MONITORING AND CONTROL ELEMENT LEVEL RISK REGISTER

Document number WP2-005.065.020-RE-001
Revision .... B
Author .... TJ Stevenson
Date 2011-10-24
Status.. Draft

Name	Designation	Affiliation	Date	Signature
Additional Authors				
Duncan Hall SPDO, Swaminathan Natarajan TCS				
Submitted by:				
TJ Stevenson	System Engineer	SPDO		TJS
Accepted by:				
Approved by:				

DOCUMENT HISTORY

Revision	Date Of Issue	Engineering Change Number	Comments
A	2011-10-11	-	First draft release for internal review
B	2011-10-24	-	Upissue following COAR inputs

DOCUMENT SOFTWARE

	Package	Version	Filename
Wordprocessor	Microsoft Word	Word 2007	WP2-005-065-020-RE-001_risk-register.docx
Block diagrams			
Other			

ORGANISATION DETAILS

Name	SKA Program Development Office
Physical/Postal Address	Jodrell Bank Centre for Astrophysics Alan Turing Building The University of Manchester Oxford Road Manchester, UK M13 9PL
Fax.	+44 (0)161 275 4049
Website	www.skatelescope.org

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

CDR..............................Critical Design Review
CoDR............................Conceptual Design Review
COTS ....Commercial Off The Shelf (hardware, software)
DRM ....Design Reference Mission
PEP ....Post PrepSKA Project Execution Plan
PrepSKA.......................Preparatory phase of the SKA
M&C ....Monitoring & Control
PDR..............................Preliminary Design Review
PRR..............................Production Readiness Review
SKA ....Square Kilometre Array
SPO..............................SKA Project Office
SRR..............................System Requirements Review
TPM..............................(SPO) Technical Project Manager
TRR..............................Test Readiness Review
WBS ....Work Breakdown Structure
WP2..............................PrepSKA Work Package 2
WPC ....(PEP) Work Package Contractor

1 Introduction

This document is the risk register specific to the Monitoring & Control domain of the SKA project. It supports the Monitoring & Control domain's Concept Design Review (CoDR).

1.1 Purpose of the document

This document supports risk management – identifying and categorising risks and proposing mitigation plans – for the Monitoring & Control CoDR, and in turn it informs the SKA System Level Risk Register.

1.2 Scope of the document

The flow of this document is:

- Definitions of risk likelihoods and impacts
- Derived definitions of risk exposures
- For SKA Phase 1 (SKA1) and Phase 2 (SKA2), details of perceived risks, proposed mitigation actions, and current status of proposed mitigation actions

2 References

[1] 14-mgt-040.040.000-mp-001-1-riskmanplan

[2] MGT-090.010.010-RE-003: SKA Project Risk Register, Revision C, 2011-02-15

[3] WP2-040.010.010.RE-001-A_SKASPRiskRegister

3 Risk Exposure Definitions

The risk perceived likelihood estimates and risk impacts for the Monitoring & Control aspects of the SKA shown in the tables below conform in general form to the levels defined in the PrepSKA System Risk Management Plan [1] and Risk Register [2]. However, due to the relatively low accuracy at the Concept Design Review stage in estimating the likelihoods and impacts of risks associated with software development, a 3x3 matrix has been adopted – rather than the 5x5 matrix presented in [1].

Thresholds adopted for the Monitoring & Control Concept Design Review are shown below:

Likelihood:

- Low : less than estimated 20% likelihood of occurrence
- Medium : at least 20% but less than 80% likelihood of occurrence
- High : at least 80% likelihood of occurrence

Impact:

Impact	Cost	Schedule	Performance
Low	Less than 10% impact	Very minor or no slip in milestone, i.e. order one month	Very minor or no impact
Medium	Order 10% to 50% impact	Moderate slip in milestone, i.e. up to 6 months	Moderate functional impact or reduction in performance, performance almost acceptable but would require redesign
High	Greater than 50% impact	Critical slip in milestone, i.e. more than 6 months	Critical functional impact or reduction in performance, performance not acceptable and requires new design

Table 1 M&C CoDR Risk Impact Definitions

Exposure:

The risk exposure is a function of the perceived risk likelihood and risk impact is as follows:

		Impact		
		Low	Medium	High
Likelihood	High	Medium	High	Very High
	Medium	Low	Medium	High
	Low	Very Low	Low	Medium

Table 2 Risk Exposure Definitions

4 System Level delta CoDR Risks Related to Monitoring & Control (paraphrased)

The following is a derivation of System level risks flowed down by virtue of the high dependency of M&C on software.

