Extracts from the completed complexity assessment tools from the tabletop validation exercises

Matthew W. Potts

1 | EXTRACTS FROM THE COMPLETED "COMPLEXITY PROFILER"

The list below is taken from the completed Thales Group "Complexity Profiler", filled in during the tabletop exercise. The entries in the list are from the "Hypothesis" column of the "Complexity Profiler" with reference to the relevant system complexity factors (1-8). Text in bold is the corresponding entry from the "Rationale" column. The "Complexity Profiler" was produced before the "scenario inject" and was not updated after the "scenario inject". This group identified 19 distinct complexity issues against the eight predefined system complexity factors from the "Complexity Profiler".

- (1) The equipment will also be subject to a potentially harsh operating environment. Let alone the propagation effects of signals. **Sensing system already proven to operate in operational environment. However, demonstrated in operational environment does not guarantee results (i.e., TRL 7 does not mean no issues). However, what is not yet tested/proven is data processing chain and data fusing.**
- (1) The operational environment is difficult; i.e. having to operate a data link on the platform, and also getting the system to work on such a platform.
- (1) In order to mitigate effect of environment on communications we are going to work with SMEs in this area. However, we have had mixed results in the past.
- (1) Impact of environment not known on Concept of Operation - e.g., effect of autonomy, sea state requirements, do not know effect of environment on platform therefore globally on CONOPS - is the concept of autonomy fully captured in CONOPS.
- (2) Operational concept stability - changes to operations seem fairly small. Although alternatively we do not know what the impact of the autonomous vehicle is on the operational concept. Company has mixed results with vehicle - but nothing said about impact.
- (2) OCS - why would changing what you want it to do impact? I.e. , is it an opportunity as autonomy may improve outcomes. However, may not work out.
- (2) OCS - "Tau has been conducting maritime surveillance for a long time - autonomous capabilities have only recently emerged as a feasible option". **Autonomous operational concept not proven - simply do not know. If you do not know how you will use the platform to fulfil its mission. The impact could be that the end user/pilot**

are part of final customer organisation - if they are not doing their job effectively there is an impact on the mission - when it becomes autonomous capability, does responsibility for meeting the mission to the provider of the solution. Therefore means need to embed more knowledge in system - not necessarily bad but needs to be managed.

- (2) OCS - operational concept is not well known for autonomous systems - argued this is captured as a "2" in the user guide. We know going from manual to automated and these can be well defined in steps. **I.e., minor evolution from manned to autonomous, which could be handled incrementally. However, autonomy has impact on responsibility and impact on user interfaces - if we do not know about impact of CONOPS (e.g., manning, use of system) - therefore there are several threads to this - technology improvement, training, human factors/operational awareness needs.**
- (2) Minor evolution - Evolution of the operational context is planned and described in one story. Engineering steps, acquisition phases and system capability increments are defined or can be defined accordingly.
- (2) I agree. It's like I said, the 'building blocks' of the system are largely proven already in other systems, to one degree or other.
- (2) But the concept of operation is well defined and understood It may be in its infancy, but the components of the system (i.e. subsystems) have been proven in isolation. Organisation must be flexible.
- (3) Several similar users but not explicitly clear if the users for TAU and PANTHEON are looking at the same thing - not confident enough in information to say differently. **Several different users.**
- (3) similar users but maybe changes in the way they use the system (due to autonomy in the platform - therefore change in the way they impact on the system) - may impact safety (i.e. , a 2/3)
- (3) different users for using the data vs operating the platform - may be a result of not knowing op concept but in the change to an autonomous system does the MASSS have less ability to physically aid vessel in distress
- (3) This is not explicitly stated, but The vessel will need regular maintenance for fuelling, and preparing the missions, etc. There will also be maintainers, of the vessel and equipment. The Operational Area may also throw up different needs.
- (4) worked with these people before but with mixed results - common understanding but with major risk. Assume that data that is passed on to PANTHEON is data we know as the missions have been operating for a number of years although it is not stated anywhere what data is exchanged. **Could be mitigated by utilising open source interfaces as much as possible to reduce the interoperability risk (still have challenge to identify which open source interfaces but a mitigation nonetheless).**
- (5) Solution lifecycle interlacing - different parts of it are at different stages of the lifecycle - several different lifecycles (components, sub-systems, platform, communications means) - are these lifecycles interlaced with interactions? We don't know yet how certification of vessels will be done so there is a question mark about the validation of the autonomous vessel. It is major interactions but these are identifiable. There will be some processes that we may not be fully aware of at this stage, so it needs to be a 3.
- (6) Solution Engineering Effort and Criticality - score a (2) as high technology readiness, however, technologies may be proven but their integration is not, proven in operational environment but no proof that we can operate these things together. The integration is going to be the issue.
- (6) However, could also be a 4 as the autonomous platform is a critical technology - we know that the technologies and data processing work, but not proven that it will all operate together - reliant on information from outside of our control.
- (6) Concern about safety and certification and security - how will the system be demonstrated and certified. Security not talked about at all - people no longer available to respond, vulnerabilities with platform. Etc.

