Australian Government
Department of Defence
Science and Technology

Research Notes – Openness and Evolvability - Legal Assessment

Michael Haddy and Adam Sbrana (editor)*

Maritime Division
Defence Science and Technology Group

***Innovation Science**

DST-Group-TN-1543

ABSTRACT

These Research Notes form part of a series of notes extracted from work undertaken by Innovation Science in the establishment of Openness and Evolvability assessment Methods and Processes. This set of Research Notes focusses on Legal Assessment. This work was undertaken from the late 1990s to 2007 and focussed on the application to Submarine Combat Systems.

RELEASE LIMITATION

Approved for public release

Produced by

Maritime Division
DST Group Stirling
HMAS Stirling
PO Box 2188 Rockingham DC WA 6967

Telephone: 1300 333 362

© Commonwealth of Australia 2016
AR-016-662
August 2016

APPROVED FOR PUBLIC RELEASE

Contents

Glossary

IP	Intellectual Property
PMFL	Performance Monitoring Fault Location
IV&V	Independent Validation and Verification
V&V	Verification and Validation

1. Introduction

These Research Notes have been extracted from work undertaken by Innovation Science under contract to Defence Science and Technology Group during the period from the late 1990s until early 2007.

In entirety the Research Notes form a subset of the overall assessment Methodology and Processes developed to assess system level Openness and Evolvability.

The Research Notes within this report focus on Legal Assessment.

2. Legal Assessment

The legal assessment comprises a series of yes/no questions. Each question defines the maximum score that can be allocated to the legal assessment if the question is answered in the negative. If all questions are answered in the affirmative, then the legal assessment is awarded full marks.

The flowchart shown in Figure 1 summarises the assessment process. Each question within the flowchart is explained in greater detail in the sections that follow.

