Secure Automotive Software Development

Today, tomorrow, and into the future...

Presented by

Andrew Banks

Agenda

1. Safety and Security – the context...
2. The Past...
3. The Present...
4. The Near Future...
5. Looking Ahead...

LDRA Overview

Provider of Software Quality, Compliance Management & Testing Solutions

Established 1975

ISO 9001 certified company

Certified for use in safety related software development according to IEC 61508, EN 50128, ISO 26262, IEC 62304 & IEC 60880

Active participants in standards e.g. DO-178C, MISRA C/C++, CERT & ISO 26262

Offer MISRA C Training Courses delivered by the MISRA C or MISRA C++ Committee Chair Persons

CERTIFICATE NO FS/71/220/15/0105 PAGE 1/1

LICENCE HOLDER
LDRA LTD
PORTSIDE, MONKS FERRY,
WIRRAL, CH41 5LH,
UNITED KINGDOM

MANUFACTURING PLANT
LDRA LTD
PORTSIDE, MONKS FERRY,
WIRRAL, CH41 5LH,
UNITED KINGDOM

PROJECT NO-ID: K1C2-AU01
LICENSED TEST MARK
CERT. REPORT NO.: K1C20003

Tested according to:
IEC 61508:2010 Ed. 2.0
ISO 26262:2011
EN 50128:2011
IEC 60880:2006
IEC 62304:2006

Certified product(s):
LDRA tool suite
LDRAunit
LDRArules
LDRAcover
LDRAlite

Model(s): Version 9.5

Technical Data and Parameter:
Usable in development of safety related software acc. to:
- ISO 26262 up to ASIL D, TCL1 can be reached
- IEC 61508 up to SIL 4, class T2 tool
- EN 50128 up to SW-SIL 4, class T2 tool
- IEC 62304 up to SW safety Class C
- IEC 60880

Specific Requirements: The certificate is based on voluntarily tests. Any changes to the design, components or processing may require repetition of some parts of the qualification in order to retain the certification. The certificate report is an integral part of this certificate. The safety related application guidelines (refer to K1C20003) shall be maintained.

Certification Body for Functional Safety SGS-TÜV Saar GmbH
Munich, 04.11.2015
Gudrun Neumann

CERTIFICATE
No. Z10 16 09 84753 003

Holder of Certificate: LDRA Ltd.
Portside, Monks Ferry
Wirral
Merseyside CH41 5LH
UNITED KINGDOM

Factory(ies): 84753

Certification Mark:

Product: Software Tool for Safety Related Development

Model(s):
LDRA tool suite
LDRArules
LDRAcover
LDRAunit
LDRAlite

Parameters:
The certified tools, classified T2, fulfil the requirements for support tools according to IEC 61508-3 and EN 50128. The tools are qualified to be used in safety-related software development according to IEC 61508, EN 50128 and ISO 26262. It is suitably validated for use in safety-related development according to IEC 62304(ed.1)

The test report is a mandatory part of this certificate.

