IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4135

Managing Process Compliance With Standards

Larry Y. C. Cheung[1], Paul W. H. Chung[2] and Ray J. Dawson[3]
Loughborough University, Loughborough, LE11 3TU, England
[1]Tel: +44 (0)1509 228230, [2]Tel: +44 (0)1509 222543, [3]Tel: +44 (0)1509 222679, [1,2,3]Fax: +44 (0)1509 211856
{Y.C.Cheung, P.W.H.Chung, R.J.Dawson}@lboro.ac.uk

Copyright Idea Group Inc.

ABSTRACT

The current best practice of providing reliable systems is to embody the development process in recent industry safety standards and guidelines, such as IEC 61508. These standards generally define practices in terms of constraints. The degree of standards compliance can be established by checking the execution of essential activities against these constraints. However, every application is different because of the differences in project details. The lack of the ability to ensure that a process is planned and performed complying with a standard necessitates the improvements in the current workflow management systems (WfMS).

Our Compliance Flow research project aims to provide support for handling complex, ad-hoc, dynamic changing, and collaborative engineering design process. This paper describes the use of an intelligent compliance agent, called Inspector, in Compliance Flow to ensure a standard complied process. The standards that the design process intended to be complied with are modelled into a model of standards using the Standard Modelling Language (SML) we developed. The Inspector performs a number of matching processes between the model of standards and the development process to achieve the compliance. Some examples drawing on IEC 61508 are used to illustrate the mechanism of modelling and compliance checks.

INTRODUCTION

In order to provide reliable systems or services, the current best practice of development process is typically embodied in recent safety standards and guidelines. Once a standard has been adopted it is important to manage compliance with the standard. By compliance we mean that as long as there is a clear description of the design stages and, at each stage, the input to that stage (requirements) are fully and unambiguously defined, and finally the objectives and requirements of each practices of the standard are met. Standards are generic but every application is different due to the differences in project details. It is neither practical nor desirable to compel compliance at all points in the development process. Thus determining the degree of compliance with specified practices as development progresses is a challenging task.

Standards generally define development cycles in terms of constraints that must hold for documents. The document types identified by standards include typical development information along with each design stages, such as requirements and deliverables. The degree of standards compliance can be assessed by checking these documents against the constraints. Current researches such as [10] and [11] adopt a document-centred approach in which the development process is represented in the product and hence represented implicitly. The compliance has been treated as a problem that is closely related to inconsistency management in specification such as [12][13] and [14]. A document schema specification is used to elaborate and formalise the definitions of document structure suggested in the standard so that properties can be checked against them. Appropriate checks will be triggered when events occur on document during the development process. This approach can make certain that the expected deliverables are obtained passively, which matches current quality control practice where the compliance checks are performed at the end of design stages by individual assessors, but lacks the ability to manage the development process to proactively prevent unqualified deliverables as a result of wrongly planned process.

A Workflow Management System (WfMS) is a system that aims to provide computer-based support for the task of workflow management, hence inherently provides a more adequate environment to be extended than project management tools or document management tools in supporting a standard complied project. Most WfMSs can only support simple, well-defined, consistent and predictable administrative processes, but not dynamic changing, complex, collaborative processes occurred in engineering projects [1][2][9]. Recently, techniques from artificial intelligence (AI) are being used to make WfMSs more adaptive and to allow it to deal with such complex processes [4][5][6][7][8]. However, current workflow reference models, such as [15], provide no support for maintaining process consistency against particular standards. The use of software agent, we believed, is the most lightweight means to bridge this gap.

Our Compliance Flow project aims to provide support for handling complex engineering design processes. Compliance Flow has two novel features:

1. By employing compliance agent to ensure that processes specified in Compliance Flow are planned and performed in accordance with one or more industry standards.
2. By integrating a number of innovative artificial intelligent technologies to provide support for collaborative, dynamic and complex engineering design process.

Our approach to the compliance problem is to model the standards in terms of activities together with constraints into a model of standards. Compliance checks will be performed between the model of standards and user-defined process plan during both process build and run time. A user defined development cycle different from the one proposed in the standard is allowed in Compliance Flow while the compliance checks can still be performed without any problem. The required information for the documents are included in the post-conditions of their relevant processes so that the standard complied documents will be delivered if the processes are completed successfully.

