

1. Record Nr.	UNINA9910214936303321
Autore	Besnault-Levita Anne
Titolo	L'Allusion et l'Accès // Peter Vernon, Claudine Raynaud
Pubbl/distr/stampa	Tours, : Presses universitaires François-Rabelais, 2017
ISBN	2-86906-480-2
Descrizione fisica	1 online resource (253 p.)
Altri autori (Persone)	BraultElise CrowleyCornelius DechasseyEric DechaumeSandrine FerrerDaniel Friestedt-d'HalluinAstrid LouvellLiliane PalleauFrançoise PoulainPascale PoutiersClaire RegnauldArnaud SalbayreSebastien TissutAnne-Laure TubridyDerval VernonPeter VincentNathalie WinsworthBen RaynaudClaudine
Soggetti	Literature (General) allusion esthétique lecture esthétique de la réception
Lingua di pubblicazione	Francese
Formato	Materiale a stampa
Livello bibliografico	Monografia

L'Allusion et L'Accès follows on from work previously published in GRAAT, in particular *Usure et Rupture – Breaking Points* (GRAAT 13) and *Fonctions du Cliché – Du Banal à la Violence* (GRAAT 16). The present conference aimed to articulate the strategies that the literary text deploys to access the unsayable, whilst, simultaneously, keeping in mind the notion of play contained in the etymology of allusion: *alludere*. Allusion and Access, then, are two vast subjects put into juxtaposition and perspective. Allusion sets up various mechanisms of expression by Indirection while Access gives some sort of Direction although one might not know to where the direction is leading. To Allude means to say something by other means. What is that otherness which one chooses to name by substitution? What is the fundamental otherness to which access leads us, when one is dealing with meaning and is left with language as the only tool? Allusion will be understood as metaphoric play. The receiver is expected to know what the game is all about. As Pizzorusso has well said: «La notion d'allusion demande, ou demanderait, une vaste enquête : le mot, l'idée, la pratique de l'allusion.» Access meanwhile means "to reach" in terms of a path, a progress, implying a hermeneutic search. L'Allusion et L'Accès fait suite à des travaux déjà publiés dans GRAAT, notamment *Usure et Rupture - Breaking Points* (GRAAT 13) et *Fonctions du Cliché - Du Banal à la Violence* (GRAAT 16). La présente conférence visait à articuler les stratégies que le texte littéraire déploie pour accéder à l'indicible, tout en gardant à l'esprit la notion de jeu contenue dans l'étymologie de l'allusion : *alludere*. Allusion et Accès sont donc deux vastes sujets mis en juxtaposition et en perspective. L'allusion met en place divers mécanismes d'expression par l'Indirection tandis que l'Accès donne une sorte de Direction bien que l'on puisse ne pas savoir vers où la direction mène. Faire allusion signifie dire quelque chose par...

---

2. Record Nr.	UNINA9910746085203321
Titolo	Computer Safety, Reliability, and Security : 42nd International Conference, SAFECOMP 2023, Toulouse, France, September 20–22, 2023, Proceedings // edited by Jérémie Guiochet, Stefano Tonetta, Friedemann Bitsch
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	3-031-40923-X
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (291 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14181
Disciplina	004.015113
Soggetti	Computer engineering Computer networks Software engineering Application software Robotics Microprogramming Data protection Computer Engineering and Networks Software Engineering Computer and Information Systems Applications Control Structures and Microprogramming Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Safety Assurance -- Assurance Case Arguments in the Large -- CERN LHC Machine Protection System -- Identifying Run-time Monitoring Requirements for Autonomous Systems through the Analysis of Safety Arguments -- Redesigning Medical Device Assurance: Separating Technological and Clinical Assurance Cases -- Software Testing & Reliability -- A Cognitive Framework for Modeling Coincident Software Faults: An Experimental Study -- A Taxonomy of Software Defect Forms for Certification Tests in Aviation Industry -- Constraint-guided Test Execution Scheduling: An Experience Report at ABB Robotics -- Neural

Networks Robustness & Monitoring -- A low-cost strategic monitoring approach for scalable and interpretable error detection in deep neural networks -- Are Transformers More Robust? Towards Exact Robustness Verification for Transformers -- Model-based Security and Threat Analysis -- Model-based Generation of Attack-Fault Trees -- MBTA: A Model-Based Threat Analysis approach for software architectures -- Attribute Repair for Threat Prevention -- Safety of Autonomous Driving -- Probabilistic Spatial Relations for Monitoring Behavior of Road Users -- Concept and metamodel to support cross-domain safety analysis for ODD expansion of autonomous systems -- Security Engineering -- Pattern-Based Information Flow Control for Safety-Critical On-Chip Systems -- From Standard to Practice: Towards ISA/IEC 62443-conform Public Key Infrastructures -- AI Safety -- The Impact of Training Data Shortfalls on Safety of AI-based Clinical Decision Support Systems -- Data-centric Operational Design Domain Characterization for Machine Learning-based Aeronautical Products -- Online Quantization Adaptation for Fault-Tolerant Neural Network Inference -- Neural Networks & Testing -- Evaluation of Parameter-based Attacks against Embedded Neural Networks with Laser Injection -- Towards Scenario-based Safety Validation for Autonomous Trains with Deep Generative Models.

---

### Sommario/riassunto

This book constitutes the refereed proceedings of the 42nd International Conference on Computer Safety, Reliability and Security, SAFECOMP 2023, which took place in Toulouse, France, in September 2023. The 20 full papers included in this volume were carefully reviewed and selected from 100 submissions. They were organized in topical sections as follows: Safety assurance; software testing and reliability; neural networks robustness and monitoring; model-based security and threat analysis; safety of autonomous driving; security engineering; AI safety; and neural networks and testing.

---