Tested according to:
IEC 61508-3(ed.2)
ISO 26262-8:2011
EN 50128:2011

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

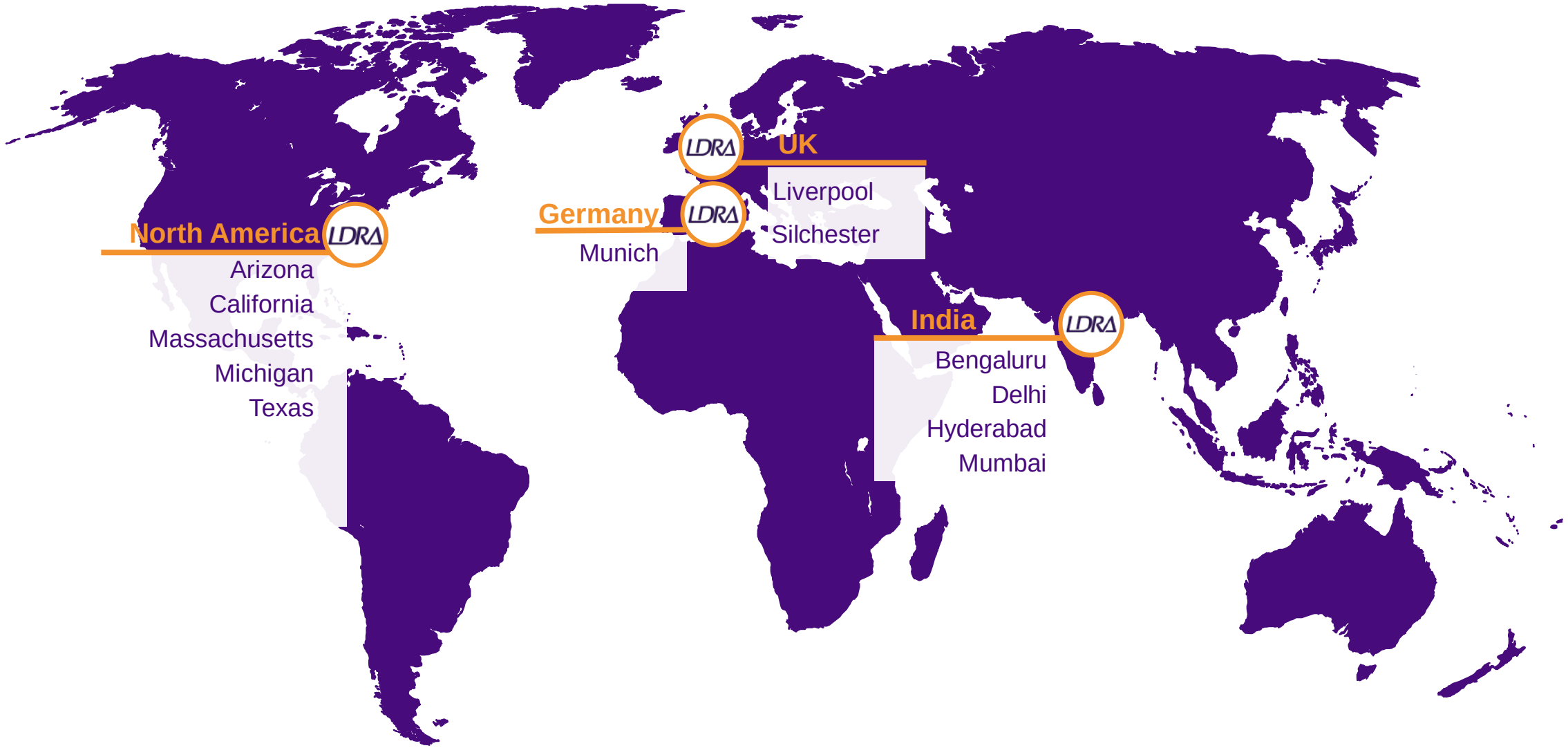
Test report no.: LW85043C
Valid until: 2021-10-03

Date, 2016-10-04
(Guido Neumann)
Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

ZERTIFIKAT ◆ CERTIFICATE ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

LDRA Office Locations



Experts in Safety and Security Critical Software

1

Safety & Security
... Design-In
... Not Bolt-On

E-Bike

Security

Safety

Netherlands Cycle Path

UK Cycle Path

You can’t “bolt on” safety or security:
You have to design it in!

How is Security Different to Safety?

- Which is the Safest?
- Which is the most Secure?

