Australian Government

Department of Defence
Science and Technology

Building Trusted Reference Information at the Tactical Edge

Andrew Walters, Simon Bou, Angela Consoli, Tim Priest, Robert Davidson, Jayson Priest and Sonya Williamson[1]

Weapons and Combat Systems Division
Defence Science and Technology Group

DST-Group-TR-3641

ABSTRACT

Reference information libraries support fully integrated computer systems, enabling automated functions, such as identification and decision support, within the context of an environment. This structured information is prepared prior to a mission, distilled from a large pool of intelligence and environmental characteristics relevant to a mission outcome. The preparation time can be lengthy, requiring rigorous verification and validation before being used to optimise a platform and its sensors. This study investigated information exchange and processing under the pressures and limitations of first responders at the tactical edge to provide insight into transitioning reference information to a dynamic 'real-time' paradigm. This preliminary work suggests that the updates to the reference information are trusted based on comparison to expectations; whether it is an expected behaviour or a more detailed construct, such as a trust ontology. Furthermore, the concept of reducing decision risk through the sharing of metadata seems key, where the metadata reflects a trustworthiness property or trust-attitude, following assessment by the information receiver.

RELEASE LIMITATION
Approved for public release

---

[1] Surf Life Saving South Australia

Produced by

Weapons and Combat Systems Division
Defence Science and Technology Group
PO Box 1500
Edinburgh SA 5111

Telephone: 1300 333 362

Building Trusted Reference Information at the Tactical Edge

Executive Summary

Reference information libraries support fully integrated computer systems, enabling automated functions, such as identification and decision support, within the context of an environment. This information is structured and prepared prior to a mission, distilled from a large pool of intelligence and environmental characteristics relevant to a mission outcome. The preparation time can be lengthy, requiring rigorous verification and validation before being used to optimise a platform and its sensors for a role. This reference information is therefore static and not adaptive to unexpected occurrences or outcomes.

Near real-time updates to the entity descriptions held within the reference library would aid in achieving the adaptability required. These updates would be an augmentation of the base library, reflecting the discovery of some new intelligence. This form of the library is called ‘dynamic reference information’. One of the key challenges facing the realisation of dynamic reference information is establishing trust in the library updates in near real-time.

The emergency services domain has been used as a surrogate for a defence joint task group environment for studying the exchange and processing of information. Emergency service personnel conducted search and rescue training scenarios while researchers collected the information flows between team members and between machines using video, audio and system logs. Three experimental runs were conducted, with durations exceeding 30 minutes each, addressing a series of incidents presented to the first responders as part of a larger scenario. Scenarios were designed to stimulate information flows and to leverage an implied reference information construct supporting dynamic reference information as well as shared situational understanding for distributed decision-making.

The preliminary results indicate the linkage between the critical events, the command and control hierarchy, information categories and implied reference information. The results indicate that a trust process runs throughout this information framework, with the concepts of trustworthiness, trust-attitude and trust-action playing out as the teams worked towards achieving their goals. Analysis indicates that the reference information supports the generation of requests, the interpretation by the receiving parties and the complementary information concept of a report. The preliminary research suggests that the updates to the reference information used in this domain are trusted based on comparison to known information of the environment and the entities operating within it. This is captured within a prescribed behaviour and can be categorised within an ontology.

The results hint at benefits derived from sharing the trust assessment throughout the team through tailored metadata. In the military context these results are key to realising the

concept of dynamic mission data. Further analysis into the specifics of the trust process applied to updating reference information held by personnel in real-time will support the generation of a trust framework needed to support rapid information updates that are validated and verified for use within a military computer system.

Contents

This page is intentionally blank.

Glossary

AMSA	Australian Maritime Safety Authority
ATV	All-Terrain Vehicle
BCHP	Port Noarlunga Beach Patrol
BID1	Boat in Distress 1
BID2	Boat in Distress 2
C2	Command and Control
DST Group	Defence Science and Technology Group
Duty10	Local incident commander known as the duty officer
GPS	Global Positioning System
IoT	Internet of Things
IRB	Inflatable Rescue Boat
IRB1	Inflatable Rescue Boat 1
IRB2	Inflatable Rescue Boat 2
JRB	Jet Rescue Boat
LS2	Life Saver 2 (Boat Name)
LS3	Life Saver 3 (Boat Name)
MANET	Mobile Ad-hoc Network
PNSLSC	Port Noarlunga Surf Lifesaving Club
RISE	Real-time Information Superiority Experimentation
RWC1	Rescue Water Craft 1
RWC2	Rescue Water Craft 2
SA	Situational Awareness
SAR	Search and Rescue
SLSSA	Surf Lifesaving South Australia
SRC	Surf Rescue Certificate
SURFCOM	Surf Lifesaving South Australia Radio Room
TEXAS	Tactical Experimentation Architecture Support

This page is intentionally blank.

1. Introduction

The combat information environment for the war fighter is shaped by the demands of the users and the restrictions imposed by the nature of operating at the 'tactical edge' [1]. Achieving a common situational understanding between members of a task group can be hindered by several confounding factors, including:

- rapidly changing, lean and poor-quality data
- incomplete information
- disparity between the currency and consistency of the information held by each asset.

The goal is to achieve mission success in the face of these challenges. This demands a type of 'information superiority' in the context of the available information, the goal of the mission and the structure of the task group (including roles and capabilities). As always, the ultimate challenge is to provide the right information to the right place at the right time.

The information relating to the combat environment can be thought of as having two forms: the near real-time component; and the information libraries supporting an *a-priori* awareness of the environment. This information is known as 'reference information'. It is also commonly referred to as 'mission data' in the military context [2]. On tactical (edge) platforms this reference information is commonly stored as a library that can be accessed as needed by the mission system or human operators.

Typically, these libraries include descriptions of entities[2] expected within the environment that can be compared with measurement in order to establish the identity of entities detected in the environment; enabling the appropriate tactical decision aids and supporting higher-level decision making. This reference information can include the physical characteristics of the entity (colour, length, features etc.), a description of their typical behaviour and a description of the surrounding environment. Reference information can also include the environmental conditions, both current and predicted, and decision support aids for how 'own platform' should respond to a situation or scenario.

There is a temporal aspect to reference information: from gathering intelligence, verifying its content, assessing and formatting and storing to become part of the reference information library. At the present time, platforms are given an initial, verified reference-information load prior to leaving for a mission that is based on a-priori information. This concept is shown in Figure 1 and Figure 2.

[2] Here the term entity is used in the context of elements described by Endsley [7] in relation to situational awareness. Where an element or entity can be an aircraft, a boat, and a landmark for instance with associated characteristics (eg. colour, size, location).

Typically, reference information libraries are static, compiled prior to a mission and designed for use in the tactical environment, optimising the capabilities inherent within a platform. For example, consider the simple scenario in which a drone is used to identify, monitor and report on the watercraft associated with a rescue team. Without reference information related to the characteristics of the individual watercraft, the drone may report all vessels on the water, which could be overwhelming to the operator. Conversely, consider the situation in which a reference information load is now added to the drone in which the colour description of an emergency craft is defined as red and yellow. The reference information load is used to optimise the camera on the drone; such as applying a filter to preferentially detect red and yellow light. This makes detection and identification of the emergency craft much simpler and reduces the amount of unnecessary information being presented to the operator. We have a more optimal system for the environment and the mission.

Due to the influence the reference information can have on the system, the verification and validation process of a new library can be lengthy, taking many months to complete. This can result in stale information in the reference library if the environment is unexpectedly dynamic. Specifically, if the environment contains characteristics not defined within the collected intelligence of the reference information library produced. Additionally, platform information storage and processing limitations can force re-programmers to balance platform system capacity against entity details required to capture the nature of the environment. This typically results in a loss of granularity in the information retained for subsequent use in building reference information libraries and can result in considerable variation in the reference libraries produced by different operators or at different times.

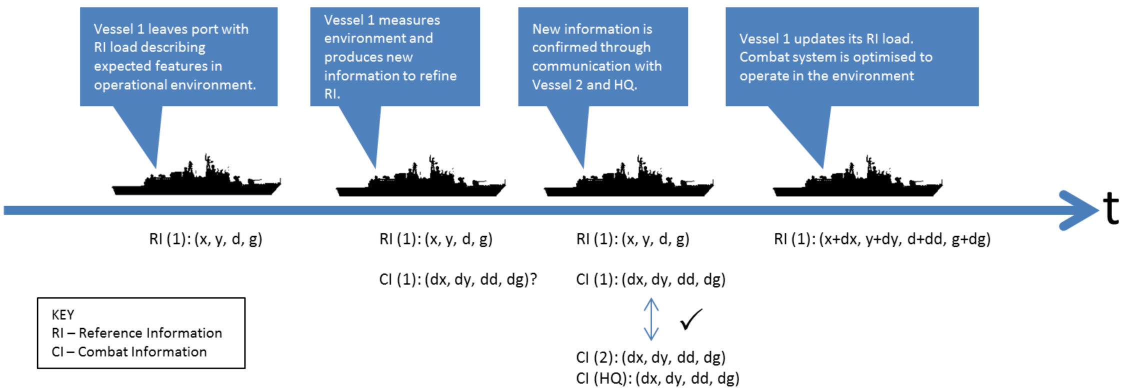

Figure 1. Reference Information example.

How can the stale nature of this reference information be mitigated? The concept of a 'dynamic reference information' library could be the key. A dynamic library is one where entity descriptions can be updated during the mission to reflect new intelligence collected either by the platform itself or shared by another platform across the communications network.

A major challenge with generating reference information is ensuring currency, relevance and accuracy. These factors form aspects of having 'trust' in the information and the updates. In addition, the consistency of information between distributed systems connected through a 'Combat Cloud' [3] type construct places further importance on the nature of the reference information utilised by individual systems. For example, differences in reference information on different distributed systems may lead to different systems arriving at different solutions for entity identification, which will lead to contention at the network level, increasing uncertainty and reducing situational understanding.

The collect, trust, and use cycle concept for producing reference information is shown in Figure 2.