Significant resources are devoted to managing standards compliance particularly in safety engineering projects. In such projects much of the time of developers, managers and quality assurance teams is occupied with identifying breaches in compliance and with tracking and managing the compliance of a project. Thus, our treatment of this problem is strongly industrially motivated.

This paper mainly describes the work around the first feature where the international safety standard IEC 61508 is used to perform the evaluation. The next section describes how an industry standard can be modelled into the model of standards using our Standard Modelling Language. Section 3 introduces the compliance agent and how it performs compliance assurance. Section 4 provides a discussion on the degree of coupling between the compliance agent and the model of the standards. Finally, Section 5 concludes with a summary of our principal contributions.

STANDARD MODELLING LANGUAGE

Standard Modelling Language (SML) is used to describe a standard in terms of activities and their constrains that will be used as a check spelling process in which a number of matching mechanisms will be performed by the Inspector to verify whether the objectives of each

This paper appears in *Issues and Trends of Information Technology Management in Contemporary Organizations,* the proceedings of the Information Resources Management Association International Conference. Copyright © 2002, Idea Group Inc.

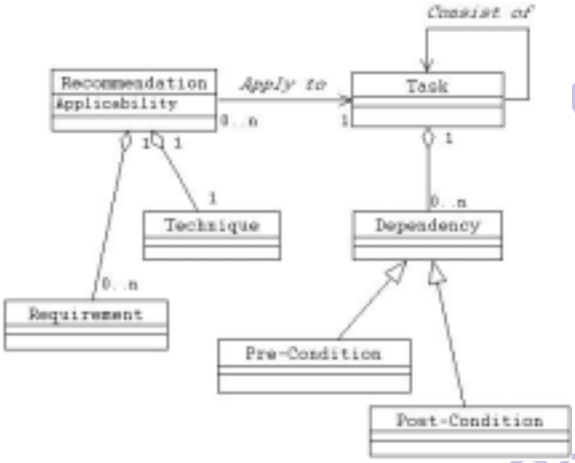
practices defined in the standard will be achieved in required sequence and are fully included. These objectives will be expressed on the structure or the contents of documents. Thus, qualified documents will be obtained if the relevant activities are planned correctly and performed successfully. The SML is devised to be capable of modelling a wide range of standards. It can model two important aspects of standards in terms of workflow management:

3. The development lifecycle, which is used as the key framework to deal in a systematic manner with all the activities necessary to achieve the required quality of products or services.
4. The techniques, measures, tools or methods that are recommended by the standard to be used to achieve specific objectives or requirements.

Most of the standards emphasize that the activities should be performed by qualified persons. The capability of identifying suitable person for performing particular activity is left to our workflow process model. Details can be referred to [18].

The language has successfully modelled IEC 61508 with its two important concepts: the Safety Lifecycle and Safety Integrity Levels (SIL). The meta-model of standard modelling is illustrated in Figure 1.

Figure 1: Meta-model of standard modelling



The Safety Lifecycle proposed by IEC 61508 is modelled into a hierarchical task network (HTN) in which the tasks correspond to the activities in the Safety Lifecycle. A task is a basic unit of work, which can be hierarchically decomposed into subtasks until the required details are modelled as long as the parent and child relationship between tasks are maintained.

Each task is associated with two sets of conditions: pre and post conditions. These conditions will be detailed as their associated tasks and are decomposed into subtasks. The post-conditions of a task are sometimes the pre-conditions of its subsequent tasks. To perform a task requires the fulfilment of its pre-condition, and to do so, the preceding task that satisfies those conditions as post-conditions must be completed successfully in advance. Therefore the order of the execution of tasks is constrained by their dependencies.

IEC 61508 views the requirements simply as the input to a distinct stage in the lifecycle, and the design specification as the output of that stage. The pre and post conditions are related to the requirements and the specification of each stage respectively that have to be achieved under the recommended sequence in order to comply with IEC 61508. A condition is presented in the form of checklists, and is stated as fulfilled when all items in the checklist are checked.

