CDR of the

Wire Scanner Acquisition System

RAMI

Author	Checked by – date	Approved by – date
Mario Ferianis	Mario Ferianis	
Raffaele De Monte		
Sandi Grulja		
Stefano Cleva		

Table of Contents

1. Introduction

1.1. Purpose of the Document

A typical tool needed for assessing that an “User-oriented” accelerator facility provides an adequately high up-time, enabling a significant scientific production, is the RAMI analysis. RAMI is defined as [1] [2]:

- **Reliability**: capability of providing *continuous correct operation*; deep knowledge of system hardware architecture and components is usually not sufficient to determine its reliability; it is necessary to rely on a functional analysis and to take into account the environment and operating conditions.
- **Availability**: availability of a device must be regarded as a performance. It is the probability that the device is in a state to perform the required function for which it was designed. Referring to *delivery beam operation*, availability is an integral measure of the maturity of corresponding technology. Operation is characterized also by the following parameters:
    - **MTTF** (Mean Time To Failure): duration of correct operation before the failure
    - **MTBF** (Mean Time Between Failure): average length of time between 2 consecutive failures of a repairable component
- **Maintainability**: ability to undergo *repairs and modifications*; to design looking for performance without neglecting the possibility of failure: it is very important to consider what would happen in case of failure. Maintainability is directly related to the ease and economy of maintenance, like: rapidly recognizing, isolating and correcting a malfunction or apply technical data for the maintenance technician.
- **Inspectability**: ability to undergo visits and controls; it is defined as that characteristic of design and integration that allows in situ monitoring of equipment performance, including accessibility to equipment and diagnostics to determine incipient failure.

This document provides some preliminary considerations for a RAMI analysis for the WS Acquisition System.

Being the ad-hoc designed hardware modules for the WS ACQ SYS a recent in-house development of Elettra, at this CDR stage, it is possible to derive only estimations, based on the experience on:

- similar in-house designed electronics modules (FERMI cavity BPM detectors)
- the data sheets of the manufacturers of the chosen components/parts.

- operation lifetime of electronics modules in ESS-like facility

1.2. Definitions, acronyms, and abbreviations

In the document, we have used the abbreviations reported in Table 1.

Abbreviation	***Explanation of abbreviation***
WS	Wire Scanner
ST	Elettra Sincrotrone Trieste
ESS	ESS ERIC
ACQ SYS	Acquisition System
AFE	Analogue Front End module
OFE	Optical Front End module
BE	Back End module
BE_{mod}	Modified Back End module

Table 1 – Abbreviations

1.3. Assumptions on ESS operating conditions

The different modules of the WS ACQ SYS will operate either in the ESS accelerator tunnel or inside specific racks in the Service Gallery of ESS which are both temperature controlled environments.

It has to be noted, though, that the AFE will be located inside the machine tunnel resulting in a moderate exposure to ionizing radiations during delivery beam (ie during operation with commissioned machine) which could result to be severe during the commissioning period.

The hardware modules of the WS ACQ SYS do not dissipate high heath amounts. Therefore, operating in a temperature controlled environment will be beneficial to their performances.

In the estimation of the RAMI for the WS ACQ SYS, we make the following assumptions:

- Air Temperature in Service Gallery: 22.5°C ±5 °C
- Annual Operating hours: 5,000 hours/year
- Total number of Units: 32 (AFE+OFE+BEs)
- Exposure to ionizing radiation: moderate on the AFE
- Pessimistic estimation of MTBF of HW modules > 100,000 hours
- Required [1] MTBF: >70,000 hours
- Expected level of integrated ionizing radiation….

