Albeanu Grigore,

Averian Alexandru,

Duda Iordan
Spiru Haret University, Bucharest, Romania

Towards web applications reliability engineering

Keywords

web application, software reliability, software vulnerability, software security

Abstract

There is an increasing request for web-based software systems, some of them to be used very intensive. The customers ask not only for fast design and implementation, but also for a high quality product. Considering reliability as an important quality attribute, this paper describes the current state of the art in designing, implementing, and testing web-based applications. An important attention is given to web-based software vulnerabilities and how to deliver secure software. Then, reliability modeling in the case of secure web-based software is discussed.

1. Introduction

Recently, a special class of distributed software was born, and is used intensively by people working on their terminals, situated in office or at home. The object talking about is called *web application*, which "is a collection of servlets, html pages, classes, and other resources that can be bundled and run on multiple containers from multiple vendors", according to [4]. However, the term is used generic for web sites (web servers), and every software application using Internet environment.

According to Pickering [16], "in most server architectures, the failure of any one system or service in the path between server and user will in effect cause failure of the entire application as far as the user is concerned". The term *failure* is used according to [18], i.e. "the event of a system deviating from its specified behaviour". Another important aspect deals with security aspects [1]. Even the security is managed separately; before the security hole is patched any failures of the application will have great impact on the application reliability. This makes difficult the usage of the standard software reliability growth models for insecure systems. When speaking about web-servers, we have to take into account many technologies (hardware and software), each one having its own failure modes and sources of delay and unreliability, as proved in [16].

The reliability of the web-based applications can be considered as special case of distributed software running on distributed computer systems [18], over different kind of networks (local area networks, wide area networks etc.). If the nodes of the network are assumed to be perfect and the connections among nodes are assumed to fail in a statistically independent manner, then the network reliability can be computed as in [21]. However, if the nodes are imperfect, then the usage of the algorithm provided by Lin et al. in [12] is an efficient solution.

The aim of this paper is to describe the relevant aspects of web-based software coding, testing and reliability analysis and to outline some best practices when thinking in terms of web-based software reliability engineering.

The above ideas motivate us to organize the paper as follows. The second section considers the web-based software design for reliability, and covers the state of the art in implementing and testing web applications. The management of the software vulnerabilities is described in the third section. For a secure web-server, aspects concerning the reliability growth modeling are considering in the fourth section. Finally, a case study is discussed, and concluding remarks are formulated.

2. Web-based software engineering

As a general rule, the web-based software is built in order to provide some functionality using different web services protocols and frameworks oriented to a specific application [3]. For instance, *E-business XML* (or ebXML) is a useful protocol when processing electronic business information over various platforms. Also, *ApacheAxis2* is a framework supporting many protocols, including SOAP *(Single Object Access Protocol)* for exchanging information in a decentralized distributed environment. We refer to SOAP, because "web services usually use SOAP over HTTP" as mentioned by [15].

Some years ago, speaking about the future of software reliability engineering, Lyu said [14]: "the traditional solution that software designers adopted – carefully elicit change requests, prioritize them, specify them, design changes, implement and test, then redeploy the software – is no longer viable." Nowadays, agile methodologies based on software components, including open source, are used to deal with rapidly software releasing, increasing reliability and diminishing the software costs.

According to Wasserman, "the most heavily used websites are characterized by high reliability, high availability, high security, and rapid interactive response". The discussion, in [26], is oriented to the following design principles: abstraction, modularity, multi layer architecture, and logging for analyzing and testing. It is important to notice that these principles are independent on the web services provided by the web application.

The *abstraction* is used in all web-application life cycle [19], [26]: requirements' specification (use case diagrams, scenarios, work flow models, conceptual data models etc.), project design (by objects: images/audio/video, menus, buttons, text fields etc.), coding (based on templates), testing (failure trees, root cause analysis, etc.).

Modularity promotes the component-based paradigm and the reuse principle, a smart usage of reusable components for constructing quality software by reducing the verification costs, increasing the software reliability, and reducing the development time [1].

Recently, the application software follows a *multi-layer architecture*, being developed similar as some parts of the operating systems. Three-tier architecture is based on the following entities: client, server, and database. As Wasserman said in [26], web applications have "well-known and widely followed *n-tier* site architecture" based on pattern design (configuration modes described using XML or other pattern languages), plug-ins (assuring an extensible architecture), with a modular structure using a specific user interface (based on languages and technologies like HTML, Flash, Javascript, etc.).

