



info@imglobal1.com

© IMS GLOBAL
USA - Europe (Spain) - Mexico - Colombia - Brazil
www.imsglobal1.com



V 1.33

RISK, (PROCESS) SAFETY & INFO/CYBER SECURITY
FOR CRITICAL INFRASTRUCTURE





We protect Critical Information Infrastructure (CIIP) as well as industrial Critical Infrastructure (CIP) assets, including IACS/ICS, throughout their entire value chain and life cycle.



We optimize the balance between (industrial) process safety and multidimensional cybersecurity, including AI/ML, to safeguard critical infrastructure.



We prepare you for what's next by developing & strengthening risk management capabilities to build resilient process safety & security architectures, supporting informed decision-making, in a world of a complex set of compliance challenges and an escalating cyber-crime and threat landscape.



We continuously innovate in technologies and processes by leveraging in our rich knowledge base of advanced techniques, best-industry practices, the state of the art, compliance, and strategic insight.



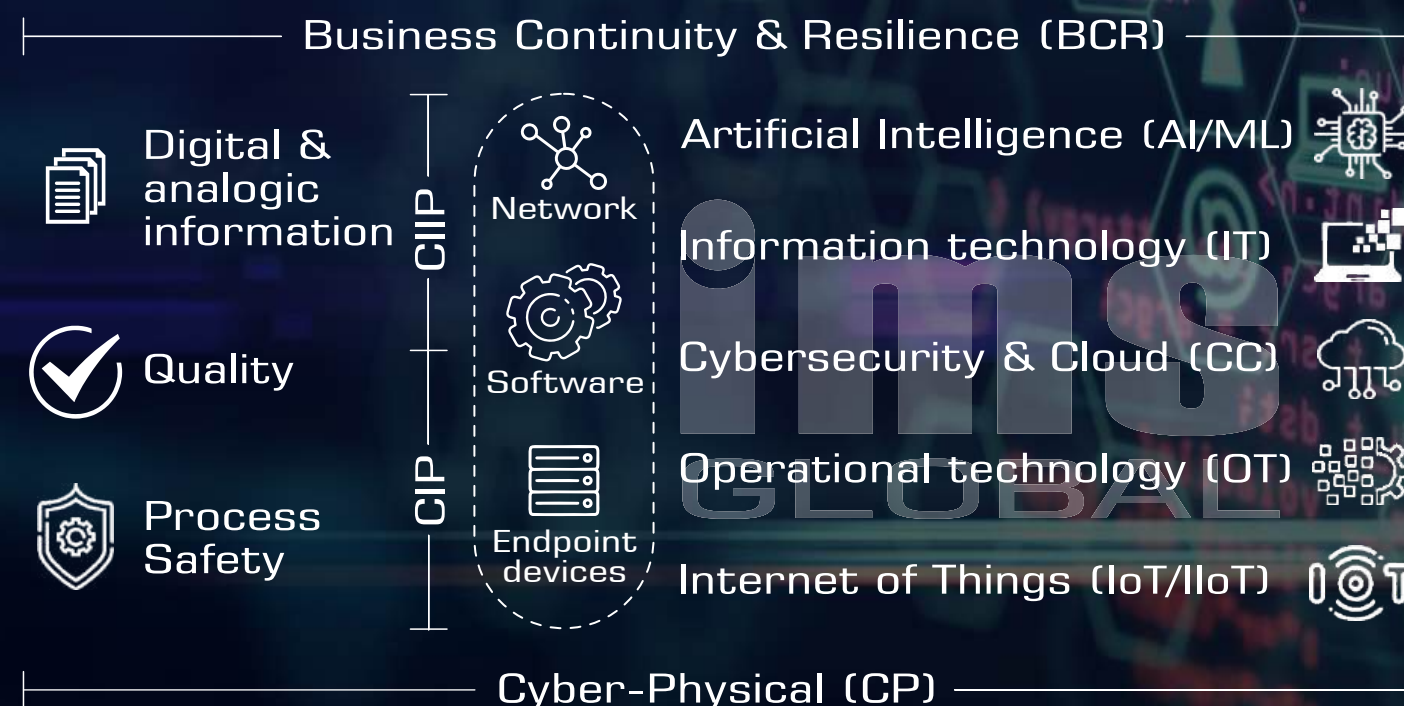
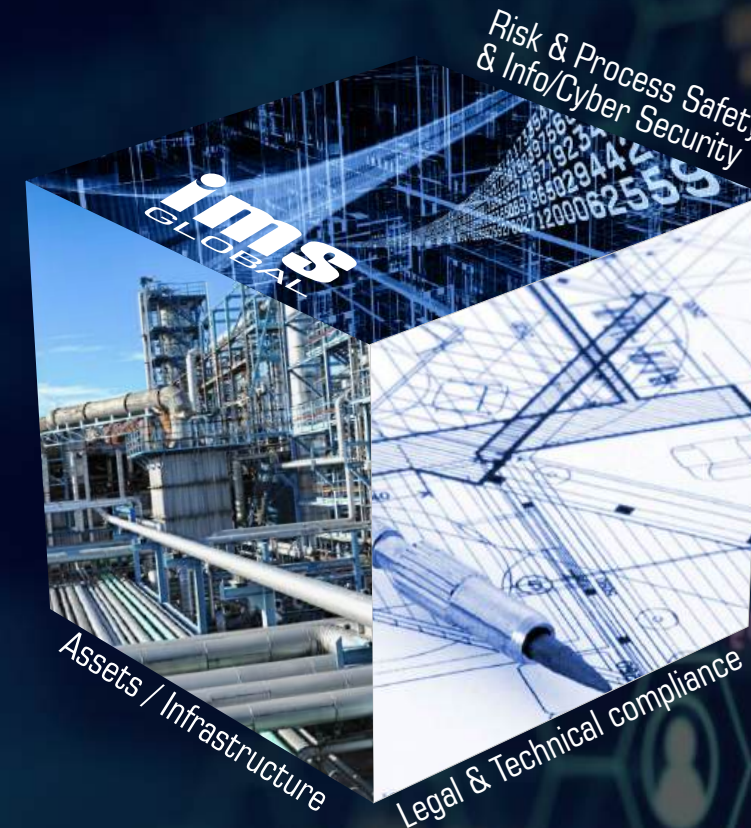
We apply and integrate key risk management frameworks: SO 31000, ISO 31010, ISO/IEC 27005, ISO/IEC 27032, ISO 14971, ISO 10418, ISA/IEC 62443, ISO/IEC 61511, IEC 62351, Norsok Z-013, NIST SP 800-30, NIST SP 800-37, NIST SP-800-39, NIST CSF 2.0, CCPS-CPQRA, NERC, NIST AI RMF...



