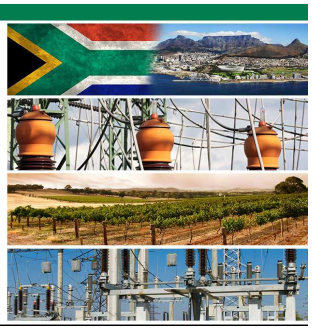
8TH SOUTHERN AFRICA REGIONAL CONFERENCE

14 - 17 NOVEMBER 2017



Electricity Supply to Africa and Developing Economies – Challenges and Opportunities

Planning for the future in uncertain times

Addressing Emergency Decision Making in Complex incidents: Implementation of Advanced Incident Command System in Eskom

A. José Correia, Robert Koch, Liza van der Merwe, Sajedah Mahomed
Eskom
South Africa

correiaj@eskom.co.za

Abstract

Eskom has chosen to integrate its emergency response structures using Incident Command System (ICS) as used by FEMA et al. ICS was chosen because of its success in managing incidents of any size from local emergencies to disasters like the Deep Water Horizon oil rig failure and large wild land fires, covering both foreseen and unexpected events. This system is now also being adopted by the South African emergency response community. Integrating with the responders from various agencies will be much more efficient if all the country's response structures are using the same system. Eskom has extended the application of ICS to emergencies which could exceed even the disasters mentioned, i.e. a national blackout.

ICS provides a structured way for person managing the incident to create order in the chaos of an emergency. In the first few hours of a major incident, however, particularly one that has not been encountered before by the incident manager, the pressure of the incident, the inherent uncertainty of such complex conditions and the need to do something immediately, can force an unsure manager to make decisions that turn out to be detrimental to the resolution of the emergency. Eventually the management of the incident will become more tenable, with larger incidents requiring more time, information and coordination before an effectively integrated response can be implemented.

Since a blackout in South Arica, with almost any amount of planning, remains an event that no-one can possibly be familiar with yet, it fits the above description. In addition, the first few hours of the blackout will a critical period for coordinated planning, as telecommunications systems will become progressively compromised until the electricity supply is restored. These two characteristics mean that there is unlikely to be enough time to understand the full context of the incident and plan for it before the failure of the telecommunications system.

This paper examines the use of the Cynefin framework to provide insight on how to approach the management of a major incident (or planned event). Cynefin is a simple framework that enables sense to be made of the incident context. This paper explores the application of this decision making framework to ICS and how to address gaps identified in the application of ICS.

1. Introduction

Eskom has embarked on a company-wide *Enterprise Resilience Programme* which includes strengthening its emergency response systems and structures by embedding international good practice, i.e. the Incident Command System (ICS). Eskom's emergency response structures have matured over the last 10 years to include well developed and utilized strategic and operational response structures. These have recently been augmented with tactical structures at a divisional/functional level, which have been used to shape Eskom's disaster management plans for its identified disaster scenarios.

Resilience is defined in various ways in different fields. This paper uses a definition for resilience which has emerged from experience in responding to threats, managing large incidents, and from accident modelling undertaken in post-incident investigations – i.e. that resilience may be defined as "*the ability to manage complexity under pressure"* [9]. Incident command and the structures and the processes and systems that support this, play a vital role in supporting this ability.

2. Incident Command System

The Incident Command System [1] is an organisational system developed in the USA to manage incidents of any size, from a two vehicle collision to incidents as large as the September 2001 attacks in New York and the Deep Water Horizon disaster. It matches Eskom's requirements as a national organ of state since it is specifically designed to allow agencies with different mandates to coordinate their activities efficiently. The system also supports great efficacy, through the application of a detailed, real-time planning process that takes place over regular planning and execution cycles during the incident. When implemented across Eskom's strategic, tactical and operational structures, ICS naturally situates each response structure within the standard ICS hierarchy, appropriate to the size and nature of the incident.

