PRELIMINARY SPECIFICATIONS RFID SOLUTION

IO/CFN/14/11075/WDT

SCOPE OF WORK

The ITER organization seeks to make use of an RFID/RTLS solution to manage parts sourced globally for a sizeable multi-year construction/installation at a single site in Cadarache, France. Post completion use of the RFID/RTLS solution is also wished for in terms of installed parts and spares identification and condition monitoring. ITER seeks the supply and maintenance support of a quality solution including hardware, software/middleware (interfaces and operator system management tools including service status monitoring), planned preventative maintenance and non-planned service intervention.

The Project's intent is that the RFID/RTLS solution yields value through informing and guiding ITER's operators who are predominantly own staff or on-site contractors via the established material management software Smart Plant Materials from Intergraph. ITER's suppliers will apply RFID/RTLS devices and may access the ITER's system to verify that the correct association of transponder to item has been made (TBC), but it is not yet certain that this will require the ITER's suppliers to do anything more than reading the RFID/RTLS device's bar code, or manually entering the device's serial number and capturing the part's identifier via bar code or manual entry of the information found on the part or part's label. Additionally as well as yielding information of direct value to ITER's processes the RFID/RTLS solution must provide all RFID/RTLS system management tools for principle use by ITER's staff.

This RFID/RTLS solution needs to be scalable from the outset. This is because the RFID/RTLS solution used from the start of the first Pilot is expected to be in daily use over a period of 5 to 10 years without the need to accommodate multiple incompatible devices and support each of their unique interfaces. Scalability also means providing capability to reliably and efficiently address increased volumes of RFID/RTLS transponders, event capture, processing of data, etc.. Adapting to an increasingly wider scope of functionalities and, maintaining sufficient user support are other essential requirements. The approach of progressive steps to full implementation is not designed to test several RFID/RTLS technologies. The approach efficiently ramps-up only one RFID/RTLS solution which will be in operation for ten years or more from 2014.

Functional Requirements Overview

ITER's key priority objectives are to positively identify and locate parts efficiently in order to diminish delay risks to the installation plan. Location within this project refers to ITER defined zones at their site in St Paul lez Durance, Bouches Du Rhone, France. The identification priority is verification of inventory status as some parts may both enter and leave the site several times before they are installed. These priorities also extend to monitoring parameters which indicate that the part may need inspection, further specific processing or replacement.

Part location

Location resolution is an important consideration. Location predominantly refers to 2D ground level areas, even if there is both planned and anticipated use of vertical storage solutions both outside and inside. The ITER zones at their site range in size, shape and, nature and refer to areas both indoor and outdoor. ITER zones provide the ability for the logistics team through use of INTERGRAPH Material Management System SPMat to reliably plan and execute the movement of material arriving and departing the site and, being relocated around the site. Another consideration is that some zones will be temporary and others ad-hoc depending upon the nature of the parts and the site's construction and installation schedules.

Future indoor warehousing will include significantly sized provision of condition controlled storage e.g. temperature and humidity. Once installation is complete temporary and ad-hoc zones should largely have been eliminated.

Part identification

Identification while essential to gaining value from location capture is also necessary in terms of overall inventory visibility. It is of critical importance that the RFID/RTLS solution reliably identifies a wide variety of ITER parts such as piping and spools material, electrical drums, metallic structure, bulk material…

Part level sensing

In order to track Safety Issue Components, it is ITER's intent to benefit from RFID/RTLS solutions to monitor and measure a variety of parameters depending upon the part, while the part is being shipped and, on site at ITER site and while the part is being processed off-site by ITER sub contractors. The sensor generated data is to be transferred to SPMat through use of the RFID/RTLS interrogator system installed at ITER. This communication is only expected when the RFID/RTLS sensor transponder returns to ITER and NOT real time during transportation.