1.4. References

[1] ITER_RAMI_ANALYSIS_PROGRAM_28WBXD_v4_3
[2] 2_CFE_Technical_Specifications_TPMRE9_v1_0

[3] *Concise Guide to Formal Methods; Theory, Fundamentals and Industry Applications.* G. O'Regan, Springer, ISBN 978-3-319-64021-1

[4] http://whatis.techtarget.com/definition/Reliability-Availability-and-Serviceability-RAS

2. The hardware modules

2.1. The Analogue Front End (AFE) module

The AFE module, with respect to the RAMI issues, is probably the most critical HW module of the WS ACQ SYS as it is installed in the accelerator tunnel.
Medium to high levels of ionizing radiations are expected in this area of the ESS accelerator complex, especially during the commissioning period. Not only, but also in Beam Delivery operating mode burst of ionizing radiations may occur due to general faults.
Furthermore, in case of AFE hardware faults, the removal of the AFE from its installation site could require some not negligible time due to the normally not accessibility of the tunnel itself.
Finally, servicing faulty AFE module may not start immediately as it may present significant activation levels and therefore it needs first to “cool down”.
Due to the above motioned reasons, the AFE has been conceived as reliable by design, by adopting some good practice rules like:

- to avoid the use of digital electronics in it
- to avoid on board power supply
- to use RAD-tolerant electronic components
- …

…
….
….

Also the location of the AFE inside the tunnel, on the magnet girder, has been carefully chosen in team with the WS mechanics design team (ESS Bilbao) by matching two opposite requirements: on one side having as short as possible signal cables between. On the other side to locate the AFE in a “rad safe” location shielded as much as possible and off the beam axis.

2.2. The Optical Front End (OFE) module

The Optical Front End has been safely located in the diagnostics rack in the service gallery and, therefore, has far less critical operating conditions than the AFE. Being connected to the in-tunnel installed scintillators by means of long run fibers, it is also in a much better position with respect to the EMC viewpoint.

The OFE design has been implemented in such a way that each WS assembly is managed by a single OFE. It is an 8 input channel module suitable for the readout of the optical signals from 4 scintillator assemblies.

Also the OFE is powered via the associated modified Back End housed, close to it, in the same rack.

2.3. The Back End (BE) module and the Modified Back End (BE_{mod}) module

The Back End and the Modified Back End modules adopt a modular design: as a matter of fact, the modified BE houses two BE boards in a single chassis upgrading the number of input channels from 4 to 8.

Both types of BEs are installed inside diagnostic racks, in the service gallery.

All needed power supplies are also accommodated inside the BE, which is in turn powered by mains though a double isolation power supply unit.

This solution has also allowed to implement a very careful and low noise supply voltages generation and distribution to the AFE and OFE below it.

2.4. Electronic Components used on WS ACQ SYS hardware module

In the following paragraph, some information on the used electronic components are given, with special reference to reliability.

2.4.1. Passive electronic components

Monolithic ceramic capacitors, tantalum capacitors, and thick film resistors form the core group of *passive SMD*. The shapes are generally rectangular and cylindrical. The mass of the components is about 10 times lower than their through-hole counterparts. The *surface mount resistors and capacitors* come in various case sizes to meet the needs of various applications.

2.4.2. Surface mount resistances

There are two main types: thick film and thin film. Thick film surface mount resistors are constructed by screening resistive film (ruthenium dioxide based paste or similar material) on a flat, high purity alumina substrate. The resistance value is obtained by varying the composition of resistive paste before screening and laser trimming the film after screening. In thin film resistors the resistive element on a ceramic substrate with protective coating (glass passivation) on top and weldable terminations (tin-lead) on the sides. The terminations have an adhesion layer (silver deposited as thick film paste) on the ceramic substrate, and nickel barrier under plating followed by either dipped or plated solder coating. Resistors come in 1/16, 1/10, 1/8 and ¼ watt ratings in 1 ohm to 100 mega ohm resistance in various sizes and various tolerance. Commonly used sizes are: 0402, 0603, 0805, 1206, and 1210.

2.4.3. Tantalum SMT capacitors

For Surface Mount capacitors, the dielectric can either be ceramic or tantalum. Surface mount tantalum capacitors offer very high volumetric efficiency or a high capacitance-voltage product per unit volume and high reliability. The wrap-under lead capacitors, have leads instead of terminations and a beveled top as a polarity indicator. They are available in two sizes – standard and extended range. The capacitance value for tantalum capacitors vary from 0.1 to 100 µF and from 4 to 50 V dc in different case sizes

2.4.4. Ceramic SMT capacitors

Surface mount capacitors are ideal for high frequency circuit applications because it does not have any leads and can be placed underneath the package on the opposite side of the PCB. *Surface mount capacitors* are used for both decoupling applications and for frequency control. They are available in different dielectric types per EIA RS-198n, namely COG or NPO, X7R, Z5U, and Y5V. Surface mount capacitors are highly reliable and are used in high volumes in under-the-hood automotive applications, military equipment and aerospace applications.