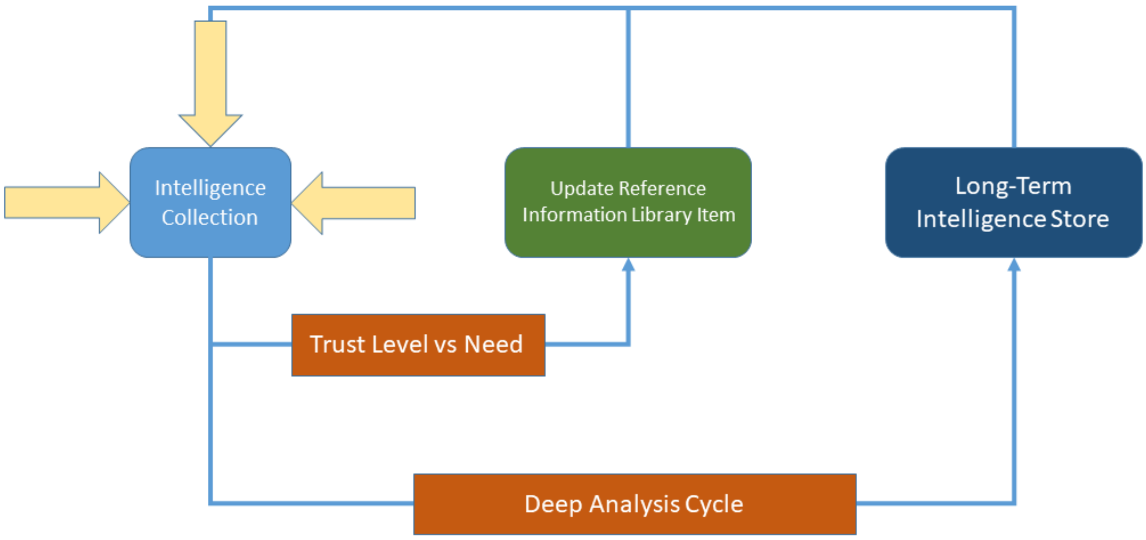

Figure 2. Reference information intelligence cycle.

Considering Figure 2, intelligence is gathered through either human observation or through data collection from sensors. These data are interpreted based on the current environment (or context) to form or update information. This information is then assessed for currency, relevance and accuracy and assigned a trust level. The resultant trust level may determine if this information is to be used to support the current task objectives, discarded, or elaborated within a deeper analysis cycle to produce an enduring intelligence artefact for future use. For dynamic reference information, updates are an augmentation of the original library, with the trust level process playing out in real-time. Challenges include how to process the data, identifying what section of the library to update, how to verify and validate the update, understanding its effect on the wider system and to do all of this in near real-time.

The trust ontology work by Ceolin et al. [4] and general trust definition work by O'Hara [5] provide a framework against which the trust process may be characterised. Ceolin et al.

[4] call trust a 'leap of faith' when relying on a source of information and the information content itself. Firstly, the main components and participants identified in any trust process can be defined using the concept of trustworthiness, behaviour and belief. Three agents are identified: **X**, **Y** and **Z**. In the context of this report, **X** is the receiver of information, **Y** is the sender/source and **Z** is an authority responsible for creating and disseminating the behaviour **R**, against which **Y** conforms. This all plays out within a given context **C**. The trust process is broken down into three major components:

- Trustworthiness – A source of information **Y** conforms to a behaviour, **R**, within the context of an environment **C**, as claimed by **Z**
- Trust-attitude – The receiver of the information **X** believes that the information source **Y** conforms to the expected behaviour **R** through observations made
- Trust-action – The receiver **X** performs an action as risk based on the trust-attitude.

This treatment of the trust process provides a convenient methodology of quantifying the considerations for dynamic reference information. It could be considered, in the context of reference information, that **X** is the user of a current reference library (e.g. mission system), while **Y** is the source of a new piece of information (e.g. another platform) that is assessed as an update to the current reference library. **R** are the behaviours (characteristics, rules, governance etc.) in relation to **Y** and **Z** is the authoritative organisation in the context **C** **(**e.g. Department of Defence in the context of protecting the nation). A role of Z is to disseminate **R** to **X** in relation to **Y**.

In [4] it is noted that the trust of an information source is made at risk, due to the possibility of uncertain or unpredictable behaviours within the context of the environment. Ceolin et al. continue this discussion, illustrating that this risk can be managed and even reduced by sharing the trust properties, such as trustworthiness, in the form of metadata. This highlights the strength of leveraging a distributed environment towards overcoming the challenges of dynamic reference information. The next step is to implement this trust methodology and apply it within a domain whereby the coordination and cooperation challenges are reduced. This report details defence relevant research conducted within an unclassified surrogate domain to facilitate rapid research on building trusted reference information during a mission.

2. Background

In November 2017, an initial experiment was conducted under the RISE[3] initiative to investigate the use of the emergency services domain as an appropriate defence surrogate to enable low-cost rapid turn-around research. An additional aim was to identify the nature of reference information that may support Australian Defence needs into the future. This initial experiment confirmed the usefulness of the emergency services domain as a surrogate and highlighted a strong defence equivalence when studying the

[3] RISE – Real-Time Information Superiority Experimentation

management of information for enhancing the situational awareness of a tactical team [6]. This experiment also assisted in identifying the reference information routinely used within the surf lifesaving domain, helping to define a reference information framework upon which future experiments could be based.

An example of the entities that made up the reference information library identified from Experiment 1 are shown in Table 1.

Table 1. Reference Information Examples.

Order Of Battle	Characteristics & Performance	Geographical Intelligence
Jet Ski has rescue mat	Length	Reef location
Inflatable Rescue Boat (IRB) has radio	Colour	Water Current Hazards
Jet Rescue Boat (JRB) operates with IRB	Typical Speed	Weather Phenomena linked to geography
SURFCOM is primary C2 unit	Registration Number	Boat Ramp
Command Structure	Features	Map

Within Table 1 the Order of Battle category covers information that includes:

- Command structure (SURFCOM (leads), Duty10 (lead onsite), Patrol Captain (leads surf life savers assigned to a particular beach)
- Force composition (e.g. a patrol has surf life savers, mobile unit (vehicle), inflatable rescue boat)
- Force strength (e.g. numbers of platforms)
- Equipment fit (e.g. a rescue boat has a radio, sonar, GPS unit and first aid kit).

Characteristics and Performance covers:

- Physical characteristics of a craft (e.g. colour, length, registration number)
- Typical performance characteristics (e.g. speed, manoeuvrability, operational range).

Geographical intelligence covers:

- Maps
- Navigation charts
- Cultural features
- Geographically referenced activities (e.g. regular yacht race)
- Topographic information.

In addition to these categories there is also a broad range of miscellaneous information that describes the environment such as:

- Weather data
- Communication plans
- Icon and symbology assignments.

Identifying a reference information framework within the surf lifesaving domain provides the opportunity to study the optimal characteristics of the reference information, such as the amount needed, its resolution and what level of assurance is required to support different operational scenarios. In a dynamic environment, reference information is available from both implicit and explicit knowledge and can be used to increase situational awareness (SA) in a dynamic environment.

The processes involved in gaining SA, as stated by Endlsey et al. [7], can vary extensively. The knowledge that individuals gain from learning, from experience or training is thought to be somewhat static in nature [7]. Sarter et al.[8] page 52, elaborates by arguing that situation awareness of an entity is continuously updated by information that is "available or can be activated". This information can be implicit or explicit. In the tactical military domain, the use of reference information by platforms is typically explicit, as it provides a mission or combat system the context of the environment in which it is operating. Implicit reference information is largely contained within the operators of the platforms. Although the Surf Lifesaving South Australia (SLSSA) assets do not contain mission or combat systems, the explicit and implicit use of reference information can nonetheless be studied through observation of the information exchange, processing and subsequent action.

Reference information exists in the RISE experimentation environment in two forms: explicit (TEXAS environment and configuration files) and implicit (knowledge and experience of SLSSA personnel). The goal of the present research was to test and understand trust in the context of reference information from both the explicit and implicit viewpoint. Specifically, how trust is coupled with reference information in a real-time context, whereby information updates are assessed and then trusted, realising a potential approach to dynamic reference information.

3. The Experiment

RISE Experiment 2, known as 'The FIDES Experiment', was named for the Roman Goddess of trust. The aim was to investigate the process of building trusted reference information between heterogeneous platforms (differing capabilities/roles) when operating at the tactical edge.
The experiment utilised the reference information framework developed in Experiment 1 [6] to gauge the real-time use of these operationally-relevant information libraries and support the study of the optimal nature of reference information in a military context. The FIDES experiment focused on the nature and forms of reference information and looked to

characterise the nature and aspects of the reference information cycle illustrated in Figure 2. This report details the FIDES experiment: its design, evolution and preliminary outcomes.

On 6 October 2018, Defence Science and Technology (DST) Group and collaborators conducted the FIDES experiment. FIDES consisted of three experimental runs, each with a different rescue scenario. It was based out of the Port Noarlunga Surf Life Saving Club (PNSLSC) and covered the coastal region ranging from O'Sullivan Beach to Moana Beach, as shown in Figure 3. The experiment included staff from SLSSA, DST Group, Consilium Technology, Adelaide University and the Maritime Safety Authority (AMSA). Some of the team involved in the experiment are shown in Figure 4.

Figure 3. Experiment region along the coast centred on Port Noarlunga.

The experimental scenarios were conducted entirely by SLSSA personnel and equipment, apart from the experimental equipment used by the researchers for instrumentation purposes.

Figure 4. FIDES Experiment Team.

The SLSSA equipment/assets involved in the experiment are shown in Table 2, Figure 5, Figure 6 and Figure 7. More detailed descriptions of the SLSSA assets and their capabilities can be found in [6].

Table 2. List of SLSSA assets involved in FIDES.

Designation	Asset Type	Number of Crew
SURFCOM	Headquarters	4
Duty10	Local incident command	3
LS2 (Lifesaver 2)	Jet Rescue Boat 2	2
LS3 (Lifesaver 3)	Jet Rescue Boat 3	2
RWC1	Jet Ski 6	1
RWC2	Jet Ski 7	1
IRB 1	Inflatable Rescue Boat 1	2
IRB 2	Inflatable Rescue Boat 2	2
BID 1	Boat in Distress (IRB)	2
Noarlunga Patrol	Beach Patrol Operations Tent	6
ATV	All-Terrain Vehicle	2
BID 2	Unmarked Jet Ski	1

Figure 5. Local incident commander and team.

Figure 6. Jet rescue boats involved in the exercise.

Figure 7. Beach patrol and rescue assets.