The recommended techniques, measures, tools or methods that have to be used for specific tasks to achieve the specified objectives are modelled with four parameters: (1) the task for which the technique is required, (2) the requirement for applying the technique, (3) the technique itself, (4) and the level of recommendation. The value of parameter 2 can be null, implying that no requirement is necessary to apply the technique.

IEC 61508 introduces sets of techniques for specific development activities with different level of applicability according to the SIL of the product to be developed. The SIL is normally achieved after the safety requirements are addressed. Therefore, the level of SIL (from 1 to 4) becomes the requirement for applying the recommended techniques. These techniques are categorised into four levels of recommendation in IEC 61508 namely Highly Recommended (HR), Recommended (R), No Recommendation (-), and Not Recommended (NR).

These recommendations can be modelled, for example, IEC 61508 recommends that the technique 'Structure Methodology' (parameter 3) is Highly Recommended (parameter 4) during the achievement of objective of Clause B.30 (parameter 1) when the SIL of the product being developed is equal to 1 (parameter 2).

Standard Modeller is the tool used to model the standards. Figure 2 is a snapshot in which the Overall Safety Lifecycle [16] in IEC 61508 is modelled.

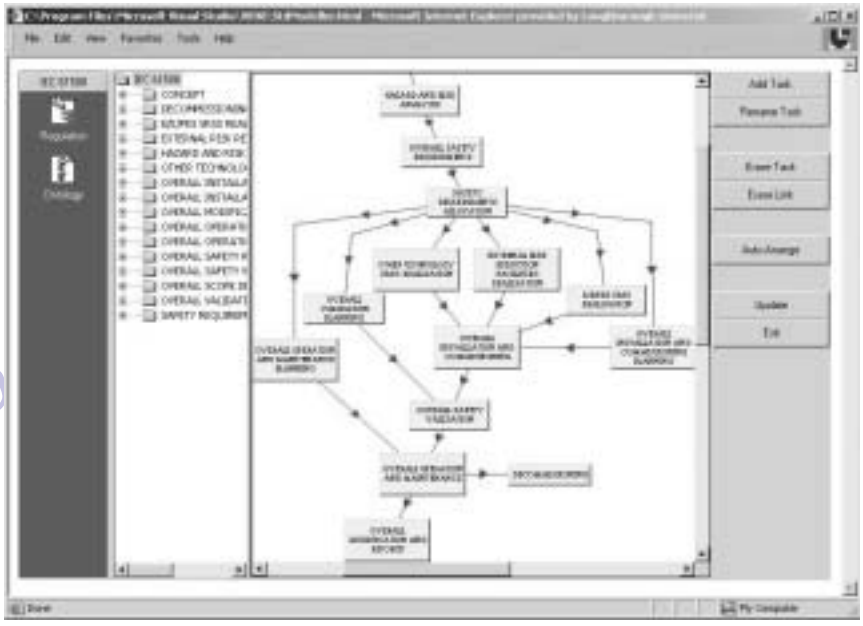
COMPLIANCE AGENT AND COMPLIANCE ASSURANCE

Agent Inspector is a piece of software that continually monitors the planning and the execution of activities to ensure that the development process are planned and performed in accordance with a particular standard, in this case IEC 61508 safety standard. Inspector performs following duties:

During Process Build-Time: Inspector provides three kinds of consultative services (compliance check) during task planning, namely correctness check (ordering), completeness check, and cross-referencing to help users in devising a standard compliance plan.

During Process Run-Time: Inspector actively prevents the task from being executed incorrectly.

Figure 2: Snapshot of standard modeller



Copyright Idea Group Inc
Copyright Idea Group Inc
Copyright Idea

During Process Build-Time and Run-Time: Inspector ensures that the recommended techniques have been fully considered.

