

DEVELOPING SAFETY TARGETS AND RISK TOLERABILITY CRITERIA FOR NETWORK ENABLED ENTERPRISE EMERGENT SYSTEMS (NE3S)

David Reid (1) & Richard Maguire (2)

(1) SCS Limited, Henley-on-Thames, UK
dreid@scs-ltd.co.uk

(2) SE Validation Limited, Salisbury, UK
rlm@sevalidation.com

Keywords: Network enabled, Enterprise safety case, Emergent properties, Targets

Abstract

Military capability relies on whole system performance to accomplish its domain requirements and operational successes. In recent conflicts there has been a push to network together the various command and control information systems to improve military agility and effectiveness, whilst reducing collateral damage and fratricide events [1].

With this change in military operational structure, we can expect the nature of hazards to change. In reaction, the nature of safety and risk analysis should also be expected to evolve. It is anticipated that network enabled systems will have beneficial emergent properties in the battlespace. It should also be anticipated that there will equally be emergent detrimental properties or vulnerabilities (potential safety hazards) from these systems [2].

As a response to growing demand for some basis from which to undertake safety assessment, this paper will report on the recent development of a risk tolerability matrix for a network based capability. The specific programme is for a new networked enabled enterprise, and although direct reference is not possible, the technique for handling the decisions and judgements required on the system's emergent safety properties is directly recorded and cited.

Introduction

The MoD is currently involved in a programme to assess and procure a network enabled capability to integrate multiple sensor products in order to provide actionable data and to provide interoperability between UK and coalition assets, whilst enhancing situational awareness and contributing to the development of the Joint operational picture.

In accordance with the contemporary defence standards, joint service procedures and project guidance, it is necessary to establish a safety management system and safety management plan. As part of these arrangements, it is necessary to establish safety targets and a reference by which risk tolerability may be judged. This remains obligatory and valid for items of equipment components, equipment systems and networks of systems, be they legacy, contemporary or emergent.

The remainder of this paper is organised as follows; section 2 considers the system description and Section 3 considers the key domains for risk in network-enabled enterprise emergent (NE3) system. Section 4 introduces qualitative descriptions of impact and frequency that may be used for appreciating safety risks in this domain and develops the boundary conditions for judging risk tolerability. Section 5 discusses the concept of dynamic temporal risk allocation as a method for how the tolerability criterion can be used to decide on separate boundary conditions for the systems building the NEC and for the NEC enterprise itself. Section 6 provides a summary to capture the main learning opportunities for future use.

The NE3S system description

There are no clear definitions of what a network-enabled enterprise emergent system actually is. The nearest available military definition is from JSP 777 [3], although it doesn't actually give a concise definition of what NEC is. It does give the potential from NEC; the likely impacts of NEC; what NEC offers the military domain; and the benefits and challenges of NEC, but not a clear definition of what NEC means. The best text comes from the section on the span of NEC which states that the span of NEC "...will impact across the strategic, operational and tactical levels of command. Command and force elements will be progressively integrated into an interoperable information and intelligence infrastructure." [3]

The addition of emergent and enterprise give the fuller definition for this paper. Emergent is defined in many dictionaries as something appearing, arising, occurring, or developing, especially for the first time. An enterprise is defined widely as a commercial business; business activities directed at profit, a new project often involving risk, confidence and initiative; and readiness to undertake new ventures. It arises from the old French word 'entreprendre' ~ enter into taking [4].

Combining these together gives the definition of NE3 as:

"The developing integration of command and force elements directed at military advantage."

With this definition in hand the whole military domain needs to be reviewed to establish where an NE3 entity can be described. Two such domain sets have been identified by the authors – the military kill chain (Find, Fix, Track, Target, Engage, Assess - F2T2EA); and the ISTAR Chain (Resource Tasking, Resource Brokering, Information Requirements Management, Exploitation, Information Processing and Dissemination). This paper will concentrate on the former of these two areas.

During the procurement of the programme to assess and procure a network enabled capability to integrate multiple sensor products, the military kill chain was modelled to enable a rigorous identification and analysis of accidents and hazards to be completed. The sanitised models are shown in the following figures.

