

SSEI Research Task Summary – T1

Task Number: SSEI/T1
Project Title : IMS for Adaptive Systems
Research Theme : *Software Systems Architectures*

Lead Delivery Organisation : SEIC

Version : 3



Objective of Work (why are we doing it ?)

Modern military systems are using Integrated Modular Systems (IMS) to reduce life-cycle costs and to ease upgrades. These systems need to be increasingly adaptive, e.g. to respond in real-time to changing operating environments, including recovery from failure, and to provide autonomy. Thus more adaptive IMS technology is needed in order to meet future military requirements. This applies both to individual platforms, in all military domains, and to the development of Network Enabled Capability (NEC).

The objective of the task is thus to investigate and demonstrate techniques for extending the current IMS approach with a view to increasing adaptive behaviour whilst maintaining dependability.

Nature of Work (what is it?)

The task will build on previous MOD-funded Avionics Systems Standardisation Committee (ASAAC) work and industry-funded research into IMS software concepts for military embedded systems. IMS is the software architectures already used on Tornado and Hawk and proposed for Typhoon and Wildcat. The task will aim to extend the current IMS capability in two directions:

- Application of IMS to more adaptive systems, in particular to support future system operations in more dynamic operating environments.
- Application of IMS to platforms in non-air systems domains, in particular to land-based vehicles.

Other modular software architectures, including civil standards, will be reviewed and the portability of applications between architecture types considered

Outcomes (what will it produce/has it produced ?)

- Report on state of the art in adaptive software architectures for dependable real-time systems.
- Report and demonstration on application of IMS to non-air systems applications, including lessons learned and future IMS research directions (that should provide benefits to future development of IMS for a range of military applications).
- Report and demonstration on application of (non-IMS) modular software architecture approaches to dependable real-time systems.
- Report and demonstration on IMS for future adaptive systems

Timescales 36 month tasks, April 2008 to March 2011

Partners BAE Systems

Related Work SSEI/T4

Task Lead Dr Alan Grigg
SEIC, Loughborough
Email alan.grigg@ssei.org.uk
Tel. 01509 635218

SSEI Research Task Summary – T2

Task Number: SSEI/T2

Lead Delivery Organisation : University of York

Project Title : Evidence-based Management

Research Theme : *Management of Software Systems Projects*

Version : 3



Objective of Work (why are we doing it ?)

The objective of the work is two-fold:

- To enable the acquisition organisation, Integrated Project Teams, Delivery Teams and supply chains to improve the collective performance of software engineering across the contractual and other interfaces involved, leading to improvement in project performance and outcomes.
- To provide organisations with the means to generate and use reliable evidence and measures to support decision making in Software Engineering Management.

Nature of Work (what is it?)

Engineering Management is an area of professional practice that can play a key role in improving the performance of defence acquisition programmes. It focuses on the planning, monitoring and supply-chain coordination of software engineering tasks and related product and service outcomes. It can be thought of as managing the *delivery of software engineering capability* to projects, the missing piece of the jigsaw between process improvement (e.g. Capability Maturity Model Integration) and project management.

Decision-makers in Engineering Management roles require accurate and dependable information. This task addresses research issues concerned with meeting these needs, focussing on the identification of key technical measures and decision-support mechanisms and their application throughout the procurement lifecycle

Outcomes (what will it produce/has it produced ?)

Core Research - strategy reports on:

- Software Engineering Management Capability to Improve Project Performance
- Measurement Principles for the Engineering Management of Software-Intensive Systems
- Measurement Guidance for the Engineering Management of Software- Intensive Systems

Case Study Engagements – collaborative, practical studies on:

- Delivering evidence-based practice and decision support to projects, developing and sharing practical guidance, models, key technical measures.

Timescales 36 month task, March 2008 to March 2011

Partners

Related Work SSEI/T3

Task Lead Dr John Murdoch
john.murdoch@ssei.org.uk
01904 567836

SSEI Research Task Summary – T5

Task Number: SSEI/T5

Lead Delivery Organisation : University of York

Project Title : Model-Driven Integration of Software Systems

Research Theme : *Integration of Software Systems*

Version : 3



Objective of Work (why are we doing it ?)

For software acquisition to be cost-effective, it is sometimes necessary to obtain software systems from multiple, disparate suppliers. In particular, there may be a need to integrate newly purchased software systems with existing legacy systems. Enabling such software systems to interoperate poses a significant integration problem.

A key question is to determine whether integration can even be undertaken. Significant cost savings can be obtained by having an early understanding of the suitability of candidate systems for integration.

The emphasis is on automated checking techniques, which are essential for the techniques to be practical and scalable.