ICS has proven itself to be very effective in managing large emergencies once the nature and details of the emergency are known, and the systems and infrastructure necessary to keep track of the incident are in place. The ICS planning process delivers a very clear and specific plan (Incident Action Plan) to personnel on the ground who must implement the plan. This plan is rapidly updated in a structured manner over the duration of the incident. Once the context of the incident is determined based on the available information, the ICS structure will actively track and monitor even rapidly changing emergency conditions, to maintain the necessary levels of awareness that detailed real-time incident response planning requires. A general statement can be made about the nature of disaster incidents themselves: in the first hours of a major incident, no amount of information that can be gathered will allow an accurate enough understanding of the incident to develop a plan that can be relied on to resolve the incident. On the other hand, the impact of a major incident or disaster is strongly dependant on the amount of time the incident is allowed to propagate without effective management, so this gap in information to support real-time planning is relevant to most disasters. It often takes the first operational period, a full cycle in the ICS planning process, before the quality of the shared situational information has reached a point where the plans that are developed will be adequate in coordinating the management of a major incident.

Eskom has legislated responsibilities for disasters in which the time component is especially important in the management of the incident. One of these is a national blackout which, in most plausible cases, will not be anticipated. Within a few hours of the beginning of a blackout the cellular communication systems, so relied on by our society, can be expected to be compromised by virtue of the failure of their battery backup systems. This is not nearly enough time to develop the necessary Incident Action Plan (IAP), which also cannot be executed if it cannot be communicated. The unfolding complexity in such scenarios will require careful consideration of how decision-making is undertaken and what is required to be in place for this to be effective.

3. Cynefin- a framework for decision making

This paper explores the use of the Cynefin framework [2] as an approach to decision-making, based on the nature of the incident context and the information available to decision-makers. A major incident will require various types of decisions to be taken by multiple decision-makers at various levels of the organisation and across multiple agencies (e.g. from those made by operators of emergency backup plant using standard operating procedures, to strategic decisions that could have reputational, socio-political and economic outcomes that are unpredictable and even unprecedented). We seek to apply the Cynefin framework to associate aspects of the incident context with different decision domains, thereby enhancing the clarity on the approach to decision-making that is most helpful. The Cynefin framework establishes the following decision domains and approaches to decision-making (see Figure 1) [2], [3]:

- **Obvious Domain** (sometimes called the domain of "known knowns"): *This is a space where cause and effect are understood and predictable, hence "everyone" knows what to do about the issue*. In this domain observations can be categorised and responded to in a standardised manner, using standard operating procedures based on "*best practice*".
- **Complicated Domain** (sometimes called the domain of "known unknowns"): *This is a space where cause and effect relationships may be difficult to derive or understand, but the right people, given sufficient time and resources for analysis, can discover these*. This domain is best suited to managing issues that require experts to apply their knowledge to analyse the information to directly resolve the problem. Here more than one possible solution exists based on "*good practice*", as opposed to "*best practice*".
- **Complex domain**: *This is a space where cause and effect are only apparent retrospectively. What appears logical after the fact, i.e. "when the dots have been connected", is but one of many other possible logical outcomes that could have occurred*. This domain is best suited to managing issues which must be approached using general heuristics rather than being directly or simply resolved. This applies particularly to managing complex adaptive systems and people, which exhibit complex, nonlinear interdependencies. Engagement in this context requires sense-making and emergent practice.
- **Chaotic domain**: *This is a space so turbulent that cause and effect are unknown; there is little point in investigating them.* This domain is best suited to contexts in which the active agents, people, are not yet self-coordinated, and require the application of local order – i.e. urgent intervention is required for stability. In this context decisions are required, without the time to probe or analyse the situational information available. This is termed "*novel practice*."

A fifth domain called "**disordered**" (labelled as "*unknown* " below) refers to the aspects of the decision space that are not yet well enough understood to place in one of the other domains.

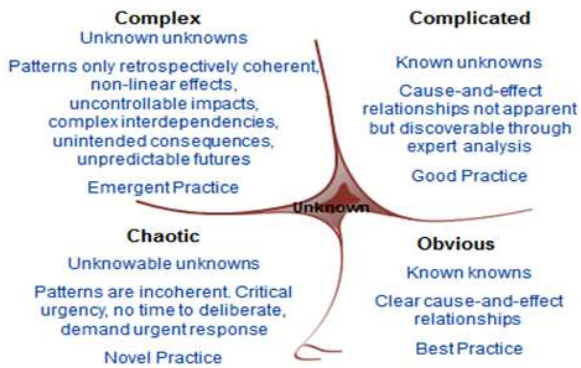


Figure 1: Cynefin Sensemaking Framework, [2]

We now consider how these domains appear in a major incident or disaster. From the point of view of someone trying to understand the whole incident it might at first appear to be entirely disordered (Figure 2- on the left).

