BUGS IN THE BRAVE NEW UNWIRED WORLD

A Failure mode catalog of risks and bugs in mobile applications

ABSTRACT

In the research reported in this paper, we present a failure mode catalog of wireless applications running on handheld devices. We populate the failure mode catalog with a broad range of actual and potential problems that can occur in mobile applications running on wireless networks. Entries made within the catalog include hypothetical failures (some published, some based on our own analyses), examples of real-life failures reported in the trade press, bug databases, magazine articles and other relevant sources, plus some causal analyses. These entries clarify the scope and meaning of failure categories. Testing is challenging in the handheld wireless world because it is new and some of the problems are new (or at least they show up in new ways). A failure mode catalog of the type we present here helps testers do risk-based testing. The risk-based tester creates a list of risks (ways the program could fail), assigns priorities to each, and performs tests that explore the risks of interest. We believe that a failure mode catalog designed to help testers generate test ideas will be particularly useful for an experienced tester who lacks domain expertise in this class of applications. It gives him ideas about how failures arise, or at least, what to test for, in this new breed of applications. The resulting set of the tests should be broader, targeted towards more risks, and probably often more powerful because they are designed to detect a plausible error. Additionally, even very experienced testers have blind spots -- bugs they haven't encountered or don't often think about. A broad taxonomy helps the tester recognize blind spots and get past them by using the list as an idea generator.

ABOUT THE AUTHORS

Ajay K. Jha, ajha@fit.edu is a Software Engineering graduate student at Florida Institute of Technology, specializing in software testing. He has almost three years of experience in testing and troubleshooting electro-mechanical, embedded, and general computer-based systems. His current interests include heuristic risk-based testing of mobile applications and exploring agile methods for testing and development of software.

Cem Kaner, J.D., Ph.D., kaner@kaner.com, www.kaner.com, is Professor of Computer Sciences at Florida Institute of Technology. He is senior author of *Testing Computer Software*, of *Lessons Learned in Software Testing*, and of *Bad Software: What To Do When Software Fails.*

MAILING ADDRESS

Florida Institute of Technology
Department of Computer Science
150 West University Blvd
Melbourne, FL – 32901

This research was partially supported by NSF Grant EIA-0113539 ITR/SY+PE: "Improving the Education of Software Testers." http://www.testingeducation.org. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation (NSF).

INTRODUCTION

Handheld devices are evolving and becoming complex with the addition of newer features and functionalities. One of the drivers of this change is the rapid proliferation of the IP-based wireless networks and the maturation of the cellular technology. In a recent issue of *Wired* magazine, Arthur C. Clarke suggested that it was high time to listen to the technology and change the name of the magazine from *Wired* to *Unwired.* Wireless and mobile applications are a natural extension to the current wired infrastructure. Traditional mobile applications like e-mail and PIM have been widely adopted in the enterprise and consumer arenas and wireless data services enabling B2B and B2C transactions are rapidly making inroads. In the consumer arena, Japan leads the world with adoption of 3G and introduction of a plethora of applications for the mobile users.

Testing is challenging in the handheld wireless world because some of the problems are new (or at least they show up in new ways). To facilitate risk-based testing in this area, we present and organize a broad set of failure modes (publicly reported or potential failures) associated with wireless applications running on handheld devices.

WHAT IS A MOBILE APPLICATION?

Definitions of *mobile application* vary. In this report a *mobile application* is any application that runs on a handheld device like a PDA, smart phone, tablet PC or similar device. Five different types of applications can be developed for handheld devices, applications that:

- Stand alone, running on the handheld device itself;
- Connect to the back-end through synchronization software;
- Work with a back-end through packet switched wireless connectivity;
- Work with the back-end through circuit switched wireless connectivity;
- Vertical, using special networks like SMR (Specialized Mobile Radio) or paging networks.

We are most interested in mobile applications that connect with the back-end using either circuit switched or IP based wireless connectivity. This includes applications used to provide access to databases or application servers, to enhance classroom interaction, or to provide computer capabilities on smart phones. As we see with communications-enabled PDAs and smart phones, computing and communication technologies are converging.

One challenge associated with testing mobile applications is the difficulty of reproducing the production environment. Most testing must be performed using simulators and emulators. Even if we can simulate some aspects of the application, the handset for example, we can't be sure what happens when we try it over a real wireless network. This results in many field failures.

Another challenge is that, as the technology emerges, the market (developers and customers) is still figuring out what makes mobile applications great or less-than-great. Quality criteria are in flux and will stay that way until the market matures. Despite the uncertainty, testers must look carefully at the application under test, asking whether this is as good a product as it should be. One of our goals in developing a broad failure mode catalog is to broaden the risk analysis that testers use to guide their testing. A catalog provides a wider range of examples (and categories of risk) than any one person is likely to think of while designing her or his tests.

FAILURE MODE AND EFFECTS ANALYSIS

Failure mode and effects analysis (FMEA) is a traditional hardware engineering technique. It is less often and less formally applied in software, but FMEA-like analyses are the foundation of risk-based testing.

We will briefly describe the FMEA discipline here, but focus the paper on failure modes for wireless mobile applications, setting aside the rest of the FMEA analysis.

A *failure mode* is, essentially, a way that the product can fail. A failure mode's *effect* is the probable result of that particular type of failure.

In failure mode and effects analysis (FMEA), the analyst identifies the failure modes of a system, component by component. S/he evaluates the likely effects of each type of failure and prioritizes work accordingly. For the higher priority failure modes, s/he determines what could cause the failure, how to test for the failure, and how to eliminate or reduce the chance of the failure.

For more information on FMEA in general (http://www.fmeca.com/ffmethod/methodol.htm) is a good summary. For ideas on applying the full FMEA discipline to software, see the discussions in (http://www.stuk.fi/julkaisut/tr/stuk-yto-tr190.pdf). There is no explicit standard for software FMEA (SWFMEA), but the standard IEC 60812 published in 1985 is often referenced when carrying out FMEA for software-based systems.

RISK BASED TESTING AND FMEA

Amland (1999) explains risk-based test management in his paper where testing is prioritized to concentrate on the areas to test next.

James Bach (1999) explains risk analysis for the purpose of finding software errors. The steps followed in his approach are:

- Make a prioritized list of risks;
- Perform tests to explore each risk;
- As risks evaporate and new ones emerge, adjust your test effort to stay focused on the current risk set.

A risk points you to a way (or ways) that the software could fail. The challenging part in building a prioritized risk list is figuring out all the ways the software could fail, i.e. the failure modes.

Over the past year, we've been using 25 to 50 broad categories to classify failures that can occur in wireless applications. Our current category list is in Figure 2. This is a continuously evolving list. I will publish the final version in my M.Sc. thesis. For each category, we provide examples of publicly reported failures (with links to the press reports) and potential failures (problems we expect to happen, and would want to look for as testers, but that haven't been discussed in public bug reports). The public and potential failures together make up a set of *failure modes* within a category.

One of our goals in developing a broad failure mode catalog has been to broaden the risk analysis that testers use to guide their testing. A well-structured catalog provides a wider range of examples (and categories of risk) than any one person is likely to think of while designing his or her tests. Another of our goals has been to provide training material, to help testers new to wireless mobile applications start from a pre-structured risk profile and so come up to speed more quickly.

TAXONOMIES

The American Heritage® Dictionary of the English Language: Fourth Edition 2000, defines a taxonomy to be:

> **"1.** The classification of organisms in an ordered system that indicates natural relationships.
>
> **"2.** Division into ordered groups or categories."

A taxonomy is an effective way of structuring and classifying information or data.

A few examples of well-known taxonomies are:

- The science of systematics, which classifies animals and plants into groups showing the relationship between each;
- Bloom's taxonomy (Bloom, 1956) of levels of knowledge, which educators use to develop teaching goals and assessments (such as exam questions);
- Beizer's (1990) taxonomy of software errors, which classifies bugs in terms of the lifecycle, phase in which they were introduced (design, implementation, etcetera)

For more examples of interest to software readers, see Vijayaraghavan (2003). As Vijayaraghavan pointed out, there are disputes over whether the structured risk lists (e.g. in security), structured bug lists, and many other structured lists can be called "taxonomies" if they do not provide orthogonal classifications. We're sidestepping that issue by calling our structured list a "catalog" instead of "taxonomy."

Kaner, Falk and Nguyen (1993) published a catalog of common software errors in their book's Appendix A. Some of our thinking about how testers can use a failure mode catalog came from experience with many readers' reports of their uses of this bug list.

Vijayaraghavan (2003) published a useful taxonomy of e-commerce failures.

Bach (2003b) points out that testers work more effectively with risk catalogs whose structure is immediately obvious to the reader. Testers especially benefit from clear structure when trying to decide what area(s) to focus on at a given point in a project.

We think that Bach's (2003a) *Heuristic Test Strategy Model* (Figure 1) provides a clear structure that we can fit failure modes into. Accordingly, we have reworked Vijayaraghavan's taxonomy into this structure and are extending it to mobile and handheld applications. We have adapted the model slightly by splitting Bach's qualitative failure categories into operational and developmental subcategories.

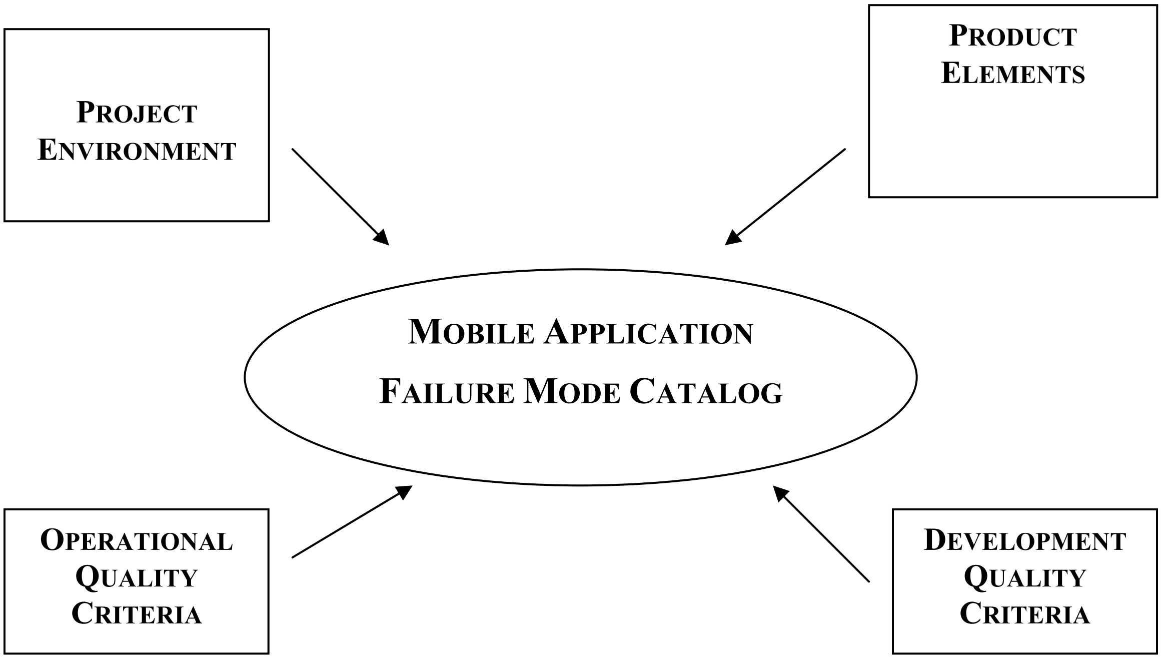

PROJECT ENVIRONMENT
PRODUCT ELEMENTS
MOBILE APPLICATION FAILURE MODE CATALOG
OPERATIONAL QUALITY CRITERIA
DEVELOPMENT QUALITY CRITERIA

Figure 1. Bach's Heuristic Test Strategy Model

HOW TO USE THE CATALOG

We provide a top-level outline of our catalog in Figure 2, and more detail in the Appendix.