Interfaces

The RFID/RTLS solution comprises of a number of elements centred upon the objective of assisting identify, locate and sense parts they are attached to and associated with. The logistics software SPMat from Intergraph © is the principle human interface for information related to parts. Interfaces to SPMat and middleware/software are envisaged to be a part of the RFID/RTLS solution. A part of the middleware/software includes the processing and storage of information which SPMat is not adapted for and this will include some user interfaces, especially those related to RFID/RTLS system management. It may also extend to providing user interfaces for sensor historical data queries, detailed part movement analysis, etc., exploiting the granularity of information available within the RFID/RTLS solution which SPMat may not be suitably adapted to accommodate.

Intergraph, supplier to ITER of SPMat software, has committed to providing resources to develop SPMat interfaces with the RFID/RTLS solution and, SPMat functionalities which will exploit elements of data provided by the RFID/RTLS solution. Intergraph will support the RFID/RTLS solution provider's own interface developments and tests by providing information about SPMat.

It is expected that the provider and Intergraph will agree on a file exchange system and both parties will design and program the output/input data from their software to the exchange file(s)

Services

Apart from hardware and software, services are a major component of the RFID/RTLS solution. Services include the installation, maintenance and support of hardware. It also extends to the installation, maintenance and support of software which is anticipated to encompass some development and testing, especially with respect to interfaces with SPMat. Services also encompass the management of the RFID/RTLS transponders and sensors including transponder validation and the dispatch to ITER suppliers internationally.

It will also be required that the provider will come on site in St Paul lez Durance in order to apply transponder to the parts at the 1st shipment arrival and help ITER personal/contractor with the association.

Standards and regulations

ITER acknowledge that there are many international standards and regulations which exist and have influence over RFID/RTLS systems. ITER does encourage mention within their tender submission of all such details and any other references which indicate that the solution offered includes proven components. The RFID/RTLS solution provider will be totally responsible for the RFID/RTLS solutions regulatory compliance both upon delivery to ITER and throughout the solutions lifetime. It is ITER's intention that the RFID/RTLS solution provider will be the principle operator.

Technical Requirements Overview

Conformance

Legislative requirements from the perspective of regulations are an important matter. It is imperative that the RFID/RTLS solution conforms to all international regulatory requirements enabling the transponders to be in operable state in all countries, being both ITER supplier and intermediary transit countries. Maintaining conformance to regulations is a matter for the RFID/RTLS to take full solution life-time responsibility for. Interrogator regulatory compliance requirement for this Project is considered to be France only[1]. Electronic copies of all device regulatory compliance certificates must be provided to ITER.

While conformance standards are not a specific requirement all information related to conformance standards to which offered solution devices have received test certifications should be provided to ITER by way of background supporting information.

Interoperability

Interoperability between RFID/RTLS devices and the overall solution is the responsibility of the RFID/RTLS solution provider.

The solution communications connections with ITER communications infrastructure must comply with ITER device interfaces, configuration and security requirements. Solution interfaces with SPMat is a shared responsibility. There are no specific or essential predefined interoperability standards to conform to.

Performance Criteria

Principle performance criteria of RFID/RTLS systems are:

Read distance.

- During the Pilot the focus is upon ensuring that transponders can be identified and located at the ITER site at site entrances, goods receipt and storage areas.

- Read distances include the transfer of sensor data.

Write distance.

- With the possible exception of sensors there are no write operations. Therefore write distances from interrogator to transponder are ignored. Nevertheless such information is of interest to ITER and should be provided by way of background supporting information.

[1] This must extend to include other countries where the RFID/RTLS solution provider offer involves the supply of interrogators to ITER suppliers. Such elaborate solutions are not particularly encouraged but ITER remains open to all proven concepts meeting ITER's requirements.

Air interface data exchange rates.

- Although the intent is to minimise data transfer the quantity of ITER parts with transponders and ITER parts with sensors within the RFID/RTLS system/device read area/zone may during the roll-out phase place a significant demands upon the air interface data exchange rates. Therefore high data exchange rates (of unique transponder communications) are sought to offer a tolerance or margin with the objective of ensuring that all parts and their locations are captured reliably.

