

## ITT2B -Scenario: High Integrity Software Based Systems

### Question

#### Background:

High Integrity Software (as part of a system) is characterised as being :

- A critical function (or complex set of interacting functions that when combined deliver critical functionality)
- Dependable; specifically meeting high-performance demands in one or more aspects of safety, availability, security, and demand.
- Where high impact results from a failure to meet the requisite dependability requirements
- Developed to a high level of quality, to minimise unforeseen emergent properties and facilitate longevity.

The software competence and capability associated with these characteristics are:

- Understanding of the whole-system solution, including requirements, environment, people factors and how the end-system (of which the software is a part) delivers what is needed of it.
- Experience of specification, design, development, testing, delivery, migration and acceptance of high-integrity systems in transport (especially railway) or similar domains.
- Experience of developing or working under a quality management system specifically designed to support the delivery of high integrity software.

The activities associated with the delivery of High Integrity software/systems vary (largely on the basis of Life-Cycle) and include:

1. The specification and design of a high-integrity software-intensive system from a set of business requirements.
2. The planning and management of bringing in to service high-integrity software including the necessary controls, measurements and reporting (including specification of KPIs). Identification or development of the software management quality processes to be used.
3. The design and construction of subsystems, products, and associated software coding, testing and assurance to an agreed level of quality.
4. The review, audit, checking and reporting of the application of the quality processes and outcomes. Provision of an independent perspective (cf ISA or ISwA) with respect to the attainment of the dependability requirements of products, subsystems or systems of which the software is an integral part.

TfL is a user of high integrity software and the associated services described above. We wish to establish your understanding of this subject area from the viewpoints of three parts of the supply chain:

- Development of software code, and the management and controls of the developing software, including product-level assurance.

- Integration of a number of products and subsystems to provide controls and assurance that the developed or procured products (including 3<sup>rd</sup> party) or subsystems deliver a high-integrity system that meets all the requirements and the emerging properties are managed.
- Providing authoritative independent review of the software quality and/or development process.

### **Response Required :**

In no more than 2000 words contained in a maximum of 5 sides of A4 (pictures, diagrams etc. may be included in the sides of A4 limit) state your capability and understanding in relation to the above domains by responding to all three questions below. Examples should be provided where appropriate.

### **Viewpoint 1: High-Integrity Software Developer**

Describe how a Software Developer would develop and deliver high-integrity products or subsystems into operational service. Describe the quality and software management processes that would be used. State how the developer would demonstrate process maturity. Describe how the design and specification process would be quality assured. Explain how client requirements would be managed in relation to generic products and how the quality of all products is subsequently maintained. Describe the testing and validation process to be used and how assurance of quality of the end-product is provided. State how software would be migrated, delivered and maintained over the lifetime of the product and specific applications.

Describe how the delivery as a whole would be demonstrated to be credible, including what is controlled through a Software Development Plan and a Software Management Plan (or equivalents).

### **Viewpoint 2: High-Integrity Software Systems Integrator**

Describe how a System Integrator of High Integrity Software Systems would deliver high-integrity systems that rely on a number of components, some of which themselves constitute high-integrity software sub-subsystems.

Explain how the environmental factors (including application, interfaces and people) would be considered and their impacts understood and managed.

Describe the approach that would be taken to ensure the delivery as a whole is credible, including development of an integrated set of Software Development Plans and Software Management Plans. Explain the process of integration and integration testing to ensure the system as a whole delivers the requisite quality. Describe the processes to be adopted for integrated fault resolution and performance management across multiple suppliers (including internal, 3<sup>rd</sup> party and client organisations).

### **Viewpoint 3: Independent reviewer**

Describe how an Independent Reviewer would undertake independent assessments or assurance of high-integrity software-intensive products, subsystems or systems as elements of a major project or programme. Describe how the criticality of the systems would be assessed and the response to the potential impacts of deficiency, and the measures that are taken to mitigate their occurrence.

Describe what an Independent Reviewer would do over the design, development, test and delivery phases of the system/software lifecycle. Explain how coverage of specialist knowledge from the client organisation or 3<sup>rd</sup> party organisations would be applied to ensure the overall quality of output, whilst maintaining the reviewer's independence. Explain how difficult issues could be managed such as disagreements with developers over classification of severity of observations or imperatives to accept due to schedule pressures.