Due to unforeseen complications with the SLSSA radio system, SURFCOM was based at PNSLSC rather than the originally planned West Beach location. This did not impact the running of the experiment as the SURFCOM personnel were kept isolated from the surf life savers operating in the field.

FIDES consisted of three runs containing different search and rescue scenarios. Each experimental run consisted of one major theme with smaller events occurring within them. The scenarios involved a mixture of Search and Rescue (SAR) targets which included live patients, plastic tubs representing patients, training dummies and SLSSA assets representing disabled water craft (examples can be seen in Figure 8 and Figure 9).

Figure 8. SLSSA staff in the IRB playing the part of injured scuba divers.

Each scenario was designed to stimulate activity and information flow between the rescue teams and the command and control units over 30 to 60 minutes. The goal was to generate enough data to discern meaningful trends, whilst keeping the stress level of the participants to an acceptable level. The three scenarios are detailed in the following experimental maps, shown in Figure 10, Figure 11 and Figure 12 and the subsequent run sheets.

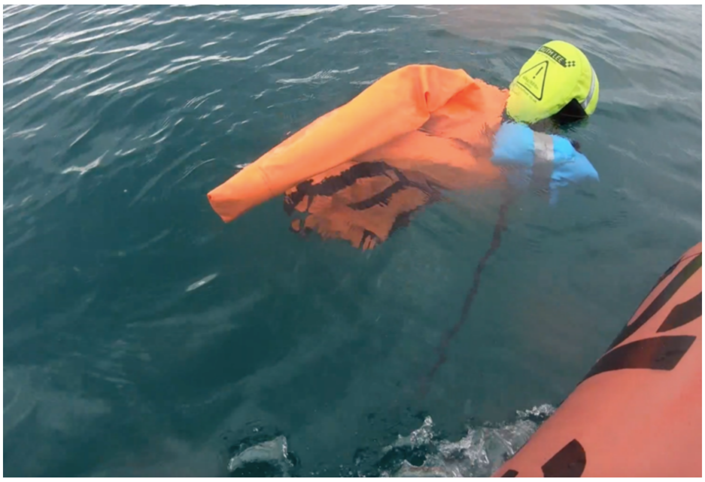

Figure 9. The RUTH Dummy used as a rescue target.

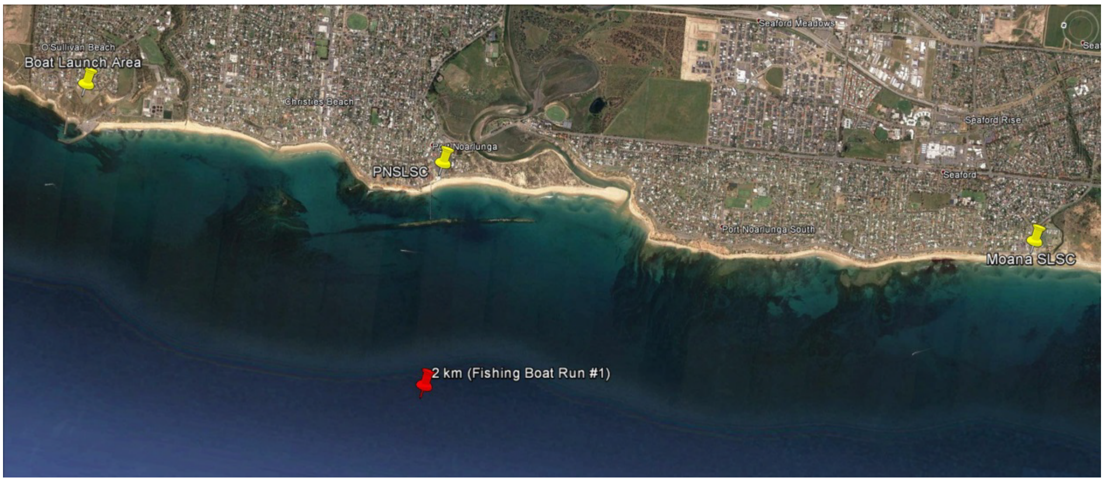

Figure 10. Experimental setup, running sheet and map for Run #1.

Figure 11. Experimental setup, running sheet and map for Run #2.

Figure 12. Experimental setup, running sheet and map for Run #3.

RUN #1 The Fishing Trip of Horrors

THE FIDES EXPERIMENT

SETUP

ITEM: Fishing Boat	TYPE: IRB	ID: EXP-BID1

POSITION: Move from PNSLSC to location 2km off-shore from Port Noarlunga

DST EQUIPMENT:
1. TEXAS Phone
2. GPS Tracker
3. GoPro 6

PATIENTS: 4
Patient 1 – Broken Leg (TUB)
Patient 2 – Head injury (TUB)
Patient 3 – Unconscious (excessive alcohol consumption) (TUB)
Patient 4 – Aggressive – intoxicated (TUB)

NOTES:
1. Fishing boat drivers to wear high-vis vest to show they are not in scenario. Boat damaged in severe weather and not operational
2. Need IRB crew to tell SLSSA personnel that there are two people that tried to swim to shore

ITEM: Swimmers	TYPE: SRC	ID: EXP-SWIMPAD

POSITION: Two swimmers to enter water 'a safe distance from shore' near Christies Beach (TUB)

DST Equipment:
1. GPS Tracker in tub

PATIENTS: 2
Patient 5 – Unconscious
Patient 6 – Unconscious

NOTES:
1. Deployed by Boat in Distress

RUNNING SHEET

09:10 SURFCOM:
1. Broadcast "Exercise, Exercise, Exercise. Run 1 is go"
2. .... Rescue, rescue, rescue ....
3. SURFCOM: All stations, a family member has reported to SAPOL that a fishing boat with 5 – 8 people on-board left O'Sullivan's Beach boat ramp at 4 am, was due back no later than 8:00 am and has not been seen or held from yet. Number of people is uncertain. Not sure of registration number, colour orange/red

Start Time + 10mins SURFCOM:
1. SURFCOM: All stations, keep look out for rogue Jet Ski, last seen causing nuisance off of Seacliff, now heading south. Report came in from SAPOL

No later than 09:50, SURFCOM: Signal EXERCISE END

NOTES:

1. **SLSSA** to conduct tasking/search/rescue/Transport phases as per standard practices. No treatment phase required for exercise.
2. **Observer boat not feeding information to duty10 for this Run**
3. DST staff will monitor information exchange, track the use of reference data through spreadsheet tracking application and take written notes of the activity
4. **Exercise End:** Once all patient are safely under the Port Noarlunga Beach Patrol tent.

All craft to finish at Port Noarlunga for debrief

RUN #2 The Rogue Jet Ski

THE FIDES EXPERIMENT

SETUP			RUNNING SHEET
ITEM: Unmarked Jet Ski	**TYPE:** Private Jet Ski	**ID:** EXP-RWC3	**10:50 SURFCOM:** 1. Broadcast "Exercise, Exercise, Exercise. Run 2 is go" 2. …. Rescue, rescue, rescue …. 3. SURFCOM: All stations, SAPOL has reported that a member of the general public has witnessed a black jet ski colliding with a board paddler off of Christies Beach. The board paddler is drifting and looks injured. The rogue Jet Ski left the scene at speed and was travelling south.
POSITION: Moves to a position 1 km off-shore from Moana beach. Jet ski has crashed (big wave) and driver is injured.			
DST EQUIPMENT: 1. TEXAS Phone 2. GPS Tracker 3. GoPro 6			**Start Time + 10mins SURFCOM:** 1. SURFCOM: All stations, a jet ski has been reported drifting off of Moana beach approximately 1 km out from shore. Report came in through SAPOL from the general public.
PATIENTS: 1 Patient 1 – Under the influence of alcohol, has head injury, broken left wrist and left shoulder			
NOTES:			
ITEM: Board Paddler	**TYPE:** SRC	**ID:** EXP-Board	**Start Time + 20mins SURFCOM:** 2. SURFCOM: All stations, IRB 2 driver has suffered a suspected heart attack. Crew member is treating on scene but needs assistance as motor non-responsive
POSITION: Board paddler to paddle safe distance off from Christies Beach			
DST Equipment: 1. TEXAS Phone			
PATIENTS: 2 Patient 2 – Head injury and shock			**No later than 11:30, SURFCOM:** Signal EXERCISE END
NOTES: 1. Need SLSSA or DST person to act as a watch for board paddler from shore (not in exercise, wearing high-vis) 2. Board paddler is IRB (BID) crew from first run			**NOTES:** 1. **SLSSA** to conduct tasking/search/rescue/Transport phases as per standard practices. No treatment phase required for exercise. 2. **Observer boat is actively feeding information to duty10 for this Run** 3. DST staff will monitor information exchange, track the use of reference data through spreadsheet tracking application and take written notes of the activity 4. **Exercise End:** Once all patient are safely under the Port Noarlunga Beach Patrol tent. **All craft to finish at Port Noarlunga for debrief**

RUN #3 When Scuba Turns Bad

THE FIDES EXPERIMENT

SETUP			RUNNING SHEET
ITEM: Scuba Boat	**TYPE:** IRB	**ID:** EXP-BID1	**14:10 SURFCOM:** 1. Broadcast "Exercise, Exercise, Exercise. Run 2 is go" 2. …. Rescue, rescue, rescue …. 3. SURFCOM: All stations, o Public on Port Noarlunga Jetty report to PNSLSC Beach Patrol that they have seen three scuba divers injured by a series of large waves hitting the reef. Two have made it back to their boat that seems to be drifting and the third never resurfaced.
POSITION: Moves to a position 1.5km South west of the Port Noarlunga Jetty			
DST EQUIPMENT: 1. TEXAS Phone 2. GPS Tracker 3. GoPro 6			
PATIENTS: 1 Patient 1 – Head injury Patient 2 – Broken leg and shoulder			**Start Time + 20mins SURFCOM:** 1. SURFCOM: All stations, suspected shark attack at Christies beach. Victim is on shore with members from the general public. Call went out to SAPOL and SA Ambulance. Need immediate aid from SLSSA
NOTES: 1. Boat engine is not operational in story 2. Need driver for Scuba Boat with high-vis vest (not part of scenario) 3. Driver will take boat back to shore after patients have been rescued			**No later than 15:00, SURFCOM:** Signal EXERCISE END
ITEM: Drifting Diver	**TYPE:** RUTH	**ID:** EXP-RUTH	**NOTES:** 1. **SLSSA** to conduct tasking/search/rescue/Transport phases as per standard practices. No treatment phase required for exercise.
POSITION: Into the water between the shore and the reef, North of Jetty at Port Noarlunga, slightly submerged (attached to anchor)			2. **Observer boat not feeding information to duty10 for this Run**
DST Equipment: 1. GPS Tracker in bag			
PATIENTS: 1 Patient 3 – Unconscious, Head injury			3. DST staff will monitor information exchange, track the use of reference data through spreadsheet tracking application and take written notes of the activity
NOTES: 1. Observer boat to deploy RUTH on the way out to their position			4. **Exercise End:** Once all patient are safely under the Port Noarlunga Beach Patrol tent. **All craft to finish at Port Noarlunga for debrief**

Information flows within the experimental runs were captured using video (GoPro cameras mounted on assets and personnel) and through the TEXAS[4] framework running on mobile and fixed computers. Data was extracted from the videos through post-analysis transcription and then coded using the NVivo[5] software package for further analysis. The goal was to determine the information categories, hierarchies and characteristics present within the scenarios to investigate and understand the role of reference information and information trust within each scenario.