Nature of Work (what is it?)

This work provides a mechanism through which integration of disparate software can be better understood at an early stage and could be greatly improved.

The research will investigate Model Driven Engineering (MDE) techniques for software systems integration. MDE involves the use of abstract, machine-checkable models for describing software systems. Automated tools can then be used for analysing, transforming, comparing, merging and manipulating models.

The MDE techniques could thereafter be combined with code generation and transformation to support system generation.

Outcomes (what will it produce/has it produced ?)

This task will produce:

- A state-of-the-art survey of model-driven software systems integration.
- Techniques for checking compatibility between software system models, based on both structural and behavioural models.
- Techniques and tools for model integration.

Timescales 32 month task, July 2008 to February 2011

Partners

Related Work SSEI/T4

Task Lead Professor Richard Paige
paige@cs.york.ac.uk
01904 433242

SSEI Research Task Summary – T6

Task Number: SSEI/T6

Lead Delivery Organisation : University of York

Project Title : Software Safety Cases – Establishing a Systematic Approach

Research Theme : *Developing Dependable Systems*

Version : 3



Objective of Work (why are we doing it ?)

Conflicts about the adequacy of software safety cases can arise between developer and acquirer software authorities. This often occurs late in the project, once the majority of the safety case is developed, so results in significant project risk, leading to delays and cost overruns. The late identification of the requirement for additional software safety evidence is particularly problematic as it can significantly delay entry into service.

This task aims to provide guidance and 'standardisation' in the way that software safety arguments are presented and supported, giving improved transparency to all parties, earlier in the programme. It is expected that this will help all parties to reach agreement by significantly reducing subjectivity

Nature of Work (what is it?)

It is increasingly recognised that software safety cases should be hazard-focused and evidence based. However, there is insufficient guidance on how such safety arguments should be established, structured and presented, in the context of DS 00-56. In addition, many developers are unclear about how existing software assurance and software safety lifecycle activities relate to the problem of establishing a software safety case.

The aim of this task is to develop practical and accessible Standards of Best Practice (SoBP) that will address the concerns highlighted above and enable developers to construct software safety cases, acceptance authorities to review and accept these cases, and acquirers to guide and control safety-critical and safety-related software intensive projects.

Outcomes (what will it produce/has it produced ?)

This task will produce three outputs:

- SoBP for software developers and acquirers on establishing clearly structured, hazard-based arguments for software safety
- SoBP for software developers and acquirers on evidence selection for software safety cases, and determining the assurance offered by different forms of software safety evidence
- Case study examples of the application of the SoBPs

Timescales 36 months, March 2008 to February 2011

Partners

Related Work SSEI/T11, SSEI/T21, SSEI/T22

Task Lead Dr Tim Kelly
tim.kelly@cs.york.ac.uk
01904 432764

SSEI Research Task Summary – T7

Task Number: SSEI/T7

Lead Delivery Organisation : Newcastle University

Project Title : Dependability Explicit Metadata

Research Theme : *Developing Dependable Systems*

Version : 3



Objective of Work (why are we doing it ?)

Many defence systems need to be able to maintain capability whilst undergoing either imposed change, e.g. due to failure, or to support mission change. It will also be necessary to preserve dependability, a term which encompasses such properties as safety, security, availability, etc. This ability to maintain a dependable service is known as “resilience”, and is central to achieving the benefits of Network Enabled Capability (NEC), such as agile mission groups, through dynamic reconfiguration.

Many systems, including NEC, are data intensive. The use of dependability explicit metadata, that is, information about the data itself, such as its source, timeliness, independence or credibility, is a promising approach to achieving resilience hence its feasibility should be established.

Nature of Work (what is it?)

This task will investigate the support for dynamic reconfiguration of software intensive systems as a means of achieving resilience.

This task will identify, in the context of network-enabled systems, dependability properties that can be defined and stated explicitly. These will be supported by policies for governing system configuration to maintain dependable levels of service.

The work will be demonstrated by prototype tool support, which will include a monitoring and reasoning framework, to provide a “proof-of-concept” demonstration of metadata-based dynamic resilience in a network-enabled environment.

Outcomes (what will it produce/has it produced ?)

The task will produce five outputs.

- A summary report on the state of the art in dependability explicit computing and initial dependability classifications.
- Summary presentation on properties, policies and mechanisms.
- Extended report on properties, policies and exemplary application to case studies.
- Prototype tool support framework for evaluating metadata approach.
- Final report and research roadmap.