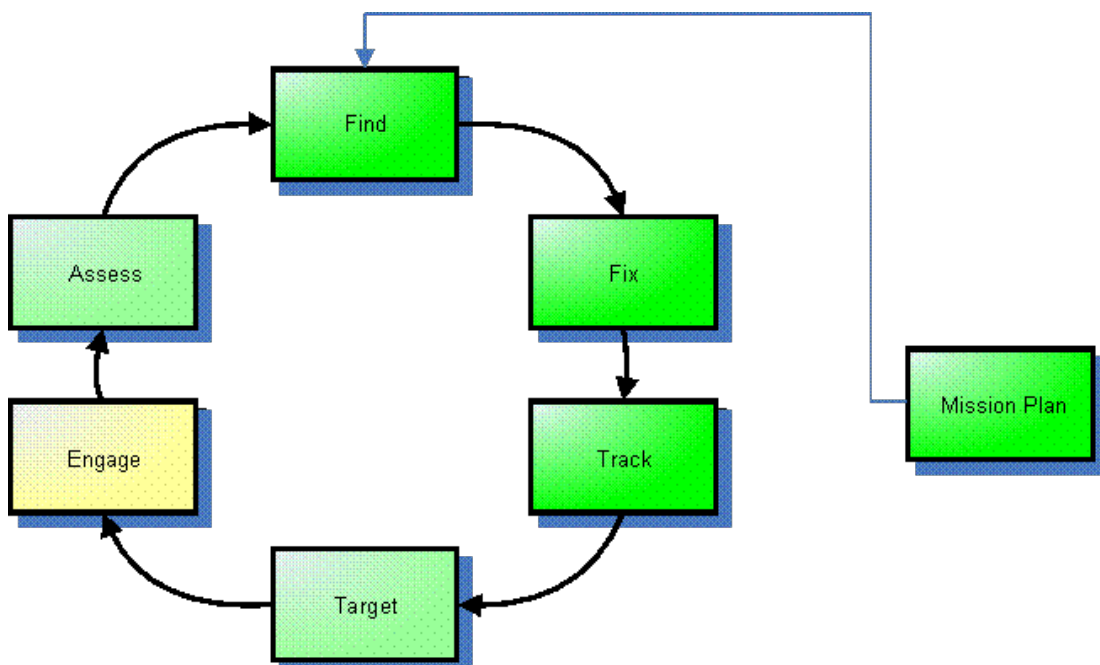


Figure 1 : F2T2EA Enterprise component model

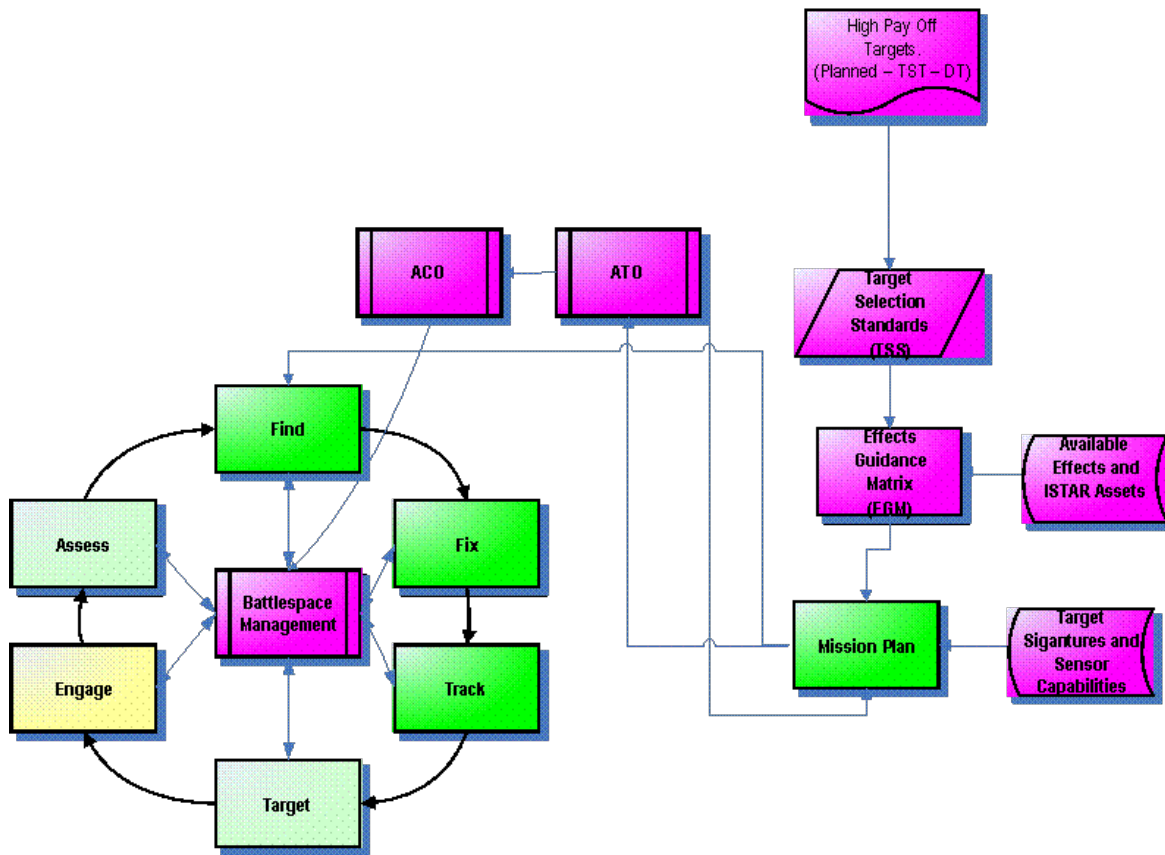


Figure 2 : Expanded F2T2EA Enterprise component model

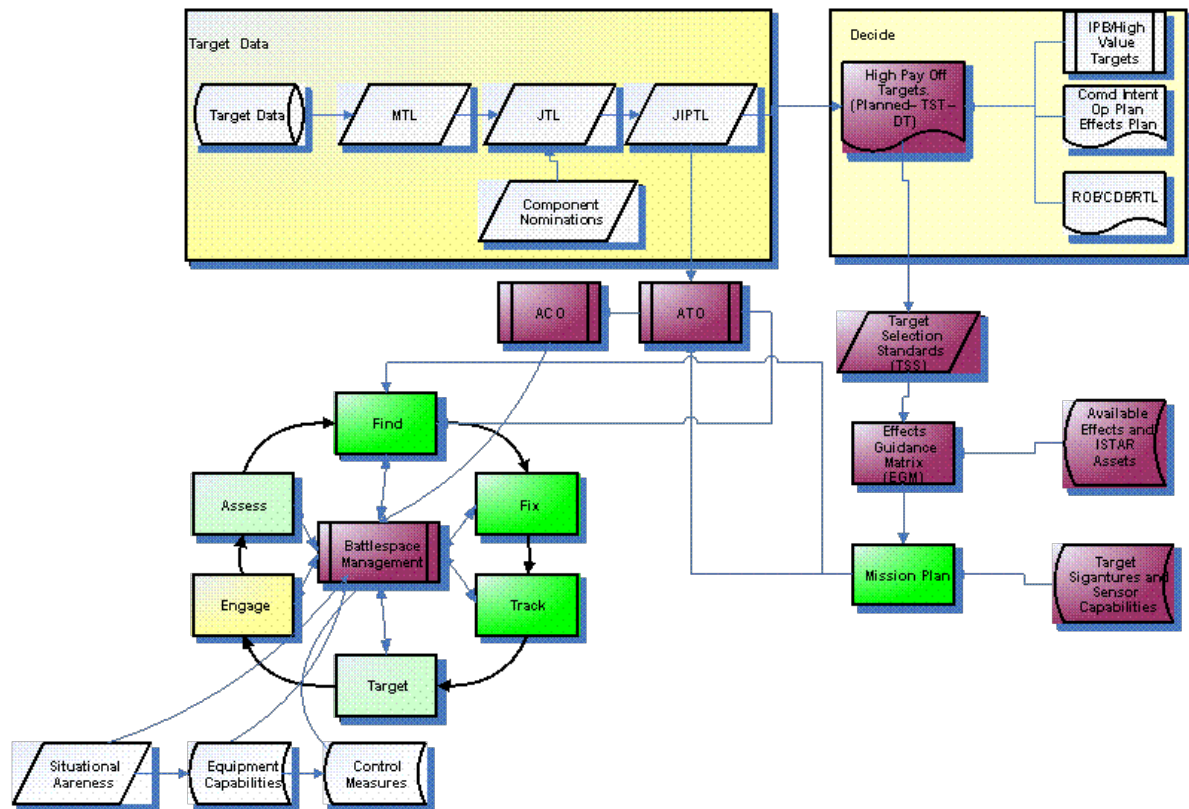


Figure 3 : Full F2T2EA Enterprise model

As can be seen from the complexity of this model, the origin of hazards and accident sequence are not trivial assessments. However, in this whole enterprise the accident event itself can only really impact assets in one small node – the Engage node. Yes, there are physical hazards of handling and using the associated equipment throughout the enterprise chain, but the high-severity consequential accident outcomes can only occur in the battelspace, outside the enterprise boundary, through the Engage node.

Key domains for risk in NE3S

In this specific NE3 system the military requirement was to prosecute targets in a more timely manner. The whole network described above was given the task to identify two key data items to be able to do this: target location and target description – both to a fidelity that produces information above a pre-defined engagement quality metric. Previous work [5] has proposed key NEC hazards based on deliberate firing on non-enemy entities that could result in two accident outcomes of fratricide and ‘neutricide’. The following matrix describes how each of the two key data items of the NE3 system under consideration can produce the key hazards and progress to the accident events.

		Target type	
		Correct	Incorrect (Key Hazard 1)