We do not know how we are measuring the performance of the system (a-f of key criteria/measures of performance) - how do we know the technologies will meet the needs. Fundamentally do we have something that meets user needs. See A4 from aide memoire.	We may not be able to validate the design - how does the customer agree/how do we tell the customer that we have done something properly.	Break measures of effectiveness down into derived requirements and model expected performance of solution against those. Alternatively define what MASSS is capable of achieveing. User scenarios could help or user workshop. Issues compounded by the lack of design information about the vessel, new required interoperable, upgrade to P C4i all impact on solution - (Worsening, mitigation not working) Interopability is another measure of effectiveness that we do not understand - CONOPS/CONEMP around data fusion is a cause for concern	How was this issue identified?	Pre-ITT based on scenario and development details.
			What is the extent or scope of the issue?	The project itself which encompases the stakeholders.
			Does the issue implicate other processes or activities?	Sales and business development activity
			Who should be in the loop for this issue?	Customer, sales and BD, project team, users, PDA
			How likely is the mitigation to succeed?	Confident that the activity would then enable a good Gate 1 decision (bid or no bid decision) - this mitigation action will ensure we make a better informed decision.
			When should consideration of this issue by revisited?	Pre-gate 1, gate 2 and gate 3 (checking assumptions have not changed)
			Who has responsibility for dealing with this issue?	Capture lead and PDA

FIGURE 1 First entry in the "Complexity Register" completed by the group of Thales Group personnel

- (6) A lot of te technologies have been proven; the sensors, the comms links, the platform, etc. but getting them to work together and fusing the data may be the problem. Also the fact that the way of using the system will be different and may drive system design. Security issues compounding.
- (6) Scenario talks about difficulty validating, acquisition, public perception etc - could copy that line from scenario that argues significant challenges from this.
- (7) System behaviour stability. How the system will perform, behaviour of the platform, behaviour of the actors, re-allocation of data and learning etc. Public perception cannot be predicted. Legislation risk.
- (8) Requires multi-discipline approach. Not only question of quantity but question of quality - size, specialities (safety assessments, V & V, communications/PR around autonomy and human impact socioeconomically, need specialists for communications - external, power). Engineering effort done outside of organisation - therefore a 4
- (8) Depends on organisations ability to do outsourcing. MASSS is within the boundary provided by the customer as well as being a Prime. The boundaries are complex and may not be easy to manage, with different relationships at different interfaces.
- (General) When I have seen these sorts of methods being used in the past (and that includes providing cost estimates, etc) people have a preconceived view of the answer and almost work the tool to get the result rather than let the tool give you a result. If that makes sense.