The aim of using the Cynefin framework is to identify aspects of the incident that will be most appropriately managed through the *practices* associated with one of the four *decision domains*. It is important also to understand that this is a dynamic process, i.e. *novel* practice in the "*chaotic"* domain may rapidly shift the decision context to the "*complex"* (or eventually "*complicated"*) domain. Similarly, a decision context misinterpreted as "*ordered"* could rapidly shift the context to "*chaotic*". The figure below illustrates how a better understanding of which type of decision making is required assists in reducing the perceived "disorder". Importantly, identification of these decision domains provides resilience practitioners with a vocabulary to better communicate their approach to specific aspects of the problem in disaster preparedness, response, and recovery.

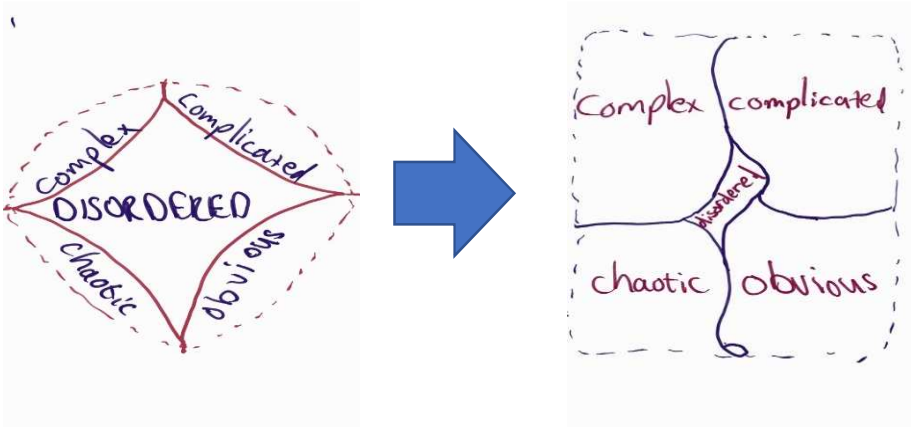


Figure 2: Cynefin framework – making sense of a perceived sense of disorder.

A particular note about the "*chaotic"* domain: people who are active in responding to their circumstances, do not stay in this domain for long and will act to secure their safety, their property and in the case of vocational professionals, their mandate. In so doing they can be expected to *eventually* self-coordinate locally and move their context within the larger incident, into the *complex* domain. If these coordinated areas can be actively encouraged and resourced, observed and managed, once observed, they can form pockets of response which contribute to the overall effective resolution of the incident. This is particularly the case in major incidents or disasters where prior planning parameters have been substantially exceeded – and the incident takes on the form of what is sometimes referred to as a "catastrophe". Emergency response is local before it becomes coordinated.

4. Applying Cynefin to Incident Command

The question we now explore is how the Cynefin decision framework can be used together with ICS in the management of extreme incidents. We show how the Cynefin approach to analysis and understanding supports the ICS objectives of coordinating management and control during an incident.

The ICS planning process can be seen as balancing certainty and flexibility by providing operational staff with comprehensive plans, which are then reviewed and updated and reissued to the response personnel after a prescribed time period, generally around 8-12 hours, or however long the operational period is. The ICS process begins by identifying the incident objectives, that is, by describing what the outcome of the response must look like once the incident is sufficiently under control for normal business processes to manage it. Once the nature of an incident is understood in relation to the information available, in parallel to the operational management of the incident, the

ICS planning process contains a sequence of activities that deliver a plan for implementation by personnel on the ground for the next operational period.

While the plan is being executed the incident as a whole is being observed for the following aspects:

- **Incident stability**: is it increasing in size and complexity?
- **Safety**: Are there any safety issues?
- **Objectives**: Are the objectives still effective, will they move the incident to a point that normal business can manage?
- **Prognosis**: How long will it be until the objectives are completed?
- **Resourcing**: What is the current status of resources and people? Are they in good condition? Are there sufficient resources?

From these insights, the plan will be adjusted to reduce the damage, cost and duration of the incident.