Target Location	Correct	Target is prosecuted in the correct military manner	Target is prosecuted but effectiveness of action may not be complete
	Incorrect (Key Hazard 2)	No military target is prosecuted – potential for fratricide and neutricide	No military target is prosecuted – potential for fratricide and neutricide

Table 1: Potential outcomes when key hazards are manifested

Deriving an NE3S risk tolerability matrix

Within the MOD, the key policy requirement is that safety will be, so far as is reasonably practicable, at least as good as that required by statute i.e. MOD should aim to be as safe as an equivalent civil organisation. As a result, tolerability criteria should be initially based on appropriate civil equivalents [6]. Unfortunately, there are no civil equivalents to network-enabled enterprise emergent systems, so a more system agnostic derivation methodology has to be used. One such method is described in [7] and starts with the construction of the risk axes of severity and likelihood.

For severity, four categories have been chosen, this is seen as good practice and is familiar to many safety and some non-safety personnel. Table 2 gives the definitions used in this case;

SEVERITY CATEGORY	INTERPRETATION
Catastrophic	Multiple deaths.
Critical	Single death and/or multiple severe injuries or occupational illness.
Major	Single severe injury or occupational illness and/or multiple minor injuries or occupational illness.
Minor	At most a single, a minor injury or minor occupational illness.

Table 2: Severity category descriptions