- Air interface performance should be stated in terms of unique transponder read events (transponder ID only) per second. Also separately the air interface should be described in terms of the transfer of sensor data performance.

Location.

- The resolution of the overall process must ensure that the highest accuracy between the part's real location and that indicated within SPMat.

  - 95% of parts must be indicated in a zone which matches their physical location.

  - The remaining 5% must be indicated in a zone adjacent to the zone where they are physically located. Allowing for parts located on the boundary of a zone.

  - The RFID/RTLS system should provide location resolution within 1 metre of the parts physical location.

  - There must be no false reads no notification of wrong locations.

- The location must be verified and updated daily within SPMat.

- Location verification and updates should take a minimum of human intervention.

Sensors.

- The calibration process where applicable must be suitably aligned with ITER's measurement requirements in terms of range, sensitivity and tolerance. The calibration process must be recorded and offer full traceability to ITER and the RFID/RTLS solution provider.

Reliability.

- Component. The selection of RFID/RTLS solution components (devices, interfaces, etc.) must be matched with the overall solution reliability requirements. The solution provider must record and be able to provide evidence of this to ITER Cadarache.

- Overall system.

- Measured as a percentage of the transponders on site at ITER Cadarache the RFID/RTLS solution must provide 99.5% of all transponders IDs and locations to SPMat each day. This is not an average but a daily minimum.

- Sensors must:

  - Capture and record into device data storage all (100%) events while applied to ITER parts in transit and while on site at ITER, Cadarache. Device data storage may be reused once data has been transferred to the application but only after the application[2] has confirmed and validated the device data that is to be removed from the device memory.

  - Transfer data from device data storage to the RFID/RTLS application on request with no overall system data loss or data corruption.

  - Capture measurements within the tolerance requirements of each of the applications and maintain this performance without any degradation throughout the devices life.

- Battery life (where applicable).

  - Transponder (including sensors) battery life should as a minimum be capable of 5 years of active service.

  - All portable handheld battery powered devices should have minimum battery autonomy of one ITER use cycle (5 hours) during the first two years of service.

Solution response time.

- The RFID/RTLS system needs to establish the position of each transponder daily.

- Sensors must capture be sufficiently reactive to capture all events they are entrusted to monitor.

Up-time.

- The RFID/RTLS system must be available every day for sufficient time to capture the location of transponders and sensors.

- The RFID/RTLS solution must be accessible by ITER each day during normal working hours.

- Sensor transponders must at a minimum be capable 24/7 to capture events that they are to measure during part shipping from the point of depart at the original supplier through until the sensor transponder is removed from the part by ITER.

[2] Application and system security features must be sufficient to ensure that suitable authority validation controls can be applied to prevent data access, deletion, modification, etc..

Security.

- Access control. Enabling ITER and the RFID/RTLS solution provider dynamic and full control over who can access all aspects of the RFID/RTLS solution with respect to physical installations, devices and also ICT/information systems.

- Protection of part identity. The solution architecture should consider and orientate towards protection of the identity, location and condition (real and historical) of parts by non-authorized personnel. Protection applies to all elements of the solution including sensors.

- Compatible and compliant with ITER's information and general security requirements.

- Single sign on capability with Active Directory would be preferred

Traceability.

- In addition to SPMat's traceability capabilities it is expected that the RFID/RTLS solution will store and archive all data necessary to provide full traceability related to devices forming the RFID/RTLS solution and including all identification, location and sensor events, software/firmware upgrades, device maintenance/use/etc. and related data.

Environmental protection.

- Transponders must be protected from the environment, assembly and installation processes.

- The RFID/RTLS interrogator system including edge processing hardware, cabling, communications devices, power supplies, etc. must be suitably protected from the environment.