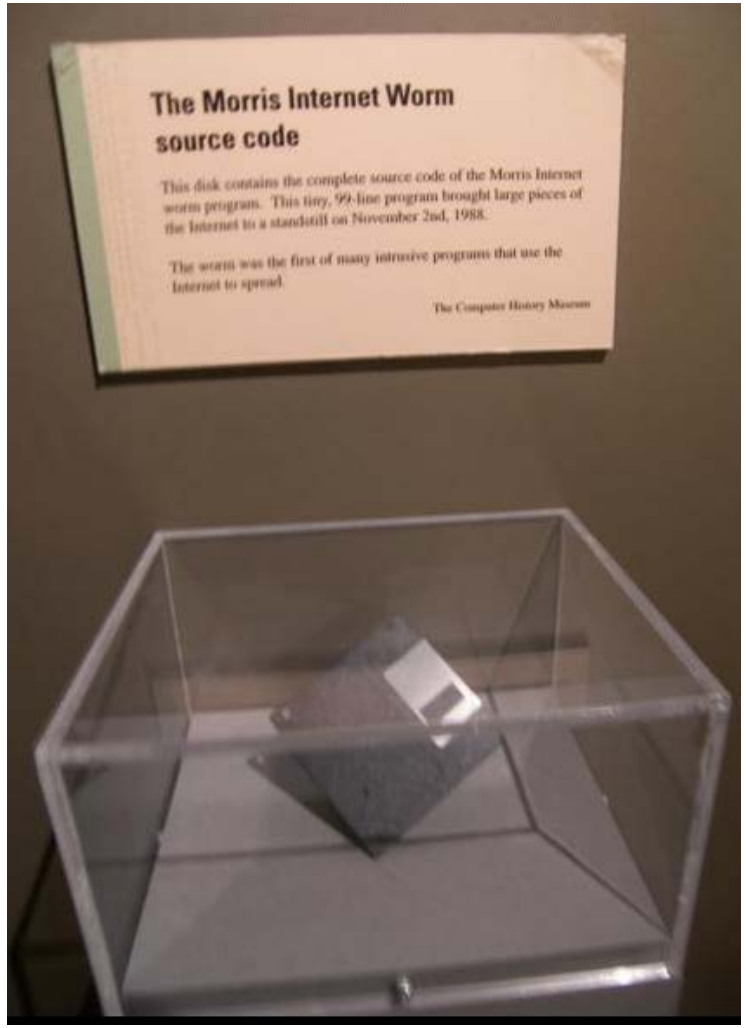
1962 Jaguar E-Type

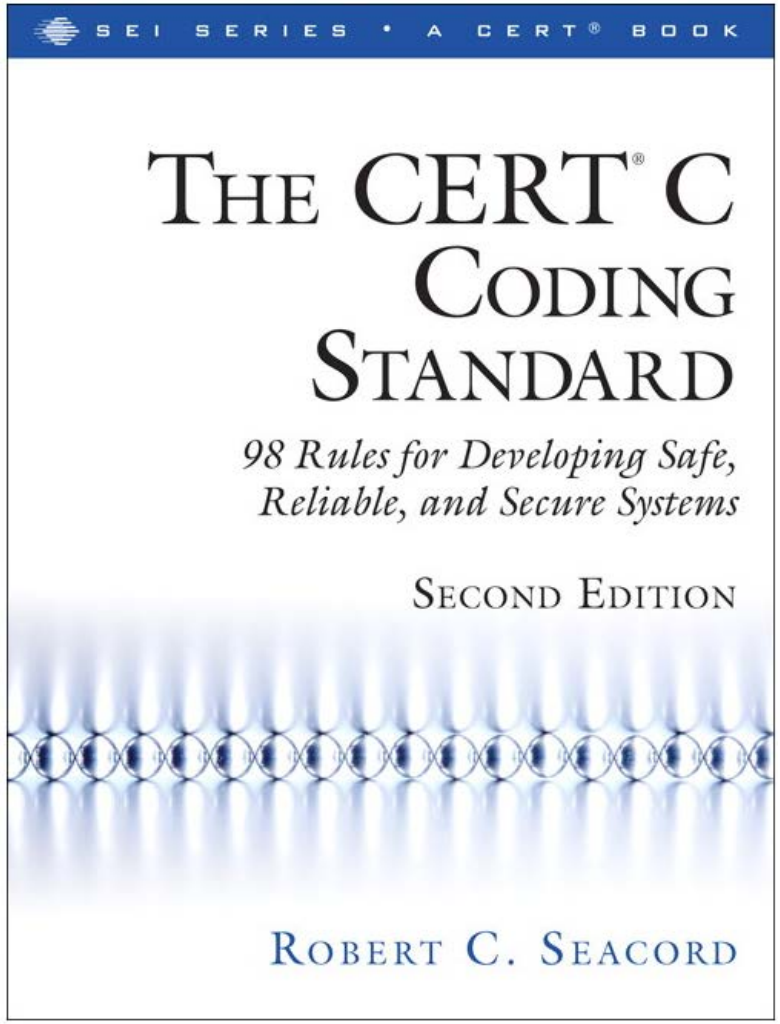
2018 Jaguar I-Pace

2

The Past

Computer **E**mergency **R**eadiness **T**eam



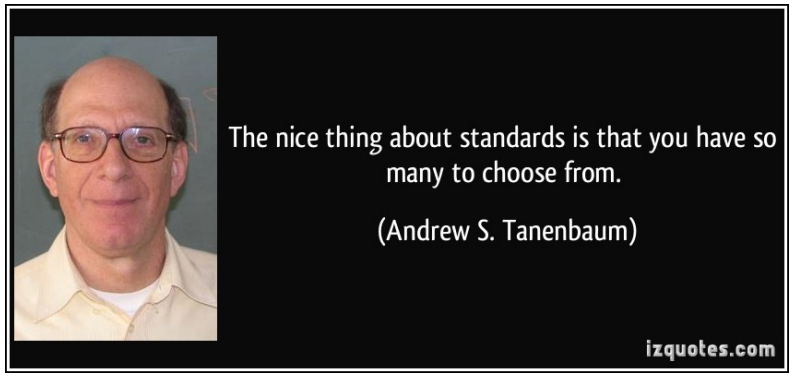


Security Standardization... The story so far

Information Security Management Systems

- 1995 BS 7799
- 2000 ISO/IEC 17799
- 2005 ISO/IEC 270xx
  ... now a family of 34 standards, totalling 46 parts
  ... With further development in the pipeline

- Derivative for Industrial Automation & Control Systems
- 2005 ANSI/ISA-99
- 2007 ANSI/ISA 62443
- 2011 IEC 62443



Eric Byers (May 2009)

What Makes a System Unsafe and Unreliable?

- A failure to contain communications in appropriate areas or sub-systems.
- Issues in one area can migrate to another area due to poor (or non-existent) separation strategy.
- Not Unusual… The North American Electrical Reliability Council (NERC) lists their #2 vulnerability in control systems as:

  "Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms"

- The solution is the use of ***security zones***.

https://www.slideshare.net/tofinosecurity/ansi-isa99andintrinsicallysecuresystemsmay2009101118152658phpapp01

