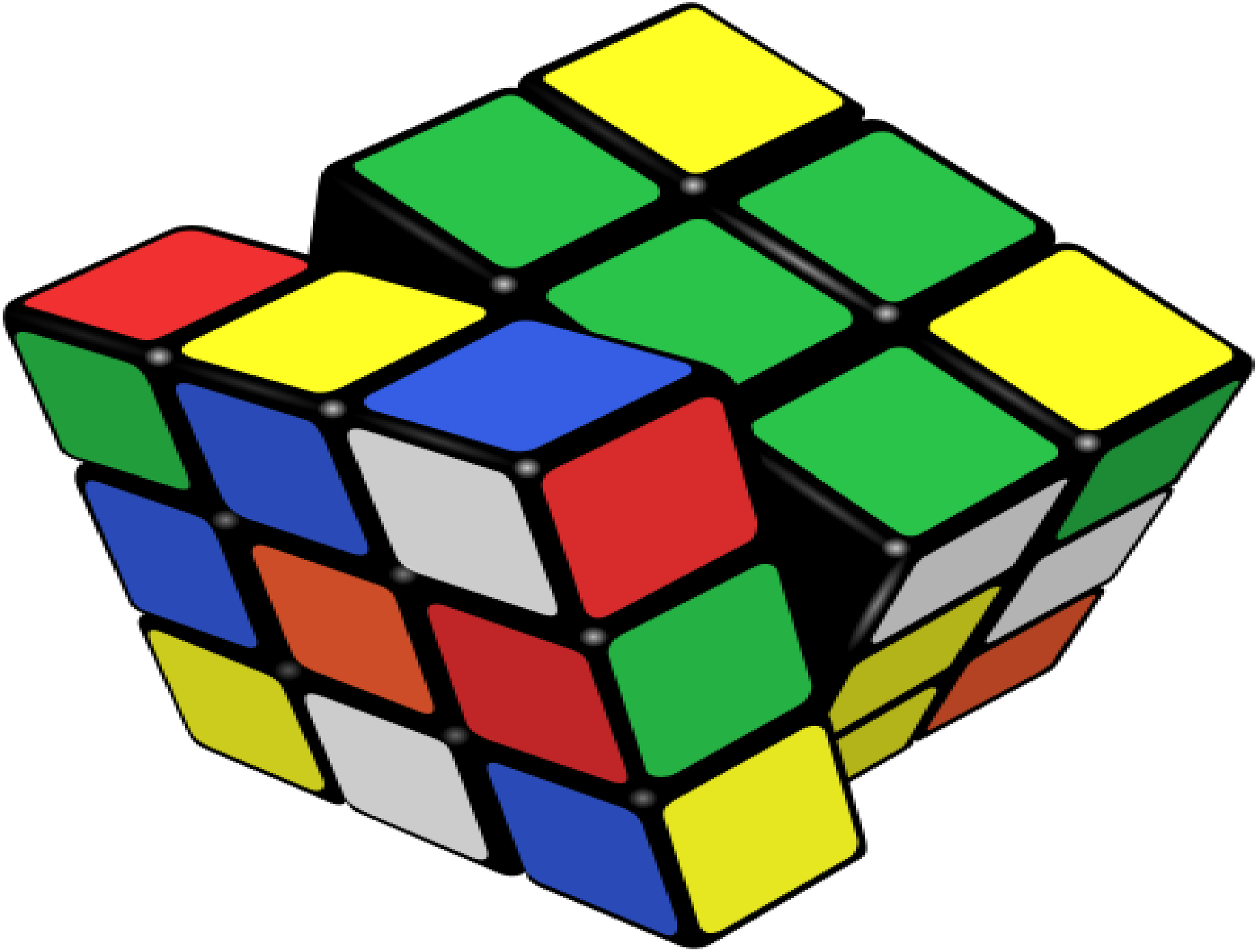
http://www.sicurezzanazionale.gov.it/sisr.nsf/index.html

» Cultura della sicurezza

ıltura della sicurezza

crescere la consapevolezza per i temi dell'interesse nazionale, e della sua difesa, in tutte le declinazioni che esso assume di fronte alle sfide
ı globalizzazione e alle minacce transnazionali e geo-traslate che, noncuranti di delimitazioni territoriali e "cippi confinari", arrivano dentro il
ema Paese" mettendo a rischio la sua integrità patrimoniale e industriale, la sua competitività, la sicurezza delle sue infrastrutture e dei sistemi
rmativi.