A catalog like this is intended to help the tester generate a list of risks. No catalog can be a complete list of failure modes for every application, not even for every PDA-based wireless application. The idea is to provide a source of ideas that can inspire a risk-focused tester. The tester reads a description of a category of potential failures, reads some examples within the category, and asks herself:

- Could this application fail in some way that would fit in this category?
- Could it misbehave like any of this category's examples?
- What about other, similar ways?

Exploration by analogy generates the list the tester actually uses. Our list is merely, but usefully, a starting point.

We believe that a catalog designed to help testers generate test ideas will be particularly useful for an experienced tester who lacks domain expertise in this class of applications, because it suggests problems to test for in this new breed of application. The resulting set of tests should be broader, covering more risks, and may be more powerful because each is designed to detect a plausible error. Additionally, even very experienced testers have blind spots—bugs they haven't encountered or don't often think about. A broad taxonomy helps the tester recognize blind spots and get past them by using the list as an idea generator.

FIGURE 2: OVERVIEW OF THE MOBILE / HANDHELD FAILURE MODE CATALOG

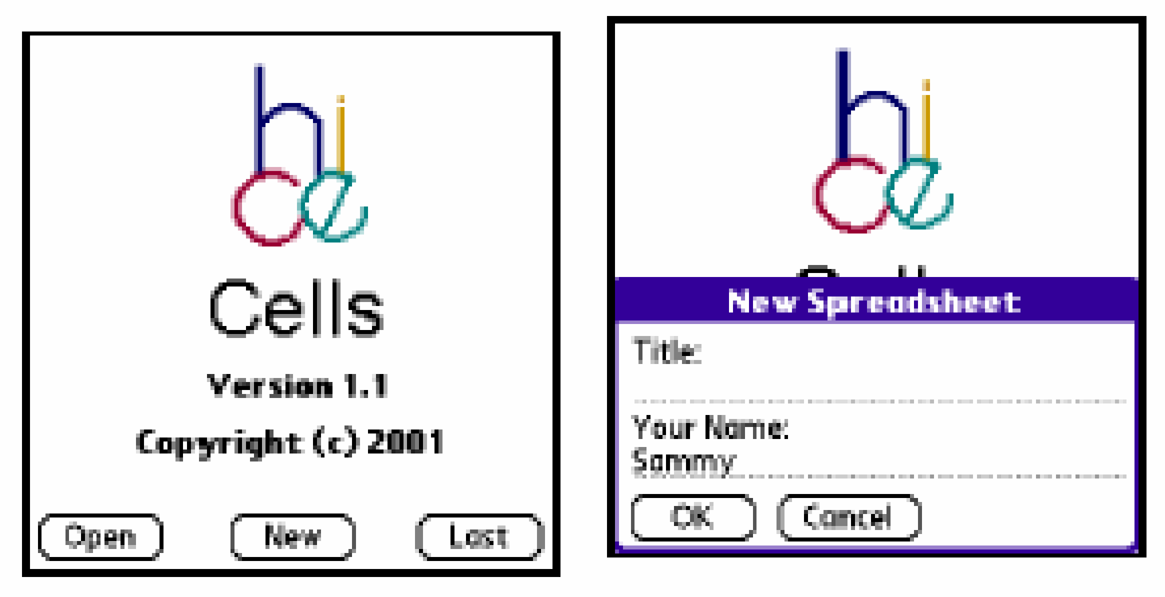
OPERATIONAL QUALITY CRITERIA	**Functionality**	• Suitability • Compliance • Accuracy • Interoperability
	Usability	• Efficiency • Memorability • Satisfaction • Learnability • Error Messages
	Quality of service	
	Performance	
	Dependability	• Maturity • Fault tolerance • Recoverability
	Security	• Authentication • Wireless network security • Data integrity • Privacy and confidentiality • Access control • Availability
DEVELOPMENT QUALITY CRITERIA	**Maintainability**	• Analyzability • Changeability • Stability
	Testability	• Field Failures
	Portability	• Adaptability • Installability • Conformance • Replacability
	Scalability	
PRODUCT ELEMENTS	**Structure**	• WAP gateway failures
	Functions	• Navigation • Calculation • Mobile middleware interface
	Data	• Real time failure • Data instance failure
	Platform	• Third party software failures • Hardware failures • Micro-browser failures • Wireless network failures • Host location register / visitor location register / location database • Mobile database
	Multi-function operations	• Mobility management • Location management • Software upgrade errors • Transaction errors • Data handling
	Synchronization	• Software interface • Hardware interface • Wireless Synchronization
	Memory management	• Memory leaks
PROJECT ENVIRONMENT	**Customers** **Information** **Team** **Equipment and tools** **Schedules** **Test Items** **Deliverables**	

A Sample Application: Mobile Computing in Education

One sector where mobile computing has proved useful is education. Handhelds can be integrated into the curriculum to deliver notes or assignments to students, to help the teacher monitor what the student is doing, and to collect results (work-in-progress or completed assignments) and feedback from the students.

Many kinds of wireless networks, handheld devices and mobile applications are used for this kind of application. Typical wireless networks are the 802.11-family and infrared-based beaming stations. Among the handhelds Palm (http://www.palm.com/us/education/), Pocket PC (http://www.microsoft.com/education/?ID=PocketPC) and Blackberry (http://www.blackberry.com/products/handhelds/index.shtml) devices are most commonly used. There are some specialized handhelds meant exclusively for educational use like the Texas Instruments TI 83 and TI 89 (http://education.ti.com/educationportal/index.jsp).

Examples of applications in use are Cells, Handysheets, and PicoMap from University of Michigan's Center for Highly Interactive Computing in Education (2003a), and CellSheet and LearningCheck from Texas Instruments (2003a). Teachers can integrate these applications, and interact with students' devices, using wired or wireless access, with products like the Palm OS Application Assessment Manager (PAAM) (GoKnow, 2003a) and the TI-Navigator (Texas Instruments, 2003b).

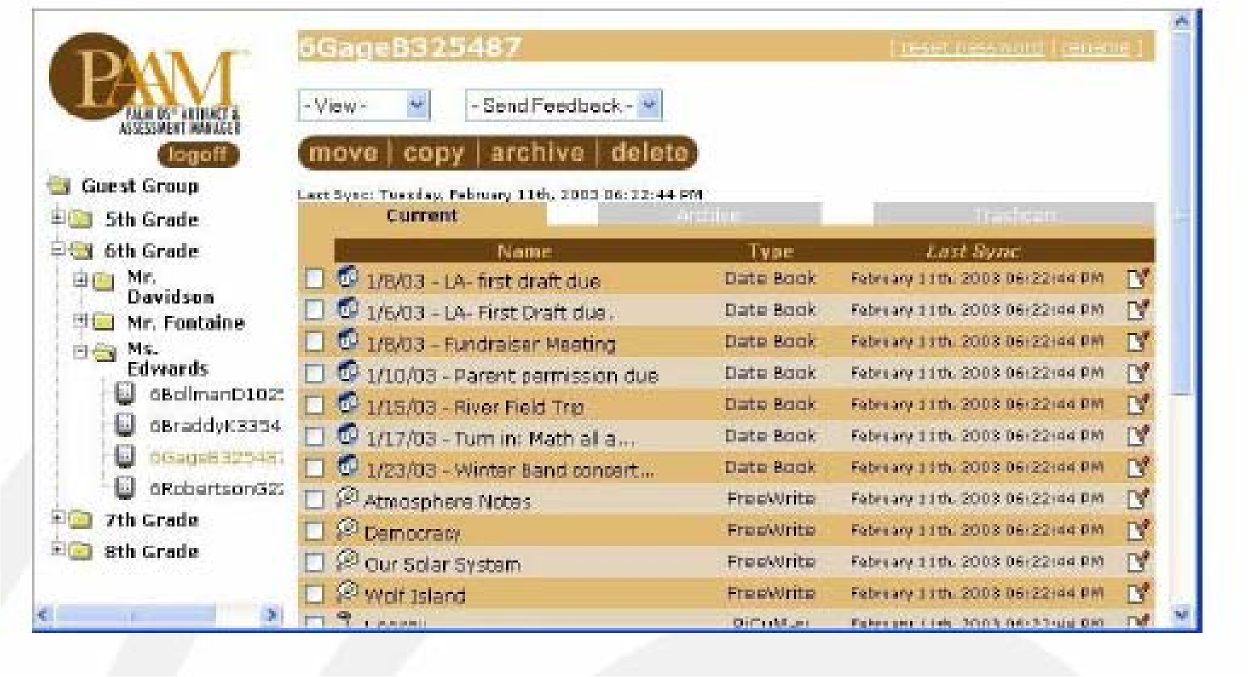


Title:

Your Name: Sammy

Figure 3: Source: Cells 1.1 Quick Start Guide (Center for Highly Interactive Computing in Education, 2003c)

In this paper, we use a sample application called Cells (Center for Highly Interactive Computing in Education, 2003b) which enables students to enter data into a spreadsheet on their PDA. We demonstrate how to use the failure mode catalog to generate test cases for this application and its integration into PAAM.



PAAM
PALM OS™ ARTIFACT & ASSESSMENT MANAGER

logoff

- Guest Group
  - 5th Grade
  - 6th Grade
    - Mr. Davidson
    - Mr. Fontaine
    - Ms. Edwards
      - 6BollmanD102
      - 6BraddyK3354
      - 6GageB32548
      - 6RobertsonG2
  - 7th Grade
  - 8th Grade

6GageB325487 [reset password | [illegible]]

- View - | - Send Feedback -

move | copy | archive | delete

Last Sync: Tuesday, February 11th, 2003 06:22:44 PM

Current | Archive | Trashcan

	Name	Type	Last Sync	
□	1/8/03 - LA- first draft due	Date Book	February 11th, 2003 06:22:44 PM	
□	1/6/03 - LA- First Draft due .	Date Book	February 11th, 2003 06:22:44 PM	
□	1/8/03 - Fundraiser Meeting	Date Book	February 11th, 2003 06:22:44 PM	
□	1/10/03 - Parent permission due	Date Book	February 11th, 2003 06:22:44 PM	
□	1/15/03 - River Field Trip	Date Book	February 11th, 2003 06:22:44 PM	
□	1/17/03 - Turn in: Math all a...	Date Book	February 11th, 2003 06:22:44 PM	
□	1/23/03 - Winter Band concert...	Date Book	February 11th, 2003 06:22:44 PM	
□	Atmosphere Notes	FreeWrite	February 11th, 2003 06:22:44 PM	
□	Democracy	FreeWrite	February 11th, 2003 06:22:44 PM	
□	Our Solar System	FreeWrite	February 11th, 2003 06:22:44 PM	
□	Wolf Island	FreeWrite	February 11th, 2003 06:22:44 PM	
□	[illegible]	[illegible]	February 11th, 2003 06:22:44 PM	

Figure 4: Source: Walkthrough: PAAM™-Palm OS Artifact and Assessment Manager (GoKnow, 2003b)

APPENDIX 1: FAILURE MODES FOR WIRELESS / MOBILE APPLICATIONS

Let's set some expectations. This is a work in progress. It is incomplete. The complete version will be Ajay's M.Sc. thesis, which will be published at www.testingeducation.org later in the year. The catalog is most thoroughly worked, at this point, in the sections on security, usability, functionality, synchronization and performance.