2.4.5. Small Outline IC (SOIC and SOP)

The integrated circuit (SOIC or SO) is basically a shrink package with leads on 0.050 inch centers. SOICs come in mainly two different body widths: 150 mil 300 mils. The body width of packages having fewer than 16 leads is 150 mil; for more than 16 leads, 300 mil widths is used. The 16 lead packages come in both body widths.

2.5. Cables used for the WS ACQ SYS

The AWG - American Wire Gauge - is used as a standard method denoting wire diameter, measuring the diameter of the conductor (the bare wire) with the insulation removed. AWG is sometimes also known as Brown and Sharpe (B&S) Wire Gauge. The AWG table below is for a single, solid, round conductor. Because of the small gaps between the strands in a stranded wire, a stranded wire with the same current-carrying capacity and electrical resistance as a solid wire, always have a slightly larger overall diameter. The higher the number - the thinner the wire.
The main physical and electrical properties for different AWG cables are shown in Table 1.

AWG	Diameter [inches]	Diameter [mm]	Area [mm^2]	Resistance [Ohms / 1000 ft]	Resistance [Ohms / km]	Max Current [Amperes]	Max Frequency for 100% skin depth
0000 (4/0)	0.46	11.684	107	0.049	0.16072	302	125 Hz
1	0.2893	7.34822	42.4	0.1239	0.406392	119	325 Hz
10	0.1019	2.58826	5.26	0.9989	3.276392	15	2600 Hz
11	0.0907	2.30378	4.17	1.26	4.1328	12	3200 Hz
12	0.0808	2.05232	3.31	1.588	5.20864	9.3	4150 Hz
13	0.072	1.8288	2.62	2.003	6.56984	7.4	5300 Hz
14	0.0641	1.62814	2.08	2.525	8.282	5.9	6700 Hz
15	0.0571	1.45034	1.65	3.184	10.44352	4.7	8250 Hz
16	0.0508	1.29032	1.31	4.016	13.17248	3.7	11 k Hz

17	0.0453	1.15062	1.04	5.064	16.60992	2.9	13 k Hz
18	0.0403	1.02362	0.823	6.385	20.9428	2.3	17 kHz
19	0.0359	0.91186	0.653	8.051	26.40728	1.8	21 kHz
20	0.032	0.8128	0.518	10.15	33.292	1.5	27 kHz
21	0.0285	0.7239	0.41	12.8	41.984	1.2	33 kHz
22	0.0254	0.64516	0.326	16.14	52.9392	0.92	42 kHz
23	0.0226	0.57404	0.258	20.36	66.7808	0.729	53 kHz
24	0.0201	0.51054	0.205	25.67	84.1976	0.577	68 kHz
25	0.0179	0.45466	0.162	32.37	106.1736	0.457	85 kHz
26	0.0159	0.40386	0.129	40.81	133.8568	0.361	107 kHz

Table 1 AWG cable physical and electrical properties; not all sizes shown.

The table below indicates the current ratings of PVC-insulated single and multicore wiring cables. Always check manufactures data before detailed engineering.

AWG	**Diam. [mm]**	**x-sect. [mm²]**	**Res. [ohm/km]**	**Current Load Ratings *(amps)*[1)]**					
				1 Core	**Multicore**				
					up to 3 core	**4 - 6 core**	**7 - 24 core**	**25 - 42 core**	**43 and above**
30	0.25	0.049	351						
28	0.33	0.08	232.0						
27	0.36	0.096	178						
26	0.41	0.13	137						
25	0.45	0.16	108						
24	0.51	0.20	87.5	3.5	2	1.6	1.4	1.2	1
22	0.64	0.33	51.7	5.0	3	2.4	2.1	1.8	1.5
20	0.81	0.50	34.1	6.0	5	4	3.5	3	2.5
18	1.02	0.82	21.9	9.5	7	5.6	4.9	4.2	3.5
16	1.29	1.3	13.0	20	10	8	7	6	5
14	1.63	2.0	8.54	24	15	12	10.5	9	7.5
12	2.05	3.3	5.4	34	20	16	14	12	10
10	2.59	5.26	3.4	52	30	24	21	18	15

Table 2 AWG cable physical and electrical properties; not all sizes shown.