TEXAS appeared to the participants as a blue force tracker that provided near real-time updates on the position, orientation and status of all assets participating in the experiment (Figure 13 and Figure 14).

Figure 13. TEXAS was installed on phones carried by the rescue team.

TEXAS also provided the participants with simple decision aids and the ability to broadcast the location of objects of interest within the environment. The features and concept behind TEXAS are documented in [6]. Using the lessons learnt and user feedback from Experiment 1, TEXAS was further developed for the FIDES experiment, adding the ability to show historical tracks, bearing lines for triangulation, independent GPS system integration and cloud-based control and configuration update concepts. An overview is shown in Figure 14 and Figure 15.

[4] TEXAS – Tactical Experimentation Architecture Support
[5] NVivo Software - https://www.qsrinternational.com/nvivo/what-is-nvivo

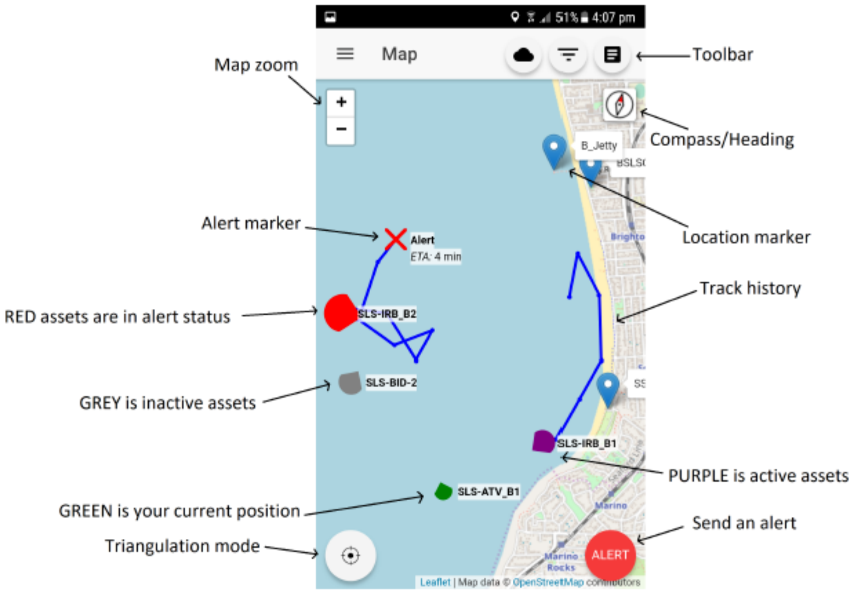

Figure 14. TEXAS display on a smart-phone.

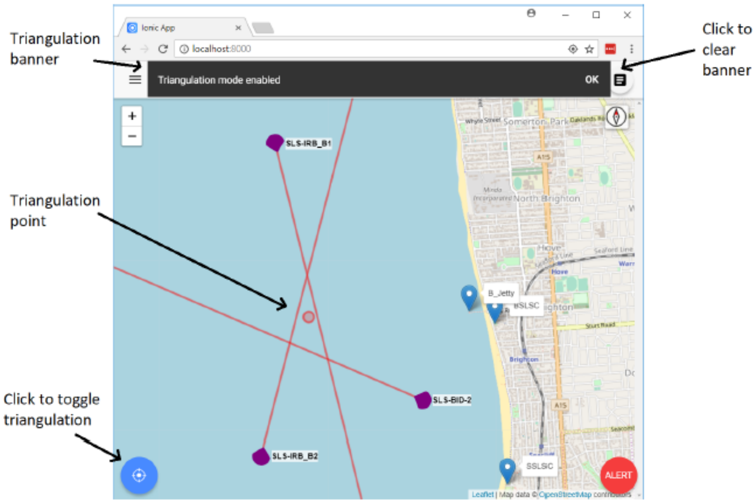

Figure 15. TEXAS display with triangulation mode enabled on three devices.

A triangulation mode was accessible by the local incident commander, Duty10, whereby lines of bearing could be requested from any of the devices running TEXAS within the field. The TEXAS frameworks then provided the geometric centroid of the bearing lines, helping to advise Duty10 where to start searching for the target of interest. All information being exchanged by the devices utilising TEXAS was recorded using log files, with time stamps for post-analysis.

An additional 'real-time' data collection method was trialled during the FIDES experiment to provide greater focus on the use of the reference information and provide additional information on the role of trust. The goal was to use researchers listening to the audio exchanges between the exercise participants to discern the use of pre-defined reference information categories in achieving the activity goals. The hypothesis was that by monitoring in real-time, experimental runs could be slightly modified on-the-fly, allowing for further and deeper analysis into particular aspects of the reference information use cycle if needed. An excel spreadsheet was developed for this purpose and contained the categories and data items shown in Table 3. Each category contained subcategories or data elements. Figure 16 shows the excel spreadsheet for the reference category "Order of Battle".

Table 3. Reference Information Categories and data items.

Order of Battle	Characteristics & Performance	Geographical Intelligence	Patients
Jet Ski	Type	Reef	Number of
IRB	Number of Vessels	Current	Injury
Jet Boat (Lifesaver)	Length	Surf/Waves	Age
Surf Club	Colour	Weather	Name
Duty 10	Speed	Jetty	Sex
SURFCOM	Estimated Time of Arrival	Boat Ramp	Condition (L,M,H, D)
Unknown	Name/Registration	Map	Contact
All Assets	Other	Other	Other

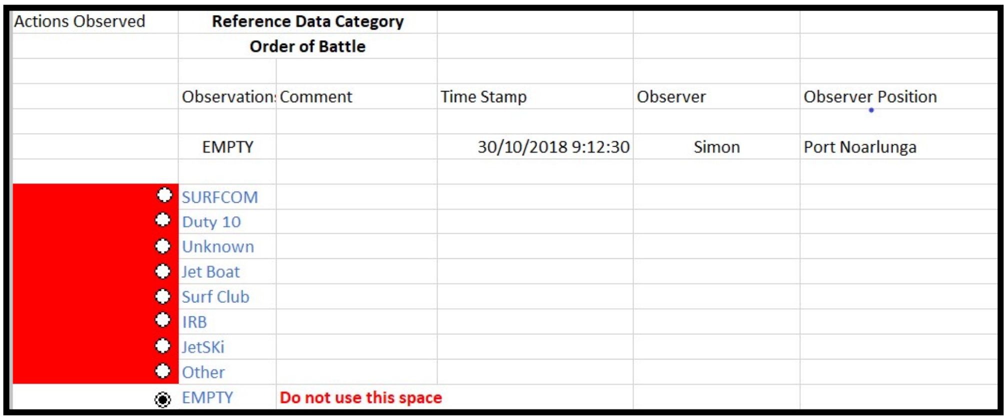

Figure 16. Reference Information tracking sheet.

The radio buttons (Figure 16, red box with white circles) for the Order of Battle category represented the different asset names only and not the detailed descriptions shown in Figure 17.

Listening for detailed descriptions in real-time was deemed too difficult. As a result, the link to reference information was to be confirmed through post-experimental analysis. The reference information items in a particular category were tracked using functional radio buttons which, when clicked by a researcher, automatically recorded the subcategories into a result sheet with an appropriate time stamp. The data items listed in Table 3 are high level and do not contain the detailed reference information discussed in Section 0 and shown in Figure 17.

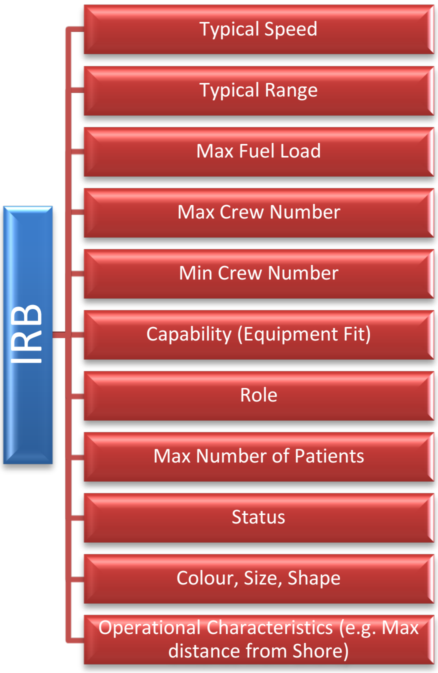

Figure 17. Inflatable rescue boat (IRB) reference information description.

4. Results & Discussion

The premise of the RISE experimentation series was to conduct defence-relevant research in a domain that facilitates rapid investigation in a collaborative environment with industry and academia. Experiment 1 [6] confirmed the utility of the SLSSA environment to conduct information interoperability research, while the present (FIDES) experiment focused on a particular information component, namely reference information.

Although the SLSSA domain does not support true machine-to-machine information exchange with the military concept of mission data, it does support a raw human based form of reference information that is well suited to studying the nature and use of reference information.

The three experimental runs were successfully completed on 6 October 2018, with video, audio and TEXAS logs being the primary forms of data. After an initial analysis of the data a methodology for deep analysis was developed and is shown in Figure 18.