Timescales 36 month task, March 2008 to February 2011

Partners

Related Work

Task Lead Dr Steve Riddle
Steve.Riddle@ncl.ac.uk
0191 222 5156

SSEI Research Task Summary – T8

Task Number: SSEI/T8
Project Title : Dependable Use of FPGAs
Research Theme : *Developing Dependable Systems*

Lead Delivery Organisation : University of York

Version : 3



Objective of Work (why are we doing it ?)

Field-Programmable Gate Arrays (FPGAs) offer considerable advantages for the developers of modern high-integrity systems. They can mitigate the effects of obsolescence, provide more flexible, quickly reconfigured processing platforms and can be used to enhance the survivability and fault-tolerance of systems. The potential of these devices is not yet being fully exploited within MOD, however. One reason for this is a lack of established practice and guidance as to how safety assurance can be achieved for FPGAs.

This task aims to develop industry consensus guidance on the safety assurance of FPGAs in the context of DS 00-56 Issue 4, and to consider the safety and dependability implications of the use of FPGA technology in model-driven development approaches.

Nature of Work (what is it?)

This task will establish typical use contexts for FPGAs, based on current research and industrial practice, and will provide guidance as to the potential benefits and pitfalls associated with these contexts, in order to inform future procurement decisions. Example application areas include direct compilation of a design onto a device and the use of FPGAs to replace legacy components. Guidance on the safety implications of FPGAs in system development will address both the nature of process and product evidence required to support certification and how the system can be designed for safety and maintainability. A series of design recommendations will be produced, recommending design restrictions to achieve better fault-tolerance in likely failure conditions.

Outcomes (what will it produce/has it produced ?)

This task will produce three outputs:

- Guidance on potential benefits and safety-related issues concerning the use of FPGAs
- Guidance on verification and certification issues associated with the use of FPGAs, including tool support options and future tooling requirements
- Case study examples of the application of the guidance, across high- and low-integrity systems

Timescales 36-month task, May 2008 to February 2011

Partners

Related Work SSEI/T13

Task Lead Dr Iain Bate
iain.bate@cs.york.ac.uk
01904 432786

SSEI Research Task Summary – T14

Task Number: SSEI/T14

Lead Delivery Organisation : YorkMetrics Ltd.

Project Title : Managing Value of Upgradeability in Software-intensive Systems

Research Theme : *Management of Software Systems Projects*

Version : 2



Objective of Work (why are we doing it ?)

Future defence capability will be supported by fewer platforms that can adapt to different missions as needs arise and incorporate newly emerging technologies. Software will play a central role in providing through-life adaptability, but designing software systems for adaptability - by means of modularity – increases development costs. The initial investment decision is made with the objective of reducing the through-life costs of providing platform adaptability.

Research aims to link together (a) estimated initial investment costs of different software architecture, upgrade and incremental delivery strategies; (b) estimated through-life software change costs, and (c) adaptability benefits in the context of uncertain, requirements and technology evolution.

Nature of Work (what is it?)

Research will provide software acquirer and supplier decision makers with the means to conduct cost/benefit trade-offs between different software architecture, upgrade and incremental delivery strategies in the context of uncertain requirements and technology evolution.

The task will develop models of the initial investment costs and through-life costs and benefits of identified software upgrade strategies. A 'business case' type of approach is to be adopted, to inform choices between different types of initial architecture investment. A key concept is to enable decision makers to associate a value with 'change options'; future requirements and technology evolution will always be uncertain, but there is value in providing options for future adaptation. How much initial investment is justified to provide these options?

Outcomes (what will it produce/has it produced ?)

This task will produce four outputs:

- Catalogue of upgrade options and estimates
- Measurement model and operational verification
- Models of modular archetypes in software upgrades
- Interim Standard of Best Practice on software modular upgrade options

Timescales 20 month task, October 2009 to July 2011

Partners

Related Work SSEI/T3

Task Lead Graham Clark
graham.clark@ssei.org.uk
01904 5678 34

SSEI Research Task Summary – T15

Task Number: SSEI/T15

Lead Delivery Organisation : BAE Systems Ael

Project Title : Through Life Risk management for Software Intensive Systems

Research Theme : *Management of Software Systems Projects*

Version : 2



Objective of Work (why are we doing it ?)

Identifying and controlling risks has long been identified as a key element of delivering successful projects. In practise, risk management has focussed on particular aspects of a product's lifecycle (e.g. development) and has not taken a through life approach.

For software intensive systems this through life approach is becoming increasingly important, given the move away from large scale development programmes to one of evolution and upgrade over an increasingly long product lifespan

This task aims to provide guidance to the identification of risk for future and current programmes, cross-referenced to real-world experience, and provide pointers for the future direction of research to address software-intensive programme risk.

Nature of Work (what is it?)