The higher the gauge number, the smaller the diameter, and the thinner the wire. Because of less electrical resistance a thicker wire carries more current with less voltage drop than a thinner wire. For longer distances it may be necessary to increase wire diameter - reducing the gauge - to limit voltage drop.

2.6. Connectors used for the WS ACQ SYS

In the following paragraph, the specifications of the connectors used for the WS ACQ SYS are shown.

2.6.1. DB9 connector

PHYSICAL CHARACTERISTICS
INSULATOR MATERIAL : BLACK THERMOPLASTIC UL94 V0
CONTACTS MATERIAL : COPPER ALLOY
CONTACTS PLATING : GOLD FLASH OVER NICKEL
SHELL PLATING : NICKEL/TIN

ELECTRICAL CHARACTERISTICS
RATED VOLTAGE : 250V
RATED CURRENT : 5 A
CONTACT RESISTANCE : ≤25mΩ
INSULATION RESISTANCE : ≥5000 MΩ

MECHANICAL CHARACTERISTICS
MATING CYCLES : 50 MINIMUM
RETENTION AGAINST TORQUE : 0.5Nm

ENVIRONMENTAL CHARACTERISTICS
OPERATING TEMPERATURE : -55°C TO +105°C

2.6.2. D-SUB 25 connector

PHYSICAL CHARACTERISTICS
INSULATOR MATERIAL : BLACK THERMOPLASTIC UL94 V0
CONTACTS MATERIAL : COPPER ALLOY
CONTACTS PLATING : GOLD FLASH OVER NICKEL
SHELL PLATING : NICKEL/TIN

ELECTRICAL CHARACTERISTICS
RATED VOLTAGE : 250V
RATED CURRENT : 5 A
CONTACT RESISTANCE : ≤25mΩ
INSULATION RESISTANCE : ≥5000 MΩ

MECHANICAL CHARACTERISTICS
MATING CYCLES : 50 MINIMUM
RETENTION AGAINST TORQUE : 0.5Nm

ENVIRONMENTAL CHARACTERISTICS
OPERATING TEMPERATURE : -55°C TO +105°C

3. The software modules

When dealing with software reliability, we may consider it as [3] the probability that the program works without failure for a period of time, and it is usually expressed as the mean time to failure.

It is though different from hardware reliability, in that hardware is characterized by components that physically wear out, whereas SW is intangible and software failures are usually due to design and/or implementation errors. Sometimes, however, software failures are also due to underlying hardware or low level software components (e.g. drivers) malfunctions. Software is either correct or incorrect when it is designed and developed, and it does not physically deteriorate with time however, in case of environment changes (e.g. operating system update, drivers update), a running software component could become instable or, in the worst case, completely unreliable.

In any case, even if software works perfectly fine, bugs could be discovered over the time.

Also dealing with SW "RAMI" we may rather talk of RAS: Reliability, Availability and Serviceability [4]. RAS is a set of related attributes that must be considered when designing, manufacturing, purchasing or using a computer product or component. The term was first used by IBM to define specifications for their mainframes and originally applied only to hardware . Today RAS is relevant to software as well and can be applied to application programs, operating systems, personal computers (PCs), servers and supercomputers.

- **Reliability**: refers to the ability of a computer-related hardware or software component to consistently perform according to its specifications. The Wire Scanner software is based on the EPICS environment, customized by ESS and named EEE, that is embedded on an Intel I7 CPU based board hosted in a μ-TCA crate. Due to the peculiar architecture of Epics IOC's, the programming model adopted is the data flow one. In this model, a cascade of Epics standard records is triggered in sequence; for particular operations a state machine supports the record processing mechanism. This model states that the reliability of the whole wire scanner software system is in charge of two items: the configuration and the code implementation of the records of the wire scanner IOC and the set of bridging functions (Channel Access mechanism) required for the data and control information exchange whit the underlying IOCs (motion, timing and acquisition tasks). Assuming that the set of bridging features delivered by ESS is reliable, the wire scanner software has been designed, developed and tested in order to be reliable too but, of course, not bug free. The main functions have been tested both in a simulated and laboratory environment; in such conditions the wire scanner IOC worked accordingly to its expected functions. The lack of a full operative test bench, of course, is still a weak point and only a laboratory level reliability can be assured at this stage of the project.

