

PMSafety Consultants Ltd.

Software Assurance

“The assessment of software components of a system.”

SOFTWARE ASSURANCE



PMSC Limited provides Systems Assurance advice to a wide range of customers both in the UK and Internationally.

SOFTWARE INTEGRITY LEVELS



We employ various Systems Assurance tools and techniques to be able to quantify risks to critical exposed groups. We assess both hardware and software components of a system. Hence, Software Assurance is an increasingly important part of our capability.

IEC 61508 & 61509



Currently, we use several guiding standards such as IEC61508 for generic rail systems and IEC61509 for process industries & EN50128 for Railway Signalling and Control applications. We also use the various software assurance testing techniques and the guiding standards issued by MISRA for the use of C. We have identified and utilised automatic testing tools for C and C+ and have carried out detailed assurance evaluations on the use of Teamwork's and other design configuration systems

EN50126 & EN50128



BLACK BOX/ WHITE BOX TESTING



Software Safety Integrity assurance or SIL assessment is part of our core skills base.

CODE WRITING STANDARDS



We have recently completed SIL assessments for SIL 0,1,2,3 and 4 systems involving detailed consideration on the IEC standards and guidance. PMSC has also developed Software Development Assurance Plans including practical advice on both code writing standards and complexity metrics.

For further information on PMSC and our assurance services please either visit our web site or call our office for an informal discussion.



PM Safety Consultants Limited
www.pmsafety.co.uk

PMSC Ltd. Suite D, Third Floor, Saturn Business Facility, 101 Lockhurst Lane,
Coventry, Warwickshire CV6 5SF
Tel: +44(0)2476 665770
Email: office@pmsafety.co.uk

Fax: +44(0)2476 582410
Website: www.pmsafety.co.uk



PMSafety Consultants Ltd.

Software Assurance

Software Assurance Work Undertaken by PMSC

NEC SINGAPORE

PMSC assisted with the assurance submissions to Singapore Land Transport Authority for a SIL 2 communications system. This involved review and advice on the software development and testing program. Including:-

- Generation of a Software Development Assurance Plan which achieved SIL 2 software for an onboard train controller system.
- Review and selection of a software static and dynamic analysis tool (Logiscope was selected)
- Generation of software development coding standard (using a restricted C language subset taken from MISRA)
- Review of test cases and generation of additional test cases to follow the methods specified from IEC 61508
- Review of static and dynamic tool results and generation of additional test cases to increase test coverage and to determine required coding changes
- Liaison with the Independent Software Verifier and authorities during development of the Software Development Assurance Plan and throughout the software project to address their comments and produced the Software Development Compliance report demonstrating the method of compliance with SIL 2 requirements

NEC SINGAPORE

PMSC reviewed the TETRA Radio System after a disagreement between the customer and the system supplier. After more detailed analysis including a Software HAZOP the software in the TETRA system was assessed as SIL 0.

TSC CONSORTIUM (KAWASAKI, TOSHIBA & MITSUBISHI)

PMSC assisted during Concept and Preliminary Design with the assignment of Software Integrity Levels for over 50 railway systems with software components. This included Rolling Stock, communications, Signalling and Wayside Equipment. The assignment was according to IEC 61508 and was undertaken in parallel with the HAZOP's.



PM Safety Consultants Limited
www.pmsafety.co.uk

PMSC Ltd. Suite D, Third Floor, Saturn Business Facility, 101 Lockhurst Lane,
Coventry, Warwickshire CV6 5SF
Tel: +44(0)2476 665770
Email: office@pmsafety.co.uk

Fax: +44(0)2476 582410
Website: www.pmsafety.co.uk