The Cynefin framework can be used to assess the incident context to decide which decision making process to apply to particular areas of the problem. In the complex domain it talks about the execution of *safe-to-fail* experiments, the accentuation of positive outcomes (*amplification*), active reduction of negative outcomes (*dampening*) and the development of heuristics.

The proposal here is to see the ICS actions as being in-incident manifestations of the complex domain interventions:

- Safe to fail experiments are activities which will not result in unacceptable consequences even in the worst outcome. In Cynefin these are used as probes into complex contexts that allow better understanding and thoughtful responses. Incident Action Plans (IAP), the main deliverable of the ICS planning process, must be carried out by personnel on the ground, to achieve objectives aimed at resolving the incident. They are not necessarily safe to fail, but they must be carried out under the duress of an incident. Since they must be carried out they can take the place of safe to fail experiments and can be used as probes in the incident. Adding aspects to be measured to these plans would explicitly turn them into probes.
- Accentuating the positive outcomes and reducing the negative outcomes can be compared to the ongoing regular review of the incident response and the planning cycle that delivers an IAP for each operating period. Both of these ideas create adaptive feedback cycles.
- Incident objectives can serve as guiding heuristics, loosely rules of thumb, by ensuring that all the ICS personnel are aware of the incident objectives and by extension how their part in the plan works towards achieving the objectives. Using these they can confidently manage any small gaps they encounter in the plan because they are aware of the global intent of the plan. This would meet the goal of heuristics in complex, unplanned, environments. An example here, in the case of a national blackout is the priority given to nuclear safety when considering power restoration options.

On the other hand the ICS process, in the beginning of the planning cycle, requires the re-evaluation of the incident objectives and the development of operational period objectives that can build towards the end goals. The Cynefin framework provides a way of evaluating the information coming from the various areas in the incident, dividing the problem statement into areas that are best resolved in the different decision domains of the Cynefin framework. This will allow the ICS commanders to make decisions about the various parts of the incident in the most appropriate way.
For example:

- The standard operating procedures and monitoring of emergency backup generation falls within the obvious domain;
- The supply of fuel may be complicated given the cross sector requirements;

- Or supply of fuel could be complex, if the expected sources of supply are disrupted and unavailable to planners

The comparison is intended to demonstrate that the Cynefin decision process can be used to enhance ICS incident management to achieve the complementary goals of analysis, planning and response.

By providing Incident Commanders and other decision makers within the ICS structure with Cynefin decision making concepts and tools, decisions can be made with more insight. An additional advantage of this approach could be better use of the context itself, for example, by integrating into the IAP any positive response activities that those affected have initiated.

The introduction of this type of thinking in pre-planning for major disaster scenarios is particularly helpful as it highlights the need for plans that are flexible in the face of the multiple possible progressions of an incident.

5. Proactive encouragement of order in chaos

There are two main problems that need to be solved in the beginning of an incident before the ICS process is able to provide a clear Incident Action Plan:

1. What actions should be taken by those affected at the onset of the emergency?
2. How does the Incident Management Team understand the emergency context within the first operational period, even as the context itself changes?

The first problem is experienced by the personnel on the ground responding to the incident in an initial attack since they need to be able to respond with the confidence that their actions will be considered appropriate. According to Bonno Pel, Grégoire Wallenborn and Tom Bauler, [1], "...socially innovative agency cannot be presupposed… the crucial game-changing effect is to start the game by activating the players." The meaning here is that the activities of agents on the ground must often be prompted and practiced if the expected social response of self-organisation is to take place as an immediate response to an incident or, in Cynefin terms, agents finding they are in a chaotic domain must be prompted if their response is to be rapid enough. This is assisted through the development of disaster plans, emergency protocols and standard operating procedures, as discussed below.

For each area of the business the Eskom personnel have identified mandates that they are expected to pursue even in the face of extreme contexts such as disasters. If these are clearly identified for each of the business areas these can be pursued in the initial hours of a disaster without reference to a central authority. This assumes that the personnel have been empowered to act in the interests of their mandate with the right delegation of authority vested in response structures, using emergency based procedures with which they are comfortable and pursuing activities that they have been trained on and practiced. In parallel with the initial attack of emergency responders, Eskom personnel are instructed to maintain, in order of priority:

- Safety of the incident management team, other responders and personnel and the public.
- Management of the incident itself, using any appropriate pre-approved protocols and procedures.
- Preservation of property and services- this can be interpreted in the case of an organisation as the management and pursuit of the mandate delegated to the personnel in the midst of the incident.