2 | EXTRACTS FROM THE "COMPLEXITY REGISTER" COMPLETED BY THE THALES GROUP PARTICIPANTS

The first series of entries on the "Complexity Register" by this group had all columns completed and are shown in figs. 1 to 4. The list below these figures are from the "Complexity Register" once the group switched emphasis to capturing complexity issues. The text corresponds to the column "Description of the Issue:" and text typeset in bold are the effects of "compounding risks" on these issues, as reported by participants after the "scenario inject". Some entries in the list are prefixed with a reference to the "Complexity Register" aide memoire (e.g. , B4). This group identified 18 distinct complexity issues.

A stakeholder issue of understanding the requirements - PANTHEON doing procurement activity but requirement is solely from TAU -> linked to issue above. The way that the programme is built introduces a level of obfuscation between us and our understanding of the real user needs.	We may not be able to validate the design - how does the customer agree/how do we tell the customer that we have done something properly.	Capture CONOPS/CONEMP up front before diving into detailed systems design. Make agreement of Concept documents psuedo-contractual to ensure before commitment that we really understand what the stakeholder expectations are. Require programme mechanisms (on going user groups, etc.). See A6 from aide memoire ref liability to change/stability of understanding. Planned upgrade of P C4i system may compound. Procurement plans do not seem to include PANTHEON for the airborne capability - could have different acquisition route	How was this issue identified?	Pre-ITT based on scenario and development details.
			What is the extent or scope of the issue?	Front end and back end
			Does the issue implicate other processes or activities?	Commercial angle on this issue - is this the right contracting route for this solution (what are PANTHEON adding if Alpha/Beta not contributing to requirements) - contracting structural may hinder or help.
			Who should be in the loop for this issue?	Commercial.
			How likely is the mitigation to succeed?	Not a certainity.
			When should consideration of this issue by revisited?	Pre-gate 1, gate 2 and gate 3 (checking assumptions have not changed) - if scope of design review correctly captures concept/doctrine element it can be built into the environment - the CONOPS etc need checking throughout the lifecycle.
			Who has responsibility for dealing with this issue?	Capture lead.

FIGURE 2 Second entry in the "Complexity Register" completed by the group of Thales Group personnel

Make/Team/Buy decision for SATCOM/UHF - uncertainity around how we would deliver this and who would be providing it (does customer have preferred provider driving a requirement into our solution?).	Two disperate parts of the system that cannot connect, potential for overruns if different solution required, customer might not be accepting of proposed solution.	Ask customer to identify "best athelete" that they currently have - may reduce complexity and pass some burden back to them. Refine offering wrt data - significant area of uncertainity currently e.g., bandwidth, data fusion, security, human factors etc Early little and often integration of the procured SATCOM/VHF and C2 system to mitigate risk. Could be compounded by interconnections/interoperability with new capability (bandwidth, frequency issues, IFF issues between the two systems).	How was this issue identified?	Pre-ITT based on scenario and development details.
			What is the extent or scope of the issue?	Performance of the technical system
			Does the issue implicate other processes or activities?	Sub-contracting approach, supply chain management, systems engineering (drives requirements), impact on C2 sub-system, agreeing ICDs for various interfacing systems
			Who should be in the loop for this issue?	Customer, sales and BD, project team, users, PDA (may not want to include user/customer at this stage - depends on nature of ITT i.e., if
			How likely is the mitigation to succeed?	Would mean a defined proposal that would provide increased in offering.
			When should consideration of this issue by revisited?	Pre-gate 1, gate 2 and gate 3 but also affects lifecycle of SATCOM/UHF
			Who has responsibility for dealing with this issue?	PDA and Supply Chain Management

FIGURE 3 Third entry in the "Complexity Register" completed by the group of Thales Group personnel

