

## Lecture Notes in Business Information Processing

This book constitutes the thoroughly refereed proceedings of ten international workshops held in London, UK, in conjunction with the 23rd International Conference on Advanced Information Systems Engineering, CAiSE 2011, in June 2011.

The 59 revised papers were carefully selected from 139 submissions. The ten workshops included Business/IT Alignment and Interoperability (BUSITAL), Conceptualization of Modelling Methods (CMM), Domain Specific Engineering (DsE@CAiSE), Governance, Risk and Compliance (GRCIS), Integration of IS Engineering Tools (INiSET), System and Software Architectures (IWSSA), Ontology-Driven Information Systems Engineering (ODISE), Ontology, Models, Conceptualization and Epistemology in Social, Artificial and Natural Systems (ONTOSE), Semantic Search (SSW), and Information Systems Security Engineering (WISSE).

LNBIP reports state-of-the-art results in areas related to business information systems and industrial application software development – timely, at a high level, and in both printed and electronic form.

The type of material published includes

- Proceedings (published in time for the respective event)
- Postproceedings (consisting of thoroughly revised and/or extended final papers)
- Other edited monographs (such as, for example, project reports or invited volumes)

In parallel to the printed book, each new volume is published electronically in LNBIP Online.

Detailed information on LNBIP can be found at <http://www.springer.com>

Proposals for publication should be sent to

LNBIP Editorial, Tiergartenstr. 17, 69121 Heidelberg, Germany

E-mail: [lnbip@springer.com](mailto:lnbip@springer.com)

ISSN 1865-1348

ISBN 978-3-642-22055-5



Lecture Notes in  
Business Information  
Processing



Salinesi • Pastor (Eds.)



LNBIP  
83

Advanced Information Systems  
Engineering Workshops

LNBIP 83

Camille Salinesi  
Oscar Pastor (Eds.)

# Advanced Information Systems Engineering Workshops

CAiSE 2011 International Workshops  
London, UK, June 2011  
Proceedings

Series Editors

Wil van der Aalst

*Eindhoven Technical University, The Netherlands*

John Mylopoulos

*University of Trento, Italy*

Michael Rosemann

*Queensland University of Technology, Brisbane, Qld, Australia*

Michael J. Shaw

*University of Illinois, Urbana-Champaign, IL, USA*

Clemens Szyperski

*Microsoft Research, Redmond, WA, USA*

Camille Salinesi  
Oscar Pastor (Eds.)

# Advanced Information Systems Engineering Workshops

CAiSE 2011 International Workshops  
London, UK, June 20-24, 2011  
Proceedings

 Springer

## Foreword

### Volume Editors

Camille Salinesi  
Université Paris 1 Panthéon - Sorbonne  
75013 Paris, France  
E-mail: camille.salinesi@univ-paris1.fr

Oscar Pastor  
Universidad Politécnica de Valencia  
46022 Valencia, Spain  
E-mail: opastor@dsic.upv.es

Information systems are worth billions! Our job, as scientists, academics, and engineers in this domain, is to help organizations understand how to make profits with information systems. In fact, there is more than money at stake. Social bounds, culture, rights, trust: there are diverse aspects of our daily life that can benefit from information systems. It is just a matter of innovation.

Innovation means invention and science. Both emerge from laboratories, but there is a time for communicating too. The series of workshops associated with the International Conference on Advanced Information Systems Engineering acts as a forum of discussion between all stakeholders in the domain of information systems engineering. It is the place where ground-breaking ideas about new methods, techniques and tools, or return on experience, can be shared between experts. Many of the mature research works published at the CAiSE conference were presented in CAiSE workshops when they were in their seminal phase.

This year, CAiSE had 2 associated working conferences and 10 workshops. Many more workshops were initially submitted, but we had to make choices, such as merging proposals or rejecting less mature proposals to comply with our usual quality and consistency standards. The themes of the 10 workshops this year are the following (in alphabetical order):

- BUSinness/IT ALignment and Interoperability (BUSITAL)
- Conceptualization of Modelling Methods (CMM)
- Domain Specific Engineering (DsE@CAiSE)
- Governance, Risk and Compliance: Applications in Information Systems (GRCIS)
- Information Systems Security Engineering (WISSE)
- Integration of IS Engineering Tools (INISSET)
- Ontology-Driven Information Systems Engineering Workshop (ODISE)
- Ontology, Models, Conceptualization and Epistemology in Social, Artificial and Natural Systems Workshop (ONTOSE)
- Semantic Search (SSW)
- System/Software Architectures (IWSSA)

The variety of themes and quality publications at the workshops show that information systems engineering is a healthy research domain.

We, the CAiSE 2011 Workshops Chairs, would like to thank all the workshop organizers and all the referees and members of workshop Program Committees for their hard work in arranging the workshops and ensuring their high scientific quality.