For analyzing and testing web applications, there are available a large collection of tools (components), ready to be embedded into the web application, or activated in order to monitor different aspects related to the website activity. These tools generate log files useful for "studying system performance, identifying errors, and determining general patterns of use", as mentioned in [26].

Web services are offered by different web servers for specific activities. This is why Chu & Qian, in [3], said: "e-business application development has certain characteristics that make it different from traditional software development". This observation is also valid for other fields asking for high security assurance.

According to [3], the following requirements should be taken into account for specific web applications, like those from e-business field: *service composition* (developed based on a complete system model), *formal semantics* (in order to use automated tools for service design and verification), *and systematic service design methodology* (for supporting service reuse). In this way, service reuse at different levels of granularity is also provided.

Zaupa et al. [25], using the product line concept, proposed a web application development strategy oriented on services. In this manner, there are three stages to be followed during the development process: 1) Application domain definition; 2) Services development, and 3) Application generation.

The set of requirements has to be stable when classical software development methodologies will be used [19]. However, in an agile framework, the requirements of a web application could be easy updated during the starting period of any iteration (when applying an iterative prototyping approach). The above three stages can be iterated when an agile methodology is used and will consider the requirements obtained in one of the following methods: classical, using UML notation, navigation-based templates, hypermedia modeling based on object thinking, and other ad-hoc, but documented models.

In order to decrease the number of faults (local or sub-network faults), the software team have to be experienced with existing vulnerabilities and security improvement mechanisms. Such aspects will be detailed in the next section.

Another important aspect of web applications deals with *interoperability*. Many web applications accept as input and produce as output different objects. In

order to be used/viewed/printed/listen, the object format will be a known one, and secure plug-in components will be available for clients. Here, we think about a web application in a multi server – multi client architecture. The multi server architecture is required for increasing reliability and availability by sharing connections (in a round-robin fashion and/or by load balancing). This is also the case of all software intensive systems where the *availability* is an important quality attribute [16], [20].
Web application *robustness* is another quality requirement: "the property of a system or a component that is totally correct in respect to a complete specification, thus its behavior is predictable for all possible operational environments", as defined in [2]. In order to obtain a robust web application, software engineering plays an important role. The analysis of robustness can proceed according to some methods, like those discussed in [2], but for critical applications like e-business or e-campus total management, the operational environment, including the security profile will be simulated in order to test all specified requirements.

3. Software vulnerabilities

If omitting the failures generated by cyber attacks, we refer to the intrinsic reliability. In large, the software reliability covers also aspects related with security holes that permit to attackers the crashing of the web application. These security holes are generated by software vulnerabilities as defined in the following. Software vulnerability deals with insecure programming and the possible insertion, by mistake, of the following classes of bugs [1]:

- memory-management (buffer/stack overflow, format string vulnerability, boundary condition checking);
- concurrency-management (e.g. race condition involving a security check);
- I/O-management (e.g. input validation mistake, SQL injection, incomplete application protocol validation and verification);
- inconsistent integration of security technologies (e.g. configuration errors, environmental errors, incomplete access control procedures);
- numerical inconsistencies (e.g. integer overflow, division by zero, XOR based encryption);
- vulnerable entry points (command-line parameters, the environment array of strings, default input files, default passwords, inherited file data structures, inherited attributes when working with extended classes, incorrect specification of web graph nodes).