For likelihood, six categories have been chosen (this is primarily due to limitations in the MoD preferred tool for hazard listing – CASSANDRA, which has six as the maximum number of categories for this property). In this case, it has been decided that qualitative labels for the different categories are not necessary, and a quantitative description has been used based on number of days as units. This is not necessarily correct for every system, but for an NE3 system that is probably going to see regular daily use, it does appear appropriate in this case. Table 3 gives the definitions used.

FREQUENCY CATEGORY	INTERPRETATION
Most frequent	Event greater than every day
	Event between 1 and 10 days
	Event between 10 and 100 days
	Event between 100 and 1000 days
	Event between 1000 and 10,000 days
Least frequent	Event less than 1 per 10,000 days

Table 3: Frequency category descriptions

The next step in the methodology [7] is to populate the risk tolerability matrix with these two axes set against each other. The first aspect of this is to fix the boundaries where a catastrophic event would be considered intolerable, tolerable and broadly acceptable. A catastrophic event on a daily, weekly or monthly basis ‘feels’ like it should be intolerable in any industry domain. Similarly at the other end of the scale, a catastrophic event beyond the working life of the system under consideration ‘feels’ like it should be OK and broadly acceptable.

NB: The reliance on judgement and feeling of safety specialists is appropriate here as there are no precedents for NE3 systems.