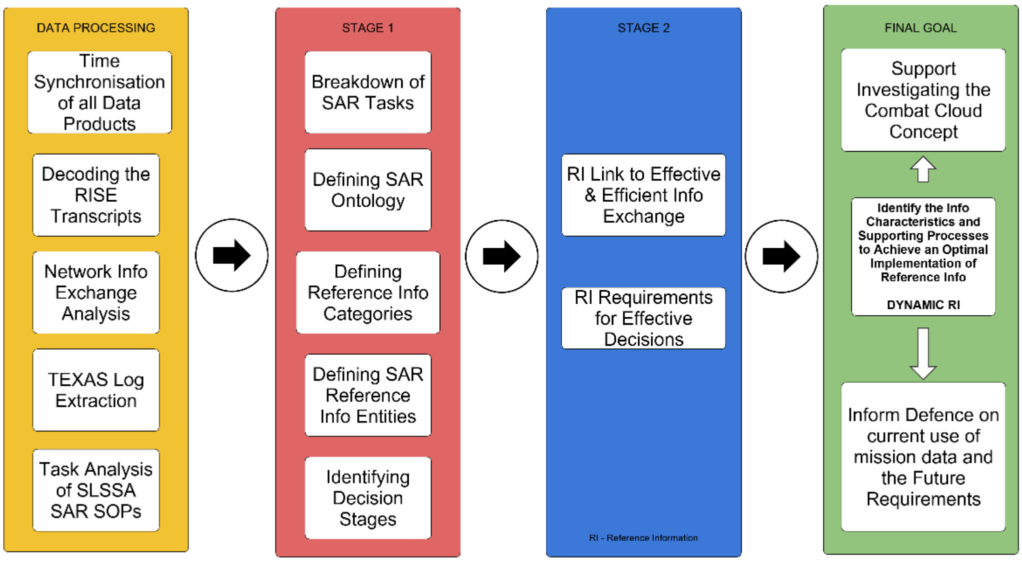

Figure 18. Reference Information Analysis Methodology.

4.1 Initial Observations

Applying this method to the data will take time. However, some initial observations are reported here, with more detailed analysis being the subject of future work.

The aggregated results from the reference information real-time tracking component of the experiment are shown in Figure 19. This illustrates the number of times a particular reference information category was used by the rescue team in addressing the situations presented to them. The data in Figure 19 also illustrates the differences between the real-time data assessed during the experiment (blue bars) to the post experiment analysis of the data (red bars). There is considerable difference between the two data sets, which likely reflects the difficulty experienced by the observers in identifying the information types in real-time from the radio chatter in a high-tempo environment.

The results in Figure 19 reflect the sentiment of the observers post experiment: real-time tracking by humans is very difficult. This fact, together with the high-level abstraction of the information required to aid in the tracking process, illustrates that post-experimental analysis is the preferable option for future experiments, with the real-time tracking adding little value.

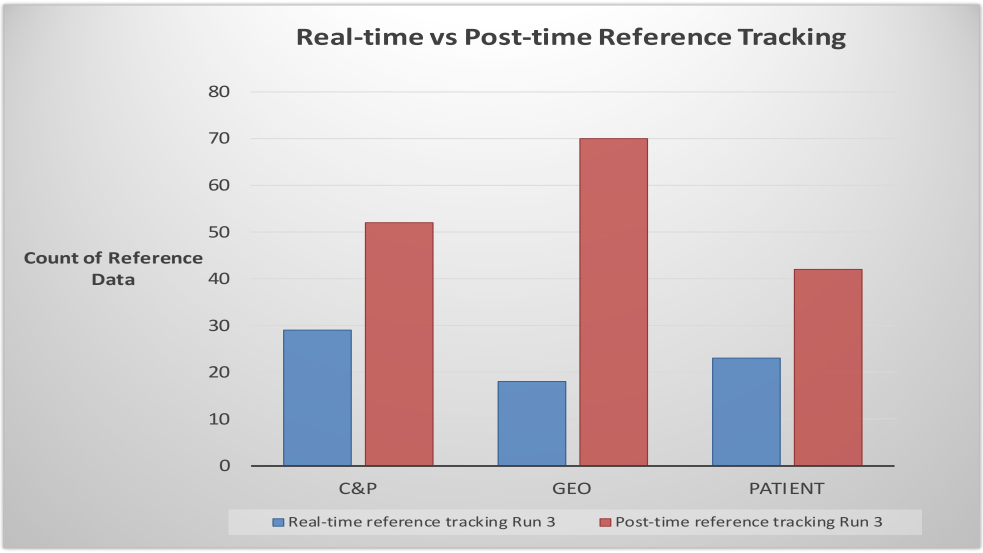

Figure 19. Real-time reference information tracking results.

4.2 Networked information analysis

For the post-experimental analysis work, the video transcripts were coded into the software package NVivo, which identified the information nodes, the information exchanged and the send and receive relationships. An event timeline was produced for Run #3 and is shown in Figure *20*. Four distinct phases are defined outside of the run's endpoints: the incident reporting; search; the rescue; and the transport/treatment phase. These phases were defined by categorising the type of events that typically occur during a search and rescue activity. By breaking down the scenario in this way, the identified tasks help characterise the context and nature of the information 'required and produced' supporting the decisions and actions that followed.

Initial results for Run #3 of the FIDES experiment from an information point of view are shown in Figure 21.

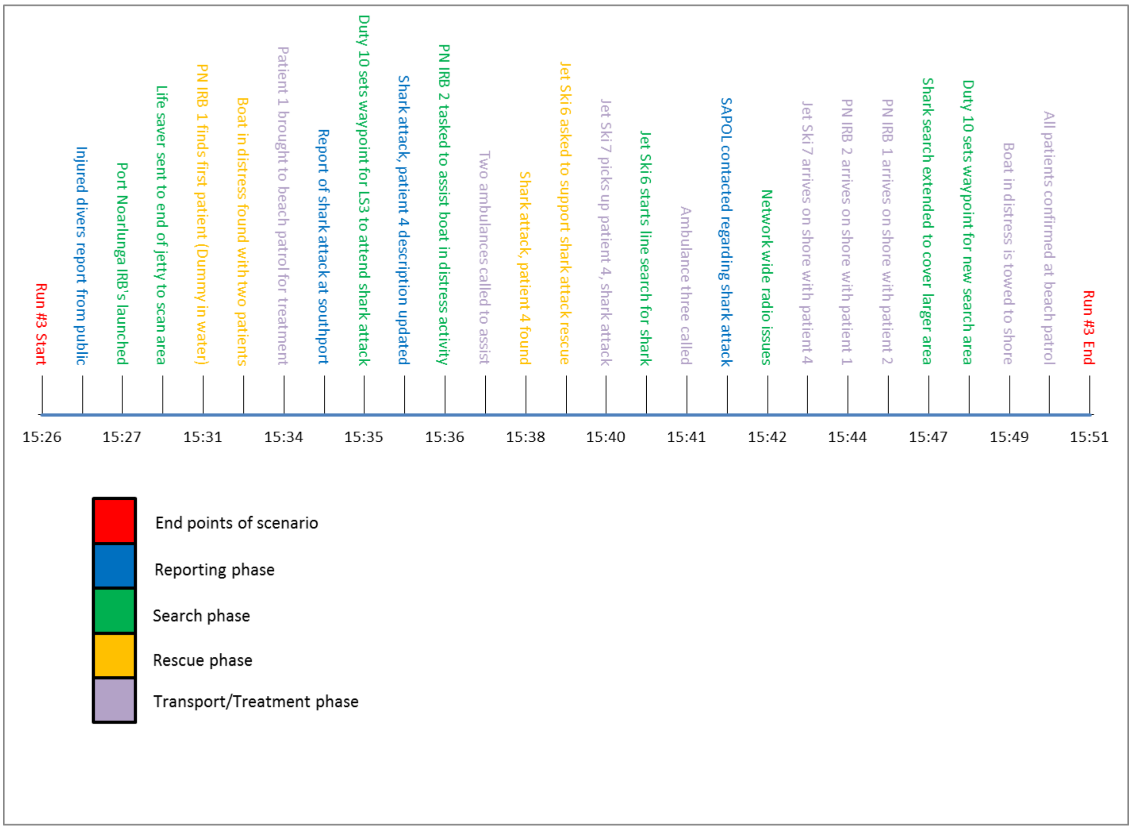

Figure 20. *Event timeline for FIDES Run #3.*

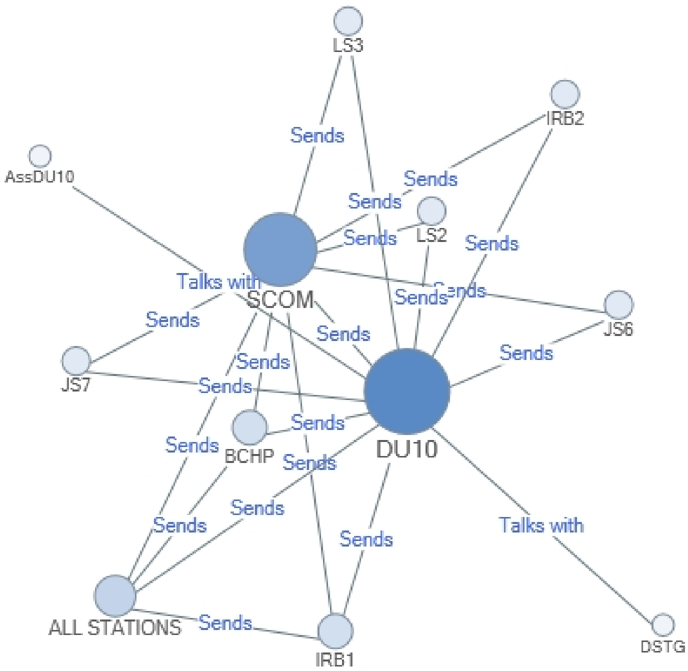

Figure 21. Network diagram of the information flow ('Sends' and 'Talks with' only) captured from the FIDES video footage- transcripts Run 3.

The network diagram in Figure 21 is based primarily on radio communication, illustrating the various connections and relationships between the nodes in Run #3. The size of the nodes illustrates the relative volume of information passing through that node during the run. Duty10 (the local commander) and SURFCOM (Head-Quarters) are the primary nodes; with all radio communication passing through them. Figure 21 indicates a strong reliance on these nodes for interpreting, assessing and acting on information in the context of the mission goals and overall success.