There are possible mistakes not only during design, but also during testing and implementation phases. Environmental and administrative mistakes are common when speaking about web-servers.
The vulnerabilities are possible to be identified: (1) manually (by experts), (2) automated (by bottom up and/or top down testing) (3) by black box testing, (4) by white-box analysis, (5) using scanners, and (6) combined various methods. The software trustability will be increased by testing using environment perturbation (taken different actions on files, other processes, network etc.).
According to [11], when coordinated security attacks are identified, "additional protection mechanisms such as closing connections over a wide area together with longer term measures such as changing cryptographic keys" are required for such faults. Non-local fault tolerance can be implemented using a specialized cryptographic protocol implemented on a cluster of servers.
If the development is based on the component-based approach, and inadequately secure components are embedded, the wrapping technique will be used for the components accommodation. Such an approach was described early in [18]: "design means of masking or of detecting and recovering from, the security errors which might arise", and used also for the projected presented in [1].
In order to minimize the security type vulnerabilities, the prevention of the cyber attacks is the best strategy and may use the following technologies [15]: security tokens, digital signatures, encryption, and other security tools according to the security management procedure. Taking into account the above classes of bugs and the mentioned security technologies, the following types of web application attacks will be rejected: imposture (impersonation), repudiation (refusing acknowledgment), information disclosure (without permission), information altering, denial of services, gaining the privilege of administrators or owner applications.
According to Guo & Sampath [8], the following classes should be taken into consideration: *data storage class* covering all possible faults related to data structures, *logic faults* generated during implementing algorithms and the application control flow (some of them being related to session/paging faults, inconsistent browser interaction parsing faults, mistakes in coding encoding/decoding and encryption/decryption algorithms), *data input faults* generated by input validation mistakes related to files and forms,

appearance faults generated by inappropriate coding for controlling the display of the web-pages, and *linking faults* due to mistakes in controlling the transfer to different locations in the World Wide Web (URL – Uniform Resource Locator). The last class is reach for the case of web applications working with URL data bases. Comparing the two classifications mentioned above we found that [1] is enough rich containing also cookies' manipulation, communication encryption, user authentication, account management, and accessing/using resources without permission.

During a web application a model that accurately describes the vulnerabilities is required. As mentioned by [1], "the most used vulnerability models use VCG (Vulnerability Cause graphs), C/DFG (Control/Data Flow Graphs), and decision trees". For the web application investigated the VCG approach was used which is similar to root cause analysis method. Other methods uses FMEA and soft computing techniques as those described in [2].

A global analysis considers both hardware and software fault categories when studying the web application reliability [13], [14], [17]. A separate analysis can be developed in the case of software faults only.

In the next section, the SMERFS [7] software was used to analysis the inter-failure data collected for a web application implementing a virtual campus.

4. Web-based software reliability

4.1. Network reliability and performability

As Pickering identified in [16], an important factor influencing the web-server reliability is the network reliability and availability. As measures of availability the most important are the connectivity and the performability. When a failure occurs, the network could not be able to perform at the same parameters as when working without failure. In this way, there is a strong relation between the network failure performability and the network reliability.

Various services are provided over multiple interconnected networks with different technologies and infrastructure by different suppliers (providers). Modelling the network as an undirected simple graph, the network reliability is studied, to assure, at least theoretically, a solution to the following problems: (1) Compute the probability that there is a path between two distinguished vertices *a*, and *b* [terminal connectivity]; (2) Compute the probability that all vertices remain connected. It is clear that both combinatorial and statistical methods are mixed in order to compute the network reliability. Analyzing network reliability is more important for the case of content replications motivated by requests for decreasing the answer time to a large number of simultaneously queries.

Considering the most used types of distributed web-servers (DWS) the following architectures are possible: *cluster based* (with virtual IP address depending on the web service visible to the clients, and a real IP address of the cluster nodes (CN), but hidden to clients), *virtual cluster* (the nodes sharing the same IP, and only one node will keep a message from clients), and distributed cluster (every node having its IP, and the message being redirected by a dynamic procedure applied related to the Domain Name System). The redistribution is implemented in a switching (SW) system.

The web based system reliability can be computed as in the case of serial systems: R(DWS) = R(SW) x R(CN). It is clear that R(CN) depends on the cluster topology, but experimentally we found that the estimation of R(CN) depends also on the method of content mirroring, the best results being obtained for complete replication.

Suppose G represents the network of cluster nodes that can perform if and only if it is connected, and G_r a random subgraph of G. If every edge *e* of G has associated a failure probability p_e, then the probability that G_r remains connected is the same as G still perform. The network reliability computation can be realized using the classical results presented in [21] and [22].

The web applications are composed by a large number of software components, many of them used in a reusable manner. The most used protocol for inter-component communication is the client-server mechanism. In this case, a component-dependency graph is built, and the component reliability is estimated (for white-box components) or approximated (in the case of black-box components) based on its average execution time, using the methodology described by Hu [10]. Based on the architecture style (sequencing, looping, concurrency supporting, fault-tolerant style, refinement, or a mixed style), and taking into account the transition probabilities among the components (estimated during a benchmarking period) the overall system reliability can be computed [5], [23], [24].

