12TH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM

ADAPTING C2 TO THE 21ST CENTURY

On Regarding 21st Century C2 Systems and their Users as Fallible ePartners

Topics: C2 Concepts, Theory & Policy; Cognitive & Social issues; C2 Technologies & Systems

Tim Grant *, Paul van Fenema *, Maarten van Veen *, & Mark Neerincx †

POC: Tim Grant *
* Netherlands Defence Academy
P.O. Box 90.002, 4800 PA Breda, The Netherlands
Tel: +31 76 527 3261 / Fax: +31 76 527 3259
tj.grant@nlda.nl

† TNO Human Factors, P.O. Box 23, 3769 ZG Soesterberg, The Netherlands

On Regarding 21st Century C2 Systems and their Users as Fallible ePartners

Topics: C2 Concepts, Theory & Policy; Cognitive & Social issues; C2 Technologies & Systems

Tim Grant *, Paul van Fenema *, Maarten van Veen *, & Mark Neerincx †

POC: Tim Grant *
* Netherlands Defence Academy
P.O. Box 90.002, 4800 PA Breda, The Netherlands
Tel: +31 76 527 3261 / Fax: +31 76 527 3259
tj.grant@nlda.nl

† TNO Human Factors, P.O. Box 23, 3769 ZG Soesterberg, The Netherlands

Abstract

The first two tenets of Network Centric Warfare (NCW) state that a robustly networked force improves information sharing, and that information sharing and collaboration lead to shared situation awareness. There is a potential danger lurking in these two tenets, namely that the information being shared may be erroneous, so that the very advantages claimed by NCW could also be its downfall.

There are limits to what can be done to eliminate errors. Firstly, errors arise from the unavoidable uncertainty and complexity in the environment. Secondly, man-made artefacts are failure-prone. Command and Control (C2) systems and telecommunications networks are no exception. Thirdly, humans make slips and mistakes. That applies equally well to the opponent as to one's own forces, including the users of C2 systems. Finally, networks differ in their propensity to propagate errors.

Users are trained to regard C2 systems with a healthy scepticism. Since users are also fallible, C2 systems should be designed to regard their human users with an equally healthy scepticism. C2 systems and their users should be viewed as electronic partners (*ePartners*), and in particular as *fallible ePartners*. This paper proposes a suitable programme of research, experimentation, and development.

1. Introduction

1.1 Motivation

Flight operations on aircraft carriers have been described (Rochlin, et al, 1987, p.87) as follows:

> "… imagine that it's a busy day, and you shrink San Francisco Airport to only one short runway and one ramp and one gate. Make planes take off and land at the same time, at half the present time interval, rock the runway from side to side, and require that everyone who leaves in the morning return the same day. Make sure the equipment is so close to the edge of the envelope that it's fragile. Then turn off the radar to avoid detection, impose strict

controls on radios, fuel the aircraft in place with their engines running, put an enemy in the air, and scatter live bombs and rockets around. Now wet the whole thing down with sea water and oil, and man it with 20-year-olds, half of whom have never seen an airplane close-up. Oh and by the way, try not to kill anyone."

The reader immediately asks him/herself: "Don't they make mistakes in such a demanding environment? And, if they do, aren't the results disastrous?" The answers, of course, are "Yes, they do" and "Yes, they are". However, accidents happen less often than one might expect (Weick & Roberts, 1993). Successful organizations operating in such environments have been termed *high reliability organizations* (HROs). HROs recognise that human variability is a force to harness in averting errors. They work hard to focus that variability and are constantly preoccupied with the possibility of failure (Reason, 2000). They spend time and effort organizing themselves for controlled information processing, mindful attention, and heedful action. In this paper we ask ourselves how we can apply the same attitudes to 21st century C2 systems.

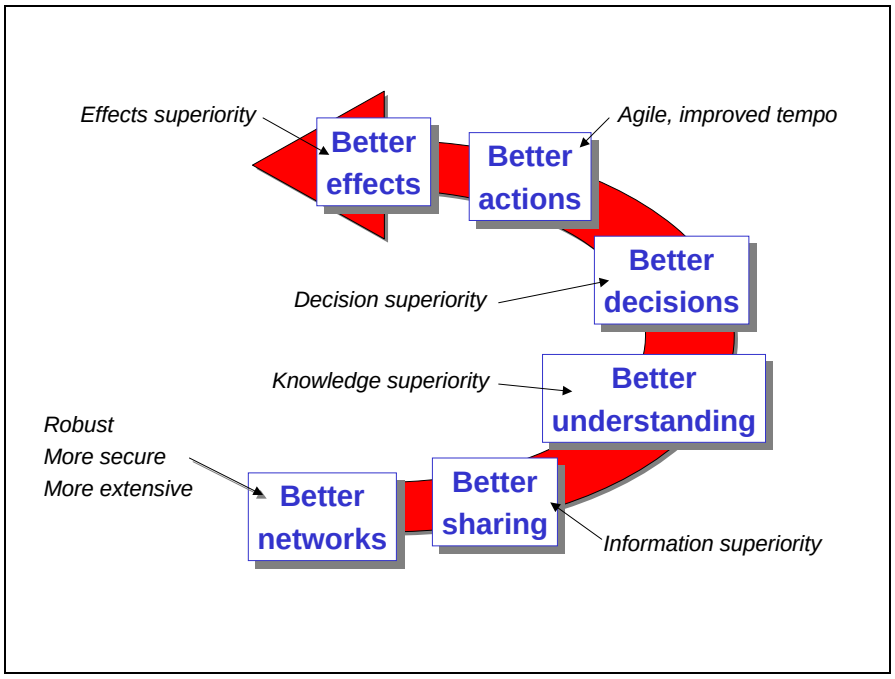

Figure 1. NCW value chain.

The NCW literature claims that (Alberts, et al, 1999):

- A robustly networked force improves information sharing.
- Information sharing enhances the quality of shared situation awareness.
- Shared situation awareness enables collaboration and self-synchronisation, and enhances sustainability and speed of command.
- These in turn dramatically increase mission effectiveness.

These claims are known as the *NCW tenets* or the *NCW value chain* (Figure 1).

The potential danger that the authors of this paper see lurking in the first two tenets is that the information being shared can be erroneous. If so, then the advantages claimed by NCW could also turn out to be its downfall. The speed of information processing that the networks make possible would enable the erroneous information to spread quickly and to be incorporated in the situation awareness shared by many teams and units. In short, erroneous information may behave in a network like a computer virus.

This paper shows that there are limits to what can be done to eliminate errors. Firstly, errors arise unavoidably from the uncertainty and complexity in the environment. Indeed, on the battlefield human opponents deliberately try to deceive one another. Secondly, man-made artefacts are failure-prone. C2 systems and telecommunications networks are no exception. Thirdly, humans make slips and mistakes. That applies equally well to the opponent as to one's own forces. It applies too to the users of C2 systems, i.e., the command staff. Finally, networks differ in their propensity to propagate errors.

If errors cannot be eliminated, then C2 systems must be designed to cope with errors. No part of the system can be guaranteed to be fault-free. We shall say that all parts – including human users – are potentially *fallible*.

Users are trained to regard C2 systems with a healthy scepticism. Since users are also fallible, we argue that C2 systems should be designed to regard their human users with an equally healthy scepticism. This approach extends the NCW principle of "power to the edge" to the relationship between a C2 system and its users. In short, C2 systems and their users should be viewed as *ePartners* (Neerincx, 2003), and in particular as *fallible ePartners*. The art comes in applying this viewpoint not just to reducing the frequency and magnitude of one's own errors, but also to increasing the frequency and magnitude of the enemy's errors. This paper proposes a suitable research programme, based on lessons from the aviation and petrochemical industries, and from manned space-flight.

1.2 Purpose & scope

The purpose of this paper is to propose a research programme into the relationship between 21st century C2 systems and their human and machine users, given that both C2 systems and users are fallible. The research should be aimed both at reducing one's own errors and at increasing the enemy's errors. The proposed research programme takes the approach that C2 systems and their users can be fruitfully regarded as ePartners. The programme is based on lessons from the aviation and petrochemical industries, and from manned space-flight.

This paper consists of six chapters. Chapter 1 is introductory. Chapter 2 reviews the relevant research on information-age C2 processes and 21st century C2 systems from the NCW / Network-Enabled Capabilities (NEC) literature. Chapter 3 identifies the causes of failure and error in C2 systems, examines how errors propagate, how errors may be managed, and reviews the lessons learned in other technology-oriented application areas. Chapter 4 describes the ePartner approach, advocates its extension to fallible ePartners, and identifies the corresponding functionality needed in 21st century C2 systems. Chapter 5 proposes a suitable programme of research and experimentation. Chapter 6 draws conclusions and makes recommendations.

1.3 Definitions

The definitions used in this paper are:

- *Command & Control*. Command & Control (C2) is defined as: "the exercise of authority over and direction of assigned forces in the accomplishment of a mission". C2 processes designed for NCW will be known as *information-age C2*.
- *C2 system*. A C2 system is defined as: "an assembly of equipment, methods and procedures and, if necessary, personnel, that enables commanders and their staffs to exercise command and

control" (North Atlantic Treaty Organisation (NATO), 2007). Note that this definition includes users (personnel) as a part of the C2 system. A C2 system that supports information-age C2 processes using robust networking will be known as a *21st century C2 system*.