This appendix lists a set of failure modes that are specific to wireless / mobile applications. We intentionally do *not* list generic examples of failure modes. We expect to eventually create a broad list that includes generic examples by merging Vijayaraghavan's (2002) thesis work, Ajay's thesis work, relevant portions of the Kaner, Falk, Nguyen (1993) Appendix and other failure (as opposed to fault, such as are available from NIST, 2000) collections. If you're interested in offering help (such as data, funding, or editorial review/writing) for that broader project, please contact Cem Kaner at kaner@kaner.com.

The overall structure of this catalog matches Bach's (2003a) *Heuristic Test Strategy Model* and we include several of his descriptions, including his heading captions, with his permission. We have modified the second-level structure in some cases to conform to other published standards or well-known discussions. Eventually, we expect that we'll reorganize to match a revision of Bach's model after he reorganizes some of the details of his model in response to our suggestions.

OPERATIONAL QUALITY CRITERIA

"*Quality Criteria* are the rules, values, and sources that allow you as a tester to determine if the product has problems. Quality criteria are multidimensional, and often hidden or self-contradictory." (Bach 2003a, p. 1) "A *quality criterion* is some requirement that defines what the product should be. By looking or thinking about different kinds of criteria, you will be better able to plan tests that discover important problems fast. Each of the items on this list can be thought of as a potential risk area. For each item below, determine if it is important to your project, then think how you would recognize if the product worked well or poorly in that regard." (Bach 2003a, p. 4)

Operational quality criteria are criteria that relate to the product in use. We distinguish them from *development* criteria, which relate to the product as a static object under development.

1. FUNCTIONALITY: *Can it perform the required functions?*

ISO 9126 defines *functionality* as, "A set of attributes that bear on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs. This set of attributes characterises what the software does to fulfill needs, whereas the other sets mainly characterise when and how it does so."

(Source: http://www.issco.unige.ch/ewg95/node14.html)

ISO 9126 further subdivides Functionality into Suitability, Accuracy, Interoperability and Compliance. These subcategories are discussed as individual categories in this qualitative fault modelling of mobile applications.

SUITABILITY

"Attributes of software that bear on the presence and appropriateness of a set of functions for specified tasks." (ISO 9126, 1991)

Failure Modes:

- No implementation or malfunction of the renaming of the cells spreadsheet;
- Unable to beam the Cells spreadsheet;
- File size too big to be served and viewed on a handheld.
- No "admin" button to carry out administrative tasks in PAAM.
- Failure to add an individual handheld to the existing subgroup of PAAM.
- Failure to delete, add or move files from one subgroup to another.
- Failure in the "filter" function of PAAM
- Failure to archive files in PAAM

Related Bugs and Links

- Incomplete functional implementation in Pocket EXCEL http://www.earthv.com/articles.asp?ArticleID=579
- Pocket PC 2002: Contact Does Not Beam

  http://support.microsoft.com/default.aspx?scid=kb;en-us;323011
- Pocket PC Calendar Does Not Correct Time Zone Changes

  http://support.microsoft.com/default.aspx?scid=kb;en-us;268249

ACCURACY

"Attributes of software that bear on the provision of right or agreed results or effects." (ISO 9126: 1991)

Failure Modes:

- Data that is beamed is inaccurate due to transmission problem
- Data not stored in the appropriate folder
- Not able to add a student's name in the subgroup of PAAM
- Application designed without taking screen size into consideration
- Misalignment of image on the screen
- Multiple copies of a file with the same name but different content exist on the handheld.

Related Bugs and Links:

- Known Issues in Pocket Excel on a Handheld PC

  http://support.microsoft.com/default.aspx?scid=kb;en-us;189502
- Known Issues in Pocket Word on a Handheld PC

  http://support.microsoft.com/default.aspx?scid=kb;en-us;188782
- Graphics Issues in Pocket PowerPoint Presentations

  http://support.microsoft.com/default.aspx?scid=kb;en-us;186757

INTEROPERABILITY

"Attributes of software that bear on its ability to interact with specified systems." (ISO 9126: 1991)

Failure Modes:

- Specific make of handheld not able to send information to PAAM
- Problem running the software due to incompatible version of the operating system of the handheld. For example certain applications developed for Palm OS requires earlier version of Palm OS.
- Application not available for all the leading handheld platforms like Palm OS, Pocket PC, Blackberry and Symbian OS.
- Application not able to run on dirty configuration. A dirty configuration is any configuration that is not supported but is very common. (Collard, 2003)
- Application can run only on one kind of network. For example, if CDMA or 1XRTT is used for voice and data, it can only work in North America and places where CDMA is in use.
- Beaming of file or data between handhelds having different operating systems not possible.
- Failure to interoperate between differing screen resolutions. Some of the common resolutions available are 160x160, 320x240, 95x65, 120x130, 1024x768, 1024x768
- Failure to interoperate between differing colors. Some of the common color schemes to be found on the handheld devices are 2-bit, 16-bit, 32-bit and varying gray levels.
- Application compatible across different microbrowsers available.
- Application complies with the differing graphics format.

Related bugs and links:

- Incompatibility bugs wireless http://australianit.news.com.au/articles/0,7204,6459892%5e15397%5e%5enbv%5e,00.html

- Problems When You Convert Files Between Excel and Pocket Excel
  http://support.microsoft.com/default.aspx?scid=kb;en-us;185921

COMPLIANCE

"Attributes of software that make the software adhere to application related standards or conventions or regulations in laws and similar prescriptions." (ISO 9126: 1991)

Failure Modes:

- Non compliance with the wireless network standard
- Application does not comply with the UI guidelines of development leading development environments like Palm OS, MSDN or BREW.

2. USABILITY: *How easy is it for a real user to use the product?*

Usability is the "effectiveness, efficiency and satisfaction with which a specified set of users can achieve a specified set of tasks in a particular environment." (ISO 9241) According to Jakob Neilson (1993), usability subsumes the notions of learnability, memorability, efficiency, error rate / recovery and satisfaction. ISO 9126 divides usability into understandability, learnability and operability.

Usability issues are highly pronounced on handheld devices due to the limitations of wireless handheld devices (Passani, 2000). They have a limited form-factor and the display units are smaller than their desktop counterparts. Designing for such small screen size needs more thinking and better navigation structures. Another factor worth taking into consideration is the data input in a PDA or smart phone. The keyboard or the soft input panel of these devices is not very spacious. This warrants new and innovative ways of reducing the amount the data that a user is made to enter. In this paper, Usability failure modes and risks are divided into learnability, efficiency, memorability, error recovery and satisfaction.

LEARNABILITY

The system should be easy to learn so that the user can rapidly start getting some work done with the system. (Neilson 1993)

Failure Modes:

- Inconsistent layout
- Information not arranged in hierarchical or tree-like structure

Related bugs and links:

- Inconsistent user interface
  http://www.cewindows.net/commentary/userinterface.htm

EFFICIENCY

The system should be efficient to use, so that once the user has learned the system, a high level of productivity is possible. (Neilson 1993)

Failure modes:

- No importance given to the main activities of the portable users and all the functionalities implemented
- Main activities of the user not implemented in the fastest possible manner
- Verbose text on a small screen
- No implementation of "Back" functionality
- Application directly transcoded to any wireless markup language from HTML
- Users not given proper feedback when they commit errors
- Users do not understand what to do when they commit mistakes

SATISFACTION

The system should be pleasant to use, so that users are subjectively satisfied when using it. Users should like the system (Neilson 1993)

Failure Modes:

- Users found it difficult to use the application.
- Application needs a lot of data entry

MEMORABILITY

The system should be easy to remember, so that the casual user is able to return to the system after some period of not having used it, without having to learn everything all over again (Neilson 1993)

Failure Modes:

- No customization of the application for the specific micro browser. This might result in content not being rendered properly on a micro browser.
- Difficulty in remembering actions needed to perform a task

3. ACCESSIBILITY. *Can it be used by everyone?*

A system is said to be accessible when it can be used by anyone irrespective of their physical or technical capabilities. With respect to people with physical disabilities, accessibility means providing supporting tools or assistive technologies like screen reader, adapted keyboards or head-mounted pointers to enable the use of product.

Failure Modes:

- Red / green color blindness not taken into consideration
- User not able to press a button on the handheld device due to improper placement of the button
- User not able to use biometric security feature of the handheld due to strict requirement of the hand movement.

4. QUALITY OF SERVICE. *Can you configure and depend on the network's service?*

A network provides high Quality of Service (QoS) if it delivers traffic consistently across a network, provides high transmission rates, low error rates and supports designated usage patterns. "*Quality of Service* (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail. QoS technologies provide the elemental building blocks that will be used for future business applications in campus, WAN, and service provider networks." (Cisco, 2003, at http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm#1020563)

Failure Modes:

- Inability to predict the network capabilities of the wireless network. Due to this exchange of parameters between the application and network is not possible.
- Loss of bandwidth or attenuation of the signal strength due to movement of the mobile node.
- Loss of communication during handover between cells. This is not significant for the voice application but even milliseconds of broken link can result in undesirable consequences in case of data application.
- Cost per unit data not very economical for customers.
- High cost to establish a connection or to access a resource.
- High bit error rate due to mobility of the node connected to the wireless network.
- Low quality of multimedia application due to limited bandwidth.
- Limitation imposed by the requirement of portability of the system. Battery life is limited and mobile computing technology requires significant power for effective transmission.

- Alteration of the QoS parameters in the wireless networks not taken into account while designing the system.
- Context management or the user environment not taken into consideration.

5. PERFORMANCE: *How speedy and responsive is it?*

Mobile applications run on wireless links that have high latency and low bandwidth. A data packet needs multiple hops before communicating with another device or application. Special consideration is required while designing the system to enhance the performance of such applications.

Failure Modes:

- Usage of HTTP/1.0 instead of HTTP/1.1 (Cheng, 1999)
- Problem in the WML (wireless markup language) timer function
- Time taken to load a page on a microbrowser very high.
- Time taken to beam a file to another handheld very high.
- No caching mechanism used to enhance the performance.
- Performance problems arising after loading third party software applications.
- Firmware problems resulting in low performance.
- Performance degrades when loading multiple pages.
- Problems arising because of poor mobile client server architecture. Fat client vs thin client approaches (Yang, 2003)
- Usage pattern of the wireless network not taken into consideration.
- Performance critical features or functions of an application not identified and optimized.
- Response time after a complex calculation very high.
- Throughput of the system very low when many users log in and try to use a feature.
- Occurrence of buffer overflows and memory leaks after exposing the system to load for an extended period of time (Collard, 2002)
- Weak point in the system detected after exposing load at a specific portion of the system considered being not so robust. This is also known as hot spot testing (Collard, 2002)
- System's performance hampers when varying the load from low to high and following some pattern of load fluctuation (Collard, 2002)
- Problem occurs when exposing the system to abrupt load. This is also known as spike or bounce testing. Load balancing and resource reallocation problems surface during such tests (Collard, 2002)

- Breakpoint of the system found to be less than expected or designed. Breakpoint of a system is defined as the load or mix of loads at which the system fails and the manifestation of the failures (Collard, 2002)
- Reduced performance when using a network for data transfer in conjunction with data transmission.
- Delay in loading bitmaps and other graphics more than expected.
- Wireless link "stalls" resulting in spurious TCP timeouts (Chakravorty, 2002)
- Delay caused due to high RTT and slow startup phase for the system to utilize the wireless link (Chakravorty, 2002)
- Excessive queuing over the downlink results in higher probability of timeouts during the initial requests for connection (Chakravorty, 2002)

Related bugs and links:

- Microsoft Active Sync 3.x slows down the system
- Dell Halts Axim Shipments Over Software Problem http://stickyminds.com/news.asp?Function=NEWSDETAIL&ObjectType=NEWS&ObjectId=6549

6. DEPENDABILITY: *Will it work well and resist failure in all required situations?*

Dependability is a term encompassing many notions like reliability, recoverability, availability and safety within itself (Malloy 2002). ISO 9126 divides reliability into three separate categories: Fault Tolerance, Maturity and Recoverability. Applications running on wired infrastructures have very high dependability because of the nature of such infrastructures. Current and emerging wireless networks and hence, the applications running on them, do not offer such levels of dependability. It is thus extremely important to concentrate on this category while testing any wireless or mobile application.