We support the achievement of your business objectives through our successful knowledge transfer ([consulting](#), [advisory](#) and [technical training](#) with 500+ courses 100% based on technical standards), assessment (auditing/inspection with 100+ standards/technical frameworks) and [delegation](#) services.



Managing process safety, cybersecurity and AI risks in a comprehensive manner





Risk Management Systems (RMS)
+ Control architectures through their life-cycle.

Process integration.

Design of

- Risk criteria
- Risk appetite
- Risk tolerance

Risk/control optimization (and rationalization).

Risk & Control architecture

- Taxonomies.
- Segmentation.
- Clustering.
- Profiles.
- Classification.

Knowledge management [ISO 30401, ISO/IEC 5392; CCPS]
Static & dynamic control, barrier, safeguard management [IMS]
Inherently Safer (chemical) Processes [CCPS]
Standard and Safe/Secure Operating Procedures (SOP).
Process Safety performance indicators [API RP 754, IOGP, CCPS]
InfoSecurity & Cybersecurity measurement [ISO/IEC 27004]
Process assessment & improvement [Series ISO/IEC 330XX]
Systems security maturity [ISO/IEC 21827, ISO 9004]

Asset & Asset-health Management Systems (AHMS)
Covering discovery, identification, classification/categorization, prioritizing, in their life-cycle, including interfaces, dependencies, collisions, and Process Safety Information (PSI) & Trade Secrets.

Risk Engineering (Safety + Security)

Probability modeling

- Probabilistic (AU).
+Statistic distributions.
+Stochastic.
+Parametric risks.
- Frequentist.
- Possibilistic (EU).
+topological analysis.
- Deterministic.
- Flash vs Slow burning.
- Bayesian networks.