- **Availability**: is the ratio of time a system or component is functional to the total time it is required or expected to function. In the case of the WS ACQ SYS software, it is expected full availability if any kind of hardware (μ-TCA boards, motion controller, Back End and network connection) and low level software (underlying IOCs, Back End firmware) works fine. If this assumption is not true, the wire scanner IOC is not supposed to continue to work, neither with reduced performance.
- **Serviceability:** is an expression of the ease with which a component, device or system can be maintained and repaired. Due to the wire scanner IOC modular architecture, it can be easily serviced in case of bug fix; adding new features, on the contrary, could have heavy impact on the IOC "code". Early detection of potential software problems has not been planned. A porting to an updated release of the EEE environment has even not been planned.

3.1. Key elements of RAS applied to WS ACQ SYS software

Considering the key elements of RAS which can be found in the relevant literature on software engineering, in the following we list the ones which have been applied to the WS ACQ SYS software.

- Over-engineering, i.e. designing systems to specifications better than minimum requirements, has been considered in order to optimize the data propagation between the records of the wire scanner IOC.
- Due to the usual (not mission critical) application of wire scanner systems redundancy has not been implemented.
- Automatic updating, which keeps OS and applications current without user intervention, is strongly discouraged in order to maintain matched EEE environment and IOC code.
- Data archiving has not been considered because ESS has planned to use the Epics native archiver.
- In order to maintain the data exchange performance between the low level IOCs and the wire scanner one the use of virtual machines is strongly discouraged.

4. Possible source of failure and preventive/corrective actions

4.1. The AFE

As previously mentioned, the AFE is the most critical HW module of the WS ACQ SYS being located inside the accelerator tunnel.
Two main faults may occur to the (WS + AFE) assembly:

- breaking of the in-vacuum WS wire(s)
- fault of one or both amplifiers chains inside the AFE

The AFE provides also for the WS wire integrity check, by applying a known voltage on one wire end and reading it back on the other input. Therefore, should the wire break up, the WS ACQ SYS would immediately signal it to the ICS for any possible preventive maintenance action.
The AFE is provided with two in-parallel trans impedance amplifiers, the first one used for the “low gain” channel and the other for the “high gain” one. Should only one of the two channels break-up, a limited operability could still be provided by the AFE hopefully not requiring for an AFE replacement.
An extra relay into the AFE is able to short the signal between the two inputs. In that way it is possible to have the certainty of the trouble, that means wire or the analog amplifier. Also a series of 4 LEDs on the BE Module indicate the correct power supply connection from the BE to his AFE.
Connectors of the AFE are very easy to connect/disconnect by an operator in case of substitution. The signal inputs are connected with a triaxial “BNC LIKE” connector that is fixed with a ferrule avoiding accidental disconnections. The connections to the BE are made with a two twisted pair cables and DB 25 and DB 9 connectors fixed by a screw, thus avoiding accidental disconnections.
Wire protection is demanded to a software with movement restrictions/rules that avoid excess of heating by the wire (i.e. due to a too high current versus time)

4.2. The OFE

The OFE is expected to have a very reliable operation over many years. Also in the OFE there is some redundancy added by design as each scintillator block is read out by means of two photodiodes, still of a different type and with different sensitivities.
The weakest element of all components are Si photo diodes therefore max attention was put in design to not exceed the max values that could in some way degrade or even damage diode or push the diode out from regular and designed normal operation.

4.3. The BE

The BE is a mixed analogue / digital kind of module adopting good design practice and therefore, it is expected to have a very reliable operation over many years. In case of failure the replacement procedure will be very easy due to a connections simplicity.
The possible failures are involving:

1. High voltage generator, which is monitored by a PIC microcontroller: in case of failure a message for the operator is available.
2. PIC microcontroller is programmed with a Watchdog feature enabled, so in case of software failure/bug a reboot will be always possible, avoiding Back End hang.