Reliability within the mobile context could be defined as the "Ability of the wireless and mobile networks to perform their designated set of functions under certain conditions for a certain operational time." (Malloy 2002) I have included the listing of failure modes with respect to Fault Tolerance, Maturity and Recoverability in this paper as that seemed to be the most appropriate way to deal with the issues concerning dependability of a wireless application and networks.

FAULT TOLERANCE

"Attributes of software that bear on its ability to maintain a specified level of performance in cases of software faults or of infringement of its specified interface." (ISO 9126: 1991)

Failure Modes:

- Unable to resume transmission of data or corruption of data due to failure of an access point.

- No auto configuration of addressing based on context (Sternbenz, 2002)
- No auto configuration of signaling and routing based on mission (Sternbenz, 2002)
- Problem in channel allocation algorithm for the cellular network
- Failure in borrowing a channel due to delay in communication (Cao, 2000)
- Failure to establish a channel due to network congestion.
- Failure to establish a channel due to communication link failure.
- Failure in establishing a channel due to mobile switching center failure.

MATURITY

"Attributes of software that bear on the frequency of failure by faults in the software." (ISO 9126: 1991)

Failure Modes:

- Mean time between Failures (MTBF) in carrying out a transaction very high.
- Frequent "stalls" in transmissions.
- Low power of transmission of the radio waves.

RECOVERABILITY

Recoverability is the capability of a system or application to maintain services during attack or when all the resources are not available.

Failure Modes:

- Application does not switch to offline mode when there is a loss in network connectivity.
- Delayed recovery after timeouts. Normally the recovery should be in milli or microseconds. GPRS networks have the recovery time in seconds after timeouts due to link "stalls" (Chakravorty, 2002)
- No adaptability of the power of transmission of the signals.
- No reconnection attempt after the device fails to establish the wireless link.

7. SECURITY: *Is the system secure?*

Security issues could be subdivided into six subcategories: privacy and confidentiality, access control and authorization, authentication, data integrity, wireless network security and availability.

PRIVACY AND CONFIDENTIALITY

Confidentiality and privacy means the protection of the information about a user or process.

Failure Modes:

- Disclosure of passwords.
- Disclosure of private data like credit card details.

Related Bugs and Links:

- Yahoo! Mobile service discloses random sensitive information to unauthorized users.

  http://xforce.iss.net/xforce/xfdb/11352
- Stolen credit card information

  http://www.cewindows.net/commentary/userinterface.htm
- Hand-helds are a hacker's delight

  http://www.ciol.com/content/developer/2003/103080301.asp

ACCESS CONTROL AND AUTHORIZATION

Access control implies as to who may have access to the physical device or data.

Failure Modes:

- Physical access to a stolen device

  http://www.kb.cert.org/vuls/id/789985

Related Bugs and Links:

- Linux PDA Security Hole

  http://www.pdacenter.net/news/static/102643633846024.shtml
- Palm Password bypass error
  http://www.securityfocus.com/bid/2429
- World readable permission in Palm desktop

  http://www.securityfocus.com/bid/2398/discussion/
- Palm Desktop For MacOS X Hotsync Insecure Backup Permissions Vulnerability

  http://www.securityfocus.com/bid/3863
- Mouse hole in device security

  http://pcw.vnunet.com/News/1123233

- Unauthorized access due to stolen device. http://www.computerworld.com/securitytopics/security/story/0,10801,78127,00.html

AUTHENTICATION

Authentication implies establishing identity of users, process or hardware components.

Failure Modes:

- No authentication mechanism used.
- Weak passwords that can be easily broken.

Related Bugs and Links:

- PalmOS Authentication Bypass Vulnerability
  http://www.securityfocus.com/bid/5538/info/
- Palm OS Weak Encryption Vulnerability
  http://www.securityfocus.com/bid/1715/info/

DATA INTEGRITY

Integrity means that the system should not corrupt the data as compared to their original state.

Related Bugs and Links:

- Corruption of file system using Zaurus vulnerability
  http://www.internetnews.com/dev-news/article.php/1402491

WIRELESS NETWORK SECURITY

This category targets the security failures that could occur in different wireless networks. Networks covered under this category are the Bluetooth, 802.11 and the cellular network. Wireless network as of now is the biggest security hole in the IT infrastructure and exposes even the wired infrastructure to attacks. A brief explanation of the networking technologies and links to relevant literature could be found in appendices at the end of the paper. Many of these failure modes are explained in detail in a special publication by NIST (Karygiannis, 2002). A new security specification called WPA (Wi Fi Protected Access) is being adopted as it fixes most of the fundamental flaws in WEP. The key features of of WPA are Extensible Authentication Protocol (EAP), Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC), and 802.1X for authentication and dynamic key exchange. WPA is a standards based solution and offers higher level of interoperability.

Bluetooth Failure modes:

- No external boundary protection

- Set Bluetooth devices to the lowest sufficient power level to ensure transmissions within bounds
- Unit keys used instead of combination keys
- Weak PINS chosen
- No alternative protocol used for the exchange of PINS
- No established "minimal key size" for any key negotiation process
- No application level (on top of Bluetooth stack) encryption used for highly sensitive data
- Security patches and upgrades not up-to-date
- Man in the middle attack
- Break of stream cipher - DES/RC4 are weaker than 3DES and AES

- Unit keys used instead of combination keys
- Weak PINS chosen
- No alternative protocol used for the exchange of PINS
- No established "minimal key size" for any key negotiation process
- No application level (on top of Bluetooth stack) encryption used for highly sensitive data
- Security patches and upgrades not up-to-date
- Man in the middle attack
- Break of stream cipher - DES/RC4 are weaker than 3DES and AES

802.11 Failure Modes:

- Eavesdropping from the parking lot within the AP range
- Radio interference resulting in DoS
- No encryption mechanism followed by the AP
- Shared key authentication

- MAC address could be spoofed even if WEP is enabled allowing access to the WLAN
- Security patches and upgrades not up-to-date
- Algorithms using shorter keys used
- Inherent weaknesses in the WEP—could be easily cracked
- If the plaintext message is known and attacker has the copy of the cipher text— key could be obtained by getting the IV and using a dictionary attack.
- Cipher stream reuse - key stream could be recovered from the WEP packet
- Fluhrer-Mantin-Shamir exploit of the weakness in the KSA—resulted in two tools: WEPcrack and air snort
- Static noise attack—resulting in DoS
- Weak AP password
- If reset option is enabled—default encryption settings could revert to no encryption
- No physical barriers—first line of defense
- Network name or the SSID is stored in clear text
- No authentication mechanism in place—EAP not enabled
- Man in the middle attack
- ARP poisoning
- Cache poisoning
- Rogue access points
- No access control list (ACL) or VPN in place
- Access to the wired network not protected
- IPSec or VPN or secure shell traffic not used

Related Bugs and Links:

- Problems with WEP and adoption of WPA

InformationWeek Wireless Fidelity Deploying WPA Today June 30, 2003

- Wi Fi users do not use security features

  SecurityFocus HOME News Study Wi-Fi users still don't encrypt

- Problem in the wireless router

  SecurityFocus discussion SMC Wireless Router Malformed PPTP Packet

  SecurityFocus HOME Vulns Info Buffalo WBRG54 Wireless Broadband Router

- Configuration problem

  SecurityFocus HOME Netgear FM114P ProSafe Wireless Router Rule Bypass

- Information disclosure due to configuration error

  SecurityFocus HOME Netgear FM114P ProSafe Wireless Router UPnP Inform

- Input validation error

  SecurityFocus HOME Netgear FM114P Wireless Firewall File Disclosure V

- Microsoft Wireless and mobile security resources

  Wireless and Mobile Security Technical Resources

- New WLAN Attacks Identified

  http://www.wi-fiplanet.com/news/article.php/2246081

Cellular network Failure Modes:

This subcategory lists the most common attacks on a cellular system. Some of the failure modes in this category are inspired by Ko's (1996) paper on attacks on cellular systems.

- Phone cloning resulting due to the ESN (Electronic serial number) and MIN (Mobile identification number) being read by attackers.
- Cell phone not equipped with PIN (personal identification number)
- Hijacking of the voice channel by increasing the power level of the cellular phone.
- No encryption of voice while transmission
- Denial of service occuring due to jamming of the RF channel using RF attack.

Related Bugs and Links:

- Handspring VisorPhone vulnerable to DoS via SMS image transfer
  http://www.kb.cert.org/vuls/id/222739
- SMS denial of service on Seimens

  SecurityFocus HOME Siemens Mobile Phone SMS Denial of Service Vulnera

- Verizon Wireless bug allows SMS tapping
  http://www.threezee.com/modules.php?op=modload&name=Sections&file=index&req=viewarticle&artid=6&page=1
- Cellular companies fight fraud

  http://www.decodesystems.com/mt/97dec/

AVAILABILITY

System availability is duration of time a system is available for use by its intended users. Opposite of availability is denial of service (DoS), when the system is not available with its services either fully or partially.

Failure Modes:

- DoS attack due to firmware problems.
- Failure initiating and maintaining the wireless link due to interference with external devices.

Related Bugs and Links:

- Airborne Viruses
  http://www.networkmagazine.com/article/NMG20001130S0001
- Palm OS - Phage virus
  http://doc.advisor.com/doc/07194
- New email virus bombards mobile phone users

  http://news.com.com/2100-1023-241489.html?legacy=cnet
- Palm HotSync Manager Remote Denial of Service Vulnerability
  http://www.securityfocus.com/bid/6673/info/
- PalmOS TCP Scan Remote Denial of Service Vulnerability
  http://www.securityfocus.com/bid/3847
- Mobile virus threat looms large

  http://news.bbc.co.uk/2/hi/technology/2690253.stm

DEVELOPMENT QUALITY CRITERIA

Development quality criteria focus on the product under development and its relationship to the development organization rather than to the user.

8. MAINTAINABILITY: *Will it be easy to maintain?*

Maintainability is defined as the ease with which changes can be made to a software system. These changes may be necessary for the correction of faults, adaptation of the system to a meet a new requirement, addition of new functionality or removal of existing functionality. Maintainability can be either a static form of testing, i.e. carried out by inspections and reviews, or a dynamic form i.e. measuring the effort required to execute maintenance activities.