Impact modeling

- Business Impact Analysis (BIA).
- Systemic vs Idiosyncratic risk.
- Downside vs Upside/Downside.
- Probable maximum loss (PML).
- Cross Impact Analysis.
- Scenario-based Analysis.
- Stress testing.

- System dynamics.
- AI assisted risk modeling.

Control architecture

Continuous

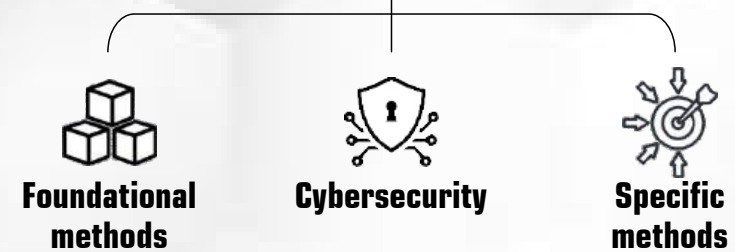
Quality Assurance (Qa) & Quality Control (Qc).
Pre-Startup/Operational review [OSHA].
Management of Change (MoC) [ISO 10020, ISO 18828-5; OSHA]
Transient Operating Mode (Start-up * Shut-down) [CCPS]
Preparation, Maintenance, Return to Service [CCPS]
Job Safety Analysis (JSA) & Hot-work permits (HWP).
Good Manufacturing (GMP), Storage (GSP) & Lab (GLP) practice.
Process Safety with Contractors & Outsourcing [ISO 37500, CCPS]
Risk-Based Inspection (RBI) [API RP 580/581]