- *Failure*. Failure is the inability of a device or system to perform its specified function under specified operational conditions. Note that failures occur in the physical domain, while the fault – the root cause of the failure - is in the physical or information domains.
- *Error*. An error is a human action that is not appropriate to the environment and/or to the human's goals. Note that the erroneous action may be in the physical or information domains, while the root cause is in the cognitive or social domains.
- *Fallibility*. Fallibility is defined as the state of being prone to failure and/or error.
- *ePartner*. An ePartner is a computer system that maintains a model of the task demands on its human users based on knowledge of their characteristics and state and that uses the model to prevent or diminish undesirable effects of its human users' operations in critical situations. In this paper we are concerned with the ePartner's ability to detect and correct or mitigate its human users' errors.
- *Cognitive engineering*. Cognitive engineering is a methodology for designing complex adaptive computer-based systems based on theoretical and empirical knowledge about human-machine partnerships.
- *Sensemaking*. Sensemaking is defined as the process of making sense of a situation that is novel to that agent. This definition is an adaptation of Weick's (1995) definition to allow for the unequal distribution of knowledge over a group of agents.
- *Trust*. Trust is defined as "an agent's state in which the agent is willing to act on the basis of another agent's recommendations, actions, and decisions in situations entailing risk". This definition combines Boon and Holmes' (1991) definition of interpersonal trust with Madsen and Gregor's (2000) definition of trust in a decision aid.

2. 21st Century C2 Systems

The purpose of this chapter is to review the relevant research on information-age C2 processes and systems from the NCW literature. We contrast traditional ("industrial-age") C2 with information-age C2 processes. The required information-age C2 process model must support both task and team processes. Then we highlight some features of a 21st century C2 system, making a key distinction between human-human and human-machine collaboration.

2.1 Information-age C2

Traditional C2 is rooted in rational decision-making and decision theory (Raiffa, 1968). A rational decision maker is one who seeks to choose the best immediate outcome to a problem. In other words, the decision maker is an optimiser. Moreover, he/she does not take into account the influence of previous problems on the current problem he/she faces, nor the influence of his/her choice on possible future problems. The option selection process is central to rational decision-making, involving the enumeration of options, their scoring against a set of attributes, and the selection of the option with the highest value based on these scores. We see this option selection process in the NATO-standard operational planning process, and the optimising nature of traditional C2 is identified in the NCW literature (Alberts & Hayes, 2003, chapter 3). The advantage of rational decision-making is that it has been proven optimal, but it has the associated disadvantages that it requires complete and perfect information and the absence of time pressure.

Organizational decomposition forms a second root to traditional C2, enabling it to cope with complexity. Military forces are decomposed into smaller subordinate units and into

specialised disciplines. Each subordinate unit and specialization has a smaller geographical or functional area of responsibility, simplifying its problem. Recursive decomposition results in organizational hierarchies. Decomposition, specialization, hierarchies, and deconfliction have also been identified in the NCW literature (Ibid, chapter 3) as characteristics of traditional C2. The advantage of organizational decomposition is that it is an idea that is simple to implement in a wide variety of situations. Its disadvantage lies in the assumption that complex problems are separable into sub-problems, bringing with it the danger of sub-optimisation.

Restricted communication has also shaped traditional C2. The restrictions have been primarily technological, mainly in limiting speed, reliability, and bandwidth. Many communications technologies restrict connectivity in that they are inherently point-to-point (e.g., pigeon post, couriers, signalling lamps, telephone lines, telex, fax). Security considerations have also played an important role in restricting communication by means of security labelling schemes and the "need-to-know" principle. Mechanisms that have been developed to cope with restricted communications include standardized symbols and jargon, doctrine and Standard Operating Procedures (SOPs), centralized planning and control, and the "reporting chain". Standardized symbols and jargon compress complex ideas, minimizing the amount of information that needs to be transmitted to express those ideas. Similarly, doctrine and SOPs are ways of codifying complex sequences of action in a compressed form. Centralizing planning and control takes advantage of the organizational hierarchy to reduce the number of places that information has to be transmitted to (and from). The "reporting chain", in which communications are constrained to move primarily up and down the hierarchy, reduces the number of communication links that have to be implemented. It also has the advantage that the flow of information can be controlled. Disadvantages are that standardized symbols, jargon, doctrine, and SOPs have to be learned. Across-hierarchy communications are often regarded as informal and are consequently poorly supported.

Command in the information age is shared, distributed, and collaborative (Alberts & Hayes, 2003). It involves:

- Defining the mission in terms of command intent by selecting the vision, developing the objectives, and setting priorities.
- Assigning resources.
- Scoping the solution by establishing the constraints and defining the rules of engagement.

Information-age control is keeping a situation within bounds while accomplishing the objectives (Ibid). This is satisficing behaviour, rather than optimisation. Control is achieved indirectly by setting initial conditions that will result in the desired behaviour. Controllers monitor the situation, adjust the initial conditions when necessary, and ensure others share their perceptions.

The technological enablers of information-age C2 are (Ibid):

- A robustly networked force.
- Information dissemination by *push and smart pull*.
- *Sensemaking*, in the sense of "putting the available information about the situation into context and identifying the relevant patterns that exist [so as to develop] situation awareness …" (ibid., p.101). Note that, unlike in Weick (1995), this definition assumes the pre-existence of the patterns.
- *Interoperability*, i.e., the ability to work together in all four domains (Alberts & Hayes, 2003, p.107-8).

- A focus on *agility*, i.e., the ability to move rapidly but sure-footedly. Six dimensions of agility are (ibid., p.128):
  - *Robustness*: the ability to maintain effectiveness across a range of tasks, situations, and conditions.
  - *Resilience*: the ability to recover from or adjust to misfortune, damage, or a destabilizing perturbation in the environment.
  - *Responsiveness*: the ability to react to a change in the environment in a timely manner.
  - *Flexibility*: the ability to employ multiple ways to succeed and the capacity to move seamlessly between them.
  - *Innovation*: the ability to do new things and the ability to do old things in new ways.
  - *Adaptation*: the ability to change work processes and the ability to change the organization.
- An edge organization, i.e., one in which authority is decentralized.

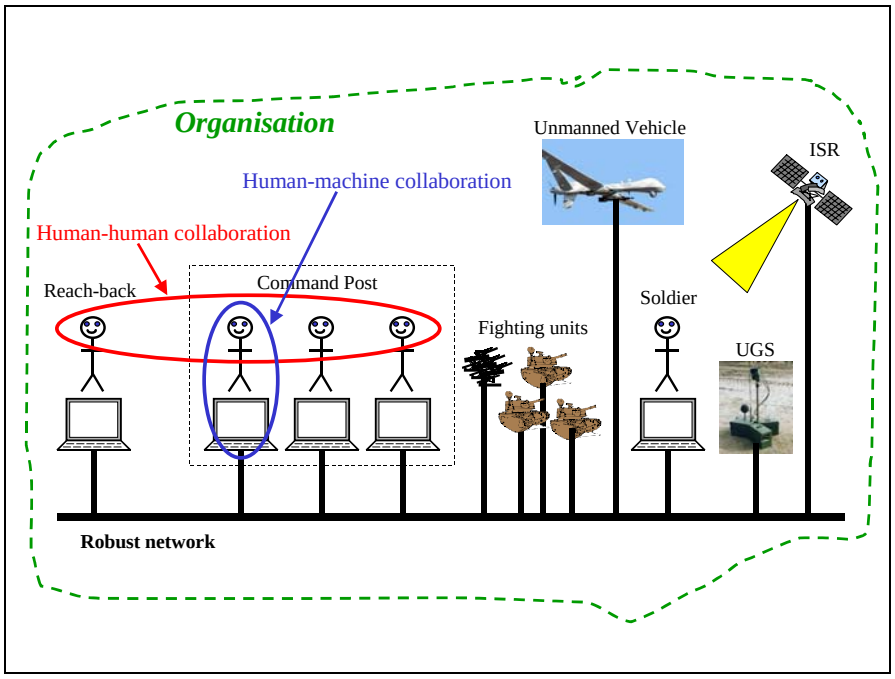

Figure 2. Example 21st century C2 system.

2.2 Features of 21st century C2 systems

In 21st century C2 systems, all individual soldiers, fighting units, unmanned vehicles, unmanned sensors, intelligence and surveillance assets, command posts, and out-of-theatre assets are nodes in a robust network; see Figure 2. All information developed by these nodes is published on the network ("post" or "push"), from where it can be discovered and retrieved by other nodes ("smart pull"). The network and nodes are embedded in a military organization, which may be a single service, a joint task force, or a multi-national coalition, possibly including civilian partners such as the emergency services, international organizations (e.g., the United Nations), non-governmental organisations (NGOs), and/or the media.

The network underlying a 21st century C2 system enables the human users to collaborate with one another in real time, e.g., to share information, to build situation awareness, to plan, and to develop command intent. This is shown in Figure 2 as "human-human collaboration" (HHC). If necessary, HHC enables collaboration across levels in the organizational hierarchy. HHC is well covered in the NCW literature. By contrast, the changing relationship between

human users and their workstations in a 21st century C2 system - shown as "human-machine collaboration" (HMC) – has received almost no attention in the literature.

The starting point for specifying, designing and implementing a 21st century C2 system is a process model for information-age C2. Such a model must represent collaboration, as well as the C2 process.

Many models of the C2 process can be found in the military, cybernetics, and psychological literatures. Boyd's (1996) Observe-Orient-Decide-Act (OODA) process model can be regarded as the *de facto* military standard. However, OODA is known to have shortcomings. Although it has been also criticized in the NCW literature for its cyclical nature (Alberts & Hayes, 2003, p.49), OODA can be readily viewed as a set of concurrent processes (Grant & Kooter, 2005). OODA lacks planning and learning processes, because it was based on the situational thinking processes of fighter pilots (Brehmer, 2005), and it lacks psychological validity (Dehn, 2004). Crucially, OODA is based on the task-oriented thinking of an individual, and hence omits team-oriented processes such as information distribution, shared awareness, team assessment, task allocation and balancing, and confirmation and authorisation of orders (Keus, 2002).