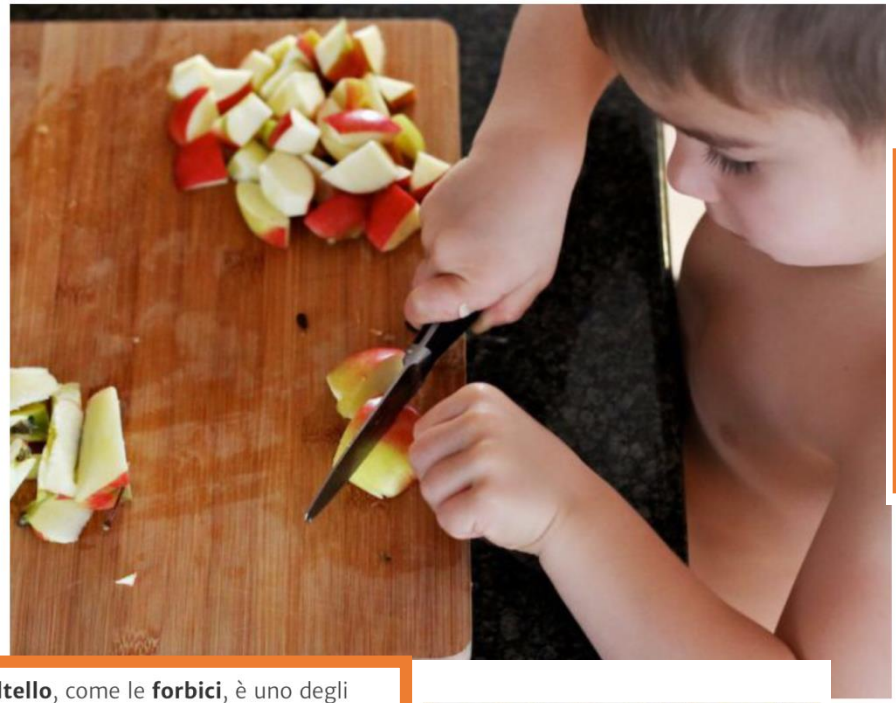
Documenti



http://www.bebeblog.it/post/4151/a-che-eta-e-come-insegnare-al-bambino-a-usare-il-coltello

A che età e come insegnare al bambino a usare il coltello

Quando i bambini possono iniziare a usare il coltello? E come possiamo insegnare loro a farlo in sicurezza?



Il **coltello**, come le **forbici**, è uno degli strumenti che più preoccupa mamma e papà, ma prima o poi i bambini dovranno imparare a usarlo, non potremo per sempre tagliare noi la carne o il pane a tavola al posto loro. Ma a che età si può insegnare ai bambini a tenere correttamente e in sicurezza il coltello in mano e come possiamo aiutarli?

Come in molte altre cose, si può cominciare fin da piccini, utilizzando quei piccoli **coltelli senza lama** che fanno parte del kit di posate per i bambini (sì, sono coltelli, non servono per spalmare la

Mamme da legare: coltelli e forbici, il terrore di ogni madre

I bambini e il loro primo approccio a coltelli e forbici.

http://www.bebeblog.it/post/178794/mamme-da-legare-coltelli-e-forbici-il-terrore-di-ogni-madre

USARE IL COLTELLO

Montessori: 10 idee per insegnare ai bambini come usare il coltello

https://www.nostrofiglio.it/bambino/bambino-1-3-anni/montessori-10-idee-per-insegnare-ai-bambini-come-usare-il-coltello?gpath=

22 Novembre 2016

Imparare a usare il coltello è un'importante abilità: sviluppa la precisione, il controllo dei movimenti, l'autostima e la fiducia in se stessi. Oggi però molti genitori evitano il più possibile questo insegnamento perché non riescono a gestire l'ansia di vedere un piccolo maneggiare un oggetto potenzialmente pericoloso. Il metodo Montessori spiega, invece, che bisogna dare fiducia al bambino e insegnargli a fare da solo facendo leva sul suo senso di responsabilità. Ecco 10 suggerimenti per l'uso del coltello.