No	Risk	Short description	Impact	Proposed mitigation	Estimated SKA1 risk exposure	Estimated SKA2 risk exposure
4.1	Scope of work	Monitoring and Control for the SKA will be multifaceted and complex. The scope of the work and the expected human resource requirement and time line for the development of the software/hardware is unknown. Risks are: • unrealistic requirements • underestimation of the cost of complexity • hardware design defines the software • classes of users are forgotten • control and other software are separately managed • software architecture is defined by the division of work	Failure to define the scope of the work will result in inaccurate costing. Software development will be a significant part of the overall project costs and schedule and underestimation will have a severe and negative impact on the project as a whole.	Initiate development of work breakdown structures and definition of the scope of the development to be performed during each stage of the project. Link deliverables to these phases. Negotiate work packages with contributing institutions on work to be performed.	High	High
4.2	Scope creep	Failure to baseline and traceably manage to requirements held in a central repository	Change requests create exponentially increased required work effort – and consequently delivery costs – in a development project.	Set up Change Control Board and related governance structures to tightly manage all requests for change, strengthen the SEMP if necessary.	High	High
4.3	Inadequate documentation	Documentation of requirements, analyses, tests and design is missing, or not of sufficient quality	Development on a large scale requires that teams distributed across the globe collaborate through exchange of documentation as well as through electronic communications media and face-to-face meetings. If any of these communications channels is impaired, the overall level of coordination and hence collaboration is negatively impacted	Planning of phased delivery of documentation along with creation and maintenance of a central documentation repository.	Medium	Medium

No	Risk	Short description	Impact	Proposed mitigation	Estimated SKA1 risk exposure	Estimated SKA2 risk exposure
4.4	Over-reliance on software development processes appropriate only for small scale projects	Lifecycle development models that are appropriate for small scale early stage development and preliminary implementations are very unlikely to work for development of large scale robust systems.	Reliance on processes only applicable for small tightly bound teams will compromise overall project risks, timelines and quality of deliverables.	Peer with organisations – both industrial and research (e.g. CERN) – that have experience in management of development of large scale software intensive systems. Adopt appropriate “industrial” software development processes.	Medium	High
4.5	Lack of attention to non-functional and performance requirements	Performance requirements can sometimes be overlooked in specifications of what is to be delivered to meet overall users’ expectations.	Insufficient performance means that the M&C system cannot provide services at full scale. Users become frustrated with the system that has been implemented which results in lack of acceptance of the system provided.	Simulation; Benchmarking; Modelling, Prototypes; Measures	Medium	High