This task will investigate the relationship between risks identified and mitigated in development and relate them to issues emerging in the later support phase of the product.

The task will use existing risks on current MOD programmes to develop a Risk Management taxonomy to assist in recognition, mitigation and avoidance of common risk types for current and future programmes.

Outcomes (what will it produce/has it produced ?)

- A taxonomy for the categorisation of Engineering Risks associated with the Through Life Management of Software Intensive Systems
- Report on the risks encountered during the life of the candidate software-intensive systems, with their mapping to the taxonomy
- A review of the mapping between significant programme through-life risk issues and the current SSEI areas of research

Timescales 9 month task, October 2009 to June 2010

Partners

Related Work

Task Lead Fraser Anderson
BAE Systems Ael, Yeovil
fraser.anderson@ssei.org.uk
01935 443067

SSEI Research Task Summary – T16

Task Number: SSEI/T16

Lead Delivery Organisation : Newcastle University

Project Title : Interface Contracts for Architectural Specification and Assessment

Research Theme : *Software Systems Architectures*

Version : 2



Objective of Work (why are we doing it ?)

Software dependent systems are increasingly component-based, with an architecture than can be characterised as “systems of systems” (SoS). Such architectures help to provide a responsive and flexible system, but at the cost of increased complexity due to the lack of central authority and coordination. This complexity affects our ability to predict emergent system-level properties including those related to safety and security, putting the system integration phase at increased risk of cost and time overruns.

An investigation of the benefits that can be gained from formal expression and analysis of interface contracts will help to advance practice in design-time analysis of emergent properties.

Nature of Work (what is it?)

The work will establish the current capability for expressing and exploiting contracts in industry-strength architectural description frameworks such as the MOD Architecture Framework (MODAF) and the Architecture Analysis & Design Language (AADL), and explore the benefits that can realistically be gained from formal expression and analysis of contracts. Building on rely-guarantee contract languages, a basic contract interface language for functional and non-functional properties will be developed. The language will be evaluated using a Service-Oriented Architecture (SOA) based, proof of concept study.

Finally a roadmapping activity will identify the research and development directions that should be taken to advance best practice.

Outcomes (what will it produce/has it produced ?)

The task will produce four outputs:

- Survey and evaluation of architectural frameworks supporting contract-based specification, including MODAF and AADL
- A basic contract-based interface specification language definition with semantics and worked examples.
- Proof of concept study: application and evaluation report
- Roadmap report

Timescales 24 month task, January 2010 to December 2011

Partners

Related Work SSEI/T10

Task Lead Dr John Fitzgerald
John.Fitzgerald@ncl.ac.uk
0191 222 8228

SSEI Research Task Summary – T17

Task Number: SSEI/T17

Lead Delivery Organisation : BAE Systems INSYTE

Project Title : Evolving Trials and Acceptance Strategies for COTS-based Combat Systems

Research Theme : *Integration of Software Systems*

Version : 2



Objective of Work (why are we doing it ?)

The assurance of combat system integrity is of utmost importance when deploying new technology or capability into an operational environment for Land, Sea, Air and/or Joint operations.

The complexity and safety critical nature of current combat systems means the trials programmes can take many months to complete, add significantly to the cost of support and capability insertion programmes, and delay the introduction of new technologies into service.

The objective of this task is to identify opportunities for reducing trials costs and duration whilst ensuring appropriate levels of system integrity can be demonstrated prior to operational deployment.

Nature of Work (what is it?)

This task will investigate how confidence in system integrity can be built quickly and effectively through the phases of the development lifecycle.

It will look at the use of incremental development models to improve visibility and customer involvement.

It will identify effective and focussed regression testing strategies where they are appropriate.

It will look into the read-across of testing evidence from trans-class trials programmes, and provide an improved understanding of how confidence levels can be established and interpreted.

Outcomes (what will it produce/has it produced ?)

The task will produce the following outputs:

- Summary report on the existing state and drivers for change;
- Report on the scope and opportunities for change, based on current approaches and best practice;
- Report on alternative testing strategies, covering industry best practice and alternative approaches;
- Report on development lifecycle and facilities, investigating opportunities for change;
- Final report consolidating the findings and recommendations and assessing the opportunities for change

Timescales 20 month task, February 2010 to October 2011

Partners

Related Work

Task Lead Paul Callaghan
BAE Systems, New Malden
paul.callaghan@baesystems.com
0208 329 5810

SSEI Research Task Summary – T18

Task Number: SSEI/T18

Lead Delivery Organisation : HP Enterprise Services

Project Title : Framework for Evolutionary Transition of Legacy Software Systems

Research Theme : *Integration of Software Systems*

Version : 2



Objective of Work (why are we doing it ?)

