

## A CASE STUDY OF THE DEVELOPMENT OF A SANDF TACTICAL DATA LINK NETWORK ENABLING CAPABILITY

Corné J. Smith and Jacobus P. Venter \*

**Abstract.** In the scope of Tactical Data Links (TDL), the South African National Defence Force (SANDF) started the journey to establish a national TDL capability with the commencement of their national Strategic Defence Procurement Packages (SDPP) in 1999. These procurement packages saw the development of fighter, helicopter, frigate and submarine platforms with requirements for TDL capabilities. In this, the SANDF pursued the development of an indigenous TDL data model and data transfer protocol standard appropriately named Link-ZA. This paper expands on the implementation evolution and challenges of the standard over the last 10 years and provides a generic TDL Capability Model with a strategy for establishing interoperability between different implementations of the standard, thus establishing a SANDF tactical Network Enabled Capability.

### INTRODUCTION

#### What is Network Enabled Defence?

US Air Force Col John Richard Boyd developed the notion of the OODA (Observe-Orientate-Decide-Act) loop based on his experience as a fighter pilot. Boyd derived the notion that the adversary who could observe his enemy earlier, orientate towards threats quicker, decide which action to take faster and most effectively act out that decision would be most likely to be a victor of that battle [1]. Out of this notion the benefits for Network Centric Defence and Network Enabling Capabilities (NEC) for defence can be quantified.

Due to high cost of defence systems and the advent of multi-role military platforms, the requirement for Network Enabled Defence is even more imperative since it provides flexibility, interoperability and expansion of defence capabilities.

According to the South African Department of Defence (DoD) