Design Talk: March 2010

Security-Critical Software Development Process and Tools

By John Greenland, VP Business Development, LDRA Technology, Inc.

Security now dominates the forefront of industries as varied as defense, finance, and energy, and transportation. Software developed for these markets must ensure that it meets new levels of assurance.

In adherence to the MILS (Multiple Independent Levels of Security) specification, software components are separated from each other to ensure that failure or breach of one component does not jeopardize the system. And, in complying with the Common Criteria for Information Technology Security Evaluation, software must prove that it meets specified security requirements and properties from the lowest levels of security (unclassified) to the highest (top secret).

The Common Criteria specifies that software must meet certain software development process requirements and adhere to a set of programming standards, software verification activities, and traceability from high- to low-level design requirements down to the resulting source and object code. Current software tools provide code analysis that enables programming standards compliance and detailed source code documentation by providing the following evaluations:

Structural coverage analysis—establishes a correlation between requirements that are tested and code structures exercised by the test to document that the code running on the host or target system meets stated requirements. It ensures that the code structure is verified to the correct security level and can confirm the absence of unintended functions. It also traces requirements through both source code (static analysis) and execution of object code (runtime analysis).

Control coupling—graphically represents the dependence of a software component on the components that call it or are called by it. This information can be mapped to the source code to demonstrate the control flow of code under test. This also illustrates the degree to which an identified control coupling is exercised at run time.

Data coupling—provides all instances a data item is accessed by a software component, tracking and reporting these instances across procedure and file boundaries, even when they are aliased as parameters to procedure calls. Dynamic data flow coverage indicates which data components are accessed at run time to provide an execution trace for a specific test data set.

Requirements traceability—proves the correctness of requirements-based development and verification by assuring that software requirements are properly

associated with the requisite test cases and can be traced from their highest level through the design to final implementation and deployment on the target system (Figure 1). Tool suites integrating requirements coverage with code review, data and control coupling and code coverage tools offer the best possible support for Common Criteria certification.