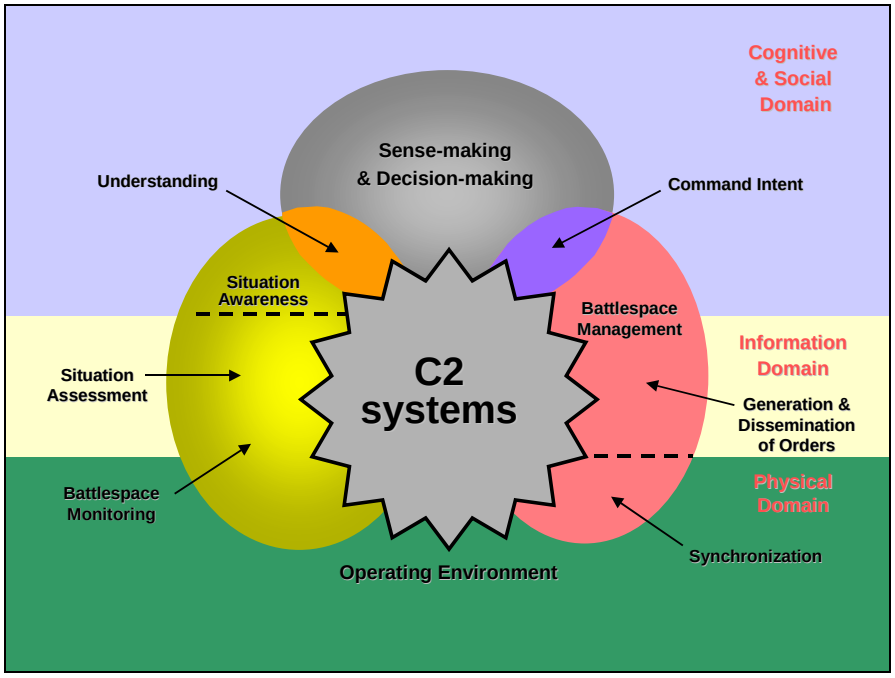

Figure 3. C2 systems embedded in network-centric C2 process.

In an attempt to refine OODA, Grant and Kooter (2005) surveyed five process models in the scientific literature, comparing them to OODA, and thereby identifying OODA's shortcomings. Independently, Brehmer (2005) developed a list of OODA's shortcomings when compared to cybernetic models of control. The two lists overlap extensively. Based on this list of shortcomings, Grant (2005b) rationally reconstructured Boyd's (1996) OODA model to serve as a 21st century C2 system architecture. He rectified the shortcomings, in particular adding processes for planning and learning[1]. The resulting rationally-

[1] Termed Sensemaking, in the Weick (1995) sense.

reconstructured OODA (OODA-RR) model was validated against a set of use-cases. Although an OODA-RR test-bed has been specified, it has not yet been implemented.

The NCW literature offers a model of C2 systems embedded in the information-age C2 process; see Figure 3. The value of this model is that it introduces the physical, information, cognitive, and social domains. Moreover, it shows how C2 systems bridge these domains. However, as regards the underlying C2 process it does not go substantially further than OODA, in that Battlespace Monitoring can be mapped to Observe, Situation Assessment and Understanding to Orient, Sense-making and Decision-making to Decide, and Battlespace Management and Synchronization to Act. As in OODA, collaboration is not represented.
Since the turn of the 21st century, various authors have proposed models of collaborative C2 processes. Keus (2002) proposed an extension of Boyd's OODA model to cooperative teams, adding Information distribution, Shared awareness, Decision confirmation and authorisation, Team assessment, and Task allocation and balancing processes.

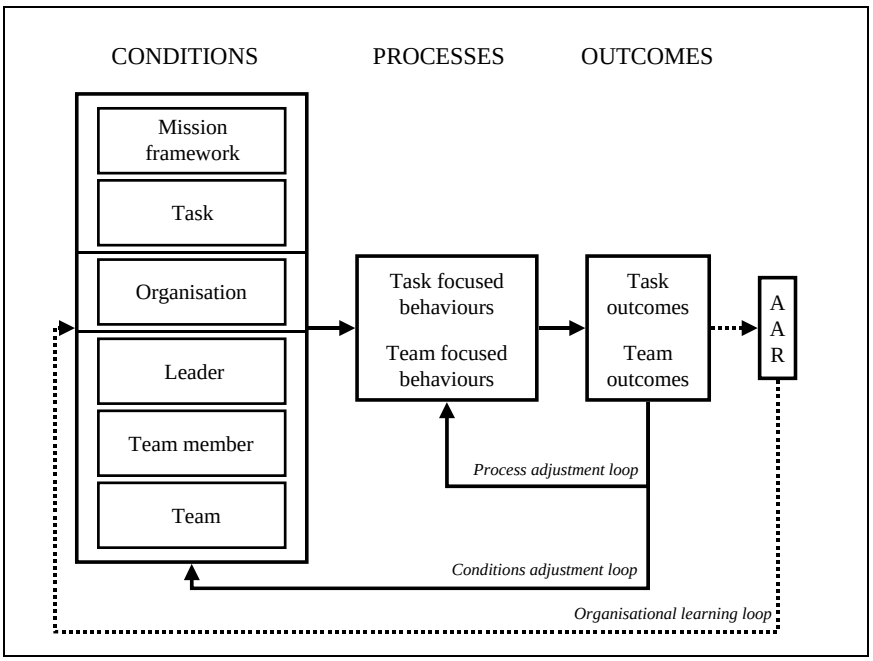

Figure 4. Command Team Effectiveness model (Essens, et al, 2005).

Within the NATO Research & Technology Organization, Task Group 023 on Team Effectiveness reviewed eight team effectiveness models drawn from the psychological literature (Essens, et al, 2005). These models serve as the basis for the development of the Command Team Effectiveness (CTEF) model and instrument. CTEF is divided into inputs ("Conditions"), Processes, and outputs ("Outcomes"); see Figure 4. The Processes include both task- and team-focused behaviours. The task-focused behaviours are Managing information, Making decisions, Planning, Directing and controlling, and Liaising with other command teams. The team-focused behaviours are Providing and maintaining vision, Maintaining common intent, Interacting within the team, Motivating, Adapting, and Providing team maintenance. Each behaviour is defined, and most are detailed into sub-behaviours. Notably, CTEF also includes three feedback loops to model Process-, Condition-, and organizational-learning. We consider CTEF worthy of further investigation as a starting point for specifying, designing, and implementing a 21st century C2 system, and subsequently for educating and training prospective users.

3. Fallibility of C2 Systems

The purpose of this chapter is to show that all parts of C2 systems are fallible. Device failure and human error are unavoidable, and contribute to the fog and friction of war. Much of the knowledge available comes from other technology-oriented application areas, particularly aviation, medicine, the petrochemical industry, and manned space-flight. We start by examining the sources of failure and error. Failures occur in the physical domain, in the environment, in platforms, and in the network itself. Errors occur in the information, cognitive and social domains, notably in the users' minds and in the organization in which the C2 system is embedded. Next we turn our attention to how errors may propagate in networks. Then we look at ways of avoiding, mitigating and managing errors.

3.1 Environmental complexity & uncertainty

Complex, real-world environments such as fire-fighting, crisis response, and military operations have the following characteristics (Klein & Klinger, 1991):

- The goals and tasks are ill-defined, can change over time, and may compete with one another.
- The conditions are dynamic and continually changing. There are multiple players.
- There is a closed loop between actions and feedback. Changing conditions require real-time reaction, but information is uncertain, ambiguous, and incomplete.
- Decision makers are under time stress, and the stakes are high.
- Decision makers are experts and form part of an organisation with goals and norms.

Keen and Scott-Morton (1978) distinguish structured, semi-structured, and unstructured working environments. A structured environment is one for which complete models are known that predict correctly and exactly how the environment will behave. Control laws can be generated mathematically from these models, enabling structured environments to be controlled automatically. Unstructured environments are those for which no models are known. Human judgement and intuition is needed to control them. In semi-structured environments, neither human nor computer alone is effective; both are needed.

Under Keen and Scott-Morton's (1978) scheme, military operations take place in environments that are semi-structured at best, and much more often unstructured. This means that it is not just a matter of "putting the available information about the situation into context and identifying the relevant patterns that exist [so as to develop] situation awareness …" (Alberts & Hayes, 2003, p.101). There may be no known models – no pre-existing patterns - for the behaviour of the environment. This was the case in 9/11 and in Somalia in 1993. Collecting intelligence or sensory information is a proven way of reducing uncertainty about the state of the environment. By contrast, reducing uncertainty about the behaviour of the environment calls for a learning process: sense-making in the Weickian sense (Weick, 1995).

Environmental complexity may be still worse. There are environments in which the solution of a problem may reveal or create another (possibly even more) complex problem. This is one characteristic of a wicked problem (Rittel & Webber, 1973). Wicked problems "have incomplete, contradictory, and changing requirements; and solutions to them are often difficult to recognize as such because of complex interdependencies" (Wikipedia, 2007). Classic examples of wicked problems include economic, environmental, and political issues. Problems whose solution require large groups of individuals to change their mindsets and behaviours are likely to be wicked problems. The current situation in Iraq may be viewed as a

wicked problem. Morphological analysis, system dynamics, and systems thinking are often applied to better understand wicked problems.

3.2 Platform & system failures

Man-made devices are prone to failure. The failure rate may be very low, but it is non-zero. 21st century C2 systems can be affected by failure in two ways:

- *Platform failure*. Devices outside the C2 system boundary that input information to or act on instructions from the C2 system can fail. Typically, these devices are military units or platforms, such as manned or unmanned aircraft, ships, vehicles, sensors, or weapons. Failure may occur in hardware or in software.
- *System failure*. Component parts of the C2 system can fail. This can affect the hardware or software in C2 workstations or in the connecting network(s).

The operational effect of failure varies both with the failure mode and with the operational situation. Some failures have no operational effect. For example, a valve jammed open in a fuel pipeline does not affect the delivery of fuel. If the valve were jammed shut, it would have no operational effect if no vehicle needed fuel for the duration of the operation. Other failures have only a limited operational effect. For example, a valve jammed shut would have a limited effect if it was one of three outlets, and the other two were serviceable. The resulting operational effect would just be a reduction in refuelling capacity. By contrast, if there were just one outlet, then the resulting total loss of in-theatre fuel supplies would have a disastrous effect on operations, especially if it took a long time to repair. In general, operational effect can be minimised by providing redundancy or functional / technological diversity. However, it cannot be eliminated entirely.