This fact is further demonstrated in Figure 22, which presents the same data as an egocentric sociogram (central node focused network diagram). The centre (ego) of this diagram is Duty10, which is represented by the star. From this perspective, SURFCOM is the closest node. This is not surprising as both nodes have the C2 responsibilities over the SAR team, where SURFCOM is headquarters and Duty10 is the local, onsite, C2 node. Figure 22 also demonstrates potential bottlenecks in information flow, which are the result of the overarching communication protocols that require information exchange to pass through the C2 nodes. An exception is when permission is granted for point-to-point communication, not represented in Figure 22 as there was no occurrence in Run #3. The data of the kind displayed in Figure 21 and Figure 22, once produced for the entire dataset, will describe the information exchange characteristics of the scenarios.

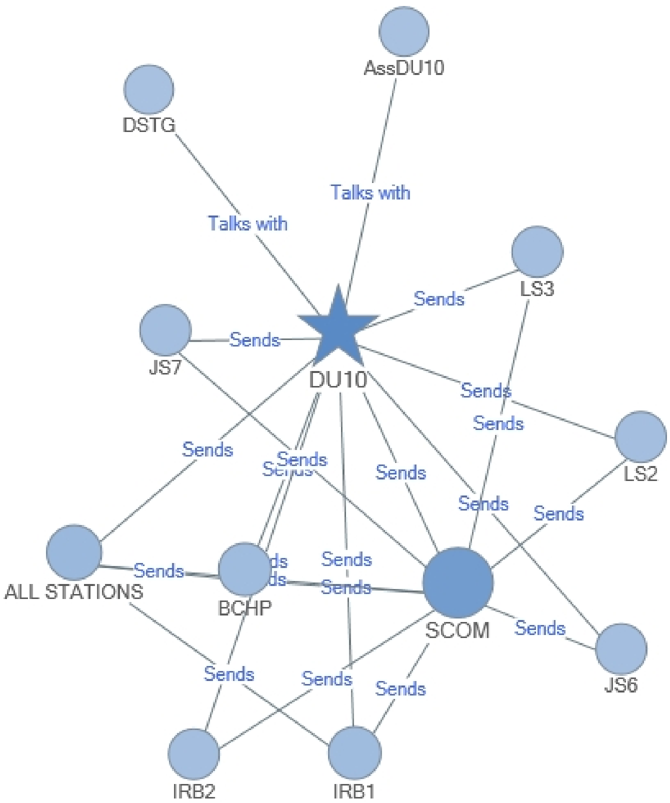

Figure 22. Egocentric sociogram for Duty10 information speed ('Sends' and 'Talks with' only) captured from the video footage-transcripts Run 3.

4.3 Ontological construction from scenarios

The next stage is to define the information categories relevant to the domain and link to the concept of reference information, as per Figure 18.

As an initial step, consider the work by LeBlanc et al. [9]. In this paper, a military C2 ontology was developed in order to facilitate the retrieval of updated mission information for the first responders where communication networks are uncertain and unreliable. The ontology enables common representation and structure of metadata over a MANET (mobile ad-hoc network) to allow sharing of observation reports, updated orders and mission-time imagery.

In relation to SAR, LeBlanc et al. define an approach for deconstructing the scenarios associated with an activity in a hierarchical manner to help support the development of the ontological categories and subcategories. This approach was used for the FIDES data to break down the communication transcripts into information categories and reference information items. Although ongoing work, some initial results from Run #3 are presented here. The preliminary information ontology is shown in Figure *23*. The information items shown in Figure *23* give context to the production, use and updating of reference information during the Run #3 scenario.

4.4 Trust and reference information

Any new information discovered, processed, assessed and then acted upon requires varying degrees of trust. The measure of trust is based on the trust components of 'trustworthiness', 'trust-attitude' and 'trust-action', as described in Section 1. In Run #3, the assessment of new information, i.e. critical events, was conducted by the C2 nodes using their authority and belief that the information collected was in the context of the environment. In essence, Duty10 and SURFCOM assign degrees of trust-attitude following their assessment of new information. Furthermore, based on their authority, each can assign a trustworthiness property to new information perceived in the environment. By virtue of assessing trustworthiness and assigning trust-attitude in relation to critical events, the C2 nodes will then explicitly use this trust process to validate the hierarchy of information nodes (or sources) and categories of information types, thus supporting the reference information. To summarise, the linkages are shown in Figure 24, highlighting the strong trust theme across the layers.

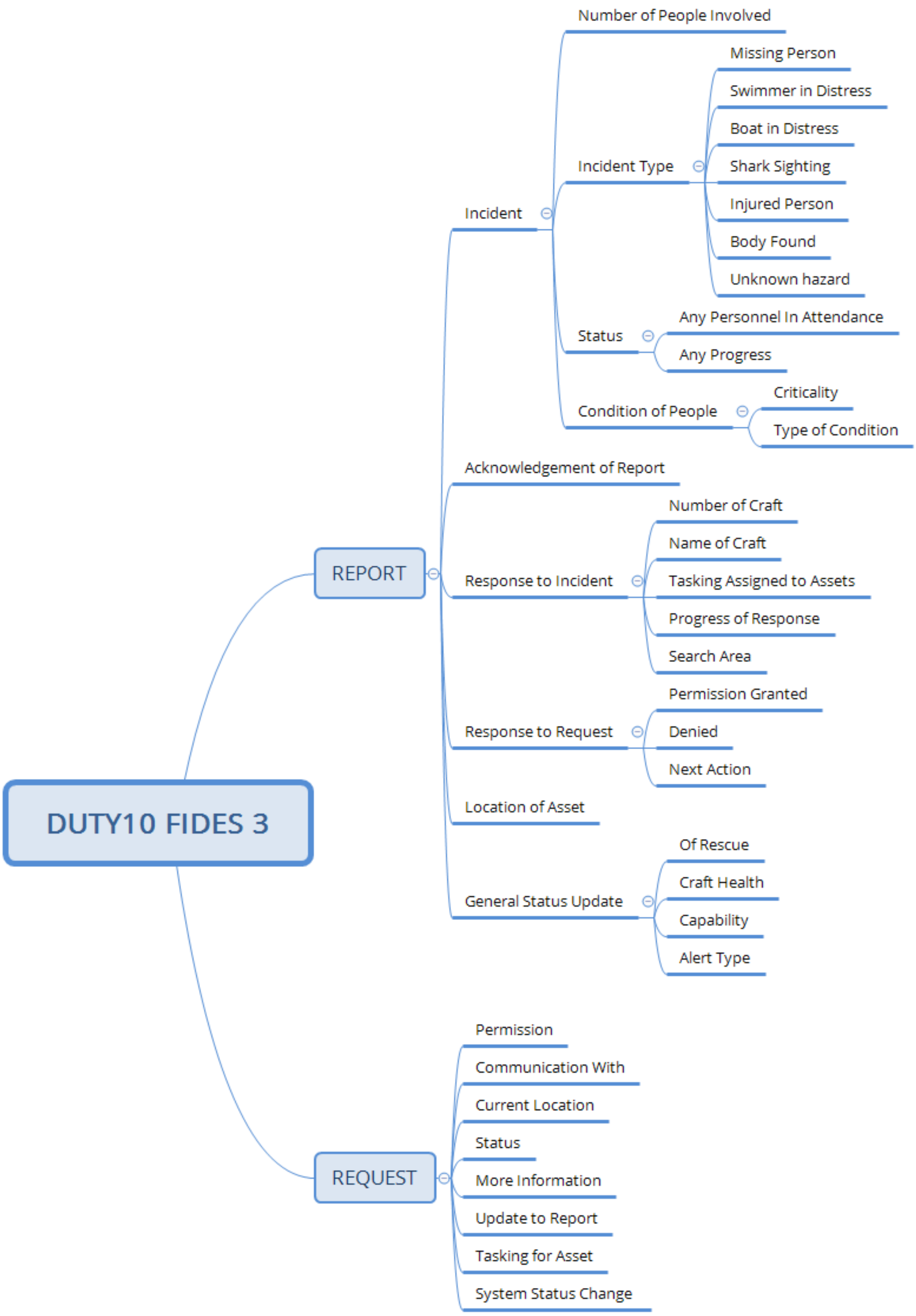

Figure 23. Preliminary information ontology for Run 3 from the perspective of Duty 10.

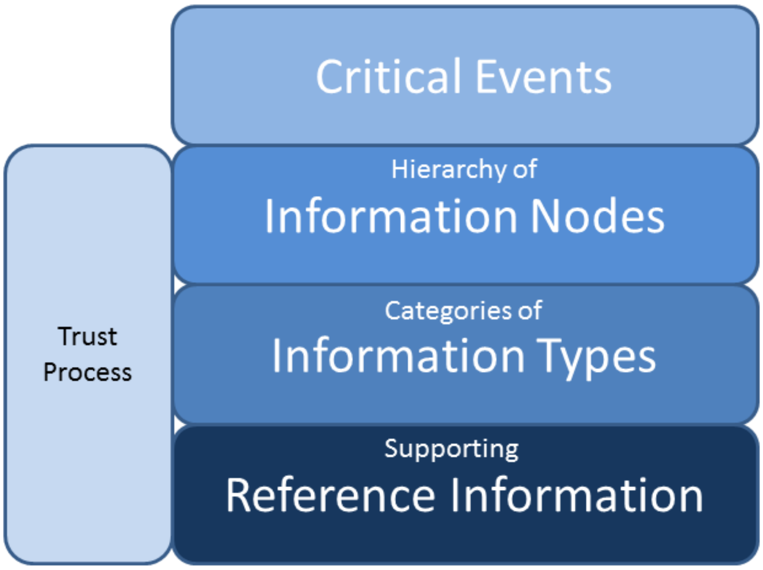

Figure 24. Linkages between the events in the scenario and the information types.

It is worth considering that there is also tension between speed of decision, trust-action, and trust-level (or trust-attitude) reached for the information. The desire to trust the information to a level before acting may be balanced against the need to act; such as sending resources to a rescue in a timely manner. This is the risk in any trust-action, as detailed in Section 0. This is where the knowledge, expertise and underlying reference information play a key role and is of particular importance in a distributed team.

To investigate this further, consider the role of reference information in sending a simple request, as diagrammed in Figure 25. For example, SURFCOM sends a request over the radio to Duty10 for more information on the progress of the rescue. In order to form this request SURFCOM needs access to prior knowledge, such as reference information. Similarly, when Duty10 receives the request, for the request to be interpreted, Duty10 also needs access to reference information to provide context of the request in relation to current activities and the environment.