Compliance Check

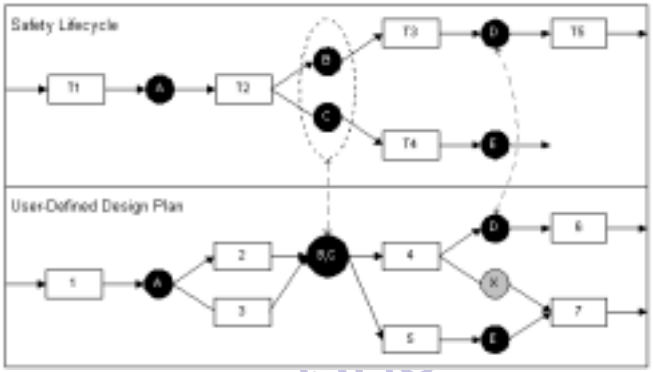
Correctness check will be performed when Inspector services the requests from users for verifying that the placement of a particular specification in a design plan complies with IEC 61508. To verify the correctness of a specification, two mapping mechanisms are required:

1. Existence Check. It maps the specification of a user-defined process plan with the specifications identified in the Safety Lifecycle proposed by IEC 61508.
2. Ordering Check. If the specification exists, the immediate previous specifications in the Safety Lifecycle are then mapped with the previous specifications in the user-defined process plan.

The success of both mapping mechanisms implies that the production of the specification is planned in a right sequence. An example is given in Figure 3.

In figures 3 and 4, rectangles with identifiers beginning with the letter T represent the tasks of a process, and circles represent pre or post conditions of tasks.

Figure 3: Example of correctness check



In Figure 3, to check the compliance of specification D in the design plan, agent Inspector will first determine whether specification D exist in Safety Lifecycle by performing a search in the model of standard. If not found, it implies that specification D belongs to the type of user-defined specification that is beyond the scope of IEC 61508 and will not affect the compliance of a process with the standard, and therefore no compliance check is required. Specification X in this example falls into this kind of situation. If found, agent Inspector will then map the immediate previous specifications defined in the Safety Lifecycle, i.e. the specification B and specification C, with the previous specifications in user design plan. If the mapping is successful, the ordering of the specification is correct corresponding to its previous specifications. In this example, both mapping mechanisms are successful and therefore specification D is placed in a right position in the plan.

It is noted that specification B and C are merged into a single specification BC in the user-defined process plan because only one document will be created for both specifications rather than two individual documents. Agent Ontologist is responsible for informing agent Inspector that specification BC in the user-defined process plan refers to the specifications B and C in the Safety Lifecycle.

The second service, the completeness check, provided by Inspector is used to ensure that all specifications defined in the Safety Lifecycle have been included in a particular user-defined process plan. Inspector will then map all the specifications in the Safety Lifecycle with the specifications in the user-defined process plan. If all specifications can be mapped, then the verification is successful. This implies that the objectives and requirements of every clause of the standard have been covered in the user-defined process plan. Otherwise, Inspector will present the missing specifications visually on its interface.

Finally, through cross-referencing function, Inspector can identify the location of a particular specification of a user-defined process plan in Safety Lifecycle proposed by IEC 61508, and present it visually. This service enables a friendly interface of the system, in which users can be aware of the progress of their ongoing works corresponding to the Safety Lifecycle.

Correctness check ensures that all the specifications in the user-defined process plan is devised in the right sequence. Completeness check ensures that all required specifications are presented in the user-defined process plan. Therefore, both correctness and completeness check are complementary to each other in ensuring that a user-defined process plan is planned in accordance with the standard.

With regard to task planning, Inspector is designed as a consultant that provides services passively: Inspector works in the background where it will not actively point out the incompliance errors until users request for the services. This is because planning normally starts from nothing and gradually evolves to a completed plan. It is assumed that the incompliance errors will always exist until the plan is completed. Thus actively prompting errors are impractical, rather, a user driven control that allows users to perform compliance check at will, through several ways and means, is a more flexible approach in ensuring a standard compliance plan.

Error Prevention

On the other hand, with regards to task execution, Inspector provides an active control to ensure that tasks are performed in accordance with IEC 61508. A distinct feature of Compliance Flow is that it supports interleaving between task planning and task execution, which enables parts of the plans to be specified while the overall process is in progress. Thus, some tasks may fall into execution while the overall design plan is still in progress and does not comply with the standard at that moment.

For example, the tasks towards the attainment of the Safety Integrity Level (SIL) of the product being developed are normally performed prior to the outlining of the details of hardware requirements. If there is any further design process, for each of which the requirements according to the IEC 61508 should correspond to SIL, have been defined in safety plan, then their executions will be forbidden by Inspector under any situation until the required SIL is achieved.