Environment (social, acquisition etc) of the system - could be issues with members of TAU not liking being monitored (or visa versa) - perceptions of system by stakeholders has impact on data transparency (how much is shared, data assurance). Data assurance between TAU and PANTHEON Operating Centres an issue.	Could provide soft blockers to the project (ie PANTHEON not accept connections if they do not have confidence), social issues if stakeholders do not want to be recorded etc. How do you achieve acceptance if TAU cannot operate vessel in the way they intend to operate vessel. May complicate documentation if different stakeholders have different needs/requirements if some things cannot be shared.	Capture in the CONOPS/CONUSE should be multi-party across PANTHEON. Defining boundaries for the system offers some protection for our organisation. At the technical layer - get early agreement of ICD between sub-systems with objective to make them common. Effective communication strategy across PANTHEON members and customer to mitigate. Impact of introduction of new airborn capability not known - inject.	How was this issue identified?	Prior knowledge of team (LL from previous projects), pre-ITT workshop.
			What is the extent or scope of the issue?	Reputational with TAU/PANTHEON/Alpha/Beta.
			Does the issue implicate other processes or activities?	Engineering activity could be de-coupled from this. Payment milestones - structure to reduce risk profile. Commercial/legal aspect to offer protection.
			Who should be in the loop for this issue?	Commercial, Legal, Capture Lead
			How likely is the mitigation to succeed?	Mitigation allows us to progress the project but the soft blockers may still remain.
			When should consideration of this issue by revisited?	As above.
			Who has responsibility for dealing with this issue?	Engineering Manager and campaign/capture lead (CONOPS/CONUSE). Communications strategy is supported by corporate communications.

FIGURE 4 Fourth entry in the "Complexity Register" completed by the group of Thales Group personnel

- Extent of integration with COTS vessel (data from sensors, platform integration). **Increased issue after inject - continued, higher degree of uncertainty - previous mitigations put in place are not working/negated.**
- Sensor performance - only TRL 7 but being sold. **Compounded by platform information issue after inject - unable to define interfaces and performances with vessel.**
- Multiple design teams - can they really operate effectively as one design team. **Compounded by platform information issues. Compounded by inject around new airborne capability - requiring new interface set ups, new equipments and need to launch new team to deliver this (potential new division to address this depending on size scale of the pie we get).**
- Diversity of systems, sub-systems components - scenario does not include all of the details of the total system. **Issues compounded by the lack of design information about the vessel. Mitigation at this point should be about reducing interfaces with the vessel and instead increasing functionality and complexity of the C2, bringing more functionality in house.**
- Encapsulation issue around the data from various sources and the need for fusion/integration/protection etc. **Could be impacted by the lack of information about vessel but not as significant as others.**
- Users - we could not get a handle on if the solution actually reduces the manpower burden - a key MoE but does our solution deliver this? I.e. personnel involved in data processing, platform maintenance, piloting etc. **Compounded by lack of detailed information about vessel i.e. , servicing requirements/maintenance perspectives of the vessel.**
- Integration is a serious worry - power supply integration to sensors and into vessel - anytime you try to break into something COTs it is never as easy as you think. Undefined areas around integration - can sensors integrate with data processing? We cannot define some of these without inputs - there are some that are in our gift to understand but some outside of our gift to understand. **Compounded by issues around platform data.**
- Security of connections (SATCOM/C2 etc) but also regulatory requirements are not known -> how mature is regulatory environment for this ie do they need to change laws to accept autonomous vessels etc? **Could be impacted by design information about vessel (e.g., collision avoidance , might not be observing of keep safe zone etc) - worsening.**
- B5 is everything using well defined interfaces/boundaries? Seems like most connections are not clear and well understood. Data flows seem to be related - data integrity/assurance will percolate through the system ie sensor data bad will affect C4I system.**Ref the vessel - compounded by lack of information about the vessel.**
- B6 - Pantheon C4i system and other players will have their own lifecycle - risk or opportunity to make money further down the line. **Compounded by lack of detailed information about vessel ref lifecycle from inject.**
- Uncertainty around the project is currently an issue. Although TRL of the sensors and C2 system is also a cause for concern (maturity of C2 system to drive the vessel and the novel sensors and power supply - complex integration challenge for developers) - what sort of development environment do we have (test beds, how much integration at sea, etc). **Compounded by the inject as a lack of detailed information about the vessel should be nailed by now at CDR - if validation strategy and design information is not currently known - we should not be passing CDR with the current lack of information ref interfaces, validation, etc.**
- C3 relationships with external organisations presents a risk due to the number of diverse external relationships.**IF we are not getting design information this issue is getting worse - caution around contractual discussions which can impact on team relationships.**
- Inject - Vessel design information inadequate to progress hosted system design
- Inject - Airborne capability inclusion - would like to be included. Interfaces and integration with the new system is not known. Opportunity for BD activity around including new capability as part of offer. Customer does not