(Source: http://www.testingstandards.co.uk/maintainability_guidelines.htm)

ISO 9126 divides maintainability into analyzability, changeability, stability and adaptability.

ANALYZABILITY

"Attributes of software that bear on the effort needed for diagnosis of deficiencies or causes of failures, or for identification of parts to be modified" (ISO 9126: 1991)

Failure Modes:

- Components like mobile middleware, programming language etcetera used in the development of the application not very clear or poorly chosen.
- Improper documentation of the design and architecture.

CHANGEABILITY

"Attributes of software that bear on the risk of unexpected effect of modifications." (ISO 9126: 1991)

Failure Modes:

- Unable to change the network configuration or type with ease.
- Unable to add more features to the application.
- Failure to personalize the application.

STABILITY

"Attributes of software that bear on the effort needed for validating the modified software." (ISO 9126: 1991)

Failure Modes:

- Addition of features makes the application difficult to use.
- Application becomes unstable after changes in the language or tool used.

9. TESTABILITY: *How easy will it be to test?*

Testability could be defined as *visibility* and *control*. *Visibility* is our ability to observe the states, outputs, resource usage and other side effects of the software under test. *Control* is our ability to apply inputs to the software under test (Pettichord, 2002)

FIELD FAILURES

These are the failures that escape the unit testing stage or any other kind of testing done using the simulators or emulators. Errors and failures are encountered when the application runs on the actual device or on the actual wireless network in the production environment.

Failure Modes:

- Application fails to connect to the back-end on the real network.
- Application fails to load and function on the actual device.

10. PORTABILITY: *How easy will it be to change the environment?*

"The ease with which a system or component can be transferred from one hardware or software environment to another" (Institute of Electrical and Electronics Engineers, 1990)

ISO 9126 sub-categorizes Portability into Adaptability, Installability, Conformance and Replaceability.

ADAPTABILITY

"Attributes of software that bear on the opportunity for its adaptation to different specified environments without applying other actions or means than those provided for this purpose for the software considered." (ISO 9126: 1991)

Failure Modes:

- Application not customizable to the user environment.
- Application does not behave well on limited bandwidth.
- Application does not adapt to network latency.

INSTALLABILITY

"Attributes of software that bear on the effort needed to install the software in a specified environment" (ISO 9126: 1991)

Failure Modes:

- Failure to install the application locally using synchronization software.
- Failure in online installation. Many applications give the benefit of wireless online install using internet or local area network.

- Failure to install the application on the emulator or simulator therby resulting in inadequate unit testing.
- Failure to install the software due to interference with another application.
- Failure to customize the installation if user has the option to do that.
- Failure to install the application at the desired location inspite of the location being valid.
- Failure to install the application on all the supported configurations.
- Unwanted results when user aborts the installation midway.
- Problems in the input field while installing the software.

Related Bugs and Links:

- Services may not start after installation

  http://www.securityfocus.com/bid/7282/discussion/
- Palm install could not handle a valid path

  http://www.faughnan.com/palm.html#Installation
- "Cannot Find Pocket Streets" Error Message When You Try to Install Pocket Streets

  http://support.microsoft.com/default.aspx?scid=kb;en-us;319689

CONFORMANCE

“Attributes of software that make the software adhere to standards or conventions relating to portability” (ISO 9126: 1991)

Failure Modes:

- Non conformance with the carrier (cellular service provider) standards and guidelines.

REPLACEABILITY

“Attributes of software that bear on the opportunity and effort of using it in the place of specified other software in the environment of that software.”
(ISO 9126: 1991)

11. SCALABILITY: *Can I increase the capacity with ease?*

“The ease with which a system or component can be modified to fit the problem area” (Institute of Electrical and Electronics Engineers, 1990)

Failure Modes:

- Problems due to large number of users.

12. LOCALIZABILITY. *Can I adapt the application to serve bigger market?*

Internationalization (sometimes shortened to "I18N, meaning "I - eighteen letters -N") is the process of planning and implementing products and services so that they can easily be adapted to specific local languages and cultures, a process called localization. The internationalization process is sometimes called translation or localization enablement. (Source: http://whatis.techtarget.com/definition/0,,sid9_gci212303,00.html)

PRODUCT ELEMENTS

"Product Elements are things that you intend to test. Software is so complex and invisible that you should take special care to assure that you indeed examine all of the product that you need to examine." (Bach 2003a, p. 1) "Ultimately a product is an experience or solution provided to a customer. Products have many dimensions. So, to test well, we must examine those dimensions. Each category, listed below, represents an important and unique aspect of a product. Testers who focus on only a few of these are likely to miss important bugs." (Bach, 2003a, p. 3)

13. STRUCTURE: *Everything that comprises the physical product.*

WAP GATEWAY FAILURES

WAP gateway is a server that is responsible for converting a WTP request made by a smart phone to an HTTP request to be processed by a web server. WAP gateway also translates an HTML web page to WML if it is required.

Failure Modes:

- Failure in transcoding HTML to WML resulting in errors serving a page to the cell phone.
- Problems arising due to cards / fonts of WML not supported on a device.
- Problems arising due to deck size of WML exceeding the device limit.

14. FUNCTIONS: *Everything that the product does.*

NAVIGATION

Failure Modes:

- Non intuitive placement of navigation buttons on the screen.
- Users reaching a deadlock while navigating. Only way to proceed further is to return to the main screen.

CALCULATION

Failure Modes:

- Improper calculation of the arithmetic functions like average, minimum, maximum etcetera
- Improper calculation at the boundary values.
- ASCII values calculated in case user enters a character other than a number.

MOBILE MIDDLEWARE INTERFACE FAILURES

A middleware is defined as: **“**An enabling layer of software that resides between the business application and the networked layer of heterogeneous (diverse) platforms and protocols. It decouples the business applications from any dependencies on the plumbing layer, which consists of heterogeneous operating systems, hardware platforms and communication protocols.” (Source: International Systems Group)

A mobile middleware is an enabling layer of software that is used by application developers to connect their applications with disparate mobile (wireless and wired) networks and operating systems. This category targets the failures that could occur in a mobile middleware.

15. DATA: *Everything that the product processes.*

REAL TIME FAILURE

Real time applications or services not only have to carry out the right computation but the time taken to carry out a specific task or providing a service in a specified amount of time is also of considerable importance. Real time applications could be broadly categorized as hard real time applications or soft real time applications depending on the real time constraints they have to satisfy (Dreamtech, 2002)

Failure Modes:

- Delay in sending localized / personalized content to a user

DATA INSTANCE FAILURE

Related Bugs and Links:

- Problem due to number of records – system stop

  http://support.microsoft.com/default.aspx?scid=kb;en-us;Q317698

16. PLATFORM: *Everything on which the product depends.*

MOBILE SWITCHING CENTER FAILURES

In the case of cellular wireless network, establishing a communication session means making a wireless channel available between a *mobile host* (cell phone) and mobile support station. Mobile host sends a request to the *mobile support station* in its cell. There are many different channel allocation algorithms to avoid channel interference and efficiently utilize the limited frequencies. All these functions are carried out at the mobile switching center. (Cao, 2000)

THIRD PARTY SOFTWARE FAILURES

Mobile Application Architecture utilizes variety of third party software applications. In the case of location based services, mapping is carried out with the help of content providers having the geographic data. Potential problems in the third party applications may lead to failures in the application under test.

HARDWARE FAILURES

Related Bugs and Links:

- Problems with Casio Cassiopeia Pocket PC 2002

  http://www.pdastreet.com/forums/showthread.php?threadid=779
- Problems in Compaq hardware

  http://www.cewindows.net/bugs/pocketpc2002-compaq.htm
- Problems in HP hardware

  http://www.cewindows.net/bugs/pocketpc2002-hewlettpackard.htm
- Problems in Toshiba hardware

  http://www.cewindows.net/bugs/pocketpc2002-toshiba.htm
- HP Jornada with Pocket Internet Explorer for Windows CE Saves Cookies When "Save my password" Is Not Selected

  http://support.microsoft.com/default.aspx?scid=kb;en-us;303676

MICRO-BROWSER FAILURES

A micro-browser offers the same basic functionality as a desktop browser. It is used to submit user requests, receive and interpret results and allow the users to surf web pages using their handheld (Nguyen, 2003)

Failure Modes:

- Application not tested for correct functionality on text only browser.
- Application fails to work on palm based browser.
- Microbrowser does not support the security mechanism like SSL
- Microbrowser does not support tables and images.
- Microbrowser not supporting cHTHL therby not able to serve i-mode pages.
- AvantGo specific problems. AvantoGo supports web channel formatted pages.

Related Bugs and Links:

- Known Issues in Pocket Internet Explorer on a Handheld PC

  http://support.microsoft.com/default.aspx?scid=kb;en-us;190307
- Pocket Internet Explorer Quits When You Connect to an SSL Site with the DES56 Cipher

http://support.microsoft.com/default.aspx?scid=kb;en-us;320894

- PRB: You Receive an Unknown Error When You Call a Method of the MFC ActiveX Control

  http://support.microsoft.com/default.aspx?scid=kb;en-us;310566

- Error Message: 500 java.lang.IllegalArgumentException: [object]

  http://support.microsoft.com/default.aspx?scid=kb;en-us;258910

- Pocket Internet Explorer: "Bad MIME Format" Viewing JPEG Images

  http://support.microsoft.com/default.aspx?scid=kb;en-us;187608

- Cannot Download .wav Files in Pocket Internet Explorer 1.1

  http://support.microsoft.com/default.aspx?scid=kb;en-us;167923

- Unable to Personalize a User Who Is Using Pocket Internet Explorer

  http://support.microsoft.com/default.aspx?scid=kb;en-us;284151

WIRELESS NETWORK FAILURES

This category targets the failures in the typical wireless networks.

802.11 Failure Modes:

- Configuration problem in the 802.11 BSS (Basic Service Set)
- Configuration problems in 802.11 ESS (Extended Service Set)
- Location of access point not appropriate leading to fading of signal
- Interference with another access point leading to loss of signal

Bluetooth Failure Modes:

- Failure in setting up a Bluetooth piconet.
- Failure to build a Bluetooth scatternet from piconets.

Cellular Network Failure modes:

- Loss of signal.
- Coverage issues.
- Loss of bandwidth due to mobility.

HOME LOCATION REGISTER / VISITOR LOCATION REGISTER / LOCATION DATABASE

In cellular systems home location register (HLR) is the database that has the permanent registry for the service profile i.e. information about the subscriber. Visitor location register (VLR) on the other hand serves as a temporary repository for the profile information. Many different algorithms are in use to manage the mobility. The most common strategy in use in North America is IS-41 that utilizes a two tier system of HLR and VLR to keep track of the mobile node.

Failure Modes:

- Failure to update the HLR on the status of the mobile host after it enters a new VLR.
- Excessive load on the network signaling resource due to the mobility of the mobile hosts.
- Excessive load on the database due to frequent updates needed resulting due to mobility of the node.

MOBILE DATABASE

There are two different approaches for the database connectivity on a handheld wireless device. There is a thin client model where technology like WAP enables users to view information that has been extracted from the database and displayed as a Web page with the help of a micro browser. Since availability of the wireless network has still some issues, this model is not very suitable for data intensive applications. The alternative model makes the significant data reside on the handheld (a local relational database on the handheld)

DATABASE SERVER

A database server is software that manages data in a database. Database management functions such as locating the actual record being requested, updating, deletion and protection of the data is performed by the database server. It also provides both the access control and concurrency control. So, while testing a mobile application that connects to the database, if there is some erratic data encountered, the database server could be the culprit and should be tested.