With our frequency scale set (Table 3), the tolerability of a catastrophic event can be described in the tolerability matrix as shown in table 4 below. 10,000 days is around 28 years, 100 days is a few months. In between these two areas is the region of tolerability if it can be shown that the risk may be considered ALARP. This paper is not a discussion on the demonstration of ALARP and readers are referred to [6] for the latest MoD advice. It is entirely deliberate that the familiar four risk classes of ‘A’ to ‘D’ have not been used – three regions are preferred. However, descriptions of tasks and actions for risks in each class can still be specified according to the particular system under analysis. This paper is not a discussion on the actions arising from particular risk classes and readers are referred to [6] for the latest MoD advice.

	CAT	CRIT	MAJ	MIN
Event greater than every day	[Red]	[White]	[White]	[White]
Event between 1 and 10 days				
Event between 10 and 100 days				
Event between 100 and 1000 days	[Yellow]	[White]	[White]	[White]
Event between 1000 and 10,000 days				
Event less than 1 per 10,000 days	[Green]	[White]	[White]	[White]

Table 4: Tolerability of a catastrophic event over a likelihood scale

As the marked graduations on the two axes are both logarithmic, the relative tolerability of the remaining possible risk positions can be filled in. The tolerable region has also been coloured to reflect the relationship to appropriateness of the mitigation measures that might be necessary within that region. The new completed matrix for the whole NE3 system is shown in Table 5 below along with a key.

	CAT	CRIT	MAJ	MIN
Event greater than every day	Red	Red	Red	Yellow
Event between 1 and 10 days	Red	Red	Yellow	Yellow
Event between 10 and 100 days	Red	Yellow	Yellow	Green
Event between 100 and 1000 days	Yellow	Green	Green	Green
Event between 1000 and 10,000 days	Yellow	Green	Green	Green
Event less than 1 per 10,000 days	Green	Green	Green	Green

Key:

SHADE	INTERPRETATION
Red	Intolerable risk
Yellow	Tolerable risk when ALARP
Green	Broadly Acceptable risk when ALARP

Table 5: Risk tolerability matrix for NE3 system

Dynamic temporal risk allocation for NE3S subsystems

Elements of traditional risk allocation are important for NE3 systems, but due to the inherent need for the ability to react to emerging military demands, a more dynamic risk allocation approach is required. This needs to allow for risk portfolios that quickly modify to emerging scenarios and increasing military-constellation make up in the networked domain.

Fixed risk apportionment of a risk budget across the entities that make up an NE3 system, such as described above, is a difficult process to go through, involving multiple analysis steps including event-tree analysis, fault-tree analysis and expert judgement. The determination of key binary characteristics and the yes/no probabilities can be difficult to carry out, explain and provide auditable evidence of suitability and proportionality. The results can sometimes be very sensitive to relatively small changes in probabilities. The main drawback noticed by the authors is that risk apportionment can also become increasingly difficult to justify when new sub-system items or emergent task types are added to the network capability. However, when controlled, risk apportionment can ensure that the risk budget is apportioned in an equitable fashion and providing new item entry is managed, it does ensure that the total risk budget is adhered to. The caution remains that significant re-work can sometimes be required to re-apportion the risk budget when 'n' systems becomes 'n+1' systems in the network capability.

One method of utilising risk allocation that appears to be very suitable to NE3 systems is a concept of dynamic temporal risk allocation, where each item in the system chain receives a fixed equal risk budget of the whole system. It is the number of items influencing the total risk that varies dynamically with time rather than acting together in accumulation. Similar concepts have been used in other research domains, notably in the predation theory on prey animals [8], risk management in economic markets [9] and in the more closely related field of information security [10], where risks are judged to be in a state of flux in a dynamic environment.

This risk allocation concept is justified in the military domain in that any specific military NE3 system will have 'n' items in its chain – our example model above has around 25, but only 10 or so can influence any specific risk or accident sequence at any one time. The particular set of the 10 items of the '25' will vary with time as military demand and task-types vary over that time period – it will not always be the same 10, but it will always around 10 from the whole 'n'; most often it may be judged that it may even be somewhat less.

The key part of the argument is linked to the concept time at risk, but viewed from the risk sources. The concept is that a valuable asset (human, aircraft, and/or environment) cannot be exposed to risk from more than (say) 10 accumulated sources at the same time – it just isn't temporally possible. However, over time, as time dynamically changes from one time-unit to the next, the make up of the sources of risk does vary, but it is never significantly more than 10 and most often several less than 10.