ISSN 1865-1348 e-ISSN 1865-1356  
ISBN 978-3-642-22055-5 e-ISBN 978-3-642-22056-2  
DOI 10.1007/978-3-642-22056-2  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011929928

ACM Computing Classification (1998): H.4, H.3.5, D.2, J.1, I.2

© Springer-Verlag Berlin Heidelberg 2011

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

We hope that you will enjoy the papers, and that this will encourage you to attend the CAiSE workshops and submit papers, or even organize workshops at CAiSE in forthcoming years.

May 2011

Oscar Pastor  
Camille Salinesi

## Table of Contents

<b>6th International Workshop on BUSInness/IT ALignment and Interoperability (BUSITAL 2011)</b>	
Preface BUSITAL 2011 .....	1
<i>Birger Andersson, Irina Rychkova, and Gianluigi Viscusi</i>	
Business IT Alignment from Business Model to Enterprise Architecture .....	4
<i>Boris Fritscher and Yves Pigneur</i>	
Modeling Competition-Driven Business Strategy for Business IT Alignment .....	16
<i>Constantinos Giannoulis, Michaël Petit, and Jelena Zdravkovic</i>	
The Quest for Know-How, Know-Why, Know-What and Know-Who: Using KAOS for Enterprise Modelling .....	29
<i>Maxime Bernaert and Geert Poels</i>	
Value-Oriented Coordination Process Model Engineering .....	41
<i>Hassan Fatemi, Marten van Sinderen, and Roel Wieringa</i>	
The Business Behavior Model: A Revised Version .....	45
<i>Noelia Palomares and Birger Andersson</i>	
The Man Behind the Curtain. Exploring the Role of IS Strategic Consultant .....	57
<i>Riccardo Bonazzi, Charlotte Ceccaroli, and Stéphanie Missonier</i>	
Enterprise Interoperability Maturity: A Model Using Fuzzy Metrics ....	69
<i>Wided Guédria, Yannick Naudet, and David Chen</i>	
Service Value Networks for Competency-Driven Educational Services: A Case Study .....	81
<i>Iván S. Razo-Zapata, Pieter De Leenheer, Jaap Gordijn, and Hans Akkermans</i>	
Business/IT Alignment in Practice: Lessons Learned from a Requirements Project at P & G .....	93
<i>Gil Regev, Julien Favre, Erich Hayek, Paul Wilson, and Alain Wegmann</i>	

### First International Workshop on Conceptualization of Modelling Methods (CMM 2011)

Preface CMM 2011 .....	102
<i>Dimitris Karagiannis and Xavier Franch</i>	
A Modelling Method for Consistent Physical Devices Management: An ADOxx Case Study .....	104
<i>Srdjan Zivkovic, Krzysztof Miksa, and Harald Kühn</i>	
EIPW: A Knowledge-Based Database Modeling Tool .....	119
<i>Ornsiri Thonggoom, Il-Yeol Song, and Yuan An</i>	
On the Conceptualization of a Modeling Language for Semantic Model Annotations .....	134
<i>Hans-Georg Fill</i>	
Modeling and Analyzing Non-Functional Properties to Support Software Integration .....	149
<i>Henning Agt, Gregor Bauhoff, Ralf-D. Kutsche, and Nikola Milanovic</i>	

### First International Workshop on Domain Specific Engineering (DsE@CAiSE 2011)

Preface DsE@CAiSE 2011 .....	164
<i>Iris Reinhartz-Berger, Arnon Sturm, Yair Wand, Jorn Bettin, Tony Clark, and Sholom Cohen</i>	
Domain Specific Languages and Standardization: Friends or Foes? – Invited Talk for DsE@CAiSE2011 .....	166
<i>Øystein Haugen</i>	
Ontology Engineering Based on Domain Specific Languages and the Application of Ontology Design Patterns .....	167
<i>Thomas Janke</i>	
A Domain Specific Metamodel for Semantic Web Enabled Multi-Agent Systems .....	177
<i>Moharram Challenger, Sinem Getir, Sebla Demirkol, and Geylani Kardas</i>	
Reconstructing the Blade Technology Domain with Grounded Theory .....	187
<i>André Zwanziger</i>	
Specification and Refinement of Domain-Specific ECA Policies .....	197
<i>Raphael Romeikat and Bernhard Bauer</i>	