For the virtual campus project was found that tree based architecture provides a high degree of reliability, and the computing of architecture reliability was fast using the MFST method [12]. For a cluster having five nodes the best performance was obtained in a partition of type (2, 3), being also a strong fault-tolerant architecture. Actually, the web application is distributed using an architecture of type (1, 1), the availability of service being 99%.

4.2. Web application testing

It is a general assumption that fault removal is successful in the case of many software reliability growth models, as already Littlewood & Strigini remarked in [13]. For web applications, only faults generating security holes are successfully removed (it is imperative necessary).

When speak about web application testing, there are two interpretations. The first one is related to software validation by [5], [6], [8], [23]:

- *establishing the level of usability* (offering an easier navigation; conformity with standards related to content organization, and the visibility of the navigation graph);
- *checking for browser/platform compatibility* (for assuring also the portability at operating system level, and provide wide access to the web site, including by mobile technologies);
- *assuring functionalities* (the content of pages inclusive the scripts is syntactically correct and free of bugs, and all links are active; all inputs are validated, cookies are checked for correctness and security; if a database is maintained then testing all aspects related to storage, code, protocols is required);
- *communication interface testing* (checking the network/cluster connectiveness and the correctness of data transportation, including encryption protocols and acknowledgement mechanism);
- *load testing* (in order to establish the level of performance under *stress testing*).
- *vulnerability scanning for security assessment* (as mentioned above and detailed by [1]);

The second one addresses the *unit testing* (by assertions on some regions of code – for assuring fault prevention) and the *debugging process* connected to failures, mainly by load testing (under heavy exposure). This kind of testing is useful to estimate the software reliability, and a journal of failures (type, level of severity, etc.), bugs (identifier, type, location, if possible to generate security holes, …), as a time series database useful to establish both inter-failure time and cumulative numbers of failures in order to support fault/failure forecasting, will be recorded.

Even already established a user profile, the web application is, in general, open to many users. This is why we decompose the user profile in a *public profile* and a *private profile*. It is compulsory to release a bug-free web application according to the public profile, even the testing was stopped for the private profile because of some schedule constraints.

When working with components, and for some of them creating some wrappers, a regression testing is required. In general, web applications are developed in an agile methodology (mainly extreme programming, or adaptive software development), and an agile testing approach is selected. In this case, the analysis of collected data is organized in batches, every batch corresponding to software life cycle iteration.

Table 1. Time between failure data along three builds

Build #	#Failure	Time between failure data [days]
1	19	1, 2, 1, 3, 5, 1, 2, 4, 8, 6, 11, 17, 19, 35, 22, 52, 28, 62, 74
2	18	1, 1, 1, 2, 1, 3, 2, 4, 3, 14, 18, 11, 33, 24, 53, 71, 59, 72
3	16	1, 1, 1, 1, 2, 2, 5, 13, 12, 10, 21, 28, 38, 58, 74, 57

4.3. Web application reliability

In the following the web application reliability is analyzed using standard software reliability models [17], as those provided by SMERFS [7]. The web application implementing the university virtual campus was developed during three versions/builds. For all versions, the time series corresponding to test debugging were collected (see *Table 1*), and analyzed using SMERFS.