17. MULTI-FUNCTION OPERATIONS. *How the product will be used.*

MOBILITY AND RESOURCE MANAGEMENT FAILURES

This category targets the failures that occur due to the mobility of the node and improper resource management to offer uninterrupted wireless connectivity to the user.

Failure modes:

- Frequent disconnection due to the mobility of the node.
- Disruption during hand-off between different networks.
- Depletion of the IPv4 addresses.

LOCATION MANAGEMENT

Location management is an extremely important functionality in location based mobile applications. A location based mobile application utilizes the knowledge of the location of the mobile node to serve location specific information. It is used in telematics, route directions, call routing, billing and several other applications.

Failure modes:

- Change in the logical identity of the device or the owner. A logical identity could be MAC address, IP address or anything else used to identify a mobile node.
- Problems arising due to not updating the Location database server.
- Problems arising due to mobile node not re-registering with the base station.
- Failure in receiving GPS data, in case of GPS being used to locate mobile nodes.
- Failure to translate the geocode (latitude, longitude) into a map by the content provider.
- Failures in the triangulation mechanism to determine location.

SOFTWARE UPGRADE ERRORS

Failure Modes:

- Application does not work with the upgraded operating system.
- Application or device freezes due to firmware upgrade.

Related Bugs and Links:

- Problem faced due to firmware upgrade on Samsung T series:

  http://www.reviewcentre.com/post64347.html

TRANSACTION ERRORS

These are the errors that occur in carrying out a typical transaction. Transaction will depend on the functionality that the application offers and is highly context dependent.

Failure Modes:

- Failure in transmitting information to the handhelds by the base unit.
- Failure in completing a task assigned due to missing information on how to transmit data.

DATA HANDLING

Failure Modes:

- Varying treatment of characters by different mobile content delivery technology not taken into consideration.
- Application vulnerable to failures at the boundary values.

18. SYNCHRONIZATION: *How the data will be synchronized*

Synchronization is a feature that enables exchanges, transforms and synchronizes data between two different applications or data stores. Synchronization could be either cradle-based or wireless. The SyncML Consortium is on a mission to get mobile application developers and handheld device makers to use a common, XML-based data synchronization technology. This category lists the different failure that could be encountered while synchronizing data between two applications.

Software Interface:

Failure Modes:

- Corruption of data files during hotsynch
- Problem in the synchML server
- Active synch problems in case of Pocket PC devices
- Problems encountered while establishing partnerships with more than one machine.
- Failure in synchronizing data due to interference with another application.

Related Bugs and Links:

- Office- Palm link

  http://www.earthv.com/articles.asp?ArticleID=579
- Intellisynch error

  http://www.pdastreet.com/forums/showthread.php?threadid=779
- Installation of another software over active synch

  http://support.microsoft.com/default.aspx?scid=kb;en-us;263450
- Problem with the USB driver of Mac

  http://www.palminfocenter.com/view_Story.asp?ID=703
- Problem with hotsynch synchronizing datebook

  http://www.geocities.com/Heartland/Acres/3216/faq_pg7.htm
- Hot synch problem with some Windows XP

  http://www.computing.net/pda/wwwboard/forum/278.html
- Database access errors during synchronization

  http://support.microsoft.com/default.aspx?scid=kb;en-us;294213
- Synchronization failure with outlook and active synch

  http://support.microsoft.com/default.aspx?scid=kb;en-us;276563
- Problem synchronizing third party applications and software

  http://support.microsoft.com/default.aspx?scid=kb;en-us;271980
- Problem with AvantGo synchronization

  http://support.microsoft.com/default.aspx?scid=kb;en-us;259938
- Problems in continuing message interchange over synchML server

  http://lists.axialys.net/pipermail/syncml/2003-April/000010.html

- Problems with multiple inboxes with single parternership

  http://support.microsoft.com/default.aspx?scid=kb;en-us;269217
- Palm hotsynch troubleshooting

  http://www.palm.com/support/hotsync.html
- Problem with hotsynch due to discrepancy in the registry entries

  http://www.geocities.com/Heartland/Acres/3216/faq_pg6.htm
- Error due to CDO collaboration object model not installed

  http://support.microsoft.com/default.aspx?scid=kb;en-us;299625
- Error in Activesynch due to missing files

  http://support.microsoft.com/default.aspx?scid=kb;en-us;281598
- Soft Reset

  http://www.mobile-and-wireless.com/Articles/Index.cfm?ArticleID=27164
- Problem in the synchronization port - COM / USB of the computer

  http://support.microsoft.com/default.aspx?scid=kb;en-us;185750
- Problem synchronizing application like money by unexpected actions during the synchronization process

  http://support.microsoft.com/default.aspx?scid=kb;en-us;263988
- No reconnection after log off and logging on again

  http://support.microsoft.com/default.aspx?scid=kb;en-us;q321935&
- Synchronization problem due to error in the server
  http://support.microsoft.com/default.aspx?scid=kb;en-us;318450
- Corrupted Data File May Prevent Mobile Application From Opening Up

  http://www.filemaker.com/ti/108092.html
- ActiveSync Reports Unresolved Items When Device Resources Are Low

  http://support.microsoft.com/default.aspx?scid=kb;en-us;295001

HARDWARE INTERFACE

In case of local synchronization, a cradle that is connected to either the serial or USB port is used to mount the mobile device to synchronize the files and other data between a desktop and the mobile device. This category lists the failures that could occur in interfacing the cradle with a desktop due to failures in the serial or USB port of the desktop. For more information on interfacing

Failure Modes:

- Failure in the USB driver installed on the desktop.

- Failure in the serial port communication.
- BIOS errors in the desktop resulting in breakdown of communication between the external device and desktop.
- Failure in the infrared port of the mobile device or partner machine.

Related Bugs and Links:

- Problem with the USB driver of Mac

  http://www.palminfocenter.com/view_Story.asp?ID=703

Wireless Synchronization

Wireless modems are also in use to synchronize data. In this wireless synchronization method, mobile device connects to the proxy server using a wireless modem and preformatted web pages stored on the web server is transferred to the device. User can then view the pages offline (Nguyen, 2003). Infrared synchronization is also in use where devices are synchronized locally using line of sight.

Failure Modes:

- Problems in the proxy server.
- Non compliance with the guidelines for preformatting the web pages for mobile devices.
- Failure in infrared synchronization.

18. Memory Management: *Symptoms of memory-related errors***.**

Mobile devices are highly resource constrained with respect to the amount of primary and secondary storage. Special attention is required while developing and testing to avoid memory leaks and wild pointers.

Memory leaks

Failure Modes:

- Failures due to memory leaks on the client device
- Failures due to memory leaks on the server side.

Related Bugs and Links:

- Memory Leak in Pocket Internet Explorer

  http://support.microsoft.com/default.aspx?scid=kb;en-us;315028
- Memory leak due to SOAP exception

  https://www.alphaworks.ibm.com/forum/wstkmd.nsf/0/001C8DD95F6E7CF2633A6F05F9275483?OpenDocument

- Crash when establishing connection with dead Web Services

  http://www.alphaworks.ibm.com/forum/wstkmd.nsf/0/896C1B509F0130669C5E7D90F1D9812E?OpenDocument

PROJECT ENVIRONMENT

Elements of the *project environment* define how the project is being run, rather than what it contains. There are really two projects for a tester to consider, the broad development project and the testing sub-project. Aspects of either can be a source of constraints, problems, or opportunities for the tester.

We've included these categories for completeness, relative to Bach's model, but these are not failure modes and so we will not elaborate on them further in this paper. This section is taken verbatim from Bach (2003a, p.2), with his permission. The only area populated in this broad category is equipment and tools.

Project Environment includes resources, constraints, and other forces in the project that enable us to test, while also keeping us from doing a perfect job. Make sure that you make use of the resources you have available, while respecting your constraints. (Bach 2003a, p. 1) "Creating and executing tests is the heart of the test project. However, there are many factors in the project environment that are critical to your decision about what particular tests to create. In each category, below, consider how that factor may help or hinder your test design process. Try to exploit the resources you have available while minimizing the impact of constraints.

1. **CUSTOMERS:** *Anyone who is a client of the testing and development project*

   Stakeholders of the project determine as to what kind of tests they want to run. Usage of the failure mode catalog will depend on the expectations of the clients.

2. **INFORMATION:** *Information about the product or project that is needed for testing*

   Mobile application is used in a variety of horizontal and vertical industries. Some of the vertical applications are stock trading, airline reservation, healthcare solutions, and warehouse inventory solutions etcetera. Among the horizontal applications, the most prominent ones are wireless e-mail and personal information management, wireless office data solutions and sales force automation etcetera. Testing will depend on the context in which the application will be used.

3. **TEAM:** *Anyone who will perform or support testing and development*

   Experience, skills and expertize in special test techniques of the people responsible for carrying out testing should be considered while formulating a test strategy.

4. **EQUIPMENT AND TOOLS:** *Resources required to administer testing and development*

   This category lists the problems and links specific to the leading software development environments for mobile application development.

   - Wireless JAVA

     http://wireless.java.sun.com/j2me/index.html

- Bugs in J2ME

  http://search.java.sun.com/search/java/index.jsp?qt=%2Bcategory%3Amid-profile+%2Bstate%3Aopen&nh=10&qp=&rf=1&since=&country=&language=&charset=&variant=&col=javabugs

- Palm OS Application Development

  http://www.palmos.com/dev/start/

- Microsoft Mobile development
  http://www.microsoft.com/windowsmobile/information/devprograms/default.mspx

- Problems in BREW

  http://www.qualcomm.com/brew/developer/resources/ds/faq/techfaq14.html

- List of known bugs in OpenWave SDK

  http://developer.openwave.com/support/bug_form.html

5. **SCHEDULES:** The sequence, duration, and synchronization of events

6. **TEST ITEMS:** *The product to be tested*

7. **DELIVERABLES:** *The observable products of the test project*

APPENDIX 2: AN OVERVIEW OF WIRELESS APPLICATIONS, NETWORKS AND HANDHELD DEVICES

The software / hardware architecture of a typical mobile application could be best visualized in a layered framework for strategizing the testing process. There are typically four levels of abstraction that could be envisioned. Many different types of devices, wireless networks and content delivery technologies are in use. Some of the wireless networks and client side applications are briefly explained in this appendix. Third appendix lists down some of the content delivery technologies and associated acronyms.