Historically, the UK MOD has developed and upgraded software systems in an application-specific manner based on defined, but often stove-piped, capability needs driven by urgent requirements.

This has led to substantial amounts of disparate legacy software whose maintenance becomes problematic and expensive over time.

In the absence of a controlled process or framework, the approach for the modernisation of application services is fragmented and costly in terms of hardware, operating environments, testing and interoperability.

This work is needed so that legacy software systems can be maintained and modernised to more effectively support the MOD's constantly evolving user requirements.

Nature of Work (what is it?)

This research will investigate a new approach whereby the transition of legacy software systems to meet future capability needs is planned and managed in accordance with demonstrated best practice.

This approach involves the development of an Evolutionary Legacy Transition Framework (ELTF) to modernise legacy software systems to meet current and future capability needs.

A representative environment will be demonstrated showcasing the ELTF with appropriate systems and processes, employing a Service Orientated Architecture (SOA) approach. This environment will be used to demonstrate effective changes to legacy software systems relevant to a modern infrastructure, thereby validating by demonstration the theoretical conclusions of the first part of the research

Outcomes (what will it produce/has it produced ?)

The task will:

- Identify ways of retaining legacy software systems and to move them into modern development environments
- Provide a Service Orientated Architecture (SOA) based framework for the evolutionary transition of legacy software systems,
- Provide a recommended Governance Approach, and a Standard of Best Practice for legacy software systems transition,
- Develop a demonstration environment to demonstrate of key principles, processes, techniques and technologies

Timescales 6 month task, timescales TBC

Partners IBM

Related Work SSEI/T 10

Task Lead David Brooks
dave.brooks@hp.com
01256 742135

SSEI Research Task Summary – T19

Task Number: SSEI/T19

Lead Delivery Organisation : University of York

Project Title : Dynamic Operational Risk Assessment for NEC Systems of Systems

Research Theme : *Developing Dependable Systems*

Version : 2



Objective of Work (why are we doing it ?)

The current drive towards Network-Enabled Capability in theatre is increasing the complexity of battlefield networks and the volume of live data available to commanders. There is a risk that this both reduces the commander's ability to understand the state of his forces in the field while at the same time providing him with huge volumes of mission data. Network-related issues such as data corruption, and source-sender ambiguity may increase risk to missions, equipment and personnel.

This task aims to provide a suite of tools to enable the commander to process the complex volume of risk-related data during operation, by producing a 'live' safety case to enable the commander to gain a full understanding of the 'risk picture' in dynamic battlefield situations.

Nature of Work (what is it?)

Conventional safety cases present a static view of system safety, which cannot support commanders in making tradeoffs between performance and safety in real time. Many current approaches to the safety of military systems are 'accident-focussed', and pay little attention to the risks caused by hostile action.

This work will build on previous work on simulation-based hazard analysis for systems of systems and recent research on human cognition and communication to develop a suite of tools to enable rapid hazard identification, hazard analysis and risk assessment during operations. A dependability model for the underlying network infrastructure will be developed, along with an approach for the establishment of a generic safety assurance argument for infrastructure in general, distinct from a specific context-of-use.

Outcomes (what will it produce/has it produced ?)

This task will have three outcomes:

- Development of a risk-modelling approach which can be applied across a system of systems in real time
- Establishment of an approach to assurance of infrastructure
- Prototype software tools for dynamic operational risk assessment, validated by case study and practitioner review

Timescales 36 month task, December 2009 to November 2012

Partners

Related Work

Task Lead

Dr Rob Alexander
robert.alexander@cs.york.ac.uk
01904 432773

SSEI Research Task Summary – T20

Task Number: SSEI/T20

Lead Delivery Organisation : Adelard LLP

Project Title : Supporting the Standardisation of Assurance Argument and Evidence Schemas

Research Theme : *Developing Dependable Systems*

Version : 2



Objective of Work (why are we doing it ?)

The ability to create and maintain an assurance case is a key capability for defence procurement, and underpins many of the SSEI's 'Hard Problems'. Standards such as DS 00-56 are seen as one of the key assurance policy frameworks, based on a demonstration and goal-based approach. Standardising the way in which claims, arguments and evidence are represented and recorded would yield significant benefits, for example interoperability, re-use, use of open systems and legacy systems and consistency. However, the full benefits of standardisation will only be realised through adoption of an industry-wide approach.

The aim of this task is to influence emerging standards for assurance arguments, to ease international procurements and to produce guidance for MOD and the SSEI on the finalised standard and its implications.

Nature of Work (what is it?)