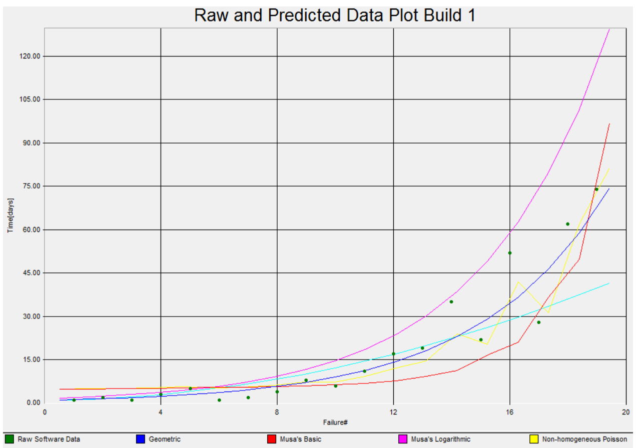

Figure 1. SRGM analysis / Build 1

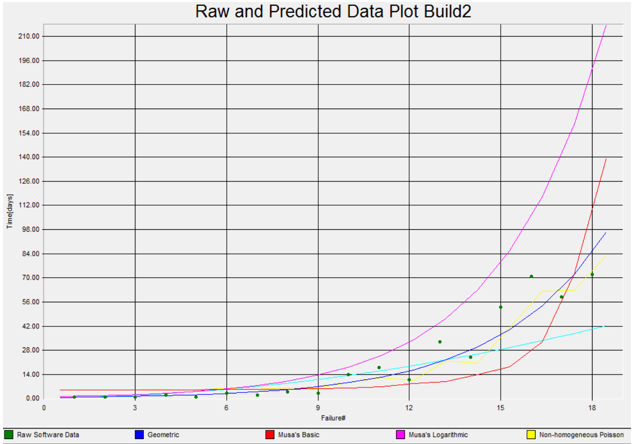

Figure 2. SRGM analysis / Build 2

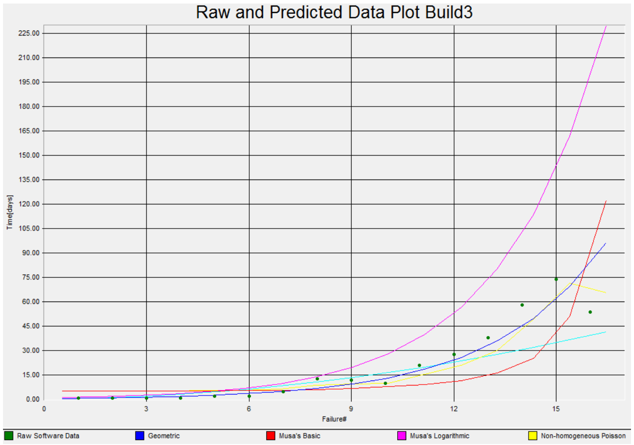

Figure 3. SRGM analysis / Build 3

Table 2. Successfully applicability results

Build #	Statistics	Model 1	Model 2	Model 3	Model 4	Model 5
1	Accuracy	42.98	44.07	48.82	43.94	48.82
	Bias	0.43	0.59	0.23	0.46	0.23
	Noise	2.79	1.97	0.00	2.46	0.00
	Trend	0.19	0.10	0.35	0.14	0.35
2	Accuracy	41.93	44.15	51.68	42.28	0
	Bias	0.5	0.64	0.36	0.51	0
	Noise	4.08	2.64	0.00	3.23	0
	Trend	0.3	0.18	0.56	0.21	0
3	Accuracy	35.46	36.89	43.92	36.53	43.92
	Bias	0.39	0.63	0.55	0.46	0.55
	Noise	2.78	1.91	0.00	2.64	0.00
	Trend	0.18	0.15	0.25	0.17	0.25

During analysis, five models were selected, namely: Model 1 - Moranda's geometric model (assuming that the software is never error-free and as debugging progresses the faults become harder to detect, with the detection rate forming a geometric progression and being constant between error occurrences), Model 2 – Quadratic Littlewood-Verall, Model 3 – Musa's basic, Model 4 – Musa's logarithmic, and Model 5 – Nonhomogeneous Poisson Process model (for execution time).

For every model the statistics concerning accuracy, bias, noise, and trend are presented in *Table 2*. These statistics follow the mathematical formulas described in the SMERFS manual and its references, and there are not described here. The results were obtained using the *Maximum Likelihood Estimation* method [14], [17]. In the *Table 3*, there are the most important estimates obtained during models' execution: IIF – Initial Intensity Function, CIF – Current Intensity Function, PrfLvl – the "Purity" Level (the ratio of the changing in the hazard rate function from the starting point to the ending and the initial value), MTBNF – Current Mean Time Between Next Failure, and KS – the measure for Goodness-of-fit calculation. Using the Goodness-of-fit measure we obtain three well-suited models for data fitting: Quadratic Littlewood-Verall, Musa's Basic, and the Nonhomogeneous Poisson Process model. These can also be identified in the pictures giving the raw and predicted data for the third builds of the project (*Figures 1-3*). It can be observed that Musa's logarithmic model is most pessimistic, while the best prediction is obtained using the fifth model, for short intervals of time.