### 4th International Workshop on Governance, Risk and Compliance: Applications in Information Systems (GRCIS 2011)

Preface GRCIS 2011 .....	207
<i>Marta Indulska, Michael zur Muehlen, Shazia Sadiq, and Sietse Overbeek</i>	
Patterns for Understanding Control Requirements for Information Systems for Governance, Risk Management, and Compliance (GRC IS) .....	208
<i>Manuel Wiesche, Carolin Berwing, Michael Schermann, and Helmut Kremer</i>	
Exploring Features of a Full-Coverage Integrated Solution for Business Process Compliance .....	218
<i>Cristina Cabanillas, Manuel Resinas, and Antonio Ruiz-Cortés</i>	
A Systematic Review of Compliance Measurement Based on Goals and Indicators .....	228
<i>Azalia Shamsaei, Daniel Amyot, and Alireza Pourshahid</i>	
Continuous Control Monitoring-Based Regulation: A Case in the Meat Processing Industry .....	238
<i>Joris Hulstijn, Rob Christiaanse, Nitesh Bharosa, Friso Schmid, Remco van Wijk, Marijn Janssen, and Yao-Hua Tan</i>	
Semantic Representation of Process and Service Compliance – A Case Study in Emergency Planning .....	249
<i>Aygul Gabdulhakova, Birgitta König-Ries, and Norris Syed Abdullah</i>	
A Framework for Organizational Compliance Management Tactics .....	259
<i>Ralph Foorthuis and Rik Bos</i>	
<b>First Workshop on Integration of IS Engineering Tools (INiSET 2011)</b>	
Preface INiSET 2011 .....	269
Tool Integration beyond Wasserman .....	270
<i>Fredrik Asplund, Matthias Biehl, Jad El-Khoury, and Martin Törngren</i>	
Integrating Computer Log Files for Process Mining: A Genetic Algorithm Inspired Technique .....	282
<i>Jan Claes and Geert Poels</i>	

### 9th International Workshop on System/Software Architectures (IWSSA 2011)

Preface IWSSA 2011 .....	294
<i>Lawrence Chung and Nary Subramanian</i>	
Ontology-Based Architectural Knowledge Representation: Structural Elements Module .....	296
<i>David Ameller and Xavier Franch</i>	
The Overall Value of Architecture Review in a Large Scale Software Organization .....	302
<i>Sofia Sherman, Irit Hadar, Ethan Hadar, and John J. Harrison Jr</i>	
Evaluating Complexity of Information System Architecture Using Fractals .....	308
<i>Nary Subramanian</i>	
Towards a Reconfigurable Middleware Architecture for Pervasive Computing Systems .....	318
<i>Gustavo G. Pascual, Lidia Fuentes, and Mónica Pinto</i>	
A Reference Architecture for Building Semantic-Web Mediators .....	330
<i>Carlos R. Rivero, Inma Hernández, David Ruiz, and Rafael Corchuelo</i>	
F-STREAM: A Flexible Process for Deriving Architectures from Requirements Models .....	342
<i>Jaelson Castro, João Pimentel, Márcia Lucena, Emanuel Santos, and Diego Dermeval</i>	
Architecting Climate Change Data Infrastructure for Nevada .....	354
<i>Michael J. McMahon Jr., Sergiu M. Dascalu, Frederick C. Harris Jr., Scotty Strachan, and Franco Biondi</i>	
A Coordination Space Architecture for Service Collaboration and Cooperation .....	366
<i>Claus Pahl, Veronica Gacitua-Decar, MingXue Wang, and Kosala Yapa Bandara</i>	
A Framework to Support the Development of Collaborative Components .....	378
<i>Hien Le and Surya Bahadur Kathayat</i>	
Resource Allocation, Trading and Adaptation in Self-managing Systems .....	385
<i>Guglielmo Lulli, Pasqualina Potena, and Claudia Raibulet</i>	

### Third International Workshop on Ontology-Driven Information Systems Engineering Workshop (ODISE 2011)

Preface ODISE 2011 .....	397
<i>Sergio de Cesare, Frederik Gailly, Grant Holland, Mark Lycett, and Chris Partridge</i>	
Ontology Mining versus Ontology Speculation .....	401
<i>Chris Partridge</i>	
Design Patterns and Inductive Modeling Rules to Support the Construction of Ontologically Well-Founded Conceptual Models in OntoUML .....	402
<i>Giancarlo Guizzardi, Alex Pinheiro das Graças, and Renata S.S. Guizzardi</i>	
Semantic-Based Case Retrieval of Service Integration Models in Extensible Enterprise Systems Based on a Business Domain Ontology .....	414
<i>Matthias Allgaier, Markus Heller, Sven Overhage, and Klaus Turowski</i>	
Sapphire: Generating Java Runtime Artefacts from OWL Ontologies ...	425
<i>Graeme Stevenson and Simon Dobson</i>	
Mooop – A Hybrid Integration of OWL and Java .....	437
<i>Christoph Frenzel, Bijan Parsia, Ulrike Sattler, and Bernhard Bauer</i>	