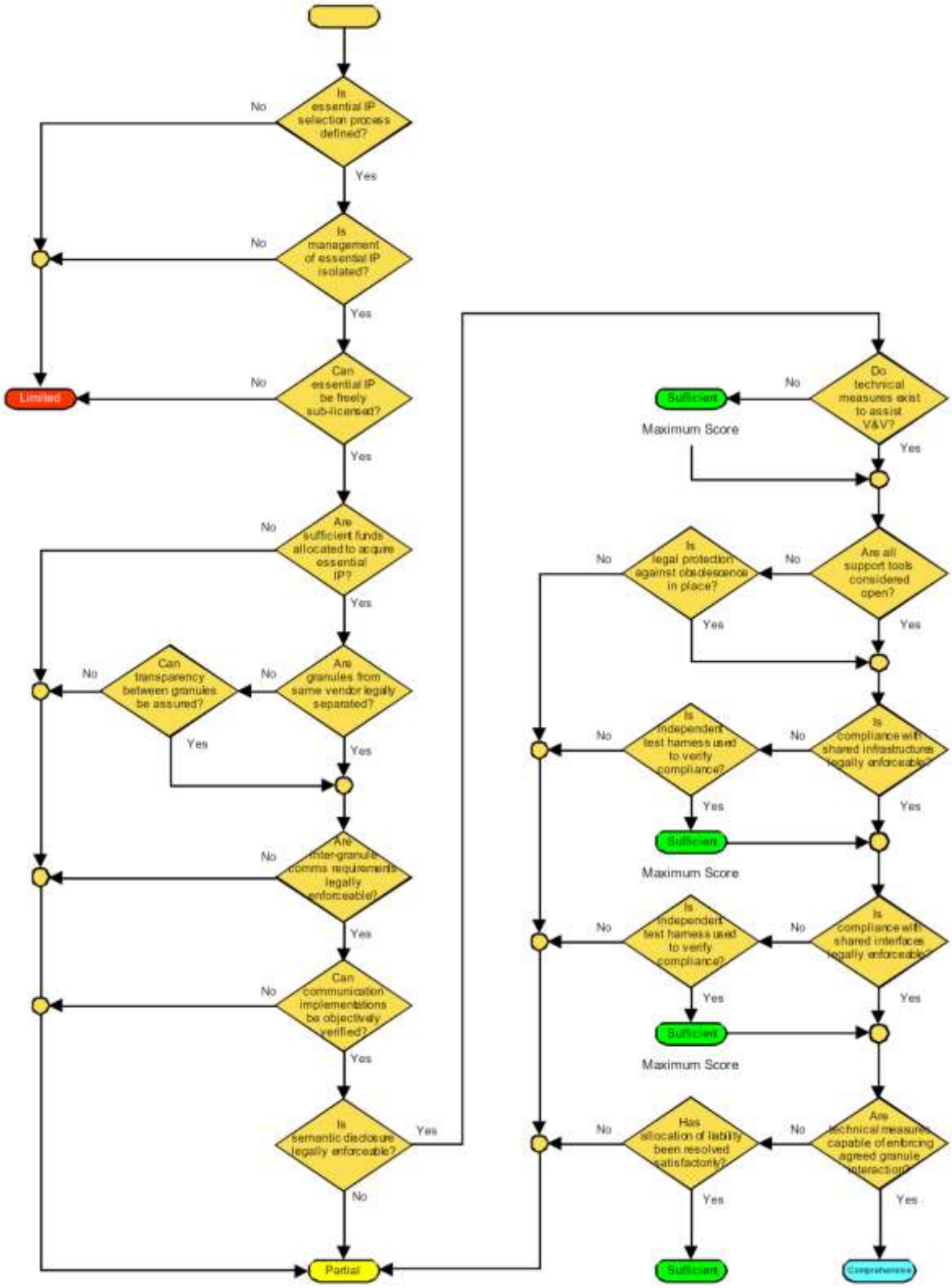

Figure 1. Legal Assessment Flowchart

2.1 Legal Assessment Questions

Essential Intellectual Property (IP) is IP within the system that is (or could potentially be) shared between different vendors. This includes (as a minimum) the system architecture definitions, published interfaces, and the infrastructures that are used to facilitate communications between published interfaces. A method (procedure or policy) is required for segregating IP that needs to be shared between vendors (that 'glue' granules together), and IP that is less critical to the multi-vendor environment. Note the term, "granule" is used rather than "component" or "subsystem". Licensing or acquisition of IP associated with infrastructures and interfaces that are utilised only between components that the customer is willing to combine into a single logical "granule", is not essential.

2.1.1 Is Essential IP selection process defined?

Determine if a process exists for determining what IP should be considered "essential". If no guidance is defined to ensure essential IP is adequately identified, a substantial risk exists that critical IP that should be accessible to all vendors, will be bundled with legal agreements permitting proprietary protection of less-critical IP (such as IP that is entirely encapsulated within a granule boundary).

2.1.2 Is management of essential IP isolated?

Segregation between IP that must be shared between vendors, and IP that is relevant only within well-bounded capability granules, offers the acquisition organisation the opportunity to best direct funding to licence or acquire only the IP that is critical to supporting independent third-party integration. Furthermore, processes for managing shared IP need to be able to be applied without imposing unnecessary restrictions (and therefore increasing compliance costs) on IP that is irrelevant to other component vendors.

Determine if management processes clearly delineate between "essential IP" and other IP within the project. Are legal templates specifically tailored to address the two distinct IP categories?

2.1.3 Can essential IP be freely sub-licensed?

In a utopian solution, essential IP would largely comprise a collection of publicly available standards bound together by published and publicly maintained specifications. However, virtually every real-world solution will comprise a custom architecture, and custom interface and/or infrastructure specifications to meet specific information exchange requirements. These specifications, reference implementations and supporting material must be available to any vendor that needs to contribute to the overall solution. Furthermore, third-party access to essential IP must not be unduly restricted by high licensing costs or non-essential security barriers.

For example, if the solution utilises an infrastructure that incorporates licensed technology which cannot be sub-licensed, third-party developers will need to acquire their own licence to be able to use the infrastructure and therefore exploit interfaces that are made available over that infrastructure. This will increase the real cost of development for the

acquisition organisation, and is also likely to hinder any speculative development of granules for possible integration into the final system.

Determine whether all "essential IP" can be freely licensed (or sublicensed) by the acquisition organisation for use by third-party developers, integrators and users to fully enable the development, integration and use of the system.

2.1.4 Are sufficient funds allocated to access essential IP?

The acquisition organisation must be certain they have sufficient legal access to essential IP in order to ensure future independent maintenance and evolution of the system. If the acquisition programme has not allocated sufficient funds to adequately licence or acquire all essential IP, a substantial risk exists that some essential IP will not be independently accessible to third-party vendors and therefore jeopardise future independent integration and the overall openness of the solution.

Sufficient access to intellectual property means that the acquisition organisation is capable of sub-licensing the IP to independent third-party organisations without notifying the original licensor. The practical method to ensure sufficient access to intellectual property in an "off-the-shelf" procurement environment would generally be a long-term licence arrangement between the acquisition organisation and the IP vendor.