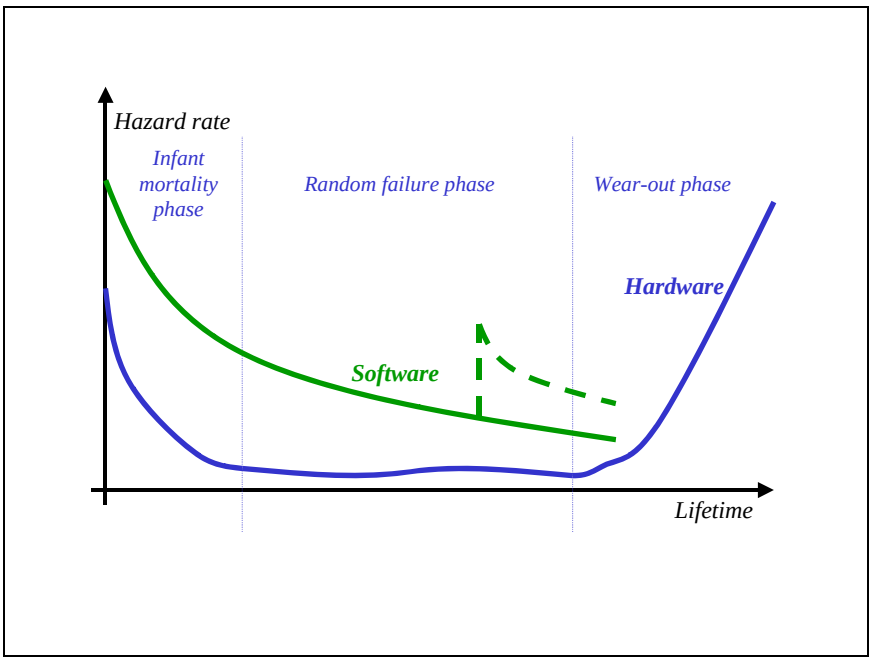

Figure 5. Instantaneous failure rate: hardware and software.

Hardware and software failures have different characteristics. Figure 5 depicts the change in the instantaneous failure rate (hazard rate) over the lifetime of a typical device, assuming it is used within its specifications. Hardware is initially unreliable because of design and

manufacturing errors. These problems are encountered and corrected early in the device's lifetime. This is known as the infant mortality phase. After this initial phase, the device reaches its peak reliability, with a relatively constant hazard rate during which components fail randomly. This is known as the random failure phase. As the device approaches the end of its useful life, the hazard rate starts to increase as components begin to wear out. This is known as the wear-out phase. Given its shape, the composite hazard rate for all three phases is often known as the bathtub curve. In practice, most devices exhibit just one of or a combination of two of the three phases.

Software reliability differs considerably from this picture. Software neither fails randomly nor wears out. Manufacturing errors (e.g., faulty copying) are rare and easily detected. The predominant cause of software failure is design error. If software errors are corrected as they are detected, then the software hazard rate has the characteristic of infant mortality alone.
Both curves in Figure 5 assume that no new errors are introduced during maintenance and repair. This assumption is usually invalid. Errors introduced during maintenance and repair – in the medical world known as iatrophic errors – cause an immediate increase in the hazard rate, followed by a renewed infant mortality phase (see dashed line). In hardware devices, iatrophic errors may also hasten the onset of the wear-out phase. If devices are operated outside their specified envelope then the random-failure hazard rate increases. Again, the wear-out phase may be brought forward in hardware devices.

For C2 systems, availability – the proportion of time that the system is in a functioning condition – is more important than reliability. Availability takes into account the speed with which a failed system can be repaired, i.e., its maintainability. Availability is often expressed as "N nines". For example, "three nines" means an availability of 99.9%, and "five nines" means 99.999%. Over (say) one year, "three nines" translates to nearly nine hours downtime. However, C2 system users would not want a C2 system to be non-functional for nine hours at the moment that they were in contact with the enemy. Even five minutes (99.999%) could be unacceptable in certain operational circumstances. Clearly, there is a complex balance between the C2 system's specifications, its design, how it is used, and the repair capabilities.

Reliability, availability, and maintainability (RAM) issues in man-made devices are generally well known. It is for this reason that users have a healthy respect for failures in sensors, C2 systems, and weapons. By contrast, human error in C2 systems is less well known.

3.3 Human user errors

Human error has been extensively studied, particular in relation to purposeful action. Psychologists such as Norman (1981) and Reason (1984a) distinguish two ways in which action can logically fail to achieve its purpose:

- A *mistake* is defined as an error of judgement or inference where the action goes as planned, but where the plan is incorrect. In other words, a mistake is an error made during planning.
- A *slip* is defined as an action that is not in accord with the actor's intention, i.e., the result of a good plan poorly executed. In other words, a slip is an error made at (plan-)execution time.

Norman (1993) observes that the consequences of a mistake are usually more severe than those of a slip. Despite this observation, research in the psychological literature has concentrated on studying erroneous action, i.e., on slips, although Grant (2001) has performed a preliminary set of experiments into erroneous planning.

There are two fundamentally different ways to consider erroneous actions (Hollnagel, 1991):

- One is with regard to their *phenotype*, i.e., how slips appear when expressed as actions. Hollnagel (1991) proposes a taxonomy of phenotypes that takes plan-based action as its starting point.
- The other is with regard to their *genotype*, i.e., the functional characteristics or mechanisms of the human cognitive system that are assumed to be a contributing cause of slips. Rasmussen, et al. (1981) and Reason (1987) propose taxonomies of genotypes.

3.4 Organizational / system errors

Reason (2000) notes that there are two approaches to the problem of human fallibility: the person approach and the system approach. As described in the previous section, the person approach concentrates on errors made by individuals, blaming them for forgetfulness, inattention, moral weakness, etc. In the past decade, research has focussed on the system approach, concentrating on the conditions under which individuals work. System errors include operational and resource constraints, vague policies, culture, groupthink (Janis, 1983), and the normalisation of deviance (Vaughan, 1996).

Errors have the potential to push a collaborative system into a state of organizational drift. In the context of military operations, organizational drift may take the form of "mission creep". At the strategic level, drift has been defined as the situation "where strategies progressively fail to address the strategic position of the organisation and performance deteriorates" (Johnson, et al, 2005, p.27). While this definition applies to strategic negligence, we could also apply this notion to tactical and operational levels. Drifting at these levels would refer to situations where intended courses of action as expressed in tactical concepts or operational routines appear unsuited for the tactical and operational circumstances in which an organization operates. Building on Snook's (2000) work, Wackers and Korte (2001) associate drift with "a gap between 'practice' on one hand and rational representations of policy goals, decision making processes, and technical design features on the other". Snook's theory of practical drift proposes that organizational units modify coordinating plans and procedures thereby deviating increasingly from the rationale behind these mechanisms, "the slow, steady uncoupling of practice from written procedure" (Snook, 2000, p.194). Organizational drifting also occurs when expectations (plans, procedures) themselves concerning a situation are irrelevant, and organization members do not agree on pragmatically improvised alternative courses of action (Weick, 1993).

The deployment of C2 systems in complex environments with high levels of stress makes drifting likely. Therefore, research is needed to investigate how C2 systems could support their users by alerting them to organizational drift and "mission creep" and how C2 system users could be trained to detect and compensate for organizational drift and "mission creep".

3.5 Error propagation

Networks differ in their resilience to failure and in their susceptibility to propagating errors (Newman, 2003) (Ormerod, 2005).

The resilience of networks to the removal of nodes has been widely studied (Newman, 2003, IIID p.15-16 & VIIIA p.38-40). The networks underlying 21st century C2 systems rely for their functioning on their connectivity, i.e., on the existence of paths between pairs of nodes. As nodes are removed from the network, the typical path lengths will increase. However, at some point, node pairs will become disconnected from one another, making communication

between them impossible. In effect, the network has then become a set of (two or more) separate networks.

Resilience to the removal of nodes has been studied in both model and real-world networks. Examples of real-world networks whose resilience has been studied in the literature include the Internet, the World Wide Web, electronic mail networks, food chains, and metabolic networks. Some authors have also studied the removal of connecting links.

A common finding (Newman, 2003) is that networks are robust against the removal of randomly chosen nodes. However, the targeted removal of highly-connected nodes has a devastating effect. This finding has already been militarily exploited. For example, in the 1991 and 2003 Iraq wars the strategic aim of the initial phase of the air war was to destroy the Iraqi C2 capability. This was done by destroying C2 centres and by cutting them off from the forces under their command. In essence, targeting emphasised the nodes with the highest connectivity and the links leading out of such nodes.

The study of the propensity of networks to error propagation is known as the study of epidemiological processes (Newman, 2003, VIIIB p.40-43). The aim of such study is to understand the mechanisms by which things such as diseases, computer viruses, rumours, and information spread over a network. In many applications, research is also aimed at how the spread can be controlled. The simplest model of the spread of disease over a network stems from the 1920s. Known as the Susceptible, Infective, Removed (or Recovered) (SIR) model, it assumes that, after infection, nodes either die or have permanent immunity. Such diseases are termed epidemic. By contrast, the Susceptible, Infective, Susceptible (SIS) model is applicable to endemic diseases, i.e., those that do not confer immunity on survivors. Endemic diseases can persist indefinitely, circulating around the network and never dying out.