### 5th Ontology, Models, Conceptualization and Epistemology in Social, Artificial and Natural Systems Workshop (ONTOSE 2011)

Preface ONTOSE 2011 .....	448
Improving the Effectiveness of Multimedia Summarization of Judicial Debates through Ontological Query Expansion .....	450
<i>E. Fersini and F. Sartori</i>	
Ontology-Based Composition and Matching for Dynamic Service Coordination .....	464
<i>Claus Pahl, Veronica Gacitua-Decar, MingXue Wang, and Kosala Yapa Bandara</i>	
Detecting Antipatterns Using a Web-Based Collaborative Antipattern Ontology Knowledge Base .....	478
<i>Dimitrios Settas, Georgios Meditskos, Nick Bassiliades, and Ioannis G. Stamelos</i>	

POWER - Politics Ontology for Web Entity Retrieval . . . . .	489	Taking into Account Functional Models in the Validation of IS Security Policies . . . . .	592
<i>Silvio Moreira, David Batista, Paula Carvalho, Francisco M. Couto, and Mário J. Silva</i>		<i>Yves Ledru, Akram Idani, Jérémy Milhau, Nafees Qamar, Régine Laleau, Jean-Luc Richier, and Mohamed-Amine Labiadh</i>	
An Error Correction Methodology for Time Dependent Ontologies . . . . .	501	Expressing Access Control Policies with an Event-Based Approach . . . . .	607
<i>Brett Drury, J.J. Almeida, and M.H.M. Morais</i>		<i>Pierre Konopacki, Marc Frappier, and Régine Laleau</i>	
An Ontology-Based Integrated Approach to Situation Awareness for High-Level Information Fusion in C4ISR . . . . .	513	An Extended Ontology for Security Requirements . . . . .	622
<i>María-Cruz Valiente, Rebeca Machín, Elena García-Barriocanal, and Miguel-Ángel Sicilia</i>		<i>Fabio Massacci, John Mylopoulos, Federica Paci, Thein Thun Tun, and Yijun Yu</i>	
Socio-technic Dependency and Rationale Models for the Enterprise Architecture Management Function . . . . .	528	A Pattern Based Approach for Secure Database Design . . . . .	637
<i>Sabine Buckl, Florian Matthes, and Christian M. Schweda</i>		<i>Jenny Abramov, Arnon Sturm, and Peretz Shoval</i>	
<b>First International Workshop on Semantic Search (SSW 2011)</b>		Analysis of Application of Security Patterns to Build Secure Systems . . . . .	652
Preface SSW 2011 . . . . .	541	<i>Roberto Ortiz, Javier Garzás, and Eduardo Fernández-Medina</i>	
<i>Paolo Cappellari, Roberto De Virgilio, and Mark Roantree</i>		Modeling Support for Delegating Roles, Tasks, and Duties in a Process-Related RBAC Context . . . . .	660
Enhancing the Interface for Ontology-Supported Homonym Search . . . . .	544	<i>Sigrid Schefer and Mark Strembeck</i>	
<i>Tian Tian, James Geller, and Soon Ae Chun</i>		<b>Author Index</b> . . . . .	669
Combining Faceted Search and Query Languages for the Semantic Web . . . . .	554		
<i>Sébastien Ferré, Alice Hermann, and Mireille Ducassé</i>			
Towards a Collaborative Framework for Image Annotation and Search . . . . .	564		
<i>Yi Hong and Stephan Reiff-Marganiec</i>			
Semantic Reasoning with SPARQL in Heterogeneous Multi-context Systems . . . . .	575		
<i>Peter Schüller and Antonius Weinzierl</i>			
Semantic Ontology-Based Strategy for Image Retrieval in Conceptual Modelling . . . . .	586		
<i>Simon McGinnes</i>			
<b>First International Workshop on Information Systems Security Engineering (WISSE 2011)</b>			
Preface WISSE 2011 . . . . .	590		
<i>Nadira Lammari and David G. Rosado</i>			



# Analysis of Application of Security Patterns to Build Secure Systems

Roberto Ortiz<sup>1</sup>, Javier Garzás<sup>2</sup>, and Eduardo Fernández-Medina<sup>3</sup>

<sup>1</sup> S21SecLabs-SOC. Group S21Sec Gestión S.A., Valgrande, 10, 28108. Madrid, Spain  
r.ortizpl@gmail.com

<sup>2</sup> Kybele Group. Dep. of Computer Languages and Systems II. University Rey Juan Carlos,  
Tulipán. s/n, 28933. Madrid, Spain  
javier.garzas@urjc.es

<sup>3</sup> GSyA Research Group. Dep. of Information Technologies and Systems. University of  
Castilla-La Mancha. Paseo de la Universidad, 4. Ciudad Real, Spain  
Eduardo.FdezMedina@uclm.es