2.1.5 Are granules from same vendor legally separated?

Grouping the development of multiple granules into a single contract or licence agreement risks bundling acceptance criteria and milestone delivery schedules. This may hide the possibility of unpublished coupling being incorporated between bundled granules. Separating the development/delivery of each granule encourages isolated testing and verification that each granule does not rely on hidden couplings with other granules.

Determine if separate legal agreements are always used to acquire/licence multiple granules from the same vendor.

2.1.6 Can transparency between granules be assured?

If the acquisition/licensing of multiple granules can be bundled into a single legal agreement, measures need to be in place to ensure the absence of hidden couplings between bundled granules. Adequate mitigation measures may include independent validation and verification (IV&V) of individual granules (in isolation from other granules), and/or technical "snooping" of all inter-granule communications channels to verify compliance with published specifications.

Determine if sufficient mitigation measures exist.

2.1.7 Are inter-granule communications requirements legally enforceable?

One of the goals of an open system is to enable individual granules to be developed by different vendors. A further goal is to support independent integration of granules into the overall system. Even though a granule vendor may not be involved in the physical

integration of their granule, the acquisition of an individual granule needs to be structured so that the vendor is still accountable for a reasonable level of integration risk.

By legally binding the vendor to meet minimum performance requirements while complying with nominated open interface and infrastructure specifications, the vendor can still be held accountable should those criteria be found to fall short during integration. It may be impractical to test all criteria during black-box or unit acceptance testing, which is why the vendor must remain legally bound to meet all requirements at least until the component has been successfully integrated into the overall system.

Determine whether or not all vendors are legally bound to meet minimum requirements for inter-granule communications.

2.1.8 Can communication implementations be objectively verified?

Is a process in place to objectively assess whether or not granule vendors meet nominated performance requirements for each of their shared interfaces? Determine how interface implementation testing is intended to be, or is being performed and decide whether or not the testing is sufficiently objective to determine if the interface performance requirements are being achieved.

2.1.9 Is semantic disclosure legally enforceable?

Are interface providers (granule vendors) legally required to disclose (including license) semantic characteristics of their interfaces to ensure a third-party can adequately interpret and use the information made available via the interface, and do the legal obligations survive beyond milestone acceptance?

For example, consider an interface to a sensor. The sensor's interface definition may be published with its message structure, required units of measure, expected performance characteristics, and appear to have comprehensive descriptions for each field within the message. However, it may be impossible to effectively utilise the data without additional knowledge about the physical characteristics of the sensor. Such information is likely to be constant and therefore inappropriate for communication via bandwidth-sensitive communications channels.

It is often appropriate to define reusable interfaces in isolation of a single specific context in which they are being deployed. However, the architecture must ensure such interfaces are accompanied by sufficient supporting, contextual information to allow the independent exploitation of the data being exchanged.

2.1.10 Do technical measures exist to assist V&V?

Does the system incorporate separate technical measures that automatically analyse, or assist in the analysis of, interactions between granules to determine whether or not individual granules are complying with agreed rules? For example, even though a granule may have been successfully integrated with test harnesses and passed all pre-determined tests, the granule's behaviour may still differ once it has been integrated with the rest of

the system. Technical measures to monitor interactions between granules to ensure continued compliance with agreed rules will allow violations to be detected and potentially localised to an individual granule.

If these kind of technical measures are not incorporated into the system, a minor penalty is applied to the legal assessment score. This is because such technical measures can simplify the resolution of disputes and inevitable rejection of blame by individual vendors that arise when a failure requires rectification either during or after integration.

2.1.11 Are all support tools considered open?

"Support Tools" encompass any software application that is used to write, maintain or manage interface and infrastructure specifications, architecture documentation, system requirements, explanatory diagrams, source code for shared components, configuration files, or any other shared architectural element that will potentially require maintenance or update throughout the system's life span.

Although this question uses the term, "support tool", what is usually of primary interest are the file formats the support tools use. For example, if Microsoft Word ® has been used to write interface specifications, the format of those documents (such as MS-Word 2003 Document Format) needs to be assessed for its openness. This can be achieved using the standards assessment process described in reference [1]. If the file format is considered open, alternative tools may be available to support continued maintenance of the file. If not, mitigation measures need to be implemented to ensure the file does not become inaccessible as the system matures.