The Object Modelling Group (OMG) Software Assurance (SwA) Initiative is working to prepare technical interoperability standards for Software Assurance. These standards address the structuring of arguments and the required supporting evidence.

This task aims to continue UK participation in driving the standard forward, maintaining awareness of the OMG's work and other emerging international standards for safety policy. SSEI members will attend and provide input to relevant meetings of the OMGSwA, and will continue to develop and influence the OMG metamodels for software assurance evidence and argumentation, ensuring that these are kept consistent with UK MOD practice and policy. Where necessary, the task will provide third-party review of OMG deliverables. The work will be communicated to defence and industry partners.

Outcomes (what will it produce/has it produced ?)

This task will have two main outputs:

- Developmental and review input to the OMG assurance argument and assurance evidence meta-models, which will be presented to the SSEI Developing Dependable Systems SIG
- Guidance describing the relationship between the OMG SwA standards and the UK safety and assurance policy framework

It is also hoped that this task will inform the ongoing work of the MOD Safety Standards Review Committee

Timescales 18-month task, September 2009 to February 2011

Partners University of York, Integrate

Related Work SSEI/T6, SSEI/T21, SSEI/T22, SSEI/T23

Task Lead Luke Emmet
loe@adelard.com
020 7490 9450

SSEI Research Task Summary – T21

Task Number: SSEI/T21

Lead Delivery Organisation : University of York

Project Title : Managing System and Software Safety Case Interface Issues

Research Theme : *Developing Dependable Systems*

Version : 2



Objective of Work (why are we doing it ?)

Most defence systems involve a substantial supply chain, and problems arise due to the problems of managing safety across organisational boundaries, both in terms of impact on product safety, and on the safety case. Safety requirements for software are often missing, inadequately defined or assumed (incorrectly) to be derivable by a lower-tier supplier. Further sub-contracts are often finalised before software safety requirements are understood, with attendant risks of substantial change. Conversely, there may be cases in which full disclosure at an organisational boundary is not desirable.

This task aims to provide guidance to support the development and expression of adequate software safety requirements. It also aims to show how safety-case architectures can be used to manage requirements across system and contractual boundaries.

Nature of Work (what is it?)

Safety-related requirements flowed down to software developers from the system level often fail to consider the specific failure characteristics of software or the ways in which these can be analysed to provide information which can usefully be deployed in a system safety case. There is also a need for contracts to be sufficiently flexible to handle the evolution of software safety requirements over the lifecycle of a system.

This task will provide practical guidance on how software requirements can be derived by exploiting knowledge of other systems. The task will produce best-practice guidance on the expression of software safety requirements, on the management of contractual specifications to allow for evolving system and software safety cases and on the associated safety-case architectures.

Outcomes (what will it produce/has it produced ?)

This task will produce a Standard of Best Practice addressing three areas:

- Guidance for software developers and acquirers on the definition of software safety requirements
- Guidance on the expression of software safety requirements across organisational, technical and contractual boundaries
- Guidance for software acquirers on the exploitation of safety-case architectures to manage safety requirements throughout the system lifecycle

Timescales 15- month task, July 2009 to September 2010

Partners

Related Work SSEI/T2, SSEI/T3, SSEI/T6 and SSEI/T11

Task Lead Dr Tim Kelly
tim.kelly@cs.york.ac.uk
01904 432764

SSEI Research Task Summary – T22

Task Number: SSEI/T22

Lead Delivery Organisation : University of York

Project Title : Updating Guidance on the Application of Civil Software Standards to DS 00-56

Research Theme : *Developing Dependable Systems*

Version : 2



Objective of Work (why are we doing it ?)

MOD's policy with regard to software development standards is that they should be "as civil as possible, and only as military as necessary". It is therefore imperative that both industry and MOD understand how to demonstrate that use of the evolving civil standards for software development – DO-178 and IEC 61508 - meets the requirements of DS 00-56 Issue 4.

This task will evaluate the proposed changes in DO-178C and IEC 61508 against UK MOD standards. In particular, it will examine the variety of methods and processes available to COTS vendors to satisfy the certification objectives of the civil standards and the possibilities the civil standards afford for novel development techniques, and provide guidance as to what additional evidence might be required to satisfy the military standards.

Nature of Work (what is it?)

Some of the proposed changes in the civil standards have not yet been assessed against UK MOD standards. These are primarily in the areas of tool qualification, model-based design and verification, the use of object-oriented technology and the deployment of formal methods. The civil standards are also less prescriptive than their predecessors, which means that techniques other than testing can be used to demonstrate the satisfaction of safety objectives.