Recommendation Check

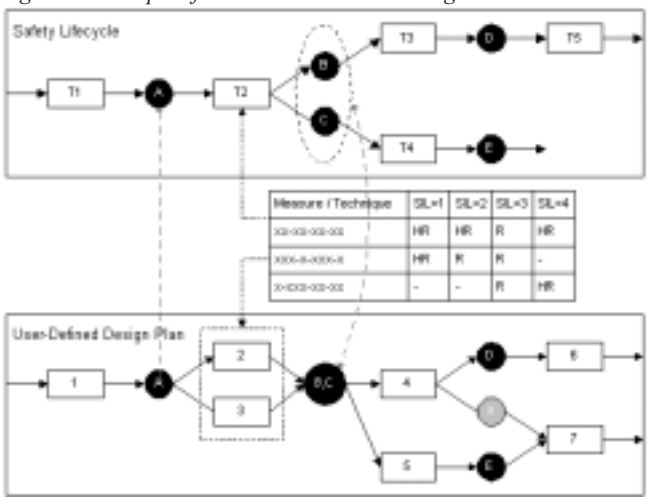
IEC 61508 recommends sets of techniques or measures for E/E/PE safety related systems for the control of failures. These techniques are grouped and graded for each System Integrity Level (SIL), in which if the highly recommended (HR) techniques or measures are not used then the rationale behind its non-usage should be detailed. These recommendations are modelled using Standard Modelling Language (SML) and are used in the recommendation check process.

During process build-time, as a user completes the planning of a particular task, agent Inspector will map the task's pre and post conditions which indicates sets of specifications with the specifications in the model of standard. Success mapping implies that the recommendations modelled for the task in the model of standard should be applied to the task in the user-defined process plan. Inspector will then ask the user to select the HR techniques in the recommendation as additional pre-conditions of the task. If the user does not adopt the recommended techniques or they choose alternatives with lower level of recommendation, an explanation is required where it will be recorded in the Tracking Server. An example of recommendation handling is given in Figure 4.

In Figure 4, a set of recommendations is associated with task T2. While the user completes the planning of task 2 and 3, and the post-condition BC is defined, Inspector will map the pre and post conditions of the task with the one in the model of standard. If found, and if the SIL of the product being developed is identified, the user will then be requested to assign the HR techniques corresponding to the SIL to be the pre-condition of the tasks. If users chose an alternative

Copyright Idea Group Inc.

Figure 4: Example of recommendation handling



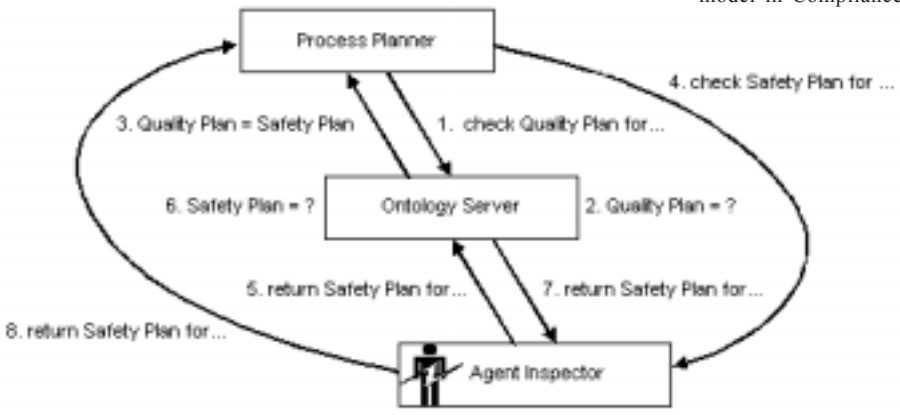
method, then an explanation have to be given and it will be recorded in the Tracking Server.

Communication

IEC 61508 allows different safety lifecycles to be used in a project without losing the compliance with the standard. This leads to a mapping difficulty as the terms used by users in describing the tasks in the user-defined process plan may differ from the one used in IEC 61508. The terms used in the standard cannot be enforced upon the users in describing their tasks because an objective or a requirement can generally be achieved through a number of methods. This explains why all the mapping mechanisms are only performed between tasks' requirements but not the tasks themselves. The terms used in system must be united in order to facilitate the compliance check operations. To do so, a compromise in using the terms among the users, Inspector and other components in Compliance Flow is vital.