Forbici e coltelli sono un pericolo per i bambini? Ecco come insegnare ai piccoli ad utilizzare utensili da cucina e posate nel modo più corretto ed in sicurezza

Spesso utensili da cucina e posate si trasformano in pericolo per i bambini, ma facendo parte

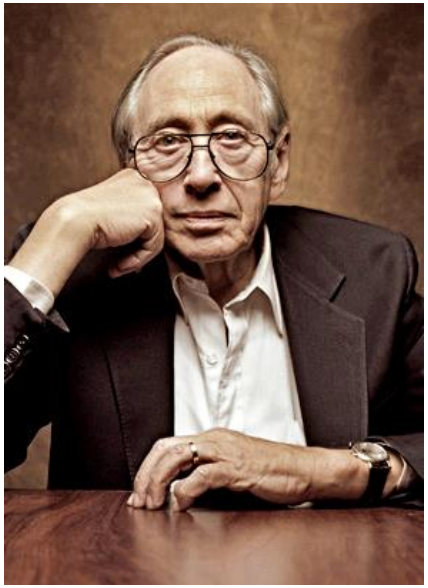
Montessori: come usare forbici e coltelli

Imparare a usare correttamente coltelli, forbici e altri oggetti taglienti insegna ai bambini a essere prudenti, autonomi e sicuri. Ecco alcune attività da proporre a seconda dell'età

https://www.uppa.it/educazione/montessori/montessori-come-usare-forbici-e-coltelli/

È tempo di ristabilire l'equilibrio….

Tra dimensione etica e culturale, quella economica, e la dimensione tecnologica e giuridica



« Ciascuna società ha le sue esigenze economiche, politiche e militari. In questo mondo tripartito, la civiltà della Prima Ondata fornisce le risorse agricole e minerali, la civiltà della Seconda Ondata provvede al lavoro a basso costo e alla produzione di massa, mentre la civiltà in espansione della Terza Ondata afferma un nuovo dominio basato sulle metodologie con cui crea e sfrutta la conoscenza. »

(Alvin e Heidi Toffler, *La guerra disarmata*, pp. 26-27)

ReD OPEN

BICOCCA RESEARCH GROUP

Responsibility and Design in OPEN ecosystems

Red Open Bicocca Research Group è un gruppo di ricerca del Dipartimento di Giurisprudenza dell'Università Milano-Bicocca. Si occupa di studiare l'impatto sociale dell'innovazione digitale cercando di proporre soluzioni normative in grado di **coniugare i processi di innovazione con i temi di governance della responsabilità individuale.**

Continuiamo con ….

Le dimensioni della sicurezza industriale

ReD OPEN
BICOCCA RESEARCH GROUP
Responsibility and Design in OPEN ecosystems

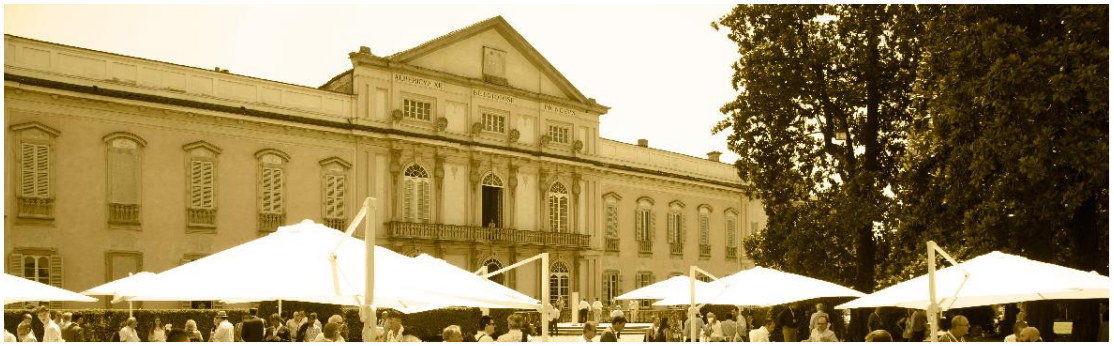
1998-2018
UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA
VENTESIMO ANNIVERSARIO

- **Cybersecurity e hardware: cosa prevede il GDPR**

- **La direttiva NIS per gli operatori di servizi essenziali e digitali**

- **Dati non personali di campo e automazione, possibili tutele di legge e contrattuali**

E ci ritroveremo….



AUTOMATION INSTRUMENTATION SUMMIT 2018

We look forward to seeing you in Belgioioso

July 4 & 5, 2018
Castello di Belgioioso Pavia - Italy

Associazione Italiana Strumentisti

ISA Italy Section

«LE DIMENSIONI DELLA SICUREZZA INDUSTRIALE»
I percorsi della sicurezza industriale dagli standard ISA/IEC 62443 ai temi della cybersecurity

Milano, 30 Maggio 2018

Auditorio TECNIMONT

Le dimensioni della sicurezza industriale

ReD OPEN BICOCCA RESEARCH GROUP
Responsibility and Design in OPEN ecosystems

1998-2018 20 UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA VENTESIMO ANNIVERSARIO

Massimo V.A. Manzari
Change Management Designer
Co-Founder ReD Open Bicocca Research Group

massimo@massimomanzari.it