1. Record Nr. UNINA990005758470403321

Autore	Enlart, Camille <1862-1927>
Titolo	1.1.: Architecture religieuse : Pèriode mèrovingienne, carolingienne et romane / par Camille Enlart
Pubbl/distr/stampa	Paris, : Auguste Picard, 1927
Edizione	[3. éd. rev.]
Descrizione fisica	CVIII, 458 p. ; 23 cm
Locazione	FLFBC
Collocazione	GLOTT. B VI e 10 (1)
Lingua di pubblicazione	Francese
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr. UNINA9910962914503321

Autore	IAEA
Titolo	Computer Security Techniques for Nuclear Facilities : Technical Guidence
Pubbl/distr/stampa	Havertown : , : International Atomic Energy Agency, , 2021 ©2021
ISBN	9789201237200 9201237200
Edizione	[1st ed.]
Descrizione fisica	1 online resource (132 pages)
Collana	IAEA Nuclear Security ; ; v.17-T (Rev. 1)
Soggetti	Computer networks--Security measures Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- 1. INTRODUCTION -- Background -- Objective -- Scope -- Structure -- 2. Basic Concepts and Relationships -- Nuclear security

and computer security -- Facility functions, computer security levels and computer security zones -- Computer security risk management -- Competing demands of simplicity, efficiency and computer security -- Conceptual nuclear facility zone model -- Computer security measures -- Computer based systems and digital assets (including SDAs) -- Cyber-attack -- Interface with safety -- 3. General Considerations for Computer Security -- Identification of facility functions -- Protection of sensitive information and digital assets -- Risk informed approach -- Risk assessment and management -- Computer security levels based on a graded approach -- 4. Facility Computer Security Risk Management -- Objective of facility computer security risk management -- Outline of facility computer security risk management -- Inputs to facility computer security risk management -- Phases of facility computer security risk management -- Scope definition -- Facility characterization -- Identification of facility functions -- Intrinsic significance of facility functions -- Potential effects of compromise of a system on facility function -- Interdependencies between facility functions -- Necessary timeliness and accuracy for facility function interdependencies -- Target identification -- Documentation of facility functions -- Threat characterization -- Sources of threat information -- Facility specific threat characterization -- Additional considerations for insider threats -- Specification of computer security requirements -- Computer security policy and computer security programme -- Assignment of systems performing facility functions to computer security levels -- Defensive computer security architecture specification. Requirements in the DCSA specification to apply a graded approach -- Requirements in the DCSA specification to apply defence in depth -- Trust model -- Relationship with system computer security risk management - performed for each system -- Assurance activities -- Evaluation -- Verification -- Validation -- Scenario identification and development -- Facility computer security risk management output -- 5. System Computer Security Risk Management -- General considerations -- Overview -- System computer security risk management process -- Overall defensive computer security architecture requirements for computer security -- Definition of system boundaries -- Definition and construction of computer security zones -- Identification of digital assets -- System computer security architecture, including digital asset analysis -- Verification of the system computer security risk assessment -- System computer security risk management report -- 6. Facility and System Computer Security Risk Management Considerations During Specific Stages in the Lifetime of a Facility -- Planning -- Siting -- Design -- Construction -- Commissioning -- Operations -- Maintenance -- Cessation of operations -- Decommissioning -- 7. Elements of the computer security programme -- Computer security requirements -- Computer security policy -- Computer security programme -- Elements of the computer security programme -- Organizational roles and responsibilities -- Management system -- Computer security indicators -- Security design and management -- Computer security requirements -- Digital asset management -- Configuration management -- Security procedures -- Personnel management -- 8. Example defensive computer security architecture and computer security measures -- Example implementation of defensive computer security architecture -- Decoupling computer security zones. External connectivity -- Example requirements -- Unassigned digital assets -- Generic requirements -- Security level 1 requirements -- Security level 2 requirements -- Security level 3 requirements --

Security level 4 requirements -- Security level 5 requirements -- Appendix SELECTED ELEMENTS OF A COMPUTER SECURITY PROGRAMME -- REFERENCES -- Annex I POTENTIAL ATTACK SCENARIOS AGAINST SYSTEMS IN NUCLEAR FACILITIES -- Annex II EXAMPLE OF COMPUTER SECURITY LEVEL ASSIGNMENT FOR A NUCLEAR POWER PLANT -- Annex III EXAMPLE OF APPLICATION OF COMPUTER SECURITY LEVELS AND ZONES -- GLOSSARY.

Sommario/riassunto

This revision provides guidance on how to establish or improve, develop, implement, maintain, and sustain computer security within nuclear facilities. This publication addresses the use of risk informed approaches to establish and enhance computer security policies, programmes; it describes the integration of computer security into the management system of a facility; establishes a systematic approach to identifying facility functions and appropriate computer security measures that protect sensitive digital assets and the facility from the consequence of cyber-attacks consistent with the threat assessment or design basis threat.