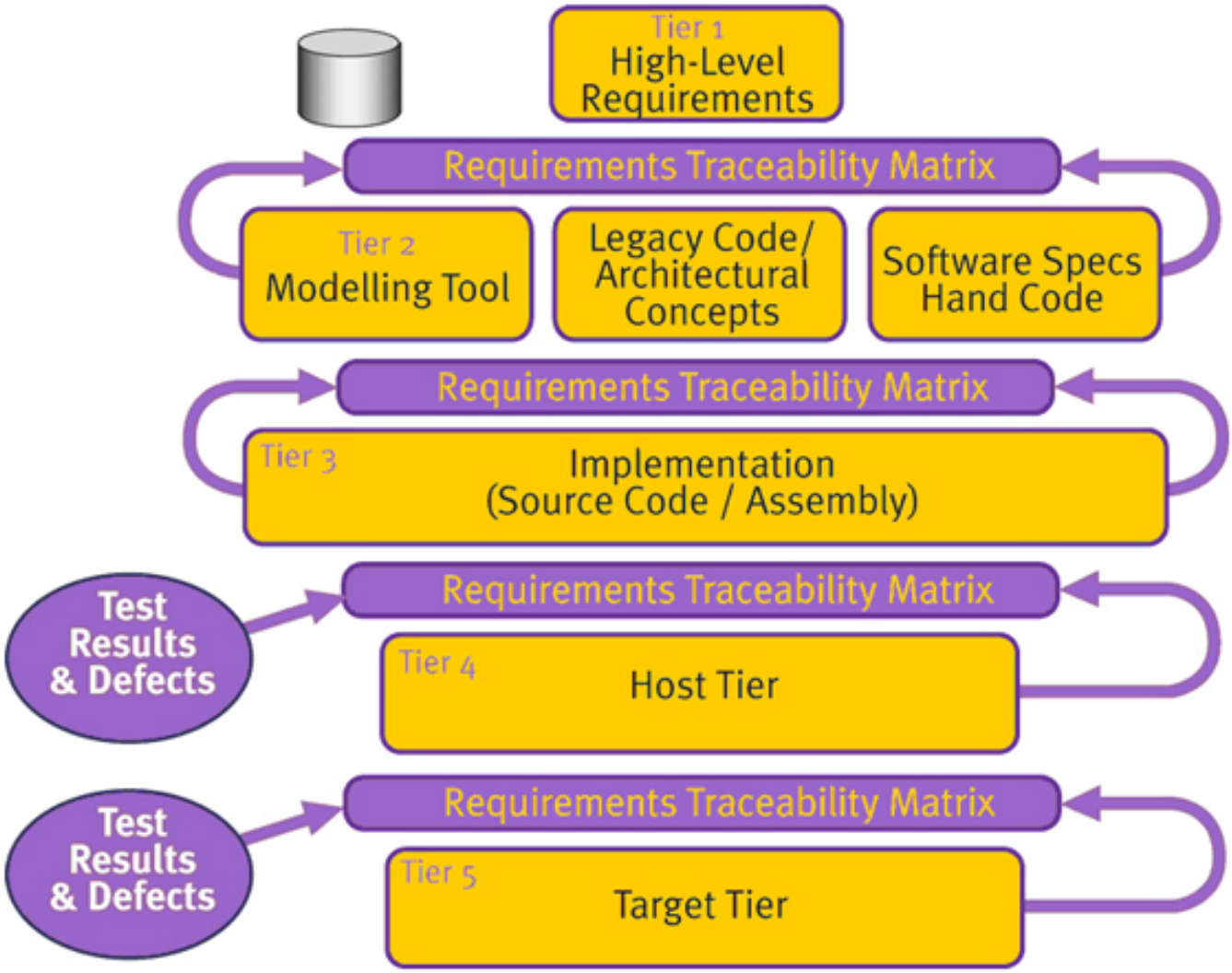

Figure 1: Requirements traceability model for security-critical systems

Testing and structural code coverage measurement—offers coverage metrics identifying code not executed at runtime. It quickly identifies missing or inadequate test data via textual and graphical reports.

Conclusion

Security-related development requires adherence to MILS and the Common Criteria processes. Automated tools offering static and dynamic analysis, test and requirements traceability ensure companies can meet certification measures without taxing resource requirements, excessive cost and schedule risk. Without leveraging these tools and processes, security-related development and verification is a much more onerous task.

John Greenland is currently serving as VP Business Development for LDRA

Technology, Inc., where he is responsible for certain sales areas, partnerships, and new market development. He possesses over 20 years experience in the embedded software development tools industry, working in various technical, sales, and marketing roles.

There's so much more to electronics design than the electronics

By Rob Evans, Technical Editor, Altium Limited, rob.evans@altium.com

At the fundamental and certainly traditional level, electronics design is about assembling and connecting electronic components together to achieve the intended, functional result. It’s a workable view that has loosely fitted the process of electronics design since its inception – even when you take into account the more ethereal concepts of embedded systems and software-defined functionality.

What’s significant about that conventional view of electronics product design is that it’s inherently centered on the elements inside the box. So the factors we consider when creating a product design that differentiates itself amongst others tend to be constrained inside that tight electronic sphere.

In practice we might seek a market advantage by making the circuitry perform faster, offer more features, or even implement new component technology that will lower the product’s street price. The tendency is, understandably, to offer new or improved product designs that are defined by an electronics-centric view.

But customers who might buy that product really don’t care about the unique way the electronics parts have been combined or how fiendishly clever the software is. What they increasingly care about is the unique and useful user experience a product delivers, outside the box. Today, this experience involves how a product interacts with the user and its own physical surroundings, what systems and networks it can interact with, and the beneficial services it can hook in to.

From the overall design perspective, creating that desirable customer experience is the really tricky bit, and involves much more than a traditional process of electronics design. Standing in the customer’s shoes, or applying design empathy, is one place to start. We need to create interfaces and connection systems that make sense to non-technical users, enclosure designs and user controls that work ergonomically. We need to avoid the response, “Oh dear, looks like this interface was designed by an engineer."

Perhaps above all though, we need to look beyond the device itself to create a whole customer experience that’s unique, valuable to the user and provides a sustainable point of differentiation in the market. That experience is increasingly being defined by externally connected systems, both within the user’s own environment (PCs and local networks) and to the wider internet structure (company servers and web-based services).

The connectivity benefits of this approach to product design are not just confined to

consumer products. Industrial, medical, military and automotive teams can all gain commercial advantage, and establish sustainable relationships with their customers, by thinking about design beyond the box of electronics hardware under development.

The value this adds to the user experience, and therefore a product's competitive advantage, is huge. And the future potential is even greater. Our designs also need to consider systems that support the rising demand for intelligent, interconnected electronic products that can independently operate in an internet-based device mesh – products that act as free nodes in the internet cloud.

Creating an electronic design that will operate in this ecosystem involves more than just the electronics that enable connectivity (the hardware and software layers). It requires the development of intelligent systems, within the product and at a company level, that deliver the functionality and user experience customers are seeking. But it also means expanding our view of electronic product design beyond the device itself, to one that encompasses all of the factors that define the next generation of electronic products.

Intellectual Property Protection

By Geoff Engelstein, President, GRT-Mars, Inc.