Given these priorities and the responsibility to be ready for anything, Eskom sites can be advised on how to prepare for such events. With pre-approved emergency plans that can be followed without

real time approval in the case of identified incidents or context the personnel on the ground can execute actions that would assist them in securing their mandates, once the prior aims of safety and incident management are in hand.

If metrics are attached to the plans in a predetermined way, a solution to the second problem, described below, can make use of the emergency response plans:

The second problem relates to the difficulty in establishing the nature and detail of the incident context rapidly enough, especially since the amount of time an emergency is allowed to propagate unopposed determines much of its damage. Additionally to the information deficit at the beginning of an incident, much of what is available is often apocryphal, particularly data relating to causes and impacts. The danger of the first sets of information is that they can be:

- Taken as fact when they should be used with scepticism.
- Misconstrued as applying to everyone in the absence of other data, when it is received only from a limited part of the incident.
- Used preferentially over later information since there is a dearth of information in the beginning of an incident.
- More subtly, if the information expected back from particular areas by a particular time is not returned, then the gap could be ignored, instead of itself being a data point.

The central management of the incident relies heavily on the completeness and quality of the data that is available. Waiting for the passive accumulation of information will delay the development of an effective IAP for too long to get ahead of the expanding impact of the incident. Cynefin suggests that, in contexts best characterised by the complex domain, safe to fail experiments are executed both to understand the context better and to identify activities in areas that can be supported to rapidly improve the situation. With this in mind, the plans being implemented by personnel on the ground in their local initial attacks can have metrics attached to them that allow the central management of the emergency response plan to rapidly put together a picture of the situation on the ground in various areas. The personnel on the ground must respond and secure their safety and their mandates; their efforts to do this must be supported centrally with resources and best practice guidance. Since this must take place anyway for the immediate management of the incident, the returning information can be used to more rapidly understand the situation.

The proposal here is that the plans being developed for any large incident take the Cynefin framework into account by “front loading” context probes into the planning, not in the form of safe to fail experiments, but as metrics attached to emergency response plans. Metrics are expected to be largely plan and plant specific, but a general metric relating to the staff might show how many personnel on site needed to leave, or skills not yet on site that need to be provided. If the information on these metrics can be automatically, or at least regularly, sent to the personnel centrally planning and managing the incident, the disordered domain can be most efficiently reduced. The data received will mostly be related to expectations of progress regarding the execution of existing plans. This will assist in understanding how the data fits into the context proactively. While this is a positive aspect of the scheme, it must be remembered that unrelated information cannot be ignored, so further development will be required to create placeholders for this information so it can be understood when the context has taken shape.

6. Legislative constraints and support

As a practical issue, emergency managers trying to get emergency plans implemented are often working against the many existing competing claims on an organisations time and resources. One way of acquiring enough support for developing these plans and embedding the right culture in the organisation could be by referring to the legislative requirements placed on all government organisations. The National Disaster Management Act (DMA) Act no. 57 of 2002, as amended,

specifies several measures that can support the management of an incident in the first few hours. The ones that have the clearest impact on the successful management of incidents are:

Institutional Arrangements:

Response teams are assigned, developed and primed to respond to an incident when it happens. Arrangements are made with external role-players from whom support will be required for emergency preparedness, response and recovery and are primed to respond to an incident for an integrated and coordinated plan. Mutual aid agreements form part of the preparedness expected by the DMA.

Preparedness and Response Measures:

This area requires that the emergency response and recovery plans for a given area are developed. Since these must be developed they can be used to meet both the proposals suggested in this paper:

- Plans based on Standard Operating Procedures that provide personnel on the ground clear and useful guidance on how to execute an initial attack in the face of a disaster,
- Metrics that can be used proactively to create a picture of the context that can be used to more rapidly develop an IAP

This actively requires and legislates the "front loading" of the activities needed to achieve both aims.

Information management:

The information management and communication system necessary to move information between the activities on the ground and the coordination at the centre by recording and tracking real-time disaster response and recovery information must be addressed as part of the legislated preparations and resources required for disaster preparedness.