Acceptance Criteria

Identification, Location Capture & Sensing requirements

Ref.	Requirements	Must	+ Should	+ Like to have
5.2.1	Identification and location capture.	Provide: 1. Device identification consistently and instantly when demanded either through remote or local requests. 2. Location of the device in 2D (not vertical) coordinates or user assigned location identifiers or names, including the time of the localization capture (as a record of system latency).	Allow: 1. The user capability to encode, store and transmit user defined identifiers. 2. Removal of RFID/RTLS devices from the part without the process requiring specialist skills or tools. The process should require only one person and be possible in the	Security features. 1. Orientated towards protection from unintentional changes to: A) RFID/RTLS device memory content: B) RFID/RTLS device configuration settings. 2. Capable of monitoring, recording and

Ref.	Requirements	Must	+ Should	+ Like to have
		Location data must be sufficient to guide staff and contractors to the immediate location. 3. Systems that can operate outdoors and indoors reliably for +10 years. 4. Interfaces and other provisions for bar code and keyboard capture, enabling distinction to be made as to the source of data capture. The overall RFID/RTLS system must yield the following information (See Tec. Spec. for details): 1. Identification serial number(s) of Transponder ID. 2. Location of transponder. 3. Time/Date/Time-zone. 4. Checkpoint. 5. Error and exception codes. Include device attachments for physical association of RFID/RTLS devices to component items. Attachments need to: 1. Ensure that RFID/RTLS devices do not become accidentally detached. 2. Require the minimum of time and effort and be possible of attachment by one person. Removal of RFID/RTLS devices from the part. The process <u>must not</u> mark/damage or irreversibly change or impact the functionality/performance of the component item.	minimum amount of time. 3. Assigning a 'search' task to a reader or group of readers in seeking to locate a transponder or, simultaneously a user defined selection of transponders. The overall RFID/RTLS system should yield the following information (See Tec. Spec. for details): 1. Location of reader. 2. Reader ID. 3. Reader type. 4. User assigned reader name and data. 5. Device exception code. 6. Last status message. 7. Date/time of last device reported event.	limiting access to system changes. The overall RFID/RTLS system might yield the following information (See Tec. Spec. for details): 1. Bar code &/or Manual entry. 2. Device ID/Name. 3. Device type. 4. Device location. 5. Priority Action notification.
5.2.2	Sensing	Deliver: 1. Accurately sense, communicate and report the condition being monitored. 2. Timely information determined by the part	Remote calibration measurement and adjustment and, a 'reset' capability enabling that the RFID/RTLS devices can be reused or have their lives extended where	Measurement and monitoring: Temperature (?). Humidity (?). Ionizing radiation (?). (+)?

Ref.	Requirements	Must	+ Should	+ Like to have
		category/type. Including: Sensor type. Measurement range. Unit of measure. Last calibration (date/time). Status/Health (e.g. On/Off, Error, etc.). (+)? 3. Measurement and monitoring. Vibration and shock. Orientation. Exemple of Sensors: 1. Acceleration sensing: ±lg vertical and ±1.2g lateral movement. 2. Nitrogen Blanket Pressure sensing: >0 barg and <0.5 barg	they are not (or not easily) accessible.	
5.2.3	Traceability		Provide: A repository of all RFID/RTLS events. These should be readily accessible for the period of the last 2 years of information and be available for a rolling period of 10 years.	Enable field delimited file export of all data to assist in undefined analytic analysis.