Table 3. Successfully estimates

Build #	Estimates	Model 1	Model 2	Model 3	Model 4	Model 5
1	IIF	1.175	1.170	0.210	0.772	0.210
	CIF	0.012	0.020	0.005	0.013	0.005
	PrfLvl	0.989	n/a	0.978	1.000	0.978
	MTBNF	93.9	45.9	215.0	406.9	n/a
	KS	0.336 (no)	0.285 (yes)	0.167 (yes)	0.311 (no)	0.167 (yes)
2	IIF	2.00	1.886	0.203	1.189	0.203
	CIF	0.009	0.019	0.003	0.010	0.003
	PrfLvl	0.995	n/a	0.984	1.000	0.984
	MTBNF	129.2	47.1	310.3	734.5	n/a
	KS	0.35 (no)	0.23 (yes)	0.174 (yes)	0.38 (no)	0.174 (yes)
3	IIF	2.002	2.011	0.194	1.180	0.194
	CIF	0.009	0.019	0.004	0.010	0.004
	PrfLvl	0.995	n/a	0.978	1.000	0.978
	MTBNF	134.2	47.1	233.0	779.3	n/a
	KS	0.415 (no)	0.272 (yes)	0.172 (yes)	0.413 (no)	0.172 (yes)

A multicriteria analysis, based on direct analysis of the performance matrix, was conducted in order to establish the best model for the project in order to understand its reliability evolution.

Table 4. The model ranking

Build #	Statistics	Model 1	Model 2	Model 3	Model 4	Model 5
1	Accuracy	1	3	4	2	4
	Bias	3	5	1	4	1
	Noise	3	1	0	2	0
	Trend	3	1	4	2	4
	Overall	1	1	4	1	4

2	Accuracy	1	3	4	2	0
	Bias	2	4	1	3	0
	Noise	3	1	0	2	0
	Trend	3	1	4	2	0
	Overall	1	1	4	1	0
3	Accuracy	1	3	4	2	4
	Bias	1	5	3	2	3
	Noise	3	1	0	2	0
	Trend	3	1	4	2	4
	Overall	1	3	4	1	4

Even Model1 and Model4 were appreciated by SMERFS with rank 1 (*Table 4*), the Model3 proved an appropriate behavior when its predictions were compared with the real evolution of the project under study. Combinations of models [9] are also possible, when they are shared basic common assumptions.

5. Concluding remarks

This paper considers a special case of distribute software, namely the web applications, which ask not only for basic quality characteristics of software, but also have to be vulnerabilities-free, that means be able to prevent, detect and recover a good state after a possible cyber attack.
Starting with the development of a virtual campus for a large size university the software team had to solve important problems related to web application software engineering, time releasing constraints and to provide a high quality product. The most part of practical aspects useful for finalizing such a project were covered and outlined above.
Finally, we appreciate that a guide of best practices for web application software reliability engineering is necessary to be developed in short time to be available for students in software engineering, practitioners, and customers.

Acknowledgement.

The present investigation has been realized according to the research program of the Faculty of Mathematics-Informatics at *Spiru Haret* University, Romania.