The Changing Face of Safety-Critical Software

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

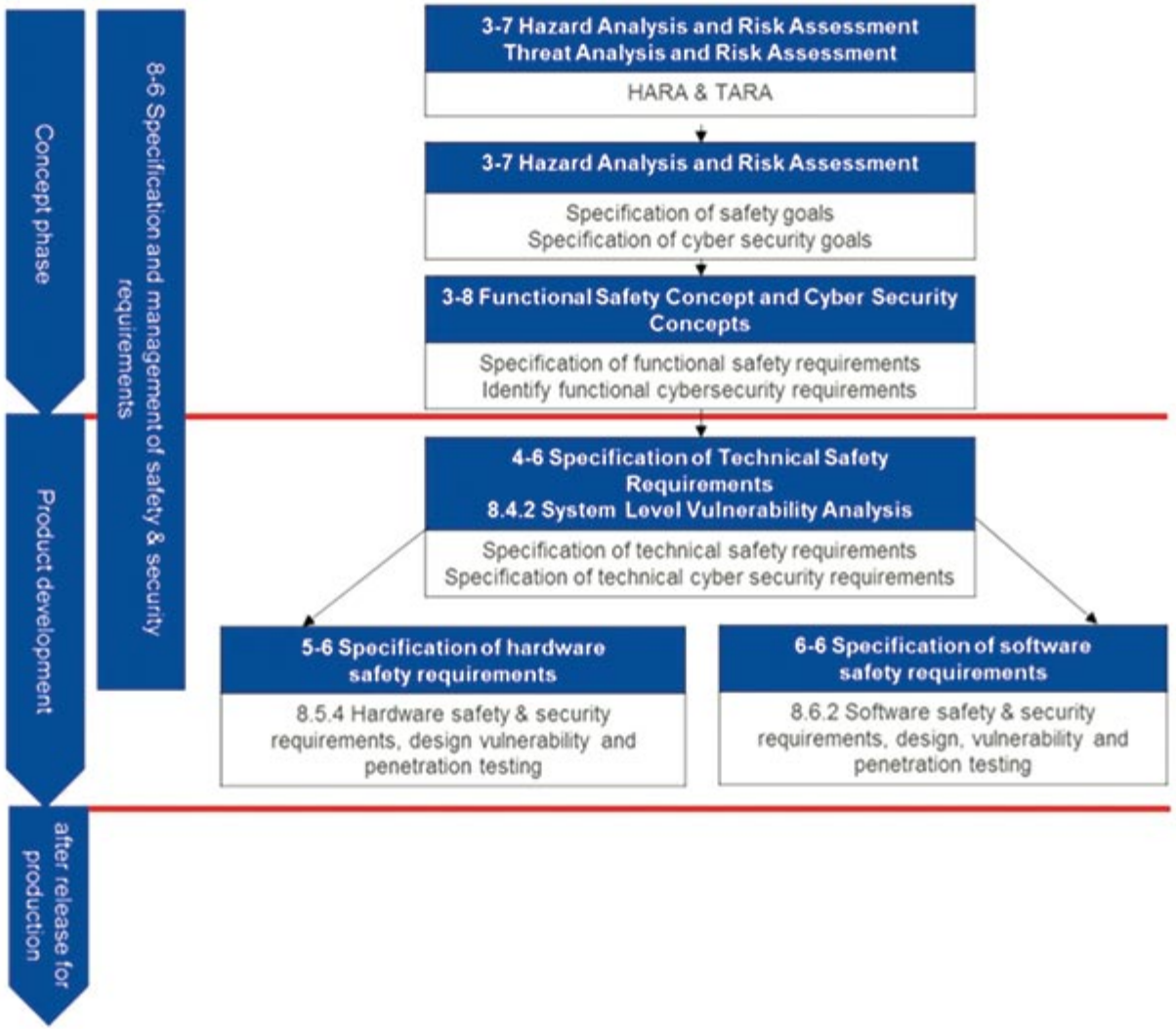
3

The Present

SAE J3061

- To provide a cybersecurity process framework and guidance to help organizations identify and assess cybersecurity threats and design cybersecurity into cyber-physical vehicle systems throughout the entire development lifecycle process.
  - Defines a complete lifecycle process framework that can be tailored and utilized within each organization’s development processes to incorporate cybersecurity into cyber-physical vehicle systems from concept phase through production, operation, service, and decommissioning.
  - Provides high-level guiding principles.
  - Provides information on existing tools and methods.
  - Provides the foundation for further standards development.

J3061 and ISO 26262



Applying SAE J3061 processes in tandem with ISO 26262's formal development environment.

Guiding Principles on Cybersecurity

- The guiding principles are tailored for cyber-physical vehicle systems, and taken from:
  - Cybersecurity from Microsoft's Security Development Lifecycle (SDL) guiding principles
  - IEEE's Avoiding the Top 10 Software Security Design Flaws

1. Know Your System's Cybersecurity Potential
2. Understand Key Cybersecurity Principles
3. Consider the Vehicle Owners' Use of the System
4. Implement Cybersecurity in Concept and Design Phases
5. Implement Cybersecurity in Development & Validation
6. Implement Cybersecurity in Incident Response
7. Cybersecurity Considerations When the Vehicle Owner Changes

BSI PAS 1885

The fundamental principles of automotive cyber security

Who is this PAS for?

- Vehicle manufacturers
- Tier-1 and Tier-2 supply chain suppliers
- Authorized service centres
- Aftermarket suppliers
- Road/highways authorities
- Service providers to both the vehicle and its occupants and/or cargo

It might also be informative for other stakeholders in the automotive supply chain and operators of automotive vehicles

4

The Near Future

ISO/SAE JWG + ISO/TC22/SC32/WG11

Introduction of ISO/TC22/SC32/WG11* Cybersecurity

Established by ISO/TC22/SC32 in October 2016

Scope of WG

Standardization of automotive cybersecurity, for functions and systems which include one or more E/E systems and which are at least partially installed in road vehicles. This work includes […]

Projects (as of September 2019)

ISO/SAE 21434 Road vehicles – Cybersecurity engineering (committee stage; DIS submission in 2019)

Collaboration

WG11 is ISO mirror group of the ISO/SAE Joint Working Group *Automotive Cybersecurity Engineering* who develops ISO/SAE 21434 as a joint ISO-SAE standard under PSDO agreement

Liaisons

- SC27/WGs 1,3,4 via ISO/TC22/SC32
- UNECE TF OTA/CS

(*) ISO/TC22 - Road vehicles
ISO/TC22/SC32 - Electrical and electronic components and general system aspects