**Abstract.** Both new technology business models and the new tendencies in the field of computing are forcing organizations to undergo a constant evolution in order to maintain their competitiveness in markets. This evolution has led to a continuous remodeling of companies' systems to enable them to adapt to the new needs. These changes increase these systems' complexity, making them more vulnerable. Computer attacks against organizations are therefore increasing considerably. If this is to be avoided, information security engineers need reliable and validated solutions with which to confront security problems, along with agile solutions to confront the new technological necessities in an optimal manner. Security patterns are good mechanisms with which to perform this task since they provide documented, validated and tested solutions to recurring problems. In this paper we carry out an analysis of those proposals that use security patterns to build secure systems when this task is performed in the information systems of a real organization, with the objective of detecting any shortcomings and new needs.

**Keywords:** Security patterns, secure systems, information security, security.

## 1 Introduction

One of the most important problems in the field of information systems in the last few years has been that of security, principally owing to the emergence of new vulnerabilities caused by the increased complexity of these systems and by the fact that organizations have opened their databases on the internet [1]. The number of attacks has therefore significantly increased and the advantages obtained by attackers are greater and greater [2].

Information security is therefore one of the main concerns of IT organizations, and these organizations' security engineers consequently find it necessary to incorporate security requirements into their systems, whilst always bearing mind business needs in order to, on the one hand, safeguard their assets and, on the other, minimize the number of attacks against their systems and reduce these attacks' effectiveness [3].

To optimize the task of incorporating security into the existing systems in an agile and optimal manner, it is necessary that engineers have reliable, validated and tested solutions at their disposal. It is also important for these engineers to offer homogeneous solutions to similar problems with the purpose of maintaining a defense strategy that is aligned within the corporation in which they work.

Security patterns are a good tool to satisfy the aforementioned necessities since they encapsulate experts' knowledge and experience regarding a recurring problem in a particular security discipline [4]. In other words, a pattern solves a specific problem in a determined context and can be adapted to different situations [5].

Information security engineers can therefore use security patterns to build secure information systems since they are a good tool for systematizing the process of solving recurring problems, and provide guidelines for the construction and evaluation of secure systems [6]. However, when information security engineers perform this task within the systems of a real and complex organization, they must take into account a set of considerations related to certain important parameters of the system or of the organization, such as compatibility, performance, cost, time spent, type of asset to be protected, organizational rules, etc.

In this paper we have therefore carried out an in-depth analysis of a set of some of the most important proposals, extracted from a previously performed systematic review, which use security patterns to build secure systems. This has allowed us to obtain conclusions concerning the current use of security patterns in information systems, along with the factors or parameters that should currently be considered when applying these patterns to an organization's real and complex systems. A discussion of the results obtained is then provided.

The remainder of this paper is organized as follows: in Section 2, we present the analysis of the selected proposals and the results. Section 3 provides a discussion of this and other related works. The paper ends with some conclusions in Section 4.

## 2 Analysis of Proposals

This section shows the analysis performed and discusses the results obtained from some of the most relevant proposals which use security patterns in specific contexts in order to build secure systems [7–17]. Both the analysis and the discussion are focused on analyzing whether these works take into account a set of the considerations that are necessary when the patterns are used to develop secure systems within a real and complex organization. Finally, the detected shortcomings and the current needs in this field are analyzed, and a series of suggestions to improve these deficiencies is proposed in order for this type of solutions to be optimally implemented in real organizations.

This task has been carried out by using Table 1, in which the selected initiatives that are compared are presented. This comparative study has been made with the use of an analytical framework (partially based on [18]). This framework contains a series of technical applicability criteria based on the considerations put forward by Kienzle et al. [19], which are detailed as follows. Each of these criteria are considerations that must be taken into account by security engineers when building a real secure system, since they are related to highly important parameters such as performance, cost, time

spent, effectiveness and learning. In order to provide details of certain consequences of disregarding some of these considerations and thus facilitate the reader's understanding, we give brief, clear and real examples to explain each necessity.