3. The reset pin of the Ethernet to serial interface is connected with an output of the PIC microcontroller. Thus in case of missing communications for an expected time, a reset can be asserted by the PIC microcontroller solving a possible communication problem.

4.4. The WS ACQ SYS software

The IOC software relies on the services offered by the underlying IOCs: the ADC one, the Timing one and the motion controller one (ref. figure 1). If the timing system doesn't generate the EVR (event receiver) local trigger, the acquisition process does not start and the Epics forward link stimulus, that triggers the WS ACQ SYS IOC by the “ADC + Timing” IOC, is not generated. In other terms, the WS IOC waits the availability of data to be processed since it is triggered by the “ADC + Timing” IOC; if no trigger event is generated, the WS IOC will wait for it forever, and any kind of beam profile measure will be impossible.

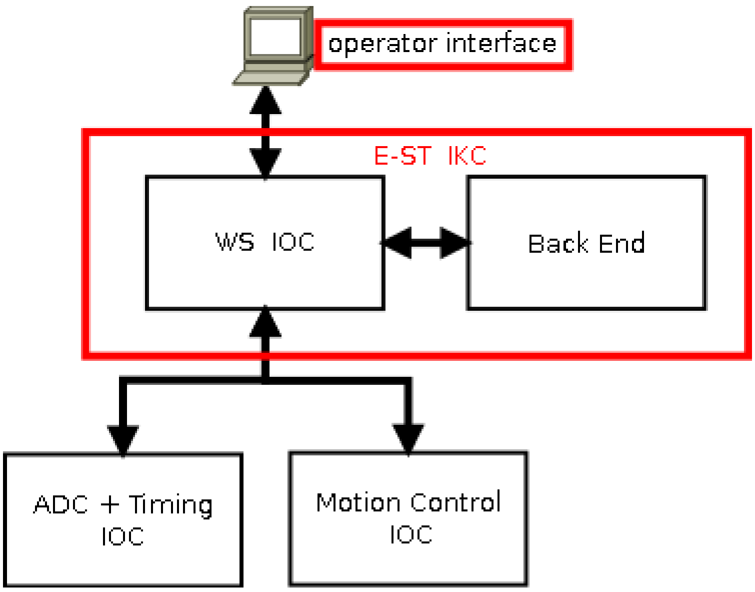

Figure 1 WS AC SYS control software block diagram

The Motion Control IOC is less critical than the “ADC + Timing” one, since it doesn't trigger the WS IOC data acquisition task. The Motion Control IOC is assumed to be up and running at the startup of the WS IOC, but if no mechanical scansion is required it will not be asked to perform any action, and the position of the wire will not change. Regardless the wire position and if the timing trigger is running, the WS IOC will read the ADC's buffers and will show them to the operator, as is expected when the wire is in parking position. The Back End is locally managed by a dedicated μ-controller that communicates with the WS IOC over an Ethernet connection; the Back End acts as a slave and the WS IOC as a master. By doing so, a set of complex operations are shifted from the master to the slave: the master sends a command and the slave performs the desired operation acting accordingly to its own timing. It is in charge of the master to check that the slave has finished the operation and, in case of failure, to manage the faulty condition; in case of non-critical failures the BE can be reset. Non-critical failure means, in this context, that the local μ-controller is able to communicate with the master; if this is not the case, it is assumed a critical failure, and a watch dog mechanism has been implemented in the BE in order to automatically reset the μ-controller.

So, in summary, the main sources of failure for the operation of the WS IOC are:

- failure in the “ADC + Timing” IOCs: if the timing trigger is not present, the WS will not start;
- with present timing signals, the ADCs may result being faulty, the WS IOC input signals will not be the one read by the BE;
- If the AFE/OFE or Back End are faulty, the WS IOC input signals could be completely wrong compared to the ones generated by the wire or, in a less severe case of failure, only the amplifying stages gain could be corrupted or not changeable. Of course, if the Ethernet connection between WS IOC and Back End controller is faulty, the behavior of the WS IOC could be different from the expected, even if the analog signals generated by the wire reach the ADC unit.
- A failure in the motion control subsystem could not be detected if no trajectory scan is performed.