References

[1] Albeanu, G., Madsen, H. & Averian, A. (2009). On the influence of software vulnerabilities on software reliability: The case of open source component based software (*submitted* to ESREL'09 Conference).
[2] Calori, I.C. & Stalhane, T. (2007). FMEA and BBN for robustness analysis in web-based applications, In Aven & Vinnem (eds). *Risk, Reliability and Societal Safety*, Taylor & Francis Group, London, 2341-2347.
[3] Chu, W. & Qian, D. (2009). Design Web Services: Towards Service Reuse at the Design Level. *Journal Of Computers*, 4, 3, 193-200.
[4] Davidson, J.D. & Coward, D. (1999). Java™ Servlet Specification, v2.2, Sun Microsystems.
[5] Davila-Nicanor, L. & Mejia-Alvarez, P. (2004). Reliability Improvement of Web-Based Software Applications. *Proceedings of the Fourth International Conference on Quality Software*, CINVESTAV-IPN, Zacatenco, Mexico, 180- 188.
[6] Eaton, C. & Memon, A. (2004). Evaluating Web Page Reliability across Varied Browsing Environments. *Proceedings of the 15th IEEE International Symposium on Software Reliability Engineering (ISSRE'04)*, France.
[7] Farr, W. (2003). http://www.slingcode.com/smerfs/compare.php
[8] Guo, Y. & Sampath, S. (2008). Web Application Fault Classification - An Exploratory Study. *Proceedings of ESEM'08*, October 9–10, 2008, Kaiserslautern, Germany, 3003-305, http://doi.acm.org/10.1145/1414004.1414060.
[9] Hsu, C.J. & Huang, C.Y. (2009). Reliability Analysis Using Weighted Combinational Models for Web-based Software. To appear in *Proceedings of the 18th International World Wide Web Conference (WWW 2009)*, April 20–24, 2009, Madrid, Spain, 1131-1132.
[10] Hu, H. (2007). Reliability Analysis for Component-based Software System in Open Distributed Environments. *International Journal of Computer Science and Network Security*, 7, 5, 193-202.
[11] Knight J.C. & Elder, M.C. (2001). Fault Tolerant Distributed Information Systems. *Proceedings of the 12th International Symposium on Software Reliability Engineering, IEEE*, 132-137.
[12] Lin, M.S., Chen, D.J. & Horng, M.S. (1999). The Reliability Analysis of Distributed Computing Systems with Imperfect Nodes. *The Computer Journal*, 42, 2, 129-141.
[13] Littlewood, B. & Strigini, L. (2000). Software Reliability and Dependability: a Roadmap. *Proceedings of the Conference on the Future of Software Engineering*, 175-188.
[14] Lyu, M.R. (2007). Software Reliability Engineering: A Roadmap. *Proceedings of FOSE*, 153-170.
[15] Maeda, T., Nomura, Y. & Hara, H. (2003). Security and Reliability for Web Services, *FUGITSU Sci. Tech. J.*, 39, 2, 214-223.
[16] Pickering, 3. (2005). *Web Server Reliability*, http://www.ipcortex.co.uk/wp/app-reliability3.pdf, Ipcortex.

[17] Pham, H. (2003). *Recent Studies in Software Reliability Engineering.* In Pham Hoang (ed.), Handbook of Reliability Engineering: 285-302, London: Springer.

[18] Randell, B. & Dobson, J.E. (1986). Reliability and Security Issues in Distributed Computing Systems. *IEEE Proceedings of the 5th Symposium on Reliability in Distributed Software and Database Systems*, Los Angeles, 113-118.

[19] Schneidewind N.F. (2003). Life Cycle Core Knowledge Requirements for Software Reliability Measurement, Reliability Review. *The R&M Engineering Journal*, 23, 2, 18-29.

[20] da Silva Filho, A. M. (2005). Toward More Available Software-Intensive Systems. *The Fifth International Requirements Engineering for High-Assurance Systems Workshop*, http://www.sei.cmu.edu/community/rhas-workshop/2005/silvafilho.pdf.

[21] Shier, R.D. (1991). Network Reliability and Algebraic Structures, Clarendon Press, Oxford.

[22] Shooman, M.L. (2002). Reliability of Fault-Tolerant Computing Systems and Networks. *The Journal of Reliability Analysis Center*, 4, 1-7 & 11-12.

[23] Suri, P.K. & Bharat, B. (2007). Reliability Evaluation of Web Based Software. *International Journal of Computer Science and Network Security*, 7, 9, 151-156.

[24] Tsai, W.T., Zhang, D., Chen, Y., Huang, H., Paul, R. & Liao, N. (2004). A Software Reliability Model For Web Services. *8th IASTED International Conference on Software Engineering and Applications*, Cambridge, MA, 144 - 149.

[25] Zaupa, F., Gimenes, I.M.S., Cowan, D., Alencar, P. & Lucena, C.J.P. (2008). A Service-oriented Process to Develop Web Applications. *Journal of Universal Computer Science*, 14, 8, 1368-1387.

[26] Wasserman, A.I. (2005). Principles for the Design of Web Applications. http://www.se-hci.org/bridging/interact2005/07_Wasserman.pdf