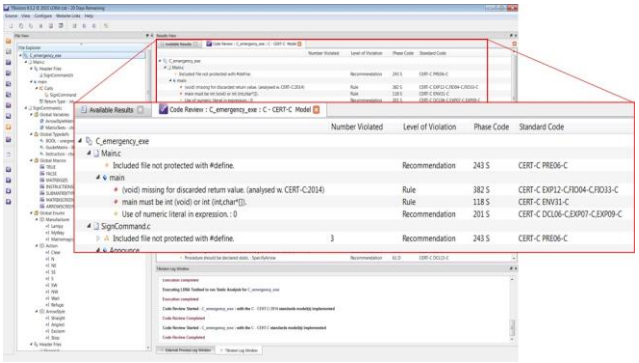
Media contacts:

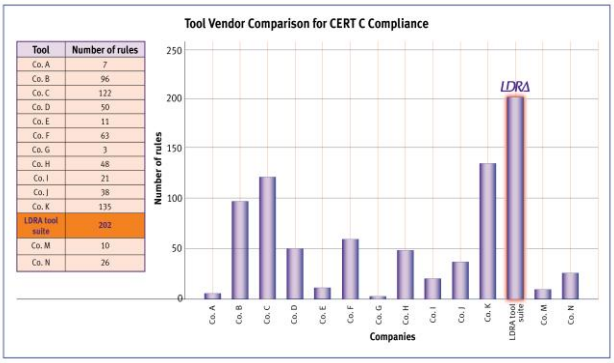
Janice Hughes, Hughes Communications, Inc., Media Relations
Mobile: +1 (705) 774-8686, Email: janice@hughescom.net

Mark James, LDRA, Marketing Manager
Tel: +44 (0)151 649 9300, Email: mark.james@ldra.com

This press release can be downloaded from www.hughescom.net.



Screenshot 1: The TBsecure module of the LDRA tool suite checks compliance for over 200 rules of the CERT C security standard.



Screenshot 2: LDRA's implementation of CERT C rules covers another 40% more rules than that of all the other tool vendors, evidence that the LDRA tool suite offers the most advanced security checker in the industry.

LDRA Tool Suite Features Industry's Most Advanced Code Checker for CERT C Compliance

LDRA TBsecure enables Internet of Things developers to easily find vulnerabilities that can lead to security exploits

Wirral, U.K. 7 October 2015 — LDRA, the leader in standards compliance, automated software verification, source code analysis and test tools, announced that its TBsecure module within the LDRA tool suite provides the industry's most comprehensive automated support for the Carnegie Mellon Software Engineering Institute (SEI) CERT C Secure Coding Standard. With checks for more than 200 CERT C rules, TBsecure helps developers identify more software safety and security vulnerabilities than any other static analysis tool available today. TBsecure specifically addresses the security concerns in the increasingly complex and growing Internet of Things (IoT) market.

With a more than 40-year track record for delivering automated code testing and software safety analysis products, LDRA's modular tool suite is used by IoT and other product developers who require early insight into potentially exploitable safety and security vulnerabilities in source code. The TBsecure module uses the most current CERT C secure coding rules to find software issues that could leave products and systems open to security attacks.

"As the number of IoT and other software-connected products in the world increases exponentially, so does the number of software security attacks. Just recently, for instance, a hack of Fiat Chrysler automobiles resulted in a recall of 1.4 million vehicles," said Ian Hennell, LDRA Operations Director. "To prevent financial losses and potential loss of life, software developers must take an automated approach to code quality improvement, fault detection, and other safety and security intelligence long before the product is manufactured and delivered to the marketplace."

Particularly well-suited for automotive, medical, and industrial IoT applications, the comprehensive checking of the LDRA tool suite delivers a commanding additional buffer over that of other code checkers on the market. With TBsecure, developers using the LDRA tool suite gain an unprecedented level of early insight into the types of coding anomalies that can expose complex products to security risks.

“The number and severity of attacks on mission-, business-, safety-, and security-critical systems has risen disproportionately with our increased dependency on these systems,” said Robert Seacord, a Principal Security Consultant with the NCC Group and author of *The CERT C Coding Standard* (Addison-Wesley 2014). “Studies indicate that a majority of vulnerabilities in these systems can be traced back to a relatively small set of common programming errors. *The CERT C Coding Standard* enumerates these programming errors so that software testing and analysis tools, such as the LDRA tool suite, can be used to discover these problems before they are deployed in production systems.”

Easy-to-Read Results
The LDRA TBsecure module, which plugs into the LDRA tool suite, shows code quality, fault detection, and avoidance measures through call graphs, flow graphs, and code review reports. Using TBsecure, managers, team workers, and developers can collectively monitor the implementation of safety and security metrics in their applications in an easy-to-read, intuitive format.

About the CERT C Standard
The CERT C Secure Coding Standard provides software development rules and recommendations designed to eliminate insecure coding practices and undefined behaviours that can lead to exploitable vulnerabilities. The application of the secure coding standard leads to higher quality systems that are more robust and more resistant to attack. Operating system and platform independent, the CERT Secure Coding Standards support popular coding languages including C, C++, and Java.

LDRA TBsecure supports a wide range of programming rules that can increase application security using the following classification of security issues:

- Dynamic Memory Allocation (A): Dynamic memory management is a common source of programming flaws that can lead to heap-buffer overflows, dangling pointers, double-free issues, and other security problems. In particular, dynamic memory management encompasses allocating memory, reading and writing to memory, and deallocating memory.

- Vulnerabilities (V): These rules are intended to eliminate insecure coding practices aside from those associated with dynamic memory. Examples of insecure coding practices include array indices out of range and dereferencing a null pointer.

Software Programming Standards Leadership
In addition to supporting the CERT C Secure Coding Standard, LDRA is a leader in programming standards enforcement and actively participates in the development of MISRA C:2012, MISRA C++:2008, and other industry standards.

Shipping and Availability
TBsecure is available now. For more information on how LDRA can assist with your CERT C Secure Coding Standard compliance, please visit www.ldra.com/cert. For general information on CERT C, please visit www.securecoding.cert.org.

Video Features
- Dr. Mike Hennell, LDRA’s Technical Director, outlines how developers can achieve safe and secure software – www.ldra.com/safety-security-video.
- TBsecure demo show how to gain compliance to the CERT C secure coding standard and identify programming errors behind software security attacks – www.ldra.com/cert-demo.

# # #

About LDRA

For more than forty years, LDRA has developed and driven the market for software that automates code analysis and software testing for safety-, mission-, security-, and business-critical markets. Working with clients to achieve early error identification and full compliance with industry standards, LDRA traces requirements through static and dynamic analysis to unit testing and verification for a wide variety of hardware and software platforms. Boasting a worldwide presence, LDRA is headquartered in the United Kingdom with subsidiaries in the United States and India coupled with an extensive distributor network. For more information on the LDRA tool suite, please visit www.ldra.com.

Please send reader enquiries to:

Mark James
Email: mark.james@ldra.com