- **Impact on other components in the system:** in this criterion, we shall analyze whether the proposals consider the pattern's compatibility with the other components in the system, along with any possible consequences of its use. The following example is presented to enable the reader to understand this criterion. An organization decides to use the security strategy of carrying out a centralized identity management in order that the people in charge of security in the organization have from a unique point the control of, for example, the digital certificates needed for systems to perform authentication and establish trust relationships with other organizations' systems. One possible solution is to use a single centralized cryptographic store that is independent of the product or system that requires it. In this case, if compatibilities between the elements existing in the system and the solution implemented by the security pattern are not considered, problems such as the unfeasibility of the solution could arise if, for example, certain Microsoft products such as Outlook are used. Since this product does not permit integration with any cryptographic stores that are external to its local store, it is necessary to perform an ad-hoc development to be able to implement the pattern in the organization's systems.
- **Impact on the system:** In this criterion, we shall analyze whether the proposals consider the possible increases in the system involved with regard to the need for storage, an increase in the memory consumed, patching frequency, process capacity, bandwidth, etc. We shall attempt to clarify the meaning of this criterion through the following example. An organization wishes to implement an access control system in its information systems. As an alternative, it decides to use RBAC [4] which is based on authenticating and authorizing access depending on the role of each user/subsystem within the organization. It is therefore necessary to consider the aforementioned parameters owing to the fact that the technical features may be affected, depending on the amount of system users, the frequency of their accesses and the different combinations needed to grant access to a resource. If, for example, the amount of users is not correctly estimated, it is probable that the system performance, the process capacity, the bandwidth, and the consumed memory will be affected, which could cause the solution to fail.
- **Solution cost:** We shall analyze whether the cost of installing or implementing the solution in the systems of an organization is considered. An example of this will be presented together with the that of following criterion.
- **Used time:** We shall verify, without going into great detail, whether the proposals estimate the time needed to implement or use a pattern in an organization's systems. The two aforementioned criteria can be analyzed from a common perspective, and are also dependent on the other criteria. This is owing to the fact that if any of the criteria shown in this section are not considered, these two criteria will be affected and this will also affect the final solution. When criteria that may affect the final solution are disregarded, these parameters might be affected because, for example a later cost increase with regard to the dimension of the problem may occur, thus leading to an increase in the time needed to solve the problem with the solution proposed by the pattern.

- **Presentation of real examples:** We shall verify whether the proposals are accompanied by a real implementation example that backs the validation of the solution. It is evident that if the application of the security pattern includes a real example in its description, this will signify that, on the one hand, it has been implemented in a real system and, on the other, it has been tested by verifying its behavior as solution.
- **Evaluation of the criticality of the asset to protect:** We shall analyze whether the proposals catalog the criticality of the asset to be protected. Not all assets have the same importance within an organization, and if they are all treated in the same way, this may significantly affect the solution. Let us take the case of the protection of a web application as an example. To do so, the use of a sequence of security patterns to ensure authentication, authorization, role-based access control along with a data ciphering in databases to ensure data confidentiality is suggested. If accessible information is of a public nature and the service availability is not critical, then the majority of controls will not be necessary, since the installation of a perimeter control such as the Firewall [4] pattern will be sufficient to avoid problems of denial of service attacks. However, if the information accessed is of a special nature and its spreading would compromise the organization, then it would perhaps be necessary to increase controls. That is to say, we should introduce security patterns such as Securepipe [4] and additional security measures to cipher the data. The generalization of solutions for apparently similar problems without considering the criticality of the assets to be protected may cause inefficiency or the failure of the solution.
- **Fulfillment of rules and regulations:** We shall verify whether the proposals consider that the different legislation of the countries in which the solution will be implemented may condition this solution, or whether changes to the organization's rules are considered. The example is as follows: Let us suppose that an organization has different subsidiary enterprises in several countries and that it intends to unify the access system in order to optimize the access control to the systems of the whole organization. A new central repository in which the credentials of all the organization's system users throughout the world are located is therefore proposed. Depending on each country's regulations, this common repository will have some characteristics or others. More specifically, if the repository is located in countries such as Argentina, Venezuela or USA, then these countries' regulations oblige their enterprises to store these data in a determined manner that does not apply to other countries. It might also occur that these countries do not allow the output of determined information concerning their local users to be shared with the organization's other subsidiary enterprises, with the exception of the main headquarters.

Having presented the criteria to be analyzed, we shall now verify whether each of the analyzed proposals completely fulfils each of the applicability technical criterion evaluated (Y), whether it refers briefly to this criterion (P), or whether it neither mentions nor considers the criterion (N). In Table 1 the vertical columns show the references to the papers analyzed and the rows show the aforementioned criteria.

As can be observed in Table 1, most of the proposals principally lack: An evaluation of the compatibilities and possible consequences with regard to the other components in the system when using a pattern. This lack may cause incompatibilities with