The original SIR and SIS models assumed implicitly that the network is fully connected, i.e., that every node is connected to every other node. In practice, this is unrealistic. Extended models representing partly connected networks predict that disease outbreaks will appear in clusters. An important result from Callaway, et al (2000) is that networks with power-law connectivity distributions are highly susceptible to targeted attack; that the network can be destroyed entirely by removing a small percentage of nodes. This result has been extended to directed networks and applied to cascading failures, e.g., in electrical power networks. Several researchers have shown that, in power-law networks, diseases always propagate, regardless of the transmission probability between individuals. Ormerod (2005) has applied the result to the extinction of (commercial) organizations.

The ideas of network resilience and epidemiology are combined in the study of vaccination against the spread of a disease. Vaccination can be modelled as the removal of susceptible nodes. Network theory then suggests that the highest-connected nodes should be targeted for vaccination, and this is already done in the medical world. Difficulties arise when it is difficult to identify the highest-connected nodes. In that case, Cohen, et al (2002) propose choosing a node at random and vaccinating a node to which it is linked, and then repeating the process.

Since the Internet and the World Wide Web have been shown to be distributed according to a power law, it is essential to investigate the connectivity of 21st century C2 systems. The air war strategy used in the 1991and 2003 Iraq wars strongly suggests that existing, industrial-age C2 systems in hierarchical organizations have power-law connectivity, making them

vulnerable to targeting key nodes. Ways of protecting 21st century C2 systems may emerge from the study of vaccination. For example, 21st century C2 systems could be designed so that it is difficult for an enemy to identify highly connected (i.e., valuable) nodes. One idea might be to try connecting all nodes equally.

3.6 Managing error

The system approach to error management tries to build defence-in-depth to avert errors and to mitigate their effects. This is often known as the Swiss cheese model (see Figure 6).

One line of defence is to design out possible sources of failure and error in a C2 system. Military specification and Commercial Off-The-Shelf (COTS) components can be selected to increase reliability. Redundancy and diversity can be provided to allow operations to continue in the presence of component failures. However, as we have seen, failures cannot be eliminated entirely. A second line of defence is to develop doctrine and to train the human users in its use. Doctrine development and training are themselves human processes, and are therefore subject to human error. Moreover, situations occur that are not covered by the available doctrine, and the available training material can lag the latest doctrinal knowledge.

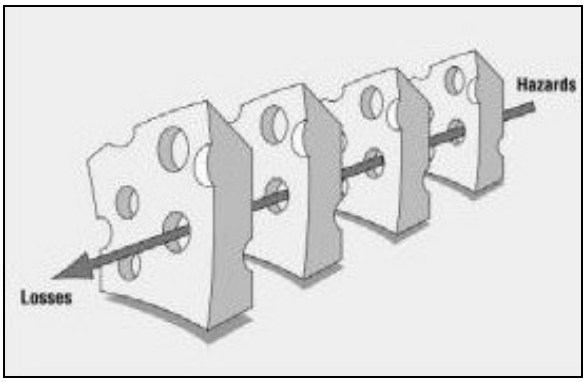

Figure 6. Swiss cheese model of how defences may be penetrated (Reason, 2000).

A third line of defence is attitudinal. We have seen that high reliability organizations operate in very demanding environments and yet manage to have fewer accidents than one might expect. This can be attributed to their mind-set. A key aspect of this mind-set is the realisation that failure and error can be reduced, but not eliminated entirely, differentiating the HRO attitude from initiatives such as ISO 9000 and Six Sigma. Weick and Sutcliffe (2001, p.10-17) have identified the following five hallmarks of HROs:

- *Preoccupation with failure*. HROs treat any lapse as a symptom that something is wrong with the system, something that could have severe consequences if several small errors happened to coincide. HROs encourage (self-)reporting of errors and are wary of the complacency that success engenders. 21st century C2 systems should assist their users by maintaining a database of past errors and warning their users if intended action has been associated with failure in the past.
- *Reluctance to simplify interpretations*. Knowing that the environment they face is complex, dynamic, and unpredictable, HROs foster boundary spanners, scepticism toward received wisdom, and negotiation mechanisms that reconcile differences of opinion without destroying nuances. 21st century C2 systems should help their users by enabling them to regard a complex situation from different viewpoints, even if these are conflicting.
- *Sensitivity to operations*. HROs realise that normal operations may reveal deficiencies that are "free lessons" that signal the development of unexpected events. They are attentive to the front line, where the real work gets done. Anomalies are noticed while they are still tractable and can

be isolated. 21st century C2 systems should support their users by signalling unexpected events and anomalies.

- *Commitment to resilience*. HROs know that no system is perfect. This is why they develop capabilities to detect, contain, and bounce back from the inevitable errors. Resilience is a combination of keeping errors small and of improvising workarounds that keep the system functioning. HROs simulate worst case conditions in an effort to train people with a deep knowledge of the system. 21st century C2 systems should make available alternative courses of action for the current situation, together with a facility to explore their consequences by means of what-if simulation.
- *Deference to expertise*. In HROs authority migrates to people with the most expertise, regardless of their rank or position in the organizational hierarchy. 21st century C2 systems can help their users by maintaining a directory of people by their expertise, as well as a database of previous incidents with links to the people who have contributed to their solution.

In the aviation industry, Crew Resource Management (CRM) is a component of an organization's safety efforts. Helmreich, et al (1999) define CRM as:

> "the utilization of all available human, informational, and equipment resources toward the effective performance of a safe and efficient flight. CRM is an active process by crewmembers to identify significant threats to an operation, communicate them to the PIC [Pilot In Command], and to develop, communicate, and carry out a plan to avoid or mitigate each threat. CRM reflects the application of human factors knowledge to the special case of crews and their interaction" (text in square brackets added).

The parallels between CRM and C2 are obvious. The first sentence is a close analogue to the definition of C2 when "mission" replaces "flight", with the PIC playing an analogous role to the military commander. The second sentence can be easily mapped to OODA-RR (Grant, 2005b): identifying threats is Observe and Orient, developing and communicating a plan are Plan and Decide, and carrying it out is Act. Only Sensemaking is missing.

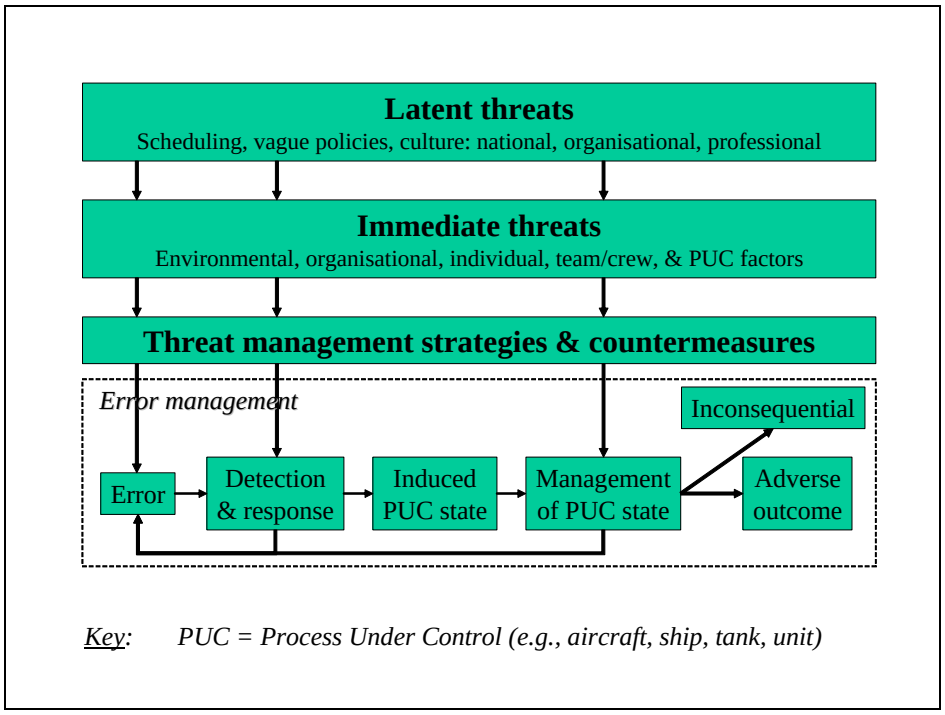

Figure 7. Helmreich's (2000) threat and error management model.

Helmreich's research group at the University of Texas has developed a general model of threat and error management in aviation, based on observing 3500 airline flights in eight flight-safety audits. As shown in Figure 7, the threat and error management model (Helmreich, 2000) shows risk as coming from both latent and immediate threats. In aviation, sources of immediate threat are terrain, weather, malfunctions, unusual commands, external errors, and operational pressure. Latent threats include planning, organizational policies, and national, organizational, and professional culture. Threat management strategies and countermeasures defend against external threats. When threats are countered successfully, this leads to a safe flight. However, the crew's response to a recognized external threat might be erroneous, leading to a cycle of error detection and response. In addition, crews may err in the absence of any external precipitating factor. The main types of error were found to be violation of regulations, procedural errors, poor communication, inadequate proficiency, and bad decision-making.

Helmreich (2000) translates the model of threat and error management successfully to medical error in the operating theatre. He has also translated it to manned space-flight. It would be interesting to investigate whether Helmreich's model could be translated equally successfully to military C2. The analogy seems straightforward, with the sources of threat and types of error in aviation all appearing to have direct counterparts in military operations.

4. Applying ePartner Approach

The purpose of this chapter is to identify the functionality needed in 21st century C2 systems when the components of such systems are regarded as fallible ePartners. We start by reviewing the ePartner concept. Next, we extend the concept to the detection and mitigation of errors. Finally, we identify the functionality needed in a 21st century C2 system to handle fallibility.

4.1 ePartner concept

In the human social domain, partners are comrades or companions who share experiences and carry out activities jointly. Their roles are established, the actions are entrusted to one another, the workload is divided, advice may be given to one another without the other having to ask for it, and the results are mutually satisfying. Their interaction progresses in a natural way. Through sharing experiences, partners come to know each other's qualities and foibles. With this knowledge, each partner can adjust its support for the other to the current situation, anticipate the other partner's needs and behaviour, and detect and correct or mitigate the other partner's errors. A set of partners can be regarded as a Complex Adaptive System (CAS) (Morowitz & Singer, 1995).