Training and awareness:

The personnel who are going to use the plans must be trained, exercised and be made conscious of the intention to inform the emergency coordinators of the response and emergency plan progress so as to accelerate the development of an IAP.

7. Conclusion

The Cynefin framework provides resilience practitioners with a *vocabulary* that allows better engagement of specific aspects of disaster planning and incident readiness, response, and recovery. This paper has explored how the Cynefin framework can be applied to a large incident that is managed using the Incident Command System (ICS), providing the following insights:

- ICS provides for the effective management of major incidents when there is enough information to compile Incident Action Plans (IAPs) that can be executed in the next operational period. ICS is faced with a gap in the beginning of an incident where the necessary information is often unavailable and adequate response structures have not yet been established. If the incident changes dramatically this uninformed state could recur. At a local level, trained staff will execute known response procedures, where these fall within the planning parameters used to develop the procedure. Where these parameters are exceeded, a level of chaos may emerge that might need to be resolved at a local level. ICS provides for this through establishment of incident command at this level, which is expanded

as the incident grows, or the response becomes coordinated for larger incidents. For such large incidents, the Incident Commander is required to rapidly probe the context of the incident and make decisions, whilst not understanding the full context of the incident, that enhance the "*evolutionary potential of the present*."

- The aim of coordinating a multi-agency response suggests that decision making is happening at multiple levels and in multiple decision domains. ICS is supported by *best practice* through *standard operating procedures* deployed by responders on the ground (e.g. fire fighters, utility field staff, power system control room staff), as well as the team managing the overall incident. Considered as a whole, ICS fits the definition of *good practice*, in that each Incident Commander (IC) will construct a unique response structure based on their expert judgment and experience in response to the unfolding context of the incident.
- Once ICS has been established, the implementation of Incident Action Plans over multiple operational periods will assist in moving the incident from the *complex* domain to the *complicated* domain. These plans, and some of their subcomponents may resemble *safe-to-fail* experiments, until the issues faced and outcomes to specific interventions become more predictable.
- An area not generally addressed by ICS is the longer-term reputational, social, and economic impact of the incident and how it is managed. This level of complexity requires further investigation, and may suggest the establishment of a team that guides the IC on the longer-term implications of decisions made.

By mapping Cynefin activities onto the emergency response space, such as using IAPs as incident probes in place of safe to fail experiments, the largely disordered beginning of an incident can be proactively interrogated and shortened. It is further shown that the necessary elements, such as emergency plans, are present as a natural, indeed legislated, part of emergency incident management. Incident Commanders and other decision makers within the ICS structure who are armed with the Cynefin framework can shorten the initial period of the incident in which there is insufficient reliable information for operational period planning, use Cynefin for the duration of the incident to make hard decisions with more insight and even make better use of the complexity within the incident context itself.

References

[1] FIRESCOPE, *"Field Operations Guide ICS 420-1, Incident Command System publication December 2012"*.

[2] Snowden and Boone, "A Leader's Framework for Decision Making." Harvard Business Review November 2007.

[3] Renaud, Cynthia. "The Missing Piece of NIMS: Teaching Incident Commanders How to Function in the Edge of Chaos." Homeland Security Affairs 8, Article 8 (June 2012).

[4] Bonno Pel, Grégoire Wallenborn and Tom Bauler, "Emergent transformation games: exploring social innovation agency and activation through the case of the Belgian electricity blackout threat." Ecology and Society Volume 21, No.2, article 17, 2016.

[5] Ramus Dahlberg, "Resilience and Complexity-Conjoining the Discourses of Two Contested Concepts." Culture Unbound, Volume 7 2015.

[6] Hannah a, Uhl-Bien, Avolio, Cavarretta, "A framework for examining leadership in extreme contexts." The Leadership Quarterly 20, 2009.

[7] Hammond, "On the Making of History: John Boyd and American Security." The Harmon Memorial lecture, U.S. Air Force Academy, 2012.

[8] Koch, Robert; "Resilience in a Changing Universe", Institute of Risk Management South Africa, 2016 IRMSA Conference, 21-22 September 2016.

[9] Erik Hollnagel, David Woods and Nancy Leveson, "Resilience Engineering – Concepts and Precepts", Ashgate Publishing Company, 2010.