What are the emergent behaviours at the system boundaries?	Information/data shared among multiple operators Potential for mismatch in data formats? System functionality may be required to address this emergence There may be conflicting non-functional constraints Complexity that arises from interoperabilty in getting data from A to B to Z - that is complex	Develop a more rigorous system architecture (logical/functional/physical) that relates to user requirements across boundaries	How was this issue identified?	Examination of the system architecture - many organisational and system interdependencies
			What is the extent or scope of the issue?	Could be up to 20 interfaces each with boundary behaviours to consider May uncover some unexpected outcomes - e.g. system A may be incompatible with system B
			Does the issue implicate other processes or activities?	Yes - hidden requirements in development details that may contradict
			Who should be in the loop for this issue?	
			How likely is the mitigation to succeed?	
			When should consideration of this issue by revisited?	
			Who has responsibility for dealing with this issue?	Prime contractor/Lead solution architect

FIGURE 5 First entry in the "Complexity Register" completed by the group of Non-Thales Group personnel

Architecture does not partition between Safety Crtical and Safety impacting functions	How do the bits work together (safety critical parts like collision avoidance vs information parts of the system) - architecture doesn't account for this; things were groups together by type. We do not have an architecture	Develop an architecture (better if done early).	How was this issue identified?	
			What is the extent or scope of the issue?	
			Does the issue implicate other processes or activities?	
			Who should be in the loop for this issue?	
			How likely is the mitigation to succeed?	
			When should consideration of this issue by revisited?	
			Who has responsibility for dealing with this issue?	

FIGURE 6 First entry in the "Complexity Register" completed by the group of Non-Thales Group personnel

seem to know what they want, how they will achieve it, etc. can lead to uncertainty and changes that could have significant impacts ie IPv4 to IPv6 changes on one system cause issues for another platform. Has its own lifecycle and may cause programmatic delays.

3 | EXTRACTS FROM THE "COMPLEXITY REGISTER" COMPLETED BY THE NON-THALES GROUP PARTICIPANTS

The first two entries on the "Complexity Register" by this group are shown in figs. 5 and 6. The list below these figures are also from the "Complexity Register". The text is typeset differently to represent different columns of the "Complexity Register", normal typeset corresponds to the column "Description of the Issue:", italic typeset corresponds to the column "Description of the issue's anticipated impact" and text typeset in bold corresponds to the column "Description of the issue's anticipated impact." Some entries in the list include a reference to the "Complexity Register" aide memoire (e.g. , B4). This group identified 19 distinct complexity issues before the "scenario inject".