By contrast, the relationship between human users and present-day computer systems is – at best – one of supervisor and subordinate[2]. Current C2 systems are a form of human supervisory control (Sheridan, 1992), an outgrowth of automated control in which human users are continually programming and receiving information from a computer system that interconnects to a controlled process or task environment through sensors and effectors. Researchers have recognised that this paradigm limits the assistance that a computer can give

[2] At worst, it is a master-slave relationship. Humans think nothing of making computers wait endlessly or of switching them off without warning. Between humans this would be regarded as bad manners or even as a cause for breaking off the relationship.

its users because it can only do as it is told. Under the heading of adaptive user interfaces (Schneider-Hufschmidt, et al, 1993), they have attempted to develop systems that can adapt the way in which they interact with their human users according to the situation. For example, they could be designed to provide only the information that the human user needs for the current situation. Unfortunately, adaptive user interfaces have failed to result in working real-world applications, largely because of a lack of a theoretical and empirical foundation to the proposed human-machine collaboration.

Neerincx (2003a) argues that developing computer systems that can adapt their user interfaces does not go far enough. Based on current developments in mental state sensing, context sensing, capacity modelling, and multimodal communication, the computer system must become an electronic partner. Such an *ePartner* has knowledge of its human partner with respect to his or her permanent characteristics (e.g., personality), dynamic characteristics (e.g., experience), base-line state (e.g., "normal" heart rate), and momentary state (e.g., current momentary heart rate). Based on this knowledge, the ePartner maintains a model of the task demands that are critical for its human partner, e.g., the risk of its human partner suffering cognitive lock-up in a complex task situation (Neerincx, 2003b). The ePartner will have a repertoire of mitigation strategies to prevent or to diminish negative effects of human operations in such critical situations by taking over tasks, guiding task performance, requesting the assistance of other partners, or subtle actions to keep the human in an adequate mental state (e.g., open-mindedness, alertness). Technologies that will be applied for the implementation of this partnership are facial expression analysis, voice analysis, physiological measurements, context recording, and task tracking (Grootjen, et al., 2006).

An ePartner and its human user is more than a CAS, i.e., "a dynamic network of many agents … acting in parallel, constantly acting and reacting to what the other agents are doing" (Waldrop, 1992). The ePartner and its human user must each know the characteristics and state of the other partner, not just how the other behaves. To really collaborate with such a sensing ePartner, the human user must trust it[3]. He or she needs to know what the "ePartner knows about him or her", setting a requirement for the scrutability of the models. Human users should be able to inspect and control the details of the information held about them, the processes used to gather it, and the way that it is used. It may be possible to change some values according to his or her view (or according to the view of another partner of the team). There is "natural or intuitive" human-machine communication by expressing and interpreting communicative acts based on a common reference.

Neerincx and Lindenberg (in press) have developed a cognitive engineering method for designing complex adaptive systems to improve task load management, trouble-shooting, and situation awareness, based on experience with previous and current Navy and space missions and on practical theories of support, e.g., the user's cognitive task load (Neerincx, 2003b). The method focuses on the performance of the mental activities of human actors and the cognitive functions of machine actors to achieve the shared operational goals.

4.2 Extending ePartner concept to error management

The original inspiration for the ePartner concept was to monitor the human user's cognitive task load along the three dimensions of task complexity, time pressure, and frequency of task switching (Ibid). The mitigation strategies available to the ePartner included taking over tasks

[3] For a review of the research literature on trust in automated systems see (Madsen & Gregor, 2000).

from the user, guiding the user's task performance, requesting the assistance of other users or ePartners, or subtle actions to stabilise the user's mental state.

We propose extending the ePartner concept to incorporate error management. In particular, we shall use Helmreich's (2000) threat and error management model to do so. From the ePartner's viewpoint, threats can come from external sources such as its human user, other components in the C2 system including other users and ePartners, and platforms outside the C2 system. In addition, the ePartner will be aware that it too is fallible. Therefore, it must be capable of monitoring its own errors, as well as threats from external entities. The ePartner will need to be provided with (or learn) strategies and countermeasures for detecting and responding to threats and errors and for managing the resulting system state.

4.3 C2 system functionality required

A 21st century C2 system based on the extended ePartner concept will need to incorporate functionality very similar to a present-day diagnostic management system (DMS). DMSs are in operational use in civil and military aircraft, in power stations, in spacecraft, and in utility grids. More than a dozen COTS DMS products are available on the market.

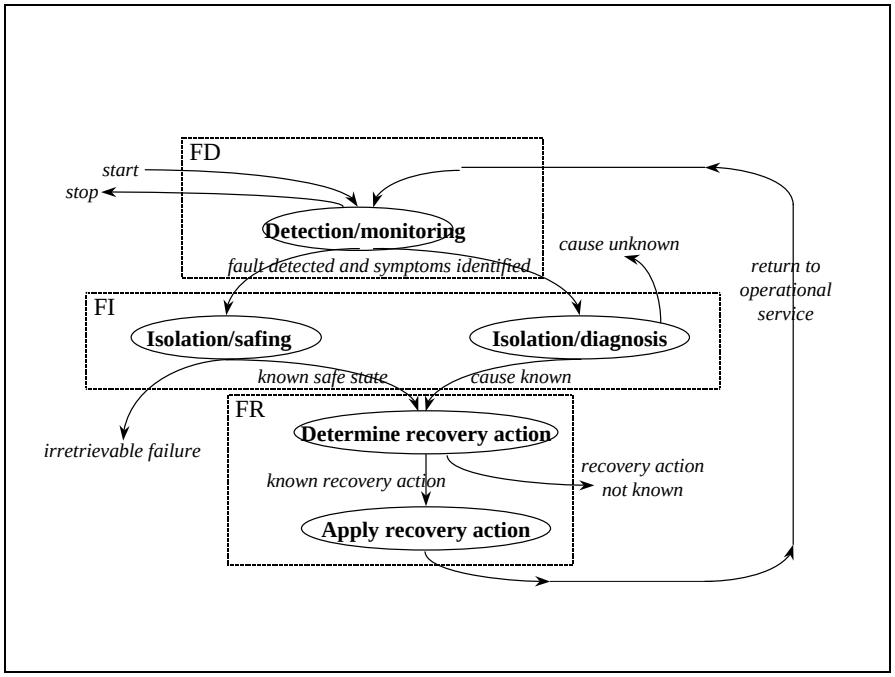

Figure 8. Fault detection, isolation and recovery (FDIR).

Figure 8 depicts schematically the functionality of a DMS in terms of interacting fault detection, isolation and recovery (FDIR) processes. Fault detection (FD) monitors a stream of sensory information coming from the process under control (PUC), e.g., a gas turbine. When FD detects a failure, it extracts the symptoms from the sensory stream, triggering two parallel fault isolation (FI) processes. One FI process is fast-acting and aimed at minimising the propagation of the adverse effects of the failure and bringing the PUC to a safe state. The other FI process is diagnostic, i.e., aimed at identifying the root cause of failure (RCOF). Once the RCOF is known, then it becomes possible to determine a course of action – if one is available – that has to be taken to restore the PUC to an operational state (possibly degraded).

The recovery action is then executed. If the recovery action is not effective, FD triggers the cycle again.

DMS technology could be readily applied in C2 systems to detect and respond to failures in platform systems such as sensors and weapons. The technology could equally well be applied to the C2 system itself. These applications would provide the necessary decision support to users in judging whether or not they could trust incoming information. The key difference in the proposed ePartner approach is that FDIR functionality would focus on the C2 system's human users. Furthermore, FDIR could be applied to the enemy's observed behaviour, but with the aim of error magnification rather than reduction. An essential prerequisite is knowledge about the sources, incidence, and types of C2 system user errors.

5. Proposed Research, Experimentation, and Development Programme

The discussion in the preceding chapters has shown that there is a need for C2 systems research, experimentation, and development.

Research is needed in the following areas:

- *Human error in C2*. The incidence, causes, and consequences of human error in C2 are unknown. There is a need for a study analogous to the audits performed by the University of Texas researchers into errors during 3500 airline flights. The study should identify the sources of threat, the types of error, and the strategies and countermeasures that commanders and their staffs use to manage threats, failures, and errors. The results of such as study could be used to determine the priorities and focus areas for other research, experimentation, and C2 systems development, as well as for user education and training.
- *C2 system connectivity*. There is a strong indication that the connectivity of C2 systems follows a power law, similar to the Internet or the World Wide Web. This has implications for the propensity of failures and errors to propagate through C2 systems. There is a need to establish whether or not the connectivity of typical C2 systems does indeed follow a power law.
- *Erroneous planning*. Although psychologists know that mistakes have more serious consequences than slips, there has been relatively little research into erroneous planning. The causes, incidence, and consequences of erroneous planning needs to be studied, together with ways for repairing faulty plans.
- *Operationalising sensemaking*. There is a need for C2 systems to adapt to novel situations. While Weick (1995) has characterised organizational sensemaking, he did not describe it in such a way that it could be implemented as an algorithm in a C2 system. Research is needed into how expert commanders and their staffs make sense of novel situations and codify the knowledge they create in the form of patterns that can be re-used. The results of this research could be used to train command staffs, as well as to determine what sensemaking support[4] C2 systems could provide them. Grant (2005a) has outlined an algorithm based on machine learning techniques that could acquire knowledge from novel situations for use in planning.
- *Cognitive engineering*. Research is needed into how to adapt existing cognitive engineering methods for the development of 21st century C2 systems. The emphasis should be on human-machine collaboration and on how to realise ePartners for C2.
- *Surprising the enemy*. The knowledge of how errors occur in C2, of erroneous planning, and of sensemaking may be reversed to discover how to increase the chance of the enemy committing errors and how to exploit these errors. 21st century C2 systems should help their users to harness Murphy's law.
- *Widening the concept of security*. There are common features to security and to RAM. Both are intended to keep a system operative in the face of threats. Fundamental research is needed into marrying security concepts with those of RAM.