5 Monitoring & Control Risks for CoDR

5.1 Risks Related to Management and Organisation of Monitoring & Control Development

No.	Risks	Short Description	Risks Becoming Issues Results in:	Proposed Plans to Manage Risks & Issues	Risk Owner	Impact: SKA1 *SKA2*	Likelihood: SKA1 *SKA2*	Exposure: SKA1 *SKA2*	Retire by:
5.1.1	Distributed Development: Task Distribution	• Task uncertainty: WPC and SPO teams don't possess the knowledge and capabilities needed • Task understanding: WPC and SPO teams don't understand the specification of the task • Task coupling: the task is not logically divided into self contained subtasks	• Gaps in WPC and SPO teams' task knowledge and required capabilities result in errors and re-work • The specification lacks clarity, resulting in errors and re-work • A major effort is required to coordinate development work across separate WPC sites • Failure to deliver on time to budget • Poor delivered quality • Risk of staff turnover	• Communication and management of dependencies between project components • Monitoring and managing progress towards delivering planned documentation • Learn from Precursor and Pathfinder experiences	TPM, WPC	High *High*	High *Medium*	Very High *High*	SRR
5.1.2	Distributed Development: Knowledge Management	• Knowledge creation, capture and integration is not managed in a sustainable manner • Not enough documentation, and not of sufficient depth or quality	• Knowledge being held tacitly, resulting in a dependence on individuals who may not pass that knowledge on • The overall level of coordination and hence collaboration is negatively impacted • Failure to deliver on time to budget • Poor delivered quality • Risk of staff leaving	• Implementation and mandated use of a widely accessible and searchable document management system • Phased delivery of documentation • Learn from Precursor and Pathfinder experiences	TPM, WPC	High *High*	Medium *Medium*	High *High*	SRR
5.1.3	Distributed Development: Geographical Distribution	• Spatial distribution: many diverse WPC and the SPO sites may be involved • Temporal distribution: many time zones may be involved • Goal distribution: diverse objectives exist across WPC and SPO teams	Barriers to collaboration result in: • Misunderstandings • Difficulties in scheduling meetings • Varying priorities • Errors and re-work • Conflict due to distance, culture and divergent motivations • Failure to deliver on time to budget • Poor delivered quality	Implement: • Formal system requirements framework • Common document templates and standards • Clear definition and communication of expectations for delivered documents • Selected review of documents prior to delivery to receiving teams • Learn from Precursor and	TPM, WPC	High *High*	High *High*	Very High *Very High*	SRR

No.	Risks	Short Description	Risks Becoming Issues Results in:	Proposed Plans to Manage Risks & Issues	Risk Owner	Impact: SKA1 *SKA2*	Likelihood: SKA1 *SKA2*	Exposure: SKA1 *SKA2*	Retire by:
				Pathfinder experiences					
5.1.4	Distributed Development: Collaboration Infrastructure	• Collaboration across WPC and SPO sites is difficult • Coordination mechanisms across WPC sites not appropriate or sufficient • Process alignment across WPC and SPO sites not appropriate or sufficient	Barriers to collaboration result in: • Misunderstandings • Difficulties in scheduling meetings • Varying priorities • Re-work • Clashes due to distance, culture and divergent motivations • Failure to deliver on time to budget • Poor delivered quality • Risk of staff leaving	• Adopt effective, efficient and commonly available tools to support electronic collaboration • Apply appropriate, internationally recognised standards for project management, including process descriptions and change management • Learn from Precursor and Pathfinder experiences	TPM, WPC	Medium *Medium*	Medium *Medium*	Medium *Medium*	SRR
5.1.5	Aggressive schedule	The schedule for the SKA is ambitious	Late delivery of software compared with initial target dates	• Plan to deliver software incrementally • Allocate resources to problem areas before they escalate • Where possible, decouple development dependencies • Plan for resource contingency • Learn from Precursor and Pathfinder experiences	TPM, WPC	High *High*	High *High*	Very High *Very High*	PRR
5.1.6	Estimation errors	Cost and effort for M&C development underestimated, due to missed tasks or optimistic task resource estimates	Cost creep Delays	• Multiple independent estimates • thorough task identification • comparison with precursor projects • contingency for unexpected additional work	TPC	High *High*	High *High*	Very High *Very High*	PDR

5.2 Risks Related to Engineering

No.	Risks	Short Description	Risks Becoming Issues Results in:	Proposed Plans to Manage Risks & Issues	Risk Owner	Impact: SKA1 *SKA2*	Likelihood: SKA1 *SKA2*	Exposure: SKA1 *SKA2*	Retire by:

5.1.7	Scope of work greater than expected	• Infeasible or unrealistic requirements
		• Underestimation of the costs of complexity
		• Required functionalities are overlooked
		• Insufficient interface definition of – and integration with – other software implementations such as science processing
		• Unnecessary development of software is initiated when existing codes could be re-used or configured
			• Under-estimates of cost, time and the resources required to meet the requirements of software and computing
			• Severe and negative impact on the project as a whole
				• Establish and maintain mechanisms to capture and assess early signs of negative scope risk
				• To constrain software development:
				  • Use existing codes wherever possible, especially COTS
				  • Top-down budgeted 'cost as a design constraint' approach to development, i.e.:
				    • First order parametric estimating models for estimating the level of software development achievable within specified cost budgets
				    • Capture and use software productivity metrics from radio astronomy incremental software developments, other science domains and industry to inform the parametric estimating models
				    • Expert judgement as checks on parametric models
					TPM, WPC	High
						High
							High
							High
								Very High
								Very High
									PDR

No.	Risks	Short Description	Risks Becoming Issues Results in:	Proposed Plans to Manage Risks & Issues	Risk Owner	Impact: SKA1 *SKA2*	Likelihood: SKA1 *SKA2*	Exposure: SKA1 *SKA2*	Retire by:
5.1.8	Scope creep	Failure to baseline and traceably manage requirements held in a central repository	• Change requests create exponentially increased required work effort • Failure to deliver on time to budget • Poor delivered quality	• Set up Change Control Board and related governance structures to tightly manage all requests for change • Use agreed common processes and tools to share requirements-related information • Ensure requirements for component work deliverables are well documented and understood by all teams • Learn from Precursor and Pathfinder experiences	TPM, WPC	High *High*	High *High*	Very High *Very High*	PDR
5.1.9	Misinterpretation and erroneous analysis of requirements	The flow down of requirements is open to misinterpretation particularly when this is solely via document handover	Delivered designs may not meet the original intention of the requirement	• Use agreed common processes and tools to share information related to requirements • Close collaboration between the parties involved in generating requirements including regular reviews of requirements • Learn from Precursor and Pathfinder experiences	TPM, WPC	High *High*	Medium *Medium*	High *High*	PDR
5.1.10	Over-reliance on software development processes appropriate only for small scale projects	Lifecycle development models that are appropriate for small scale early stage development and preliminary implementations are very unlikely to work for development of large scale robust systems.	Reliance on processes only applicable for small tightly bound teams will compromise overall project risks, timelines and quality of deliverables.	Peer with organisations – both industrial and research (e.g. CERN) – that have experience in management of development of large scale software intensive systems. Adopt appropriate “industrial” software development processes.	TPM, WPC	Medium *Medium*	High *Medium*	High *Medium*	SRR

5.3 Risks Related to Architecture

No.	Risks	Short Description	Risks Becoming Issues Results in:	Proposed Plans to Manage Risks & Issues	Risk Owner	Impact: SKA1 *SKA2*	Likelihood: SKA1 *SKA2*	Exposure: SKA1 *SKA2*	Retire by:
5.3.1	Lack of attention to non-functional performance requirements	Performance requirements can sometimes be overlooked	• Insufficient throughput means that the monitoring & control cannot keep up with tasking • Users become frustrated with the implemented system • Results in lack of acceptance of the system	Undertake: • Measures of performance of existing and prototype systems • Simulation • Benchmarking	TPM, WPC	Medium *High*	Medium Medium	Medium *High*	SRR
5.3.2	Incomplete interface identification or definition	There may be some interfaces that are not well specified or overlooked until integration testing and commissioning is in progress.	• An example could be interfaces from the control and monitoring system to data processing systems and interfaces to operators to allow a specific kind of manual override. • Late specification of such interfaces could result in increased cost, time and resources required to meet overall system requirements.	• Collaborative interfaces definition and management. • Undertake ongoing reviews of design documents, and in particular Interface Control Documents • Learn from Precursor and Pathfinder experiences	TPM, WPC	Medium *High*	Medium Medium	Medium *High*	PDR
5.3.	Localization of safety	Incorrect assumption that all safety concerns can be localized to regions, so that Central M&C is not safety-critical, and so that connectivity with Central M&C is not safety-critical	• High cost impact: network redundancy, higher development costs	• Safety threat modeling and analysis to confirm assumption.	TPM, WPC	*High* *High*	Medium Medium	*High* *High*	PDR
5.3.	M&C as part of Scientific Computing[1]	M&C viewed as purely software development as a component of Scientific Computing rather than a system design problem. Insufficient attention to systems issues.	• Safety, reliability impacts. • Poor support for operations	• M&C as independent work package with strong collaborative relationships to System as well as Science Computing, plus linkages to other domains. • Software & Computing redefined as governance layer.	TPM	*High* *High*	Medium Medium	*High* *High*	SRR