If SURFCOM receives new information from Duty10, a decision is made as to whether it should be used to update the relevant items in the SURFCOM reference information database. As previously stated, reference information supports the trust process as it is the basis for the trustworthiness property and the trust-attitude of the receiver.

We can consider this in the context of the trust elements once again. For example, staff in SURFCOM have South Australian Police (SAPOL) as a trusted information source in their internal reference information, which is a result of their experience and training. This is the trustworthiness property described in [4]. The reference information captures that SAPOL exhibits an expected behaviour. Therefore, if SAPOL is willing to conform to this behaviour it is trustworthy. A report which comes in from SAPOL is trusted and can be broadcast to all stations without further query.

In comparison, a report from the general public requires verification through a supporting subset of other information sources. This need for further verification highlights a smaller trustworthiness level for this information source compared with SAPOL and the associated lower trust-attitude assigned by the receiver of the information.

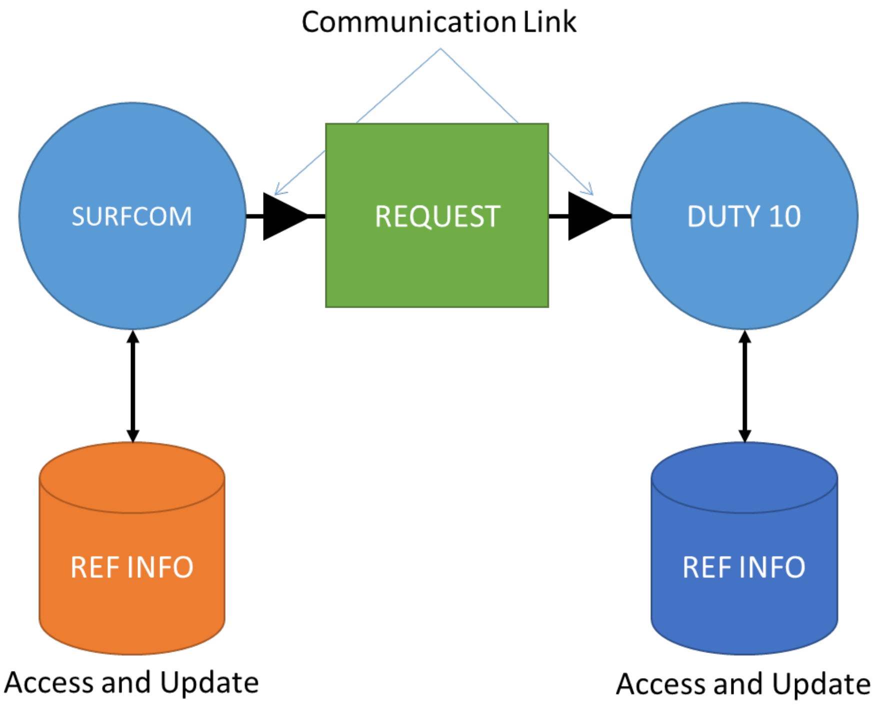

Figure 25. Reference information use.

Extending the trust concept further, there is a requirement to trust the reference information itself as a trusted library. How is the trust of the reference information library affected as a result of new information, discovered as part of the mission, being added dynamically to that library? Understanding the process of building and maintaining trust in reference information is important, particularly when seeking to move towards a dynamic reference information paradigm. In this situation, trust relies on the level of confidence the user has that a system is exhibiting expected behaviours, within the context of a mission, after incorporating the reference information library updates. The verification/validation aspect of 'building trust' in information used by the operator is an aspect that lengthens the update process of the library, but at the same time helps ensure mission success. An example within the FIDES experiment is used below to investigate this further.

Figure 26 illustrates a simple model to visualise the role of trust in updating reference information. This reference information can either be explicit or implicit and is processed by the lifesavers on the scene and in the C2 units, when an event occurs. The stages of assessment the information progresses through in a dynamic process is highlighted in Figure 26.

This model was influenced by the transparency and accountability mechanism developed by Cao et al. [10]. Their model design is used for accessing data from different sources, such as sensor data from the internet of things (IoT) [10]. In the model proposed by Cao et al. [10] data is progressed to an ontology layer and a trust layer for processing, where the data is appropriately annotated with metadata and returned to the data management layer. The assessment layer shown in Figure 26 is representative of the stored ontology proposed by Cao et al., and the trust ontology is the trust layer [10]. These items support the concepts already discussed around trustworthiness and attitude. The shared metadata is then a shared concept of trust-attitude, as detailed by Ceolin et al. [4] to support reducing the risk in the trust-action.

In Figure 26, the model shows that at any given event time (*t*) a report will generate new reference information (*I_new*), the new information is assessed against expectations (the belief or trust-attitude), trusted, and integrated (Figure 26, *Ri_0* + *I_new*) along with the existing reference information (*Ri_0*). After the integration step, the reference library is now an updated library.

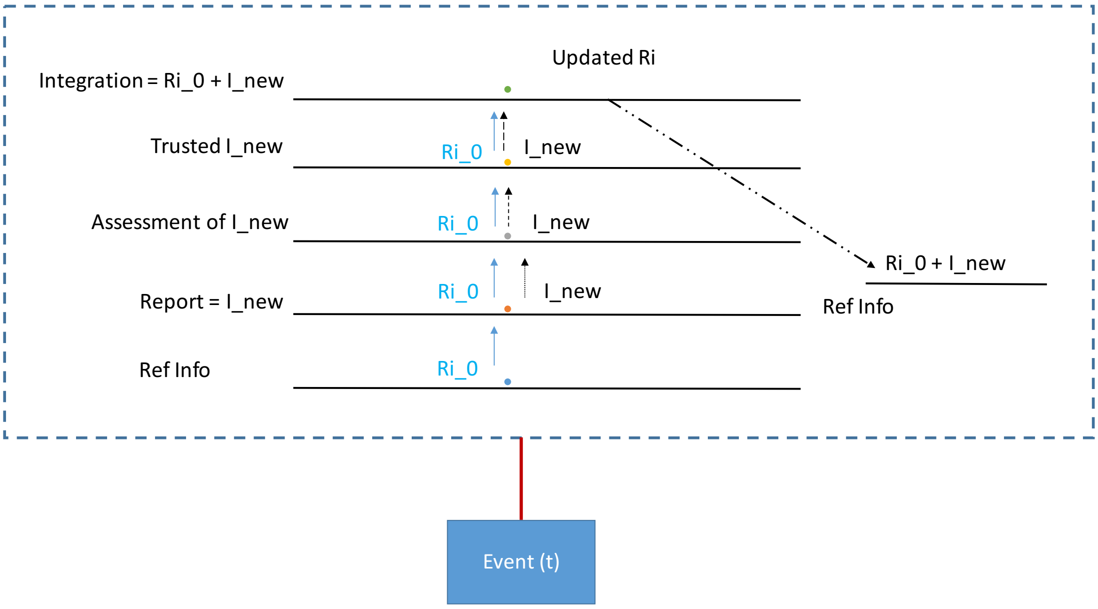

Figure 26. Energy level diagram as a map for reference information trust.

In Figure 20, events that occurred during the FIDES experiment are displayed to highlight where reference information could be utilised and exchanged amongst the different surf lifesaver assets via radio communications. Figure 27 illustrates some of the steps involved when an event occurs and highlights the link between the event, the information and the reference information. Explicit in this process is the concept of trust, as discussed above. Consider this example with some specific cases from the experimental results.

FIDES Experiment Run #3: At 15:25:05 a report from the general public is relayed by Port Noarlunga beach patrol (BCHP) to SURFCOM and the other surf lifesaver assets via a radio broadcast. Within that communication exists explicit reference information that includes information about the incident, namely:

1. The number of scuba divers, 3, involved in the incident
2. The location of the incident
3. Known details on status.

This new reference information is then assessed by all surf lifesaver assets. Whether it will be trusted or not depends on the confirmation of the report, the nature of the source and assessment against any other related information feeds.

Implicit reference information, past knowledge and experience about the area (including weather patterns and sea conditions) can be used to support the trust process. It is inferred that at 15:25:35 a level of trust is placed in the report, following the above-mentioned assessment, since BCHP reported to SURFCOM that two IRBs had been tasked to investigate the incident. This new information regarding the deployment is then assessed by Duty10 (the local incident commander) where he witnesses the IRBs leaving the beach through visual confirmation and confirms the location of the IRBs, through the TEXAS GPS tracking. The status and position of the IRBs are now new reference information to be used by the rescue teams.

Another example of gaining trust in the explicit reference information was shown in observation of the use of TEXAS in Run #3. At 15:28:40, Duty10 tasked Port Noarlunga IRB 1 and IRB 2 to move from the southern extreme of the reef in a north-bound direction. This was received and acknowledged by IRB 2 at 15.29.05. Duty10 then made the comment to his assistant *"so you might want to turn-around then boys"*. Duty10 was, at that time, referencing the location of the IRBs using the TEXAS GPS tracker locations. This statement suggests that Duty10 trusted the explicit information that was being supplied to him through the TEXAS framework and presented as blue-force position and status tracking. Once again, this new information passes through the reference information timelines, as per Figure 2 and Figure 26, on the way to being trusted and integrated into the greater reference libraries.

Examination of the transcripts produced from the FIDES experiment Run #1 revealed further evidence of trust developing in the explicit reference information. Duty10 tasked the power craft, Lifesaver 3 (LS3), over the radio at 13:00 stating *"Life saver 3, if you can, coordinate a line search approximately 2 kilometres offshore from the reef"*. This instruction was new reference information and became a part of the new base state of the system. There is implicit trust in this status update as the request came from a C2 unit, Duty10, which was a trust-attitude.

However, three minutes later Duty10 noticed a conflict between the task given and the outcome displayed on TEXAS. The update to the reference information may not have been current and accurate. Therefore, there was some ambiguity. Duty10 decided to contact LS3 over the radio at 13:03 stating *"can you just repeat back the directions I gave you, I am just looking on TEXAS you don't seem to be following the instructions I gave, I want to make sure you* *understood what I said. Over!"*. The update of reference information was in dispute as the updated status did not appear to reflect reality. From this statement, it is inferred that Duty10 was referencing the asset location information displayed by TEXAS.

Duty10 had acquired some level of situational awareness through TEXAS and perceived that LS3 was not following the commands given. This trust in the information update was then re-assessed by communicating again with LS3. At 13:03.05, Lifesaver 3 replied, *"Line search south from Christies"*. Duty10 now trusts the information update and overall status as the position of LS3 on TEXAS, and subsequent position changes, reflected the instructions given in the initial tasking request.