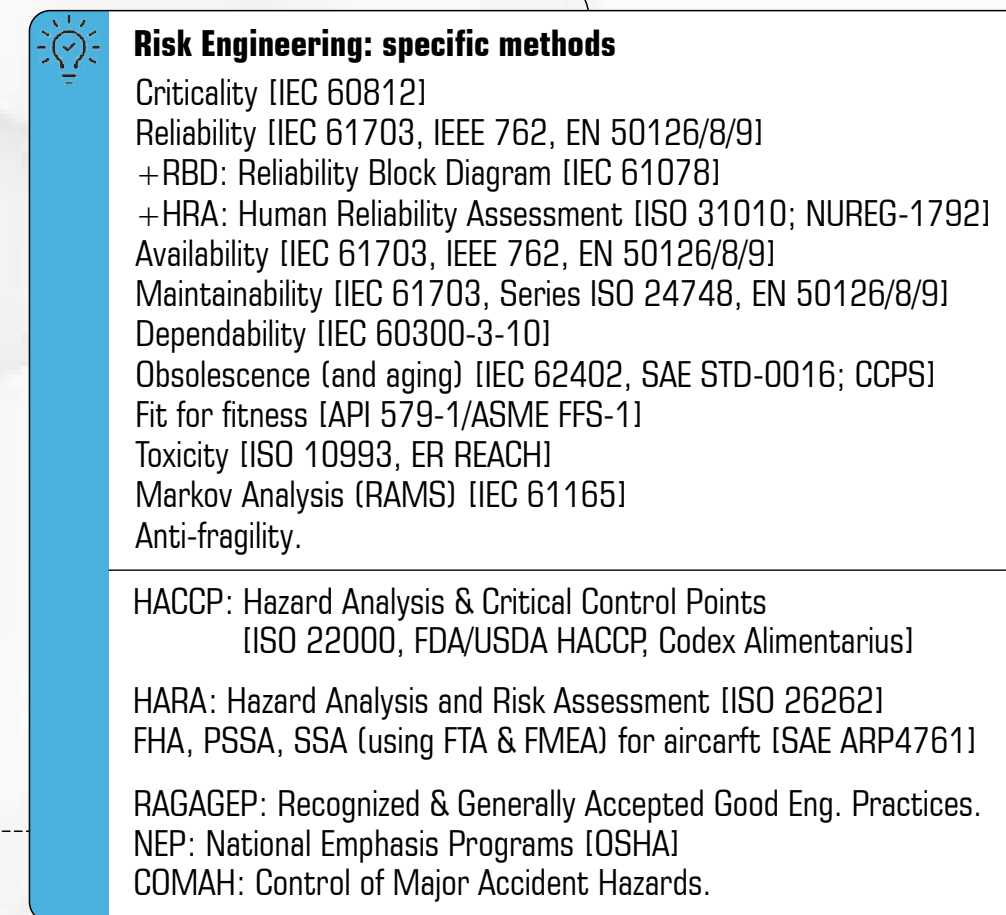
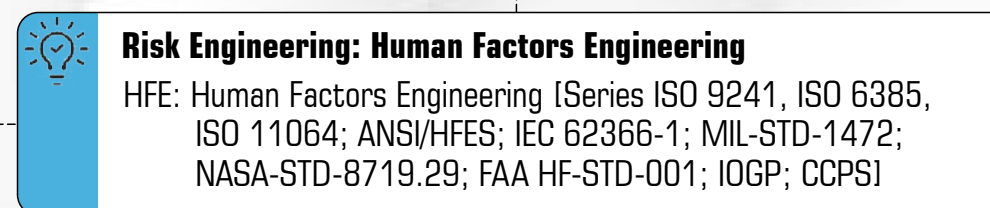
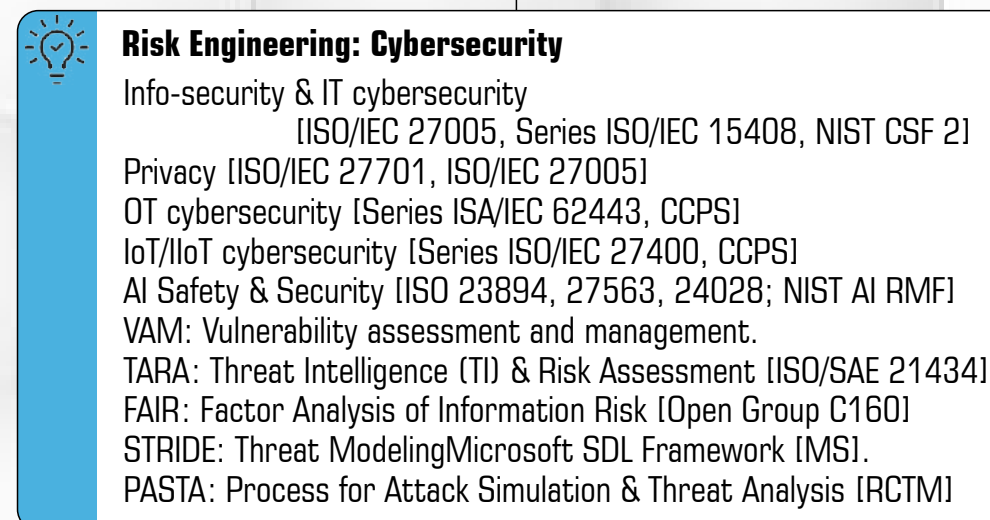
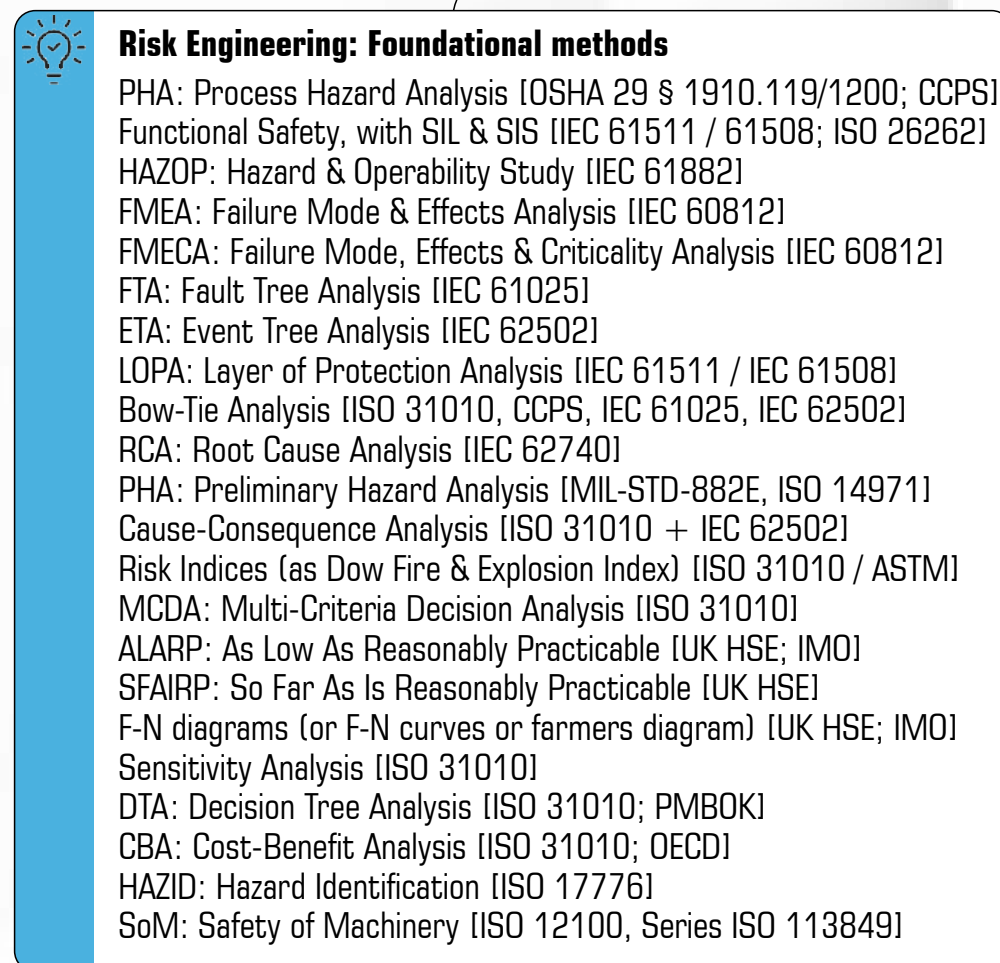
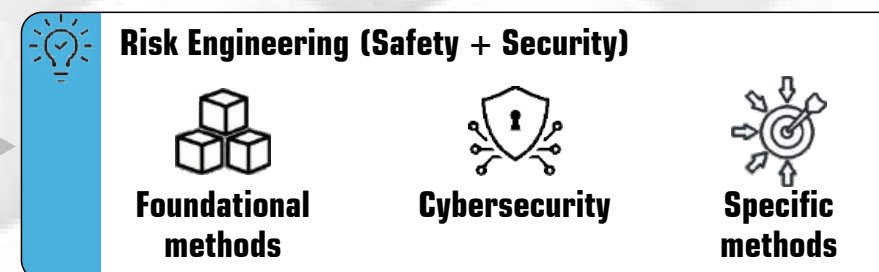
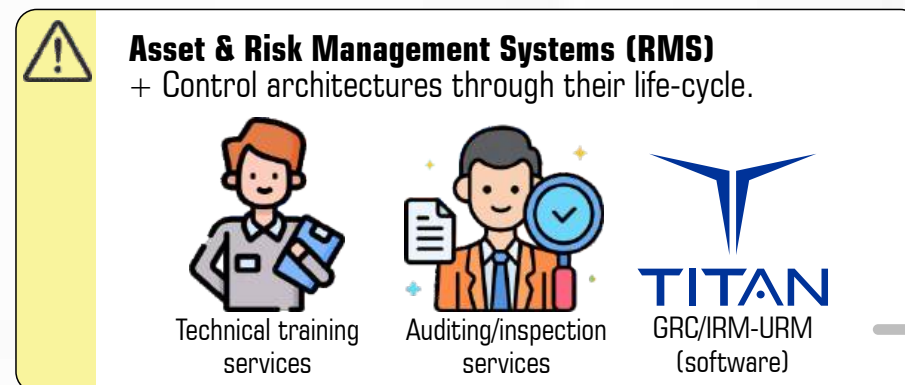
During

Loss control & loss adjustment.
Abnormal, Events/Emergencies & Crisis preparedness + response [ISO 2236X, Series ISO/IEC 27035; CCPS]
Exercises and Testing [ISO 22398]

After

Event/Incident investigation [ISO/IEC 27041/3; CCPS]
Control effectiveness assessment.





* This brochure lists the main technical standards and best practices used by us per practice.
In addition, we apply an expanded set of technical references including our own frameworks.