[4] As opposed to decision support; see Carr & McGuinness (2001).

Exploratory experimentation is needed in the following areas:

- *Structure of C2 systems*. Experiments are needed to find out how best to structure the network underlying 21st century C2 systems to maximise the difficulty for an enemy to identify key nodes and links.
- *Interaction between ePartners and users*. The interaction between ePartners and their human users needs to be studied, e.g., using cognitive task analysis. The results of this experimentation could then be incorporated in C2 system user education and training.

Development is need in the following areas:

- *Testbed*. One or more testbeds should be developed to support research and experimentation. A key capability must be the ability to inject failures and errors. The testbed could be extended to become a C2 system user training environment.
- *C2 system architectures*. A C2 system architectures should be developed and prototyped that integrates task-oriented processes with collaborative team processes, sensemaking, FDIR, and user modelling to give agility.

The key benefit of the proposed programme is that the C2 community would gain knowledge about how and why C2 systems fail and users err. Without this knowledge, the community is unable to mitigate the fallibility of both systems and users.

6. Conclusions and Recommendations

This paper has reviewed the NCW literature on information-age C2 processes and 21st century C2 systems. It has shown that all parts of C2 systems are fallible, including the human users. It has looked at the ways in which errors propagate through networks, showing that the network structure is crucial. A model for managing threats and errors has been drawn from the human factors literature on aviation.

The ePartner concept has been proposed as a means for 21st century C2 systems to detect and respond to errors made by the C2 systems' users. A description has been given of how the ePartner concept can be extended using ideas drawn from Helmreich's (2000) threat and error management model. The resulting C2 system needs additional functionality to support FDIR.

We make the following recommendations:

- Research should be done into human error in C2, C2 system connectivity, erroneous planning, operationalizing sensemaking, cognitive engineering, surprising the enemy, and widening the concept of security.
- Experimentation should be done into the structure of the networks underlying C2 systems and into the interaction between ePartners and their human users.
- Testbeds and C2 systems architectures should be developed.

The key benefit of the proposed programme of research, experimentation, and development is that the C2 community would gain knowledge about how and why C2 systems fail and users err, enabling mitigation action to be taken.

References

Adams, et al, 2003	Adams, B.D., Bruyn, L.E., Houde, S., & Angelopoulos, P. 2003. *Trust in Automated Systems: Literature review*. DRDC Toronto CR-2003-096, Defence Research and Development Canada, Toronto, Ontario, Canada, June 2003.
Alberts, et al, 1999	Alberts, D.S., Garstka, J.J., and Stein, F.P. 1999. *Network-Centric Warfare: Developing and Leveraging Information Superiority*. US DoD Command and Control Research Program, ISBN 1-57906-019-6. Also downloadable from http://www.dodccrp.org.
Alberts & Hayes, 2003	D.S. Alberts and R.E. Hayes, 2003. *Power to the Edge: Command and Control in the Information Age*, US DoD Command and Control Research Program, ISBN 1-893723-13-5. Also downloadable from http://www.dodccrp.org.
Alberts & Hayes, 2006	Alberts, D.S. & Hayes, R.E. 2006. *Understanding Command and Control*. US DoD Command and Control Research Program, ISBN 1-893723-17-8. Also downloadable from http://www.dodccrp.org.
Alberts & Hayes, forthcoming	Alberts, D.S. & Hayes, R.E. Forthcoming. *Planning: Complex Endeavors*. US DoD Command and Control Research Program. Community Review Version, 2006, downloadable from http://www.dodccrp.org.
Boon & Holmes, 1991	Boon, S., & Holmes, J. 1991. *The Dynamics of Interpersonal Trust: Resolving uncertainty in the face of risk*. In Hindle, R., & Groebel, J. (eds). *Cooperation and Prosocial Behavior*. Cambridge University Press, New York, USA, 167-182.
Boyd, 1987	Boyd, J.R. 1987. *Organic Design for C2*. Unpublished lecture notes.
Boyd, 1996	Boyd, J.R. 1996. *The Essence of Winning and Losing*. Unpublished lecture notes.
Brehmer, 2005	Brehmer, B. 2005. *The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control*. In Proceedings, 10th International Command & Control Research & Technology Symposium, June 2005, McLean, VA. USA.
Callaway, et al, 2000	Callaway, D.S., Newman, M.E.J., Strogasz, S.H., & Watts, D.J. 2000. *Network Robustness and Fragility: Percolation on random graphs*. Phys. Rev. Lett., 85, 5468-5471.
Carr & McGuinness, 2001	Carr, & McGuinness. 2001. *Metrics and Methods for Analysis of Sensemaking*. Presentation, Sensemaking Symposium, US DoD CCRP, EBR Inc., Vienna, VA, USA, October 23-25, 2001. Downloadable from http://www.dodccrp.org/events/2001_sensemaking_symposium/index.htm (accessed 2 April 2007).
Cohen, et al, 2002	Cohen, R., ben-Avraham, D., & Havlin, S. 2002. *Efficient Immunization of Populations and Computers*. Preprint cond-mat/0207387.
Dehn, 2004	Dehn, D. 2004. Private communication, National Aerospace Laboratory (NLR), Amsterdam, Netherlands, 26 February 2004.
Endsley, 2000	Endsley, M.R. 2000. *Theoretical Underpinnings of Situation Awareness*. In M.R. Endsley & D.J. Garland (eds). *Situation Awareness Analysis and Measurement*. LEA, Mahwah, NJ, USA
Essens, et al, 2005	Essens, P., Vogelaar, A., Mylle, J., Blendell, C., Paris, C., Halpin, S., & Baranski, J. 2005. *Military Command Team Effectiveness: Model and instrument for assessment and improvement*. NATO RTP technical report AC/323(HFM-087) TP/59, April 2005. ISBN 90-6464-266-4.
Grant, 2001	Grant, T.J. 2001. *Towards a Taxonomy of Erroneous Planning*. Proceedings, 20th workshop of UK Planning & Scheduling Special Interest Group, University of Edinburgh, Scotland, 13-14 December 2001, ISSN 1368-5708.
Grant, 2005a	Grant, T.J. (2005). *Integrating Sensemaking and Response using Planning Operator Induction*. Proceedings, 2nd International Conference on Information Systems for Crisis Response and Management (ISCRAM), Brussels, Belgium, 18-20 April 2005.
Grant, 2005b	Grant, T.J. (2005). *Unifying Planning and Control using an OODA-based Architecture*. Proceedings, Annual Conference of South African Institute of Computer Scientists and Information Technologists (SAICSIT), White River, Mpumalanga, South Africa, 20-22 September 2005, ISBN 1-59593-258-5.
Grant & Kooter, 2005	Grant, T.J., & Kooter, B.M. (2005). *Comparing OODA and Other Models as Operational View Architecture*. Proceedings, 10th International Command & Control Research & Technology Symposium (ICCRTS), McLean, Virginia, USA, 13-16 June 2005.
Grootjen, et al,	Grootjen, M., Neerincx, M.A. & Weert, J.C.M. van. 2006. *Task-based*

2006 *interpretation of operator state information for adaptive support*. In: D.D. Schmorrow, K.M. Stanney & L.M. Reeves. (eds) 2006. *Foundations of Augmented Cognition, 2nd Edition*, pp. 236-242. Strategic Analysis, Arlington, VA, USA. ISBN 10: 0-9789812-0-0.

Helmreich, 2000 — Helmreich, R.L. 2000. *On Error Management: Lessons from aviation*. British Medical Journal, 320, 781-785, 18 March 2000

Helmreich, et al, 1999 — Helmreich, R.L., Klinect, J.R., & Wilhelm, J.A. 1999. *Models of Threat, Error, and CRM in Flight Management*. Proceedings, 10th International Symposium on Aviation Psychology, Ohio State University, Ohio, OH, USA, p.677-682. Downloadable from http://homepage.psy.utexas.edu/homepage/group/HelmreichLAB/publications/publications.html (accessed 4 January 2005).

Hollnagel, 1991 — Hollnagel, E. 1991. *The Phenotype of Erroneous Actions: Implications for HCI design*. In Weir, G.R.S. & Alty, J.L. (eds). 1991. *Human-Computer Interaction and Complex Systems*. Academic Press, London, UK, chapter 4. ISBN 0-12-742660-4.

Hudson, et al, 1998 — Hudson, P.T.W., Lawton, R., Parker, D., Reason, J., Verschuur, W.L.G. 1998. *Bending the Rules II: Why do people break rules or fail to follow procedures? And what can you do about it?* Safety Working-group, Leiden University, Netherlands.

Janis, 1983 — Janis I. 1983. *Groupthink in Small Groups and Social Interaction*. NY: John Wiley & Sons

Johnson, et al, 2005 — Johnson, G., Scholes, K., & Whittington, R. 2005. *Exploring Corporate Strategy*. 7th edition, Prentice Hall, Englewood Cliffs, NJ, USA.

Kahneman, et al, 1982 — Kahneman, D., Slovic, P., & Tversky, A. (eds). 1982. *Judgment under Uncertainty: Heuristics and biases*. Cambridge University Press, Cambridge, UK.

Keen & Scott-Morton, 1978 — Keen, P.G.W., & Scott-Morton, M.S. 1978. *Decision Support Systems: An organizational perspective*. Addison-Wesley, Reading, Mass., USA.

Keus, 2002 — Keus, H.E. 2002. *A Framework for Analysis of Decision Processes in Teams*. In Proceedings, 7th International Command & Control Research & Technology Symposium, June 2002, Monterey, CA, USA.

Klein & Klinger, 1991 — Klein, G., & Klinger, D. 1991. *Naturalistic Decision Making*. Human Systems IAC Gateway, Volume XI, 3, 2, 1, 16-19 (Winter 1991).