- Mobile applications
- Wireless networking infrastructure
- Client-side devices
- Mobile content delivery and middleware

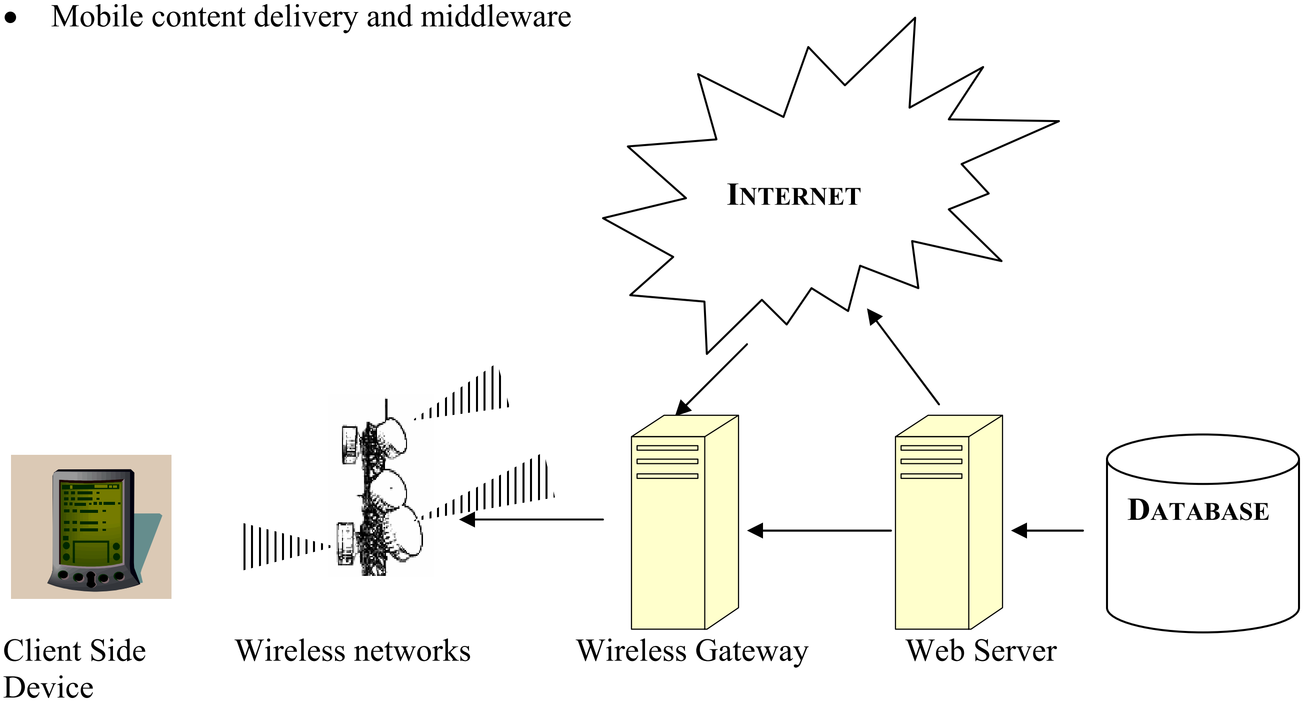


Figure 6: A Typical wireless system

I thank Scott Barber for suggesting me to include the schematic of the architecture of a wireless system and Dr. Kostanic, kostanic@fit.edu (Florida Tech) for providing me with some useful pictures. Above mentioned layers along with the technology in use for each layer are described in detail as follows:

MOBILE APPLICATIONS

Many of these mobile solutions are already in use in the vertical industry like Healthcare, Education and delivery services. Some of the commonly encountered mobile applications are

Mobile e-mail and PIM. Other applications that are in use and emerging are mobile financial applications like banking and stock trading applications, mobile advertising which is location specific, mobile entertainment services and games, mobile office products like Pocket Word/Excel, mobile education software, enterprise wireless data applications and mobile healthcare solutions. (Varshney, 2002)

WIRELESS NETWORKING INFRASTRUCTURE

Wireless Networks could be broadly divided into wide area network (WAN), Local area Network (LAN) and the personal area network (PAN) based on coverage.

WIDE AREA NETWORK (WAN)

Cellular Networks: This is the network with maximum coverage area. It is a licensed public wireless network used by Web cell phones and private radio frequency digital modems in handhelds. WAN cellular towers come in three different power configurations: macro cell, micro cell, and pico cell. There are two network architectures for the communicating devices: the circuit-switched and the packet-switched. A circuit-switched network builds up circuit for a call and establishes a dedicated connection of circuits between points. Examples of circuit-switched devices are the telephones, cellular phones, web phones and dial-up modems. In a packet-switched network, the IP-addressed data packets are routed between points on demand. Packet-switched networks exchange variable amounts of data or voice packets. Data can be transferred almost immediately as the network is always on. WAN could be then further subdivided into voice-oriented network and data oriented network. Some of the most widely used technologies for data transmission are GSM/GPRS, 1XRTT CDMA, and Edge etcetera. GPRS and EDGE overlay packet based air interface on the existing circuit-switched voice network. A new generation of wireless wide area technology known as 3G is deployed in Japan and Europe. It offers data speeds starting from 2Mbps in the fixed wireless environment, 384 Kbps at low mobility and 128 Kbps while moving in a car. 3G systems operate in 2GHz frequency band and are intended to provide a wide range of services including telephony, paging, messaging, Internet and broadband data.

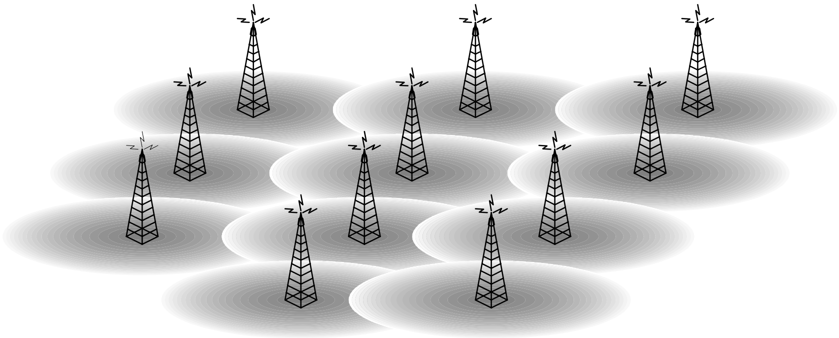


Figure 7: Cellular network

Paging network: Paging networks are of two types: one-way paging and two-way paging. They are the earliest form of networks used to send messages to mobile workers.

LOCAL AREA NETWORK

IEEE 802.11 family: These are the wireless local area networks operating in unlicensed spectrum. In 1997, the IEEE adopted IEEE Std. 802.11-1997, the first wireless LAN (WLAN) standard. This standard defines the media access control (MAC) and physical (PHY) layers for a LAN with wireless connectivity. It addresses local area networking where the connected devices communicate over the air to other devices. 802.11b working on 2.4 GHz spectrum has the physical layer data rate at 11Mbps. 802.11g, is a new IEEE standard for wireless LANs. It is backward compatible with 802.11. It can support 54Mbps raw data rate. The backward compatibility comes from the fact that it works in the same 2.4 GHz band and OFDM (Orthogonal Frequency division multiplexing) enables the high data transfer rate. Another standard of interest is 802.11a. More information is available at: http://www.wi-fi.org/OpenSection/index.asp?TID=1

HIPERLAN: In European countries the set of wireless network communication standards is known as HiperLAN. There are two specifications adopted by ETSI (European Telecommunications standards Institute), HiperLAN/1 and HiperLAN/2.

PERSONAL AREA NETWORK

Bluetooth: Bluetooth is a wireless technology used in the personal connectivity market by linking mobile computers, mobile phones, portable handheld devices, and connectivity to the Internet. It is a low power, personal, wireless voice and data network having a range of 10 meters. A Bluetooth network called Pico net can connect eight Bluetooth devices. It works in the 2.4 GHz frequency band and does not suffer from the interference by obstacles like a wall. It supports both point-to-point wireless connections without cables between mobile phones and personal computers, as well as point-to-multipoint connections to enable ad hoc local wireless networks (source: http://bluetooth.com/tech/works.asp).

Infrared: Infrared got standardized in 1994 with the publication of Infrared Data Association's standard. Infrared devices use line of sight, exchanging data by lining up their infrared lenses and have a typical range of 2 meters. They are mainly used to manually exchange information using point-to-point connection.

CLIENT-SIDE DEVICES

The first handheld computing device that acquired a significant market share was the Apple Newton. Since then, the handheld space has evolved to the point where there are literally thousands of different combinations of hardware devices, software capabilities and wireless networking features. These are some of the devices that are in use in the commercial, industrial and personal sectors.

Smart phones: They are cellular phones with the display hardware and software for the wireless Internet connectivity. They have a micro browser and some memory that is continuously being expanded. There are many different names for such phones depending on the technology used for the Internet services and information. In Japan it is known as imode phone; in Europe it's called a WAP phone, and in many places it is known as a web phone. (Beaulieu, 2002)

PDA: It is a miniature computer with special OS, storage, a keyboard or the soft input panel and a display. In general they have much more computing power than a smart phone. They again are called with different names like handheld, palm-top, communicator etcetera. There are two different kinds of handheld: the industrial and the consumer handheld (Beaulieu, 2002). The main difference is in the packaging. The PDAs used in the consumer market are mostly based on Palm OS, Microsoft Pocket PC OS and Blackberry OS. Some manufacturers of industrial handheld are: Symbol, Intermec, Itronix, Husky and others. The industrial handhelds mostly connect to the wireless LAN rather than WAN.

Pagers: A pager is a handheld wireless device that uses a paging network for data communication (Beaulieu, 2002). Pagers could be one-way, two-way or uplink. An uplink pager is used to transmit telemetry or location information, normally used for asset management. Pagers are more cost effective, time sensitive and have more battery life than a cell phone.

Appliances: iAppliances is the generic name for the class of devices with a specialized purpose and limited Internet or wireless data connectivity. Some examples of such devices are e-book readers, e-mail stations, Internet radios, et al.

The hybrids: Series of handheld compatible phones are rolled out. They could be called as the communication devices that could compute or the computing devices that can communicate. They can run high-level applications and still work as cellular phones. Java phones are the early devices in this category that delivers voice as well as data. Trend is towards development of a Swiss army knife kind of device that combines all the benefits of the above-mentioned devices into a single ideal handheld device. (Beaulieu, 2002)

MOBILE CONTENT DELIVERY AND MIDDLEWARE:

Numerous different technologies are available for content delivery and the supporting middleware. Some of these are listed in the third appendix. A more comprehensive glossary is available at http://www.devx.com/wireless/Door/11271, (last accessed August 19, 2003)

APPENDIX 3:

GLOSSARY OF MOBILE COMPUTING TERMS AND ACRONYMS

WAP / WML: Wireless markup language and Wireless Application protocol are closely tied. They are used to display information on narrowband wireless clients like cell phones and pagers. WML is used for creating web pages for handheld devices. WAP is the application communication protocol used to access services and information. A consortium consisting of Unwired Planet, Motorola, Ericsson, and Nokia was responsible for the creation of WAP and WML. More information can be obtained at http://www.wapforum.org/

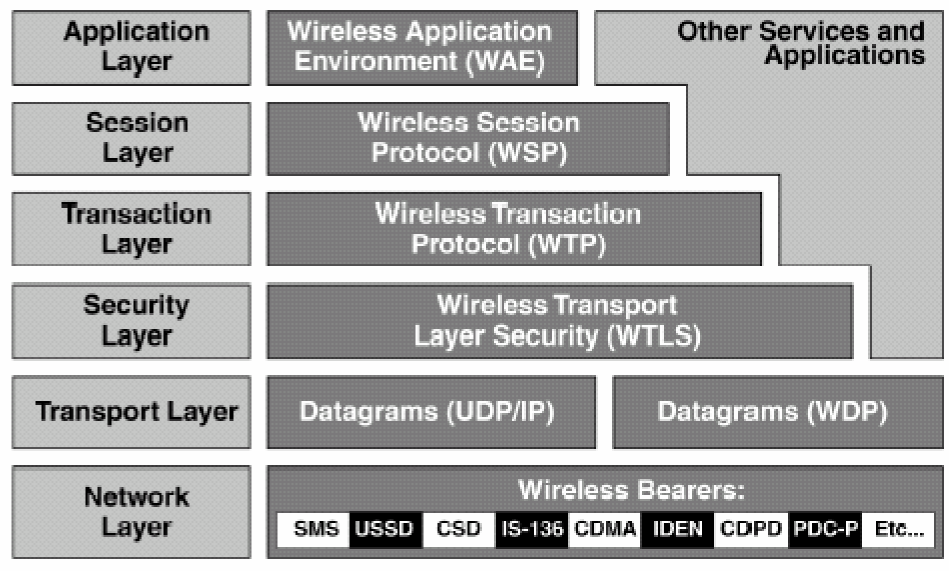


Figure 5. WAP protocol stack (WAPforum, 2000)

HDML: HDML stands for hand-held device markup language. HDML and HDTP, which is the accompanying protocol, were created by Unwired Planet in 1997. There was also a micro browser that was introduced called the "UP.browser" that runs on cell phones and similar devices.

cHTML: Compact HTML is a subset of HTML 2.0, 3.2 and 4.0. The goal of the language is quite similar to that of WML. The cHTML standard exists only as a W3C note rather than a well-established standard. Compact HTML strips down the normal HTML to the barebones making it suitable for narrowband and constrained devices. It uses normal HTTP for data transfer making it easier to serve up content for the handheld devices that support it.