If the vendor of one or more tool used to produce/maintain essential IP documentation, source code, or other supporting material, withdraws support for the product, it may not be possible to adequately maintain and evolve the supporting material. Similarly, if the tool is proprietary to a related entity (such as the systems architect), insufficient access to the IP will effectively prevent the reallocation of the (system architect) role to an alternative provider.

2.1.12 Is legal protection against obsolescence in place?

If the standards used by support tools are not open, determine whether contract or similar legal measures are in place that mitigate the risk of support for the standard being withdrawn by the current support tool vendor. Legal solutions could range from a contract agreement by the support tool vendor to provide a migration path to any future evolution of the support tool. Or, at the other extreme, could include escrow arrangements for access to the support tool application software source code in the event that the original vendor no longer supports the current standard.

2.1.13 Is compliance with shared infrastructures legally enforceable?

Do the contracting/licensing arrangements with granule vendors force them to comply with agreed shared infrastructure definitions, and do the legal agreements sufficiently allow for infrastructure evolution throughout the acquisition life span?

2.1.14 Is independent test harness used to verify compliance?

Does an independently developed test harness exist that can verify infrastructure compliance? If so, is it used to verify compliance as part of the black-box acceptance process for each granule?

2.1.15 Is compliance with shared interfaces legally enforceable?

Do the contracting/legal arrangements with granule vendors force them to comply with agreed shared interface definitions, and do the legal agreements sufficiently allow for interface evolution throughout the acquisition life span?

2.1.16 Is independent test harness used to verify compliance?

Does an independently developed test harness exist that can verify interface compliance? If so, is it used to verify compliance as part of the black-box acceptance testing for each granule?

2.1.17 Can technical measures enforce agreed granule interaction?

Are technical measures built into the deployed system to monitor interaction between granules and enforce compliance with agreed performance characteristics?

For example, an appropriate technical measure may be built into a shared infrastructure to monitor inter-granule traffic. The measure may determine if communications are within permitted performance limits. If one granule exceeds preconfigured performance thresholds when sending a certain type of message, the connection could be reported to the Performance Monitoring Fault Location (PMFL) subsystem, and perhaps also temporarily severed to ensure the recipient is not drawn into a condition that is outside its agreed operating parameters.

Such measures need to be carefully constructed to ensure appropriate quality of service conditions are satisfied, and that the overall operation of the system is not compromised by drastic action such as the severing of a communications channel between two granules. The example outlined above may not be appropriate for interaction between groups of mission critical subsystems.

2.1.18 Has allocation of liability been resolved satisfactorily?

Responsibility for liability in the event of a granule becoming rogue becomes critical when technical measures to identify when granules begin operating beyond agreed performance bounds are insufficient or absent. Few system vendors will warrant the operation of their solution if it has been independently modified or extended. It is therefore important to ensure legal measures are in place to enable independent integration with an acceptable allocation of liability risk on appropriate participants.

3. References

1. Haddy, M and Sbrana, A. (ed) (2016) *Research Notes – Openness and Evolvability – Standards Assessment* DST-Group-TN-1542

DEFENCE SCIENCE AND TECHNOLOGY GROUP DOCUMENT CONTROL DATA	1. DLM/CAVEAT (OF DOCUMENT)

2. TITLE	3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (U/L) NEXT TO DOCUMENT CLASSIFICATION)
Research Notes – Openness and Evolvability – Legal Assessment	Document (U) Title (U) Abstract (U)
4. AUTHOR(S) Michael Haddy* and Adam Sbrana (editor)	5. CORPORATE AUTHOR DST Group Stirling HMAS Stirling PO Box 2188 Rockingham DC WA 6967

6a. DST Group NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DST-Group-TN-1543	AR-016-662	Technical Note	August 2016

8. Objective ID fAV1121050	9. TASK NUMBER	10. TASK SPONSOR
	NA	NA

13. DOWNGRADING/DELIMITING INSTRUCTIONS	14. RELEASE AUTHORITY
To be reviewed three years after date of publication	Chief, Maritime Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. RESEARCH LIBRARY THESAURUS

Systems Engineering, Assessments

19. ABSTRACT

These Research Notes form part of a series of notes extracted from work undertaken by Innovation Science in the establishment of Openness and Evolvability assessment Methods and Processes. This set of Research Notes focusses on Legal Assessment. This work was undertaken from the late 1990s to 2007 and focussed on the application to Submarine Combat Systems.