- Safety and security concerns that arise from the use of open source standards and protocols. **STP Analysis would help - ID safety and security hazards (threats).**
- People - how they use the system and the pressures they are under. *People might try and subvert the system, or in time use it in different ways*.
- The EO system sounds like it might have been trained with ML - therefore might not be possible to know why it has id'd something if there is a post incident investigation/fault. *Validation could be challenging. Not sure we understand the so-what of this as engineers yet - unqualified exposure.* **Identified as an open challenge for verifying/ validating MI/AI capabilities.**
- Security requirements are not clear - what is secure enough - hard to define and always more you can do. *Could end up in spiral of increasing security costs, client acceptance, operational impact*. **Detail the security level that will be achieved in the bid - thorough understanding of architecture/bid - resource and define thinking about security.**
- Safety - what is safety critical and what is safe enough. *hard to evaluate spending required.* **Require definition of what safe enough means for PROCULUS Group, relate to other stakeholders i.e. MOD, customer.**
- Resilience to the system end to end, similar to the security. *Spiral costs, unknown.* **develop on how to understand key terrain.**
- Multiple interop points between systems, how are they captured and each area will have their PoV for what users. *Each area may have own standards and try to push their own way forward.*
- Spiral / compounding risks - are there any? i.e. fault in EO, leads to data process fault / to user misinterpretation etc. **Architecture needs to consider the potential for compounding risks relating to the data (i.e. spurious data entered into system which percolate's/spirals through the system) - error checking and error recovery - built into design as opposed to bolted on.**
- Conflicting requirements - autonomous vehicle and sensors (protection of vessel) vs detection of high priority/threat objects - how would these conflicts be managed? **Decision hierarchy and implications need to be clearly understood and defined.**
- Encapsulation - can we draw at a high level what the key blocks of the system are in terms of importance?
- Elements provided by the customer (PANTHEON C4I System and TAU Opening Centre) require understanding more.
- Is this solution even implementable?
- User community not well known - people make things complex - B2 from aide memore - not well known/understood - i.e. training, scenarios, experience, control are unknown.
- If the system is complicated, how well do decision makers in operating centres make use of the data from the system given they are complicated - each element adds a degree of abstraction to their understanding - compounded by delays (i.e. via SATCOM) - we need understanding of how well the users can operate/understand the system.
- Do PROCULUS GROUP understand their dependencies on other systems/organisations and their ability to influence the stakeholders - levels of interest/influence.
- PANTHEON - multinational organisation - requested use of open standards - these open standards may be ever changing which has implications on interoperability.
- Time perspective - what will happen over time; policies, architectures, interoperability, standards, etc, and how much will it impact us given the operational context (PANTHEON) is unknown - hard to know but it will change things.

The entries from the "Complexity Register" after the "scenario inject" are listed below, following the same typeset schema as described above.

- Introduced new requirements - and sub-systems that are at different levels of readiness / maturity. *Complexity introduced from different maturity levels.*
- There might be a number of decisions that are now wrong at CDR due to the new info / requirements. But you don't know that they are wrong. *It doesn't work*. **Phased approach. Introduced different variants of MASS platform. Option to step back in the project and declare that due to the scope of changes we need to step back and fully re-assess the offering - we would recommend re doing the architecture, requirements etc (standard se process) to fully understand. Need to understand why the customer requirement changes have occurred. Potentially our system design is amenable to this kind of update as we earlier suggested the design should be cognitive of future changes - therefore - check how we designed MASSS to date, is it truly modular, flexible, open, etc - understand the risks that we are then exposed to. Fleets within fleets - issues on maintainability, operability, potential for cost changes**
- Change in interoperability requirements - information data formats (people and software)
- Do you end up with different classes of mass platforms
- Accelerated timeline - consider a different PM approach (i.e. waterfall vs agile) - however this is not without risk in itself - comes back to system design aspect - depends on how MASSS is currently being managed. *The type of PM approach brings its own issues (agile vs waterfall) in terms of releases, funding, testing, design, etc.* **"AGILE as a mitigation to the changes/time perspective - overheads in terms of sprints/releases are paid to account for the differences. Some features get added/dropped to get us over the line."**
- Complexity around funding/acquisition - how is funding tied to delivery (MOE? Increments?)
- What LfE has been identified from the "incidents" mentioned?
- SMART goals - can we at least deliver original scope of CDR in phase 1, phase 2 can then be what else can we deliver in a specific time, Phase 3 can then be if its unrealistic to get what they want in the time they want.
- Changes in operational environment - what has changed that has made them to make such big changes and why are they confident in the proposed fix of adding new systems - need for enhanced understanding - goes back to the requirements of the system - what are the prioritised figures, maybe different solution altogether.