2.1 Operator(s) - Device Management & Reporting Tools

Ref.	Requirements	Must	+ Should	+ Like to have
5.3.1	System and device access authority	Only permit changes to device parameter settings and recorded data through authorised access. Provide protected system access authorization control functionality permitting the system administrator (user) the possibility to grant, revoke and monitor all access. Provide protected system access authorization control functionality for all solution support (remote and local) services. Monitor and record all system access attempts. Enable the system administrator (user) to allow manual password resetting to both local and remote users.	Enable the system administrator (user) to allow automated password resetting to both local and remote users. Provide automated system access reports e.g. successful and failed attempts, frequency, session duration, user actions, etc.	Provide access related alerts to the system administrator.
5.3.2	Device management and configuration tools		Enable remote configuration of all RFID/RTLS system devices. Functions may include: 1. Power settings (incl. On/Off controls). 2. Reset. 3. Data communications parameters (incl. data elements, . 4. Device memory. 5. Access control and security settings. (See Technical Specification Document for more details)	
5.3.3	System status reports	Allow visibility as to the current status of the system and solution. Report historical views of system status.		

Ref.	Requirements	Must	+ Should	+ Like to have
		Monitor, alert and report upon software interfaces to highlight in particular: Data exchange failures: Interface latency.		
5.3.4	Device health status reports		Provide reporting on system health including aggregated and detail device level views.	
5.3.5	Critical alerts response system			Deliver timely alerts to the system administrator and/or a remote support service provider indicating: 1. The nature of the alert. 2. Automatically attributing a priority (parameterized by the administrator). 3. The location of the system device and the time/date of the last communication.
5.3.6	Security		Application security preventing unauthorised access to ITER's information system. ICT security features enabled the protected operation of the RFID/RTLS solution.	

2.2 Software Support - Application Interfaces

Ref.	Requirements	Must	+ Should	+ Like to have
5.4.1	Logistics system interfaces	Alert the system administrator of all failed interface attempts. Allow automatic repeated interface exchange attempts when errors are detected. Ensure data retention of all interface data exchanges, whether successful or not. Maintain adequate access to skilled support staff to develop, support and maintain the logistic system interfaces throughout the project life cycle (minimum 10 years).	Provide preventative maintenance of all solution interfaces with performance based upon an SLA. (Ref. Technical Requirements document).	Monitor and periodically provide reports to the operator and support operator quality audits.
5.4.2	RFID/RTLS management system	Version visibility and firmware/software update administrator controls. Reporting upon firmware and software version changes. Maintain adequate access to skilled support staff to develop, support and maintain the RFID/RTLS management system throughout the project life cycle (minimum 10 years).		Monitor and periodically provide reports to the operator and support operator quality audits.
5.4.3	Continuous improvements.		A pre-planned periodic review of improvements, development, test and deployment.	
5.4.5	User support	General and solution specific technical documentation with revision release control and operator alerts.	Solution and system hardware related instructions and if necessary training documentation encompassing user and the system administrator requirements.	

2.3 Hardware Support- Preventative Maintenance & Service Support

Ref.	Requirements	Must	+ Should	+ Like to have
5.5.1	Preventative maintenance of	Ensure that all RFID/RTLS system devices are		

Ref.	Requirements	Must	+ Should	+ Like to have
	devices and including scheduled firmware and software updates	maintained in reliable working order through device data analysis and planned preventative maintenance.		
5.5.2	Service support of the ITER and their appointed contractors	Provide 24/7 help desk in English**. During the Pilot help desk support is only required during normal working hours (e.g. 08:00-18:00/Mon-Fri).** Log and report all help desk enquiries. Provide help desk resolution management system which can be accessible remotely by the systems administrator.	Provide preventative maintenance of all systems devices with performance based upon an SLA. (Ref. Technical Requirements document). Provide on-site service support in order to address performance issues and system failures. Provide adequate replacement devices or spares of system critical elements in order to meet the system SLA. (Ref. Technical Requirements document).	Report upon all service incidents, inventories of spares, resource skill availability, actions and provisions for planned and un-planned service support.
5.5.3	Continuous improvements.		A pre-planned periodic review of improvements, development, test and deployment.	
5.5.4	Technical support	General and solution specific technical documentation with revision release control and operator alerts.	Solution software and system firmware related instructions and if necessary training documentation encompassing user and the system administrator.	