The task aims to assess the certification strategies suggested by the evolving civil standards to determine whether the kinds of evidence they describe for each integrity level is sufficient to support a compelling safety argument as required by DS 00-56 Issue 4. Where there is a 'gap' between civil and military requirements, the SSEI will identify where deficiencies are likely to occur and recommend solutions to bridge the gap.

Outcomes (what will it produce/has it produced ?)

This task will produce 3 outputs:

- Guidance for software developers and acquirers as to the principal changes in the second edition of IEC 61508 and DO-178C and their implications for satisfaction of DS 00-56
- A report identifying current and future trends in military and civil safety culture, such as a move to a less prescriptive approach and an increasing dependency on COTS products. Guidance as to likely effects of these cultural changes on future civil and military standards
- Updates to the Standard of Best Practice on Software in the Context of DS 00-56 Issue 4 to address non-MOD standards

Timescales 15-month task, July 2009 to September 2010

Partners

Related Work SSEI/T6, SSEI/T11, SSEI/T21

Task Lead Professor John McDermid
john.mcdermid@cs.york.ac.uk
01904 432726

SSEI Research Task Summary – T23

Task Number: SSEI/T23

Lead Delivery Organisation : Agent Oriented Software

Project Title : Certifiable Safety-Critical Software Systems that can be Incrementally Upgraded

Research Theme : *Developing Dependable Systems*

Version : 2



Objective of Work (why are we doing it ?)

The new generation of Unmanned Air Systems (UAS) have a high degree of autonomous capability, provided by decision-making software which replaces functions performed by the human crew of a manned or remotely-piloted vehicle. These extend beyond flight control functions to a range of other critical roles, e.g. sense-and-avoid, mission management and re-routing. If such UASs are to undertake missions beyond those for which they are initially designed, it must be possible for the on-board Autonomous Mission Management system to be upgraded with the necessary additional or revised behaviours. The challenge is to permit such upgrades without the need for large-scale recertification.

This task aims to produce guidance on the design and assessment of decision-making software, including a Standard of Best Practice on incremental certification for decision-making software.

Nature of Work (what is it?)

A major challenge for the adoption of embedded, autonomous software-based systems to replace mission and flight-critical functions is the cost and time required to assess changes to the software, once it has initially been certified. Modifications often incur re-certification costs approaching the cost of the original clearance. This task aims to produce a certification process for decision-making software which makes the re-certification effort more commensurate with the scale of the change introduced. Outputs from this task will extend earlier work on software-based systems which are subject to incremental upgrade.

This task will develop a safety-case architecture for incrementally-certified decision-making software, and guidance on the argument strategies and evidence artefacts required, specialising previous work on incremental and modular certification.

Outcomes (what will it produce/has it produced ?)

This task will have three outputs:

- Guidance on the design of embedded software-based systems to support an incremental certification approach
- Guidance on the development of safety case and assurance arguments for incrementally-upgradeable software
- Guidance on the nature of the process- and product-based evidence required to support such arguments

A substantial case study will be produced, based on the addition of autonomous behaviours to an autonomous decision-making system for UAS operation

Timescales 26-month task, January 2010 to February 2012

Partners University of York, CAA, Kestrel Technology LLC

Related Work T6, T11, and the ASTRAEA Programme

Task Lead Hasan Acar
hasan.acar@aosgrp.co.uk
01223 308000

SSEI Research Task Summary – T24

Task Number: SSEI/T24

Lead Delivery Organisation : Cobham Technical Services

Project Title : Pan DE&S Management of Information Assurance for Software-Intensive Projects

Research Theme : *Developing Dependable Systems*

Version : 2



Objective of Work (why are we doing it ?)

Modern military equipment has increasingly complex requirements for missions and information-handling. At the same time, threats to the confidentiality, integrity and availability of mission information are growing and evolving. This complexity is increasingly being addressed by the procurement of software-intensive systems and the wider use of pre-developed software.

A DE&S-sponsored security survey recently identified deficiencies and inconsistencies in the MOD's procurement process. These can cause programme delays and cost-overruns, as well as unacceptable exposure to mission vulnerabilities and/or the loss of confidence in the use of mission systems in critical scenarios.

This task aims to develop a pan DE&S project-oriented Information Assurance Management System.

Nature of Work (what is it?)

A recent DE&S survey identified considerable duplications of effort in establishing management processes across IPTs and inconsistencies in the methods used to determine and record risk levels and select appropriate risk-management strategies.

This task will investigate current best practice for information assurance in MOD, HMG, industry and academia. It will develop an Information Assurance Management System for use across DE&S. The System will include process maps, step-by-step guidance and risk-management techniques, and will incorporate a reporting framework to ensure that assurance evidence is presented in a mature, consistent and auditable format. This will help to inform decision-making concerning system assurance and accreditation.