Trust is vital for highly integrated systems, where key functions rely on the entity descriptions in the reference library. The performance of the entire system can be negatively impacted if leveraging poor-quality information. The preliminary analysis of the FIDES experiment demonstrates that resource allocation and rapid decisions have an implicit and explicit process for gaining trust in the information. This manifests when transitioning information to reference information and integrating with the greater library.

There is a balance between effort required to attain the ideal trust level in the information received and timeliness of the resulting action. Response time may be vital and therefore experience can be used to short circuit a lengthy trust process. In this situation the balance of risk is important. However, some nodes in a network may require a higher level of trust in the information due to their position in the network hierarchy as well as the information assessment and production they influence.

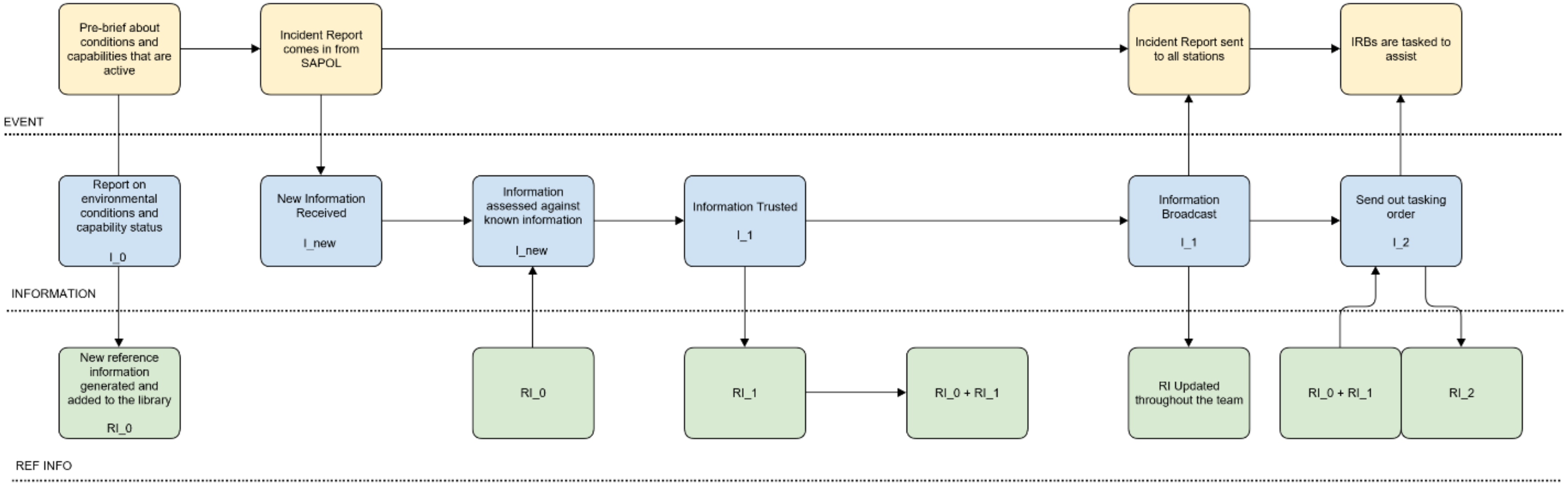

Figure 27. The role of information and reference information for an event case study.

5. Conclusion & Future Work

Reference information libraries support fully integrated systems, providing a digital description of entities within an environment for the relevant computer systems and their operators. This information is structured and prepared prior to a mission. It is distilled from a large pool of intelligence and environmental characteristics relevant to a mission outcome. The preparation time for these libraries can be lengthy, requiring rigorous verification and validation before being used to optimise a platform and its sensors for a role. Traditional reference information is therefore static and not adaptive to unexpected occurrences and outcomes.

To overcome this limitation, the concept of dynamic reference information, whereby entity descriptions can be updated in near real-time is a likely future requirement. These updates may be an augmentation of the base library, reflecting the discovery of some new intelligence. One of the key challenges facing the realisation of dynamic reference information is trust in library updates. As new information is discovered or received, what does it relate to? Where does it come from? How will it affect the system if uploaded?

Using the emergency services domain as a surrogate for a defence joint task group environment, the exchange and processing of information has been studied through the FIDES experiment. The preliminary results were studied focusing on the link between the critical events, C2 hierarchy, and information categories and implied reference information. The results indicate that a trust process runs deeply throughout this information framework, with the concepts of trustworthiness, trust-attitude and trust-action playing out when SLSSA addressed a SAR scenario.

Analysis has indicated that reference information supports both the generation of requests, their interpretation by the receiving party, and the complementary information concept of a report. The preliminary work suggests that the updates to reference information used in this domain are trusted based on comparison to expectations (e.g. whether it is an expected behaviour or a more detailed construct, such as a trust ontology). The nature of the information source and the corroboration through the integration of multiple sources was seen in the initial analysis of the information exchanges. Further, the concept of reducing trust-action risk through sharing metadata seems key. Metadata reflects a trustworthiness property or trust-attitude following assessment of the receiver.

Further work is needed to complete the analysis across the entire FIDES experiment dataset and to capture the trust concepts in a model that can form the basis of experimental investigation in the future. In addition, the concept of building trust in reference information needs to be studied in more complex domains, where multiple agencies work as a team on a common goal, and information processing centres are distributed and leverage reference libraries produced from different operational perspectives.

The emergency services domain continues to provide a rich experimentation environment with parallels to challenges faced within the military domain.

6. Acknowledgements

The authors would like to acknowledge the continued support of their Defence sponsors, collaborative partner Surf Lifesaving South Australia, Adelaide University and the Australian Maritime Safety Authority. The authors would also like to acknowledge the effort of the entire RISE team in planning and executing the Fides experiment.

The authors would like to acknowledge the late Dr Simon Bou for his contribution to this study, the transcription and analysis of the data and the preparation and writing of this report. Simon was a key member of the RISE team, approaching the research with passion, determination and true out of the box thinking. He will be truly missed.

7. References

[1] F. Danashi, "Tactical Edge Characterization Framework MTR070331," The MITRE Corporation, 2007.

[2] I. M. D. Center, "Life-Cycle Mission Data Plan Guidebook V3.1," 8 April 2014. [Online]. Available: https://www.acqnotes.com/wp-content/uploads/2016/03/LMDP_Guidebook_v3.1.pdf.

[3] K. Goztepe, I. Cehreli and S. E. Sensoy, "A Decision Framework for Combat Cloud Computing Strategy," *6th International Information Security & Cryptology Conference,* p. 4, 2013.

[4] D. Ceolin, A. Nottamkandath, W. Fokkink and V. Maccatrozzo, "Towards the Definition of an Ontology for Trust in (Web) Data," *10th International Workshop on Uncertainty Reasoning for the Semantic Web,* pp. 73 - 78, 2014.

[5] K. O'Hara, "A General Definition of Trust Working Paper," Univeristy of Southampton, Southampton UK, 2012.

[6] A. Walters, S. Bou, J. Priest, A. Consoli, T. Priest and S. Williamson, "Conducting Information Superiority Research in an Unclassified Surrogate Defence Environment, DST-Group-TR-3529," 2018.

[7] M. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors,* vol. 37, pp. 32 - 64, 1995.

[8] N. Woods and D. Sarter, "Situation awareness: A critical but ill-defined phenomenon," *The International Journal of Aviation Psychology,* vol. 1, pp. 45 - 57, 1991.

[9] E. Leblanc, D. N. Nguyen, M. Balduccini, W. C. Regali, J. B. Kopena and T. Wambold, "Military Ontologies for Information Dissemination at the Tactical Edge," *JOWO@ IJCAI 2015.,* 2015.

[10] Q. H. Cao, I. Khan, R. Farahbakhsh, G. Madhusudan, G. M. Lee and N. Crespi, "A trust model for data sharing in smart cities," *IEEE International Conference on Communications (ICC),* 2016.

Universities and Colleges
Prof Ali Babar, Computer Science, Adelaide University
Prof Cheng-Chew, Electrical and Electronic Engineering, Adelaide University

DEFENCE SCIENCE AND TECHNOLOGY GROUP DOCUMENT CONTROL DATA					1. DLM/CAVEAT (OF DOCUMENT) NIL
2. TITLE Building Trusted Reference Information at the Tactical Edge			3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED LIMITED RELEASE USE (U/L) NEXT TO DOCUMENT CLASSIFICATION) Document (U) Title (U) Abstract (U)		
4. AUTHOR(S) Andrew Walters, Simon Bou, Angela Consoli, Tim Priest, Robert Davidson, Jayson Priest and Sonya Williamson			5. CORPORATE AUTHOR Defence Science and Technology Group Third Ave, Edinburgh SA 5111		
6a. DST GROUP NUMBER DST-Group-TR-3641	6b. AR NUMBER		6c. TYPE OF REPORT Technical Report		7. DOCUMENT DATE July 2019
8. OBJECTIVE ID	9.TASK NUMBER N/A			10.TASK SPONSOR N/A	
11. MSTC Distributed Combat and Mission Systems			12. STC Combat Information Interoperability		
13. DOWNGRADING/DELIMITING INSTRUCTIONS			14. RELEASE AUTHORITY John Riley, CWCSD		
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 Australian Department of Defence and Defence Force Personnel.					
17. CITATION IN OTHER DOCUMENTS Yes					
18. RESEARCH LIBRARY THESAURUS					
19. ABSTRACT Reference information libraries support fully integrated computer systems, enabling automated functions, such as identification and decision support, within the context of an environment. This structured information is prepared prior to a mission, distilled from a large pool of intelligence and environmental characteristics relevant to a mission outcome. The preparation time can be lengthy, requiring rigorous verification and validation before being used to optimise a platform and its sensors. This study investigated information exchange and processing under the pressures and limitations of first respondents at the tactical edge to provide insight into transitioning reference information to a dynamic 'real-time' paradigm. This preliminary work suggests that the updates to the reference information are trusted based on comparison to expectations; whether it is an expected behaviour or a more detailed construct, such as a trust ontology. Furthermore, the concept of reducing decision risk through the sharing of meta-data seems key, where the metadata reflects a trustworthiness property or trust-attitude, following assessment by the information receiver.					