Maanen, et al, 2005 — Maanen, P.P. van, Lindenburg, J., & Neerincx, M.A. 2005. *Integrating Human Factors and Artificial Intelligence in the Development of Human-Machine Cooperation*. Proceedings, 2005 International Conference on Artificial Intelligence (ICAI'05), CSREA Press, Las Vegas, NV, USA

Madsen & Gregor, 2000 — Madsen, M., & Gregor, S. 2000. *Measuring Human-Computer Trust*. Central Queensland University, Gladstone, Australia.

NATO, 2006 — NATO. 2006. *Exploring New Command & Control Concepts and Capabilities*. NATO SAS-050, January 2006.

Morowitz & Singer, 1995 — Morowitz, H.J. & Singer, J.L. (eds). 1995. *The Mind, The Brain, and Complex Adaptive Systems*. Addison-Wesley, Reading, MA, USA.

Neerincx, 2003a — Neerincx, M.A. 2003a. *E-Partners Op Maat*, Inaugural lecture, TU Delft, Netherlands, Cedris, Delft, ISBN 90-75774-03-6. [In Dutch: *Tailor-made e-Partners*]

Neerincx, 2003b — Neerincx, M.A. 2003b. *Cognitive Task Load Design: Model, methods and examples*. In: E. Hollnagel (ed.), *Handbook of Cognitive Task Design*. Chapter 13 (pp. 283-305). Lawrence Erlbaum Associates, Mahwah, NJ, USA.

Neerincx, et al, 2006 — Neerincx, M.A., Bos, A., Grant, T.J., Brauer, U., Olmedo Soler, A., Lindenberg, J., Smets, N., Wolff, M. 2006. *Human-Machine Collaboration for Long Duration Missions: Crew assistant concept*. Proceedings, 16th World Congress on Ergonomics, Maastricht, Netherlands, 10-14 July 2006

Neerincx & Lindenberg, in press — Neerincx, M.A. & Lindenberg, J. (in press). *Situated cognitive engineering for complex task environments*. In: Schraagen, J.M. (ed). *Natural Decision Making & Macrocognition*. (Will appear in 2007). Ashley Press, UK.

Newman, 2003 — Newman, M.E.J. 2003. *The Structure and Function of Complex Networks*. SIAM Review, 45, pp. 167-256. Downloadable from http://aps.arxiv.org/abs/cond-mat/0303516/ (accessed 2 March 2007).

Norman, 1981 — Norman, D. 1981. *Categorization of Action Slips*. Psychological Review, 88, 1-15.

Norman, 1993 — Norman, D. 1993. *Things that Make us Smart: Defending human attributes in the age of the machine*. Addison-Wesley, Reading, Mass., USA. ISBN 0-201-62695-0.

Ormerod, 2005	Ormerod, P. 2005. *Why Most Things Fail: Evolution, extinction and economics*. Faber & Faber, London, UK. ISBN 0-571-22013-4.
Raiffa, 1968	Raiffa, H. 1968. *Decision Analysis*. Addison-Wesley, Reading, Mass., USA
Rasmussen, et al, 1981	Rasmussen, J., Pedersen, O.M., Mancini, G., Carnino, A., Griffon, M. & Gagnolet, P. 1981. *Classification System for Reporting Events involving Human Malfunctions*. Technical Report Riso-M-2240, Riso National Laboratory, Roskilde, Denmark
Reason, 1984a	Reason, J. 1984a. *Actions Not As Planned: The price of automatization*. In Underwood, G. & Stevens, R. (eds). 1984. *Aspects of Consciousness: Volume 1, Psychological issues*. Academic Press, New York, USA.
Reason, 1984b	Reason, J. 1984b. *Lapses of Attention in Everyday Life*. In Underwood, G. & Stevens, R. (eds). 1984. *Aspects of Consciousness: Volume 1, Psychological issues*. Academic Press, New York, USA.
Reason, 1987	Reason, J. 1987. *Generic Error-Modelling System (GEMS): A cognitive framework for locating human error forms*. In Rasmussen, Duncan & Leplat (eds). 1987. *New Technology and Human Error*. John Wiley & Sons, London, UK.
Reason, 2000	Reason, J. 2000. *Human Error: Models and management*. British Medical Journal, 320, 768-770 (18 March 2000).
Rittel & Webber, 1973	Rittel, H., & M. Webber, M. 1973. *Dilemmas in a General Theory of Planning*. Policy Sciences, 4, 155-169, Elsevier Scientific Publishing Company, Inc., Amsterdam, Netherlands
Rizzo, et al, 1988	Rizzo, A., Bagnara, S., & Visciola, M. 1988. *Human Error Detection Processes*. In Hollnagel, E., Mancini, G., & Woods, D.D. (eds). 1988. *Cognitive Engineering in Complex Dynamic Worlds*. Academic Press, London, UK, pp.99-114. ISBN 0-12-352655-8.
Rochlin, et al, 1987	Rochlin, G.I., LaPorte, T.R., & Roberts, K.H. 1987. *The Self-Designing High-Reliability Organization: Aircraft carrier flight operations at sea*. Naval War College Review, 40, 4, 76-90.
Schneider-Hufschmidt, et al, 1993	Schneider-Hufschmidt, M., Kühme, T., & Malinowski, U. 1993. *Adaptive User Interfaces: Principles and practices*. Human Factors in Information technology 10, North-Holland, Amsterdam, Netherlands.
Sheridan, 1992	Sheridan, T.B. 1992. *Telerobotics, Automation, and Human Supervisory Control*. MIT Press, Cambridge, Mass., USA. ISBN 0-262-19316-7.
Snook, 2000	Snook, S.A. 2000. *Friendly Fire: The accidental shootdown of US Black Hawks over northern Iraq*. Princeton University Press, Princeton, NJ, USA.
Vaughan, 1996	Vaughan, D. 1996. *The Challenger Launch Decision: Risky technology, culture, and deviance at NASA*. University of Chicago Press, Chicago, USA.
Wackers & Korte, 2001.	Wackers, G., & Korte, J. 2001. *Reliability and Vulnerability of Condition Monitoring Systems in North Sea Offshore Helicopter Transport: HUMS, Helikopter Service AS, and the 1997 Super Puma helicopter accident (Norte)*. Proceedings, 5th International Conference on Technology, Policy, and Innovation, Delft, Netherlands.
Waldrop, 1992	Waldrop, M.M. 1992. *Complexity: The emerging science at the edge of order and chaos*. Simon and Schuster, New York, USA.
Weick, 1993	Weick, K.E. 1993. *The Collapse of Sensemaking in Organizations: The Mann Gulch disaster*. Administrative Science Quarterly, 38, 628-652.
Weick, 1995	Weick, K., 1995. *Sensemaking in Organisations*. Sage, Thousand Oaks, CA, USA. ISBN 0-8039-7177-X.
Weick & Roberts, 1993	Weick, K.E., & Roberts, K.H. 1993. *Collective Mind in Organizations: Heedful interrelating on flight decks*. Administrative Science Quarterly, 38, 3, 357-381.
Weick & Sutcliffe, 2001	Weick, K.E., & Sutcliffe, K.M. 2001. *Managing the Unexpected: Assuring high performance in an age of complexity*. Jossey-Bass, San Francisco, CA, USA. ISBN 0-7879-5627-9.
Wikipedia, 2007	"Wicked problem", Wikipedia, http://en.wikipedia.org/wiki/Wicked_problems, accessed 1 February 2007.

Author biographies

Professor doctor Tim Grant (Ph.D., University of Maastricht) is the Professor in Operational ICT and Communications at the Netherlands Defence Academy, where he is responsible for the bachelors-level Communications, Information, & Command & control Systems (CICS) course for Dutch officer cadets. He is also a visiting Professor at the University of Pretoria,

South Africa. He previously held positions as a Royal Air Force officer for 20 years, working in the United Kingdom and Singapore, and as a Principal Consultant in the leading Dutch-French software house, Atos Origin Nederland b.v., for 17 years, where he worked on C2 projects for the European Space Agency, the Western European Armaments Organisation, and the Dutch Ministry of Transport and Waterways. His research interests centre on C2 architectures based on intelligent agents with OODA, planning, and learning capabilities, and on the parallels between military C2 systems, civil information systems for crisis response and management (see www.iscram.org), and process control systems.

Paul C. van Fenema (Ph.D., Erasmus University) is an Associate Professor at the Netherlands Defence Academy. He previously held positions as an Assistant Professor at the Rotterdam School of Management, and as a visiting researcher at the Florida International University. His research focuses on the coordination of global information systems projects and high reliability organizations. His work has been published or is forthcoming in *Communications of the ACM*, *International Journal of Project Management*, *European Journal of IS*, *Information Systems Journal*, *Time & Society*, *European Management Journal*, *Cognition Technology & Work*, *Organization Studies* (book review), and a number of book chapters.

Maarten van Veen is an Assistant Professor in Information Systems at the Netherlands Defence Academy. He previously held positions at the Open University of the Netherlands, at the Professional University Saxion at Deventer, and at the University of Amsterdam. His active areas of research are Information dominance, Information literacy, Representations in new media, and Usage of Information Technology. He has published in journals and proceedings of (international) conferences, and he led multiple sessions of workshops on information literacy in education.

Professor doctor Mark A. Neerincx is the head of the Intelligent Interface group at TNO Human Factors, and a professor in Man-Machine Interaction at the Delft University of Technology. He has extensive experience in fundamental and applied research on human-computer interaction, among other things in the domains of space, defence, security and health. Important results are (1) a cognitive task load model for task allocation and adaptive interfaces, (2) models of human-machine partnership for attuning assistance to the individual user and momentary usage context, (3) cognitive engineering methods and tools, and (4) a diverse set of usability "best practices". Mark Neerincx has published an extensive set of papers for peer-reviewed journals and international conferences, and has been involved in the organisation of conferences, workshops and tutorials to discuss and disseminate human factors knowledge.