The classic concern about outsourcing is that you will wake up one morning to find out that counterfeit versions of your products are being sold by a shady offshore firm. The reality is that this scenario is extremely rare. Most off-shore manufacturers are focused on contract manufacturing and have no interest in destroying their reputation by engaging in this type of activity.

However there is a larger danger in protecting your intellectual assets that is much more commonplace, and while it is primarily an issue with overseas manufacturing it can affect domestic design and production as well. We see many companies that come to us wanting to shift production from their existing supplier for a variety of reasons, including quality, delivery, and cost. But they cannot give us a complete manufacturing-ready documentation package that allows for a rapid production shift. The documentation is controlled by the manufacturer or engineering firm that helped design the product. So they end up having to reverse engineer their own products, or just end up living with the deficiencies of their current supplier.

The documentation package for your products is the key intellectual asset of your company. It should be treated like the crown jewels of your organization. All too often key pieces of documentation are only held by outside designers or manufacturers, and companies get held hostage to price increases or delivery issues. And once in this position many are afraid to push their vendors to get copies of the documentation for fear that it will trigger the very situations they are trying to avoid.

Here are some guidelines about what information you need to have on your product:

Mechanical Components:

* Solid models of all parts
* 2D Drawings
* Material Information
* Tool Drawings

Electronics:

* Schematic
* Gerber Files
* Bill of Materials
* Component Data Sheets

Software:

* Hex Code
* Source Code
* Programming Instructions

Other Items:

* Artwork
* Bill of Materials
* Test Procedures and Fixtures
* Assembly Instructions and Fixtures
* Engineering Changes

Maintaining all of this information about your product will enable you to have peace of mind knowing that you can quickly and effectively change suppliers if there are pricing or quality issues. A quality design firm, consultant, or manufacturing partner will have no problems turning any of this information over to you at the conclusion of development or at production start-up, but it should be discussed as part of the negotiations and included in a final contract. If a programmer refuses to supply source code, or a design firm refuses to give the native CAD data it should set off some alarms.

Protecting this intellectual property is even more important today. Price pressures continue to force manufacturers to re-evaluate their supply strategies. It is imperative to the health of your business that you not be locked in with a particular supplier and to have the capability to smoothly transition to a new source.

Designing Multi-Touch Products That Are More User-Centric

By Guillaume Largillier, Stantum, www.stantum.com

With the fast-growing popularity of multi-touch functionality in a wide variety of consumer electronics and professional products, not enough attention is being paid to the actual needs of the end user. Product planners, designers, and third-party integrators of multi-touch technology need to strike the right balance between look-and-feel and usability – to find the right mixture of hardware and software; and, most importantly, to design their products for the user, not their own egos.

To respond to user needs, product developers must employ multi-touch technology that literally responds to the user – and even to multiple users. There are multi-touch technologies available today that allow on-screen collaboration, screen sharing and social computing. These touchscreen systems are easier and less costly to build than those that use capacitive multi-touch. Also, because the technology is force activated, it offers so much more user-centric functionality – working not just with fingers, as with capacitive multi-touch, but with all types of contact objects, including fingernails and styli; it even works with gloved or wet hands.

When one or multiple touches occur on such touch-panels, the top layer slightly bends, thus creating contact between the two layers right below the touches. The multi-touch controller chip detects the electrical contacts and determines the exact location of the touches.

The Stantum technology uses two thin and transparent (glass or plastic) overlays covered with conductive material. The material is patterned in rows on one side and columns on the other, transforming the layers into a matrix of conductive tracks. The two layers are assembled superposed, the conductive sides facing each other and separated by a spacing material (transparent dots, air, etc.). Touch contact modifies the electrical properties, and each axis (X, Y and Z pressure) can be

measured by the microcontroller. This can be done not just for one isolated touch but for an unlimited number of touches, and simultaneously. The technology reports any change of electric characteristics, using an exceptional acquisition frame rate that enables extremely fast response. Stantum has patented a unique controlling method and combined it with algorithms to detect and track an unlimited number of synchronic contacts.

Pressure sensitivity is another hallmark of Stantum's multi-touch technology. The pressure detection can differentiate three distinct levels of pressure – soft, medium and hard. Depending on how strong the user touches the screen, the device is able to react differently, which allows implementation of safer, more sophisticated interactions with devices such as mobile phones, gaming consoles, PCs, netbooks, MIDs, PDAs, and PNDs, and digital cameras.

Stantum's type of multi-touch technology is also suitable for products sold into Asian markets because of its precision and stylus input enabling handwriting recognition. Mobile gaming is also very high on the market application list since the unlimited inputs – all with X, Y and Z data streams and fast-response – enable so many new uses for software developers to invent cool and unique applications.

Stantum is the only provider of multi-touch technology that offers such advanced features while maintaining cost and power efficiency.