ISO/SAE 21434 – Key Principles

1. Applicable to road-vehicles
2. Goal of reasonably secure vehicles and systems
3. Management activities for cybersecurity
4. Automakers and suppliers can use to show “due diligence”
5. Focus on automotive cybersecurity engineering
6. Based on current state-of-the-art for cybersecurity engineering
7. Risk-oriented approach
8. Cybersecurity activities/processes for all phases of vehicle lifecycle

ISO/SAE 21434 – Scope

Applicable to:

- The Road Vehicle
  - Its systems, sub-systems, and components
  - The software installed
- Its connection from the vehicle to any external device/network

- Is designed to be compatible with ISO 26262

ISO/SAE 21434 – Out of Scope

The Standard will **not**:

- ... prescribe specific cybersecurity technology or solutions

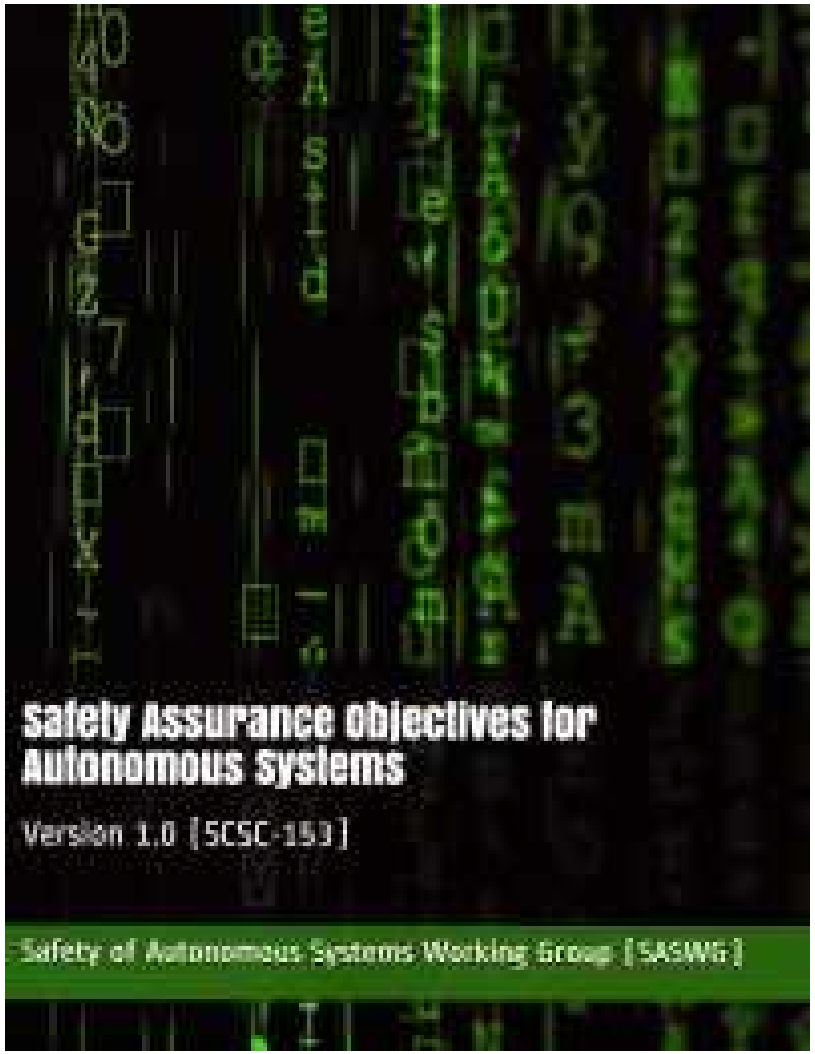
- ... include requirements on specific remediation methods
- ... include requirements for telecommunication systems

- ... specify requirements for the connected back-office
- ... specify requirements for electric vehicle chargers

- ... specify unique requirements for autonomous vehicles

What about autonomy?