We take the advantage of ontology to enable the communication among the system's components and its stakeholders. Ontology is defined by Uschold & Gruniger [3] as a "… shared understanding of some domain of interest …". Recent researches, such as [17], proved that the use of ontology can significantly improve communication and maintain the inconsistency in workflow management. Figure 5 illustrates the use of an Ontology Server as a translator to enable the communication between Inspector and a system component called Process Planner. The term "Quality Plan" (given by user) that is used by Process Planner is translated into the term "Safety Plan" (used in IEC 61508) that is used by the Inspector through the Ontology Server.

Figure 5: Ontology server as a translator



DISCUSSION

Development processes in engineering design may vary with each other due to uncertainties. Performing mapping between the user-defined process plan and the one proposed by the standard is the most flexible way to tackle the compliance problem. The degree of compliance relies greatly on the level of details the information of the model of standard can provide and the algorithm of mapping.

Occasionally more than one industry standards may get involved in an engineering project. To deal with this situation, there are two approaches: (1) employ a number of compliance agents for each of which is responsible for handling one standard, or (2) employ only one compliance agent who is capable of handling more than one standard. The difference between these two approaches is the degree of coupling between the compliance agent and the model of standard.

The first approach has close coupling where every standard may be modelled in a different way and mapping algorithms for each standard would therefore vary. This approach may describe each standard more precisely since differences exist among standards so that the higher degree of compliance can be provided. However, the system applicability is impaired as users cannot perform modelling by themselves and programming work has to be involved when the standard is updated or new standard is required.

Our research is tended to the second approach where a generic standard modelling language is developed with the capability of modelling a wide range of standards together with a comprehensive mapping of algorithm to ensure a standard complied process plan. Users are required to model a new standard only when necessary, and are allowed to amend existing model of standards to the one used in their organisation in order to achieve the necessary precision of compliance assurance, and consequently extend the applicability and flexibility of the system.

CONCLUSION

In this paper we have introduced standard compliance as an issue of importance in engineering process and have developed a standard modelling language that is capable of capturing main elements of standards for the sake of compliance checks. We have presented the Inspector, an intelligent compliance agent, and explained the compliance check mechanism together with the use of ontology to enable the communication among different stockholders. We argue that an environment that allows users to be able to plan tasks without restriction is vital while compliance check is taking place, and we have made it possible.

Unlike other researches, we believe that WfMS provides the most suitable environment for supporting standard complied project. We are advocates of taking advantage of software agent technology to bridge the gap where current workflow models provide no support for process consistency against any standards. Our approach is lightweight, in the sense that it requires relatively simple augmentation of workflow products. Currently the Inspector can only work with the workflow model in Compliance Flow that provides extra flexibilities for supporting dynamic engineering process. We expect that the compliance agent can eventually work with other workflow model through the use of standard interfaces [15] proposed by Workflow Management Coalition (WfMC).

REFERENCE

1. Alonso G, Agrawal D, El Abbadi A, & Mohan C, Functionality and Limitations of Current Workflow Management Systems, IEEE Expert, 12(5), 1997.
2. Sheth A., 1997. From Contemporary Workflow Process Automation to Adaptive and Dynamic Work Activity Coordination and Collaboration. Workshop on Workflows

Copyright Idea Group Inc.