Table 1. Analysis of Proposals

	Applicability technical criteria							
	Impact on other components	Impact on the system	Solution cost	Used time	Real examples	Criticality of the asset	Rules and Regulations	
Proposals	[7]	P	Y	N	N	Y	N	Y
	[8]	N	N	N	N	P	N	N
	[9]	N	P	N	N	N	Y	N
	[10]	N	P	N	N	N	Y	Y
	[11]	N	P	N	N	Y	N	N
	[12]	N	P	N	N	P	N	N
	[13]	Y	Y	Y	N	N	N	N
	[14]	N	N	N	N	Y	N	N
	[15]	N	N	N	N	P	N	N
	[16]	N	N	N	N	P	N	N
[17]	N	N	N	N	N	N	N	

some of the elements in the system that were not detected a priori to arise, thus causing the solution to fail; A detailed evaluation of the impact that the pattern might have on the system into which it is introduced in terms of storage, the memory consumed, patching frequency, processing capacity, bandwidth, etc. A failure to analyze these critical parameters could compromise the service's availability; A specific classification of the criticality of the assets to be protected by the pattern. If this parameter is not analyzed, the risk of not appropriately measuring the security measures to be provided exists, thus leading to excessive investments or, in their absence, leaving the system vulnerable to any attack not considered earlier; A general presentation of the impact on the cost and time necessary to implement the pattern. This lack may cause an organization to discard the solution because it is not able to assume the related costs or because it is unable to plan a business strategy for the organization since the time needed is not available; Specific considerations in relation to the limitations that may be imposed by the rules and regulations in different countries. This aspect is as critical as the others, but directly affects international organizations. When an organization's business depends on, among other factors, the regulations of the country in which its systems are located, it is necessary to include this criterion as a variable in the equation since it can condition the solution at all times. All these parameters are critical, and should therefore be decisive when using security patterns in the organization's real systems. Neglecting to analyze them may frequently cause the solution to fail.

### 3 Discussion and Related Works

In spite of the analysis results, security patterns are, in our opinion, a good tool with which to homogenize security solutions to similar problems confronted by different

engineers, along with providing agile, proved, validated and secure solutions to recurring security problems. For this reason and for all the considerations presented in the previous section, we believe that it is necessary for current security patterns to evolve to reflect each of the aforementioned considerations in order to permit their easy application in real systems. We also believe that the creation of a security pattern use methodology is necessary to help information security engineers to build secure systems in real organizations through a systematic process. This type of guided process will facilitate the process of considering all of the aforementioned aspects, since each of the considerations that may affect an organization's systems will be analyzed when implementing solutions in the form of security patterns.

Various works which are focused on the application of patterns in security systems through a systematic process are attempting to cover this need. In [20] the author puts forward a general methodology for developing secure-critical software. He uses UMLsec to extend UML to model security properties in informatics systems. This proposal has recently been extended in order to use patterns to support the modeling and verification of formal aspects of security. In [21, 22] the authors apply security patterns through the use of a secure system development method based on hierarchical architectures whose levels define the scope of each security mechanism. These works are all evolutions of the same approach, and one of their main advantages are the guidelines offered in each stage to assist the user to discover where to apply and how to select the security pattern which is most appropriate to satisfy the functional requirements or restrictions in each stage. In [23] the authors propose a systematic method with which to integrate security patterns into a software engineering process. This proposal assists experts to close the gap between the abstract solution described in the pattern and the implementation proposed in the application.

### 4 Conclusions

The principal purpose of this paper has been to perform an analysis of proposals which use security patterns to build secure systems. This analysis is focused on the way in which these patterns are used, in order to verify whether these proposals take into account a set of considerations that are necessary when solutions are introduced into real systems. A discussion of the results in which the principal shortcomings and research needs in this field were detected is then presented.

The main conclusion of this research is that the current proposals that use security patterns to build secure systems do not take into account considerations that may condition the solution, and are therefore critical considerations when the solution is implemented in an organization's real and complex information systems. That is to say, they do not consider the impact that the pattern could have on the system or on some of its components; they do not perform a classification of the criticality of the assets to be protected, generalizing solutions inefficiently. Furthermore, they do not consider the different rules and regulations that exist in different countries. The lack of analysis of these and the other considerations presented in the paper may cause a drastic increase in terms of cost and time when confronting the security problem and the solution may sometimes fail.

We are currently working on the definition of a methodology for security pattern use that will guide the security engineer, in an agile and efficient manner, at the time of developing a secure system within a real and complex organization. This methodology uses a new template that can be found in [24], in which all the parameters considered in the previous analysis are reflected.

### Acknowledgments

This research has been carried out in the framework of the following projects: MODEL-CAOS (TIN2008-03582/TIN) financed by the Spanish Ministry of Education and Science, SISTEMAS (PII2I09-0150-3135) and SERENIDAD (PEII11-0327-7035) financed by the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha" and FEDER, and BUSINESS project (PET2008-0136) financed by the "Ministerio de Ciencia e Innovación", Spain.