[1] The term Scientific Computing is this document refers to data processing directly related to the (real time) production of science output, excluding the low level execution of telescope control and the provision of low level engineering data, some of which may be at the behest of such data processing. The aforegoing is not (yet) official SKA terminology as the architecture is TBD.

No.	Risks	Short Description	Risks Becoming Issues Results in:	Proposed Plans to Manage Risks & Issues	Risk Owner	Impact: SKA1 *SKA2*	Likelihood: SKA1 *SKA2*	Exposure: SKA1 *SKA2*	Retire by:
5.3.	Scale creep	M&C scale (number of Components, monitoring points) much higher than anticipated, keeps increasing as design proceeds	• High costs to rework M&C architecture for greater scale.	• Scalable M&C architecture. • Interactions with domains to establish workload. • Investigate scalability issues for software platform.	TPM, WPC	High *High*	Medium Medium	High *High*	PDR
5.3.	Command conflicts	Auxiliary points of control e.g. domain M&C. Possibility of control conflicts among roles e.g. operators, engineers, scientists	• Loss of integrity of operational state. • Reliability impacts.	• Architectural principles to ensure single point of command, possibly augmented with carefully designed delegation models.	TPM	Medium Medium	Medium Medium	Medium Medium	SRR

5.4 Risks Related to Design

No.	Risks	Short Description	Risks Becoming Issues Results in:	Proposed Plans to Manage Risks & Issues	Risk Owner	Impact: SKA1 *SKA2*	Likelihood: SKA1 *SKA2*	Exposure: SKA1 *SKA2*	Retire by:
5.4.1	Human factors are overlooked in developing interfaces	Overlooking human-machine interface design goals such as: • Effectiveness: helping users achieve their intentions • Efficiency: reducing the time taken and the incidence of user errors • Satisfaction: offering an experience to users conducive to productivity	• Users become frustrated with the implemented system • Results in lack of acceptance of the system	• Include human factor considerations in the high level architecture design activities for interfaces for users and operators • Learn from the experiences gained from Precursor and Pathfinder projects	TPM, WPC	Medium *Medium*	Medium *Medium*	Medium *Medium*	PDR
5.4.2	Diverse M&C development	Local M&C is developed independently by dozens of Component providers, leading to potential quality, integration and maintainability issues	• Low reliability & availability • high development and maintenance costs	• Standardized Component Interface, • guidance to Local M&C developers, • System M&C prototype or dedicated facility as test/validation fixture • certification of Local M&C prior to integration	TPM	*High* *High*	Medium Medium	*High* *High*	CDR
5.4.3	Excessive technology heterogeneity	Independent choices of sensors, actuators, fieldbuses by each Component provider.	• High operations costs • poor maintainability	• Identify standard / preferred technology choices, with slightly weaker rules for off-the-shelf Components. • Trade off imposition of standards against whole lifecycle costs	TPM	*High* *High*	Medium Medium	*High* *High*	CDR
5.4.4	Technology obsolescence	M&C technology choices and capabilities get outdated over long lead time to first science and long lifetime.	• M&C missing state-of-the-art capabilities. • Decreasing maintainability • Limited evolutionary scope.	• Modularized architecture realized with replaceable off-the-shelf components adhering to 'future proofed' standards. • Anticipation of and sensitivity to technology trends, particularly in terms of advanced capabilities.	TPM	Medium *Medium*	Medium *Medium*	Medium *Medium*	CDR