in Scientific and Engineering Applications, France, September 1997.
3. Uschold M., Gruninger M.: "Ontologies: Principles, Methods and Applications", The Knowledge Engineering Review, Vol. 11, No. 2, 1996, pp. 93-136.
4. Stader J, Moore J, Chung P, McBriar I, Ravinranathan M, Macintosh A. 2000: "Applying Intelligent Workflow Management in the Chemicals Industries"; In The Workflow Handbook 2001, L. Fisher (ed), Published in association with the Workflow Management Coalition (WfMC), Oct 2000, pp 161-181, ISBN 0-9703509-0-2.
5. Dellen B, Maurer F, & Pews G, Knowledge-Based Techniques to Increase the Flexibility of Workflow Management, Data and Knowledge Engineering, North Holland, 1997.
6. Stader J, Results of the Enterprise Project, Proceedings of the 16th International Conference of the British Computer Society Specialist Group on Expert Systems, Cambridge, UK, 1996.
7. Myers K., Berry P.: "Workflow Management Systems: An AI Perspective", Technical Report, AIC, SRI International, USA, 1999.
8. Jarvis P, Moore J, Stader J, Macintosh A, Casson-du Mont A, and Chung P. 1999: "Exploiting AI Technologies to Realise Adaptive Workflow Systems"; In Proceedings of the Workshop on Agent Base Systems in the Business Context held during AAAI-99.
9. Moore J, Inder R, Chung P, Macintosh A, and Stader J: "Combining and Adapting Process Patterns for Flexible Workflow". DEXA 2000 DomE: International Workshop on Enterprise and Domain Engineering, to be held in conjuction with DEXA 2000: 11th International Conference on Database and Expert Systems Applications, London, Greenwich, 4-8 September 2000.
10. Emmerich W, Finkelstein A, Montangero C, Antonelli S, Armitage S, Stevens R.: "Managing Standards Compliance". IEEE Trans. Software Engineering, 25 (6), 1999.
11. Emmerich W, Finkelstein A., Montangero C & Stevens R.: "Standards Compliant Software Development". In Proc. International Conference on Software Engineering Workshop on Living with Inconsistency, (IEEE CS Press), 1997
12. Easterbrook S, Finkelstein A, Kramer J and Nuseibeh B.: "Coordinating Distributed ViewPoints: the Anatomy of a Consistency Check". International Journal on Concurrent Engineering: Research and Applications, 2,3, 209-222, 1994.
13. Finkelstein A, Gabbay D, Hunter A, Kramer J, & Nuseibeh B.: "Inconsistency Handling In Multi-Perspective Specifications". IEEE Transactions on Software Engineering, 20, 8, pp. 569-578.
14. Finkelstein A, Spanoudakis G, Till D.: "Managing interference". In Finkelstein and Spanoudakis [22], pages 172—174.
15. WfMC: "Workflow Reference Model Version 1.1", 1995. [Available From] http://www.wfmc.org/standards/docs/tc003v11.pdf.
16. Draft Standard IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 to 7, December 1997.
17. Moore J, Stader J, Chung P, Jarvis P and Macintosh A.: "Ontologys to Support The Management of New Product Development in The Chemical Process Industries". International conference on engineering design ICED 99 Munich August 24-26, 1999
18. Cheung L, Chung P and Ray D: "Supporting Engineering Design Process with Compliance Flow – An Intelligent Workflow Management System". Engineering Design Conference 2002 King's College London July 2002.

Copyright Idea Group Inc.
Copyright Idea Group Inc.
Copyright Idea Group Inc.
Copyright Idea Group Inc.

0 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/proceeding-paper/managing-process-compliance-standards/31734

Related Content

Analysis of Click Stream Patterns using Soft Biclustering Approaches
P. K. Nizar Banuand H. Inbarani (2011). *International Journal of Information Technologies and Systems Approach (pp. 53-66).*
www.irma-international.org/article/analysis-click-stream-patterns-using/51368

Co-Construction and Field Creation: Website Development as both an Instrument and Relationship in Action Research
Maximilian Forte (2004). *Readings in Virtual Research Ethics: Issues and Controversies (pp. 219-245).*
www.irma-international.org/chapter/construction-field-creation/28301

Synopsis Data Structures for XML Databases
Alfredo Cuzzocrea (2015). *Encyclopedia of Information Science and Technology, Third Edition (pp. 1906-1913).*
www.irma-international.org/chapter/synopsis-data-structures-for-xml-databases/112595

Research on Big Data-Driven Urban Traffic Flow Prediction Based on Deep Learning
Xiaoan Qin (2023). *International Journal of Information Technologies and Systems Approach (pp. 1-20).*
www.irma-international.org/article/research-on-big-data-driven-urban-traffic-flow-prediction-based-on-deep-learning/323455

Digital Future(s)
Lech W. Zacher (2015). *Encyclopedia of Information Science and Technology, Third Edition (pp. 3735-3744).*
www.irma-international.org/chapter/digital-futures/112810