Outcomes (what will it produce/has it produced ?)

This task will have 3 main outcomes:

- Project-oriented Information Assurance Management System for use across DE&S
- Step-by-step guidance to help IPTs manage the accreditation process consistently and ensure compliance with JSP440
- A template and process for an Information Assurance Case report, to present an evidence-based case for accreditation to inform decision-making

Timescales 24-month task, August 2009 to July 2011

Partners University of York, CESG, DSAS

Related Work

Task Lead Tim Reilly
tim.reilly@cobham.com
01372 367000

SSEI Research Task Summary – T25

Task Number: SSEI/T25

Lead Delivery Organisation : BAE Systems Ael

Project Title : ALARP Verification Assessment Modelling

Research Theme : *Management of Software Systems Projects*

Version : 2



Objective of Work (why are we doing it ?)

Def Stan 00-56 mandates “Where possible, the objective evidence provided shall be commensurate with the potential risk posed by the system, the complexity of the system and the unfamiliarity of the circumstances involved.”

This objective is easy to state, but hard to satisfy, as it is often difficult to assess the value of evidence collection, prior to carrying out the work. This task will address this problem by developing “proof of concept” models that predict and provide objective evidence of the assurance value of verification techniques (both dynamic and static) for software dependent systems, with the aim to assist MOD with “as low as reasonably practicable” (ALARP) decisions where legacy software is used or where civil standards are applied.

Nature of Work (what is it?)

This research will involve the compilation and analysis of existing project data, along with the evaluation of relevant existing models (including cost models and CBA (Cost Benefit Analysis) Models). It will assess data from recent defence and civil projects, including several major aerospace projects.

If the purchase and adaptation of an existing model is not practical the study will develop a new model.

The “proof of concept” ALARP verification model(s) will be demonstrated to the key stakeholders before being verified and refined against existing MOD projects.

Outcomes (what will it produce/has it produced ?)

- Report on the underlying data and specification for one or more ALARP verification models
- Report on the selection and evaluation of potential ALARP verification model(s)
- Report and “proof of concept” demonstrations of the ALARP verification model(s)
- Evaluation report of the ALARP model(s) against suitable MOD projects and existing MOD Cost Benefit Analysis processes.

Timescales 13 month task, November 2009 to November 2010

Partners

Related Work SSEI/T6, SSEI/T22

Task Lead

Janet Pollard
BAE Systems Ael, Yeovil
janet.pollard@ssei.org.uk
01935 445411

SSEI Research Task Summary – T26

Task Number: SSEI/T26

Lead Delivery Organisation : Civil Aviation Authority

Project Title : Assurance of Evolving Software: Open Systems and Legacy Components

Research Theme : *Developing Dependable Systems*

Version : 2



Objective of Work (why are we doing it ?)

Open Systems Architecture approaches appear to offer considerable benefits, in terms of reduced development costs and shorter timescales than traditional software development methods. The approach has been used successfully on defence-related systems, e.g. submarine sonar. However, there are unresolved issues concerning assurance and assessment of open systems themselves, and of legacy software and COTS products ported onto open systems. These issues threaten the wider adoption of Open Systems development in military and civil applications.

This task aims to provide a strategy and supporting guidance as to how legacy and COTS software can be safely integrated into modern software systems.

Nature of Work (what is it?)

Recent work on the assurance of highly-integrated software systems has identified several 'research challenges'. In terms of software design, these include the mechanics of component composition and the provision of architectural barriers to failure propagation. For safety assurance arguments, challenges include the ability to bound the impact of a change to argument and evidence, the separation of claims about infrastructure from those concerning applications, and the acceptability of using evidence from process to support claims about the safety of a product.

In terms of design, the task will provide practical guidance on the identification and classification of modules, dependencies and interfaces in existing software and infrastructure, It will also provide detailed guidance on the development of well-structured, assurance arguments for pre-existing software.

Outcomes (what will it produce/has it produced ?)

This task will have 4 main outputs:

- Guidance for software developers and system integrators on the identification and categorisation of architectural barriers within pre-existing software and the protections they afford
- Guidance on the use of process evidence in safety assurance arguments
- Guidance on the derivation of evidence concerning 'black-box' software components
- Guidance on the nature of confidence required of evidence in assurance arguments and the development of intelligible arguments

Timescales 24-month task, June 2010 to May 2012

Partners University of York, University of Bristol, MBDA

Related Work SSEI/T6, SSEI/T11, SSEI/T21, SSEI/T22

Task Lead Andrew Eaton
Andrew.Eaton@caa.co.uk
01293 573504