VoiceXML: VoiceXML is an application of XML, so it possesses the same structure, restrictions and benefits of XML. It is designed for creating audio dialogues with human beings. It allows for a combination of synthesized speech and digitized audio (output from the server side), recognition of spoken and DTMF key input, and recording of spoken input. VoiceXML minimizes the client/server interactions by specifying multiple interactions per document. The major goal is to bring the advantages of web-based development and content delivery to interactive voice response applications.

Simplified HTML: This is a simplified version of HTML. PQA (Palm Query Application) uses a subset of HTML and is one of the main browsing languages in the Palm handheld market.

XHTML: XHTML is the replacement of HTML as the web browser language as recommended by W3C. XHTML 1.0 was a reformulation of HTML 4.01 in XML. XHTML Basic is defined as proper subset of XHTML for mobile application presentation including web phones. More information is available at http://www.w3.org/TR/xhtml-basic/

J2ME: Sun Microsystems offers a highly optimized runtime environment targetted towards the handheld devices having limited resources. J2ME provides some core APIs, classes and technologies for wireless programming. More information at is available at Sun Microsystems' website http://java.sun.com/j2me/

iMode: imode is wireless data service developed by CoCoMo. It is packet based as opposed to circuit switched voice systems. cHTML is used to write imode pages. More information is available at http://www.ai.mit.edu/people/hqm/imode/

SynchML: is a mobile data synchronization protocol that synchronizes data between a network / desktop and a mobile device. It offers support for a variety of transport protocols and applications thereby enhancing interoperability.

ACRONYMS

CDPD: Cellular Digital Packet Data

GPRS: General Packet Radio Service

PIM: Personal Information Management

B2B: Business to Business

B2C: Business to Customer

CDMA: Code Division Multiple Access

TDMA: Time Division Multiple Access

FDMA: Frequency Division Multiple Access

GPS: Global Positioning System

GSM: Global System for Mobile Communication

SMS: Short Message Service

MMS: Multimedia Message Service

OFDM: Orthogonal Frequency Division Multiplexing

WISP: Wireless Internet Service Provider

WTP: Wireless Transaction Protocol

IDEN: Integrated Digital Enhanced Network

REFERENCES

- Amland, Stahle (1999), “Risk-Based Testing and Metrics” *EuroSTAR99 Proceedings.*
- Bach, James (1999) “Heuristic Risk-Based Testing,” *Software Testing and Quality Engineering, 1* (6) 22-29, http://www.satisfice.com/articles/hrbt.pdf, last accessed July 20, 2003.
- Bach, James (2003a) “Heuristic Test Strategy Model”, http://www.satisfice.com/articles.shtml, last accessed 07/17/2003.
- Bach, James (2003b) “Troubleshooting Risk-Based Testing”, *Software Testing and Quality Engineering*, 5 (3), 28-33, http://www.satisfice.com/articles/rbt-trouble.pdf, last accessed July 20, 2003.
- Beaulieu, Mark (2002), *Wireless Internet: Applications and Architecture*, Addison-Wesley, 2002
- Bloom, B.S. (1956), *Taxonomy of Educational Objectives Handbook 1: Cognitive Domain,* New York: Longman, Green & Company
- Beizer, Boris (1990), *Software Testing Techniques* (2nd Ed.), Van Nostrand Reinhold.
- Biaz, Saad; and Vaidya, Nitin, H. (1997); “Tolerating Location Register Failures in Mobile Environments”, Technical Report 97-015, Computer Science, Texas A&M Univ., December 1997.
- Biaz, Saad; and Vaidya, Nitin, H. (1998); “Tolerating Visitor Location Register Failures in Mobile Environments”, 17th IEEE Symposium on Reliable Distributed Systems (SRDS'98), October 1998.
- Cao, G (2000), "Designing Efficient Fault-Tolerant Systems on Wireless Networks", Proc. of the Third IEEE Information Survivability Workshop (ISW-2000), October 2000.
- Center for Highly Interactive Computing in Education (2003a), home page, http://www.research.umich.edu/proposals/proposal_dev/UM_Resources/CHICE.html, last accessed July 21, 2003.
- Center for Highly Interactive Computing in Education (2003b), downloads page, http://www.handhelds.hice-dev.org/beta.php, last accessed July 21, 2003.
- Center for Highly Interactive Computing in Education (2003c), downloads page, http://www.handheld.hice-dev.org/beta/nb/Cells%20Quick%20Start.pdf, last accessed July 21, 2003.
- Chakravorty, R. and Pratt I. (2002), “Performance Issues with General Packet Radio Service (GPRS)”, Journal of Communications and Networks (JCN), pages 266-281, Vol. 4, No. 2, December 2002 (ISSN 1229-2370)
- Chalmers, D; Sloman, M (1999); “A Survey of Quality of Service in Mobile Computing Environments”, IEEE Communications Surveys, **2**(1) 1999

- Cheng, Stephen; Lai, Kevin; Baker, Mary (1999); "Analysis of HTTP/1.1 Performance on a Wireless Network", Technical Report: CSL-TR-99-778, Computer systems laboratory, http://mosquitonet.stanford.edu/index.html, last accessed August 10, 2003.
- Cisco (2003) *Cisco Documentation,* http://www.cisco.com/univercd/home/home.htm, last accessed July 22, 2003.
- Collard, Ross (2002); "Performance, Load and Stress Testing", Collard and Company, Version 4.4, April 2002.
- Collard, Ross (2003); "Techniques and Processes for Reliability Testing", International Conference On Software Testing Analysis & Review May 12-16, 2003 Orlando, FL
- Dreamtech software team (2002), *Programming for Embedded system: Cracking the code,* 2002, Wiley Publishing, Inc.
- GoKnow, Inc (2003a), home page, http://www.goknow.com, last accessed July 20, 2003.
- GoKnow, Inc (2003b), "PAAM™-Palm OS Artifact and Assessment Manager", http://paam.goknow.com/files/PAAMWalkthrough_021403.pdf, last accessed o7/21/2003
- Institute of Electrical and Electronics Engineers (1990); *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries;* New York, 1990.
- ISO 9126 (1991), *International Standard ISO/IEC 9126. Information technology — Software product evaluation — Quality characteristics and guidelines for their use*, International Organization for Standardization, International Electrotechnical Commission, Geneva, Switzerland.
- ISO 9241-11(1998), *Ergonomic requirements for office work with visual display terminals: Guidance on Usability*, (1998).
- Kaner, Cem; Bach, James; and Pettichord, Bret (2001), *Lessons Learned in Software Testing*, Wiley.
- Kaner, Cem (2001); Academic course notes for SWE-5410 at Florida Institute of Technology, Fall-2001, http://www.testingeducation.org/coursenotes, last accessed July 18, 2003.
- Kaner, Cem; Falk, Jack; Nguyen, Hung Quoc (1993), *Testing Computer Software* (2nd Ed.), Van Nostrand Reinhold (reprinted by John Wiley & Sons, 1999).
- Karygiannis, Tom; and Owens, Les (2002), "Wireless Network Security", NIST Special Publication 800-48, November 2002, http://www.csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf, last accessed August 10, 2003
- Ko Hai-Ping (1996), "Attacks on Cellular Systems," GTE Laboratories Incorporated, http://seclab.cs.ucdavis.edu/cmad/4-1996/pdfs/Ko.PDF, last accessed August 5, 2003.
- Malloy, Alisha D; Varshney, Upkar; and Snow, Anrew P (2002), "Supporting Mobile Commerce Applications Using Dependable Wireless Networks", Mobile Networks and Applications, 7, 225-234, 2002.

- National Institute of Science & Technology (NIST, 2000) "Project: Error, Fault and Failure Data Collection and Analysis", http://hissa.nist.gov/project/eff.html, last accessed July 22, 2003.
- Neilson, Jakob (1993); *Usability Engineering*, Academic Press, Inc, 1993.
- Nguyen, Hung, Q.; Johnson, Bob; and Hackett, Michael (2003), *Testing Applications on the Web* (2nd Ed), Wiley.
- Passani, Luca (2000) "Building 'Usable' WAP Applications", http://www.topxml.com/conference/wrox/ wireless_2000/lucatext.pdf,last accessed July 18, 2003.
- Pettichord, Bret (2002); "Design for Testability", Pacific Northwest Software Quality Conference, Portland, Oregon, October 2002.
- Sterbenz, James P. G.; Krishnan, Rajesh; Hain, Regina, Rosales; Jackson, Alden W.; Levin, David; Ramanathan, Ram; and John Zao (2002); "Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions", ACM *Workshop on Wireless Security (WiSe),* Atlanta, GA, USA, September 28, 2002.
- Swaminatha, Tara M; Elden Charles R (2003); *Wireless Security and Privacy,* Addison Wesley 2003.
- Texas Instruments (2003a), "Handheld Software Applications (Apps) for the TI-89 and Voyage™ 200," http://education.ti.com/us/product/tech/89/apps/appslist.html, last accessed July 21, 2003.
- Texas Instruments (2003b), "TI-Navigator: Classroom Learning System," http://education.ti.com/us/product/tech/navigator/features/features.html, last accessed July 21, 2003.
- Varshney, Upkar; and Vetter, Ron (2002), "Mobile Commerce: Framework, Applications and Networking Support", Mobile Networks and Applications 7, 185–198, 2002.
- Vijayaraghavan, Giridharan; and Kaner Cem (2002), "Bugs in Your Shopping Cart – A Taxonomy", 15th International Software Quality Conference, San Francisco, USA, September 2002.
- Vijayaraghavan, Giridharan (2003), "A Taxonomy of e-commerce Risks and Failures", M.Sc. thesis, submitted to Department of Computer science at Florida Institute of Technology, May 2003.
- WAPforum (2000), "Wireless Application Protocol, white paper," http://www.wapforum.org/what/WAP_white_pages.pdf, last accessed August 2, 2003.
- Yang, S. Jae; Nieh, Jason; Krishnappa, Shilpa; Mohla, Aparna; and Sajjadpour, Mahdi (2003), "Web Browsing Performance of Wireless Thin-Client Computing", Proceedings of the Twelfth International World Wide Web Conference (WWW 2003), Budapest, Hungary, May 20-24, 2003.