- Many initiatives under way:
  - ISO/IEC
  - BSI
  - SCSC
  - etc etc

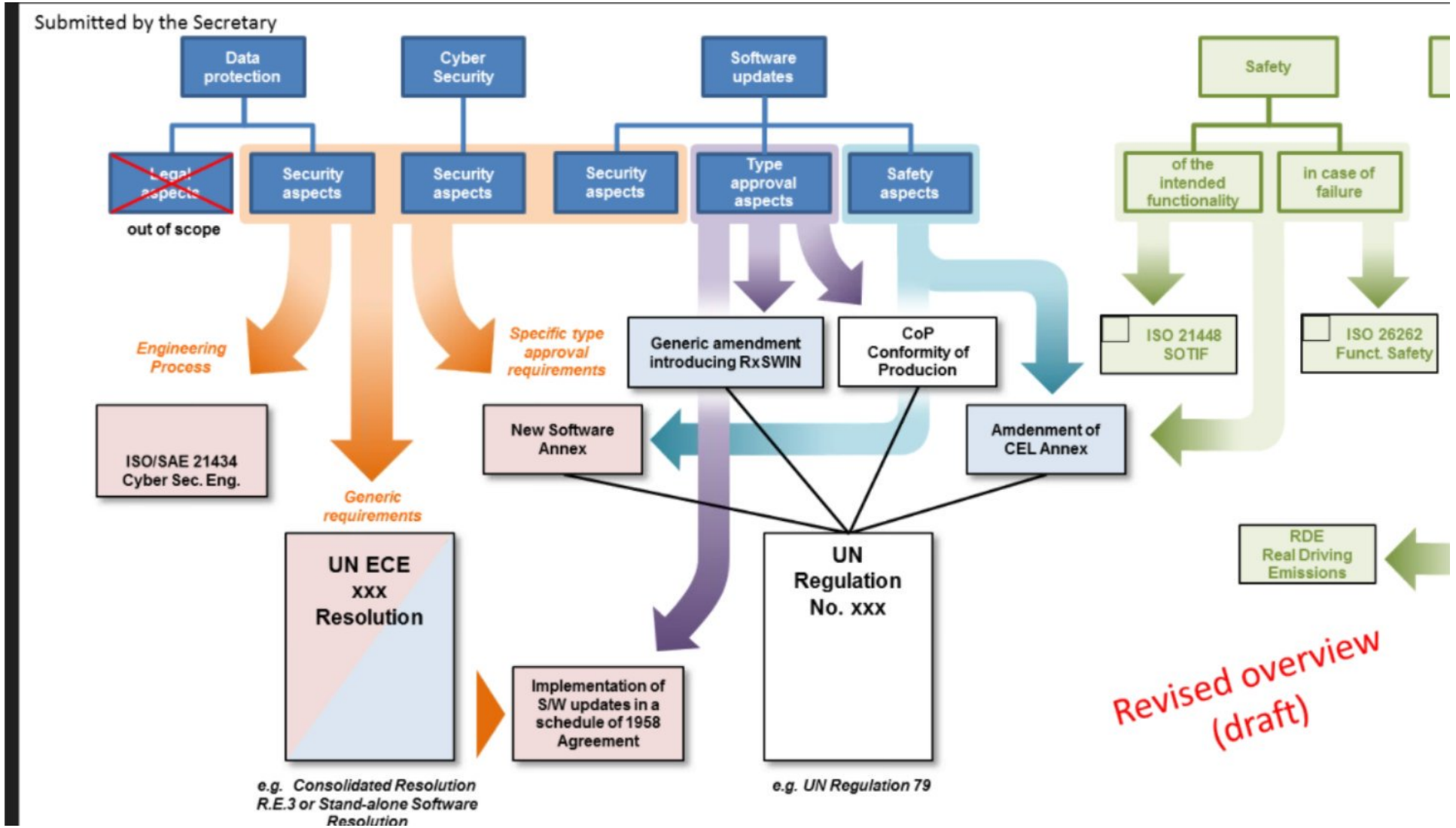


SCSC
FOR EVERYONE WORKING IN SYSTEM SAFETY

5

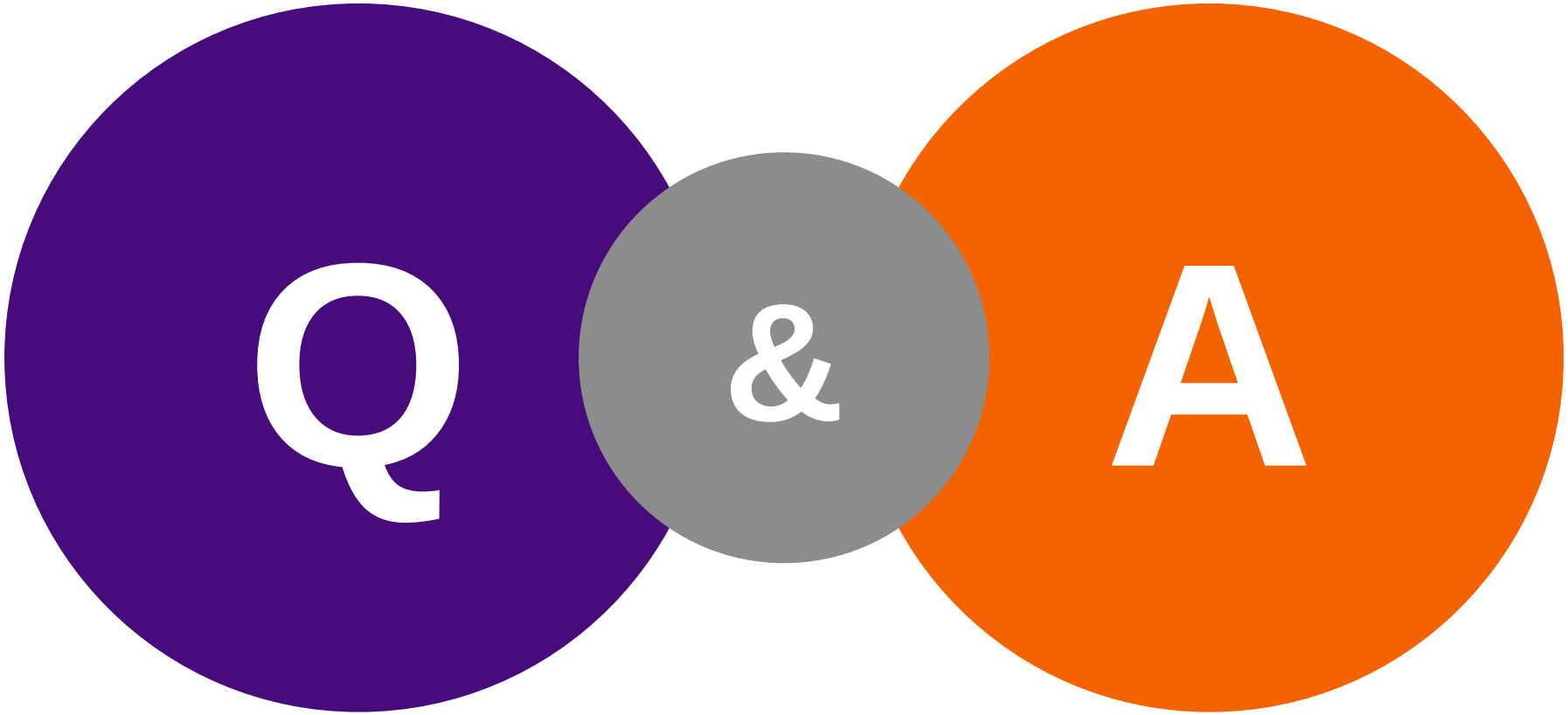
Looking Ahead

UN ECE Regulations?



Dr Hari Ramakrishnan providing us with an overview of the UNTaskForce on Cyber Security and Over the Air during the CAD Webinar on cybersecurity

Any Questions



Contact Us

Need more information?

LDRA.com

Linked in

info@ldra.com

About the Presenter

- Biography
  - Over 30 years experience in developing real-time embedded software systems, across a number of industries
  - Chartered Fellow of the British Computer Society
  - Member of the Institution of Engineering & Technology
- Standards
  - Chairman of MISRA C Working Group since June 2013...
    ... Working Group member since 2007
  - Chairman of the BSI Software Testing Working Group
    … contributor to ISO/IEC JTC1/SC7
  - Contributor to ISO 29119 “Software Testing”
  - Contributor to ISO 26262 2nd Edition “Functional Safety” etc

Andrew Banks
IEng MIET FBCS CITP

@AndrewBanks
AndrewBanks