When a new item is added to the networked system it brings with it some residual risk and its insertion into the chain brings another risk source to the system. However, the overall risk remains broadly the same because the new source cannot bring a new temporal unit of risk exposure – it has to replace some other item’s temporal unit.

So the risk exposure is dynamically allocated and re-allocated amongst the system entities depending on the function in hand. So if each system entity is allocated a conservative budget of for example, one order lower than the total, the whole product should always remain below the boundary threshold.

Applying this risk allocation concept to each of the system components of the NE3 system provides a new component risk tolerability matrix. The application has been carried out in this case by re-aligning the vertical frequency axis.

	CAT	CRIT	MAJ	MIN
Event greater than every 10 days	Red	Red	Red	Yellow
Event between 10 and 100 days	Red	Yellow	Yellow	Green
Event between 100 and 1000 days	Yellow	Green	Green	Green
Event between 1000 and 10,000 days	Green	Green	Green	Green
Event between 10,000 and 100,000 days	Green	Green	Green	Green
Event less than 1 per 100,000 days	Green	Green	Green	Green

Learning opportunities

It is already critical that SMEs are involved in the identification of hazards during the development of any safety case, however in the case of an enterprise case SMEs are required from a wide variety of interdependent disciplines and for considerably longer than the current involvement on traditional safety cases, however if we are to ensure that the safety cases truly reflect the hazards and potential accidents then this commitment must be met. It should deliver benefits in the longer term.

The enterprise also has benefits for the consideration of environmental issues as consideration of the entire process may very well lead to the enterprise being conducted in a more efficient manner thereby giving the possibility that the environmental impact of the enterprise may become ‘positive’.

The example enterprise model for the F2T2EA ‘kill-chain’ should be used as a serious starting point for constructing a full case for safety in the military enterprise domain.

The defence industry must start to develop and define enterprise safety cases for its major networked enabled, emerging systems. A methodology for doing this has been put forward in this paper along with an explicit example of how that has been done on a real acquisition programme. This methodology allows specific applications within constellations to establish their own safety boundaries, their own targets and their own tolerability criteria, whilst still remaining within the whole enterprise’s safety budget. It also allows demonstration of appropriateness and an auditable trail of evidence when making a case for safety.

References

- [1] Ministry of Defence, “Progress in Combat Identification.”, Report by the controller and auditor general, HC936 Session 2005-2006, Section 4. The Stationery Office, London, 3rd March 2006.
- [2] P. Houghton, “Potential System Vulnerabilities of a Network Enabled Force.”, Dstl, Ministry of Defence, 2004.
- [3] P. Caseley, D. Dean, J. Gadsden, P. Houghton, “Concepts of Network Enabled Capability - safety issues and potential solutions”, Dstl, Ministry of Defence; 2007.

- [4] Joint Service Publication JSP777, "Networked Enabled Capability" Edn1, 01/2005.
- [5] MSN Encarta On-line dictionary, Microsoft Corporation, 2007.
- [6] Defence Standard 00-56 issue 4 "Safety Management requirements for defence systems", Ministry of Defence, June 2007.
- [7] R. Maguire, "Safety Cases and Safety Report - Meaning, Motivation and Management", Ashgate Publishing, 2006
- [8] Maud C. O. Ferrari*, Alix C. Rive†, Camille J. MacNaughton†, Grant E. Brown† & Douglas P. Chivers* "Fixed vs. Random Temporal Predictability of Predation Risk: An Extension of the Risk Allocation Hypothesis", *Ethology* Vol. 114 Issue 3, 2008.
* Department of Biology, University of Saskatchewan, SK, Canada
† Department of Biology, Concordia University, QC, Canada
- [9] Janne Kettunen*, Ahti Salo*, Derek W. Bunn†, "Dynamic Risk Management of Electricity Contracts with Contingent Portfolio Programming", *Management Science* Vol. 21, 2001.
*Systems Analysis Laboratory, Helsinki University of Technology, P.O. Box 1100, 02015 TKK, Finland,
†London Business School, Regent's Park, London NW1 4SA, UK
- [10] G. Dhillon & S. Mishra, "The impact of the Sarbanes-Oxley (SOX) Act on Information Security Governance", Virginia Commonwealth University, USA, 2006.