### References

1. Fernandez, E.B., Pan, R.: A pattern language for security models PLoP 13 (2001)
2. Internet Crime Complaint Center. IC3, <http://www.ic3.gov>
3. Stoneburner, G., Goguen, A., Feringa, A.: Risk Management Guide for Information Technology Systems, pp. 800–830. NIST Special Publication (2002)
4. Schumacher, M., Fernandez, E.B., Hybertson, D., Buschmann, F., Sommerlad, P.: Security Patterns: Integrating Security and Systems Engineering (2006)
5. Gamma, E., et al.: Design Patterns: Elements of Reusable Object Oriented Software. Addison Wesley, London (1995)
6. Ortiz, R., Moral-García, S., Moral-Rubio, S., Vela, B., Garzás, J., Fernández-Medina, E.: Applicability of security patterns. In: Meersman, R., Dillon, T.S., Herrero, P. (eds.) IS 2010 – OTM 2010. LNCS, vol. 6426, pp. 672–684. Springer, Heidelberg (2010)
7. Busnel, P., El Houry, P., Li, K., Saidane, A., Zannone, N.: S&D Pattern Deployment at Organizational Level: A Prototype for Remote Healthcare System. ENTCS, vol. 244, pp. 27–39 (2009)
8. Brown, S.G., Yip, F.: Integrating Pattern Concepts & Network Security Architecture. In: NOMS 2006: 10th IEEE/IFIP Network Operations and Management Symposium, pp. 1–4 (2006)
9. Fernandez, E.B., Wu, J., Larrondo-Petrie, M.M., Shao, Y.: On building secure SCADA systems using security patterns. In: CSIIIRW 2009: Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research, pp. 1–4. ACM Press, NY (2009)
10. Fernandez, E., et.al.: M.M.: Designing Secure SCADA Systems Using Security Patterns. In: 43rd Hawaii International Conference on System Sciences (HICSS), p. 8 (2010)
11. Bellebia, D., Douin, J.M.: Applying patterns to build a lightweight middleware for embedded systems. In: Proceedings of the 2006 Conference on Pattern Languages of Programs, ACM, Portland (2006)
12. Fernandez, E.B., Pelaez, J.C., Larrondo-Petrie, M.M.: Security Patterns for Voice over IP Networks. In: ICCGI 2007, International Multi-Conference on Computing in the Global Information Technology, pp. 33–33 (2007)

13. Xiangli, Q., Xuejun, Y., Jingwei, Z., Xuefeng, L.: Integration Patterns of Grid Security Service. In: Proceedings of the Sixth International Conference on Parallel and Distributed Computing Applications and Technologies, IEEE Computer Society, Los Alamitos (2005)
14. Lirong, D., Kendra, C.: Using FDAF to bridge the gap between enterprise and software architectures for security. Sci. Comput. Program. 66, 87–102 (2007)
15. Schnjakin, M., Menzel, M., Meinel, C.: A pattern-driven security advisor for service-oriented architectures. In: Proceedings of the 2009 ACM Workshop on Secure Web Services. ACM, Chicago (2009)
16. Michael, M., Robert, W., Christoph, M.: A Pattern-Driven Generation of Security Policies for Service-Oriented Architectures. In: Proceedings of the 2010 IEEE International Conference on Web Services, IEEE Computer Society, Los Alamitos (2010)
17. Delessy, N., Fernandez, E.B., Larrondo-Petrie, M.M.: A Pattern Language for Identity Management. In: ICCGI 2007, International Multi-Conference on Computing in the Global Information Technology, pp.31-31(2007)
18. Khawaja, A., Urban, J.: A synthesis of evaluation criteria for software specifications and specifications techniques. International Journal of Software Engineering and Knowledge Engineering 12, 581–599
19. Kienzle, D.M., Elder, M.C., Tyree, D.S., Edwards-Hewitt, J.: Security patterns template and tutorial (2002)
20. Jürjens, J.: Secure Systems Development with UML. Springer, Heidelberg (2004)
21. Fernandez, E.B.: Security Patterns and A Methodology to Apply them. Security and Dependability for Ambient Intelligence, 37–46 (2009)
22. Fernandez, E.B., Larrondo-Petrie, M.M., Sorgente, T., VanHilst, M.: A methodology to develop secure systems using patterns. In: Integrating Security and Software Engineering, Advances and Future Vision. ch.5, pp. 107–126. IDEA Press (2006)
23. Sanchez-Cid, F., Maña, A.: SERENITY Pattern-Based Software Development Life-Cycle. In: Bhowmick, S.S., Küng, J., Wagner, R. (eds.) DEXA 2008. LNCS, vol. 5181, pp. 305–309. Springer, Heidelberg (2008)
24. Moral-García, S., Ortiz, R., Moral-Rubio, S., Vela, B., Garzás, J., Fernández-Medina, E.: A New Pattern Template to Support the Design of Security Architectures. In: The Second International Conferences of Pervasive Patterns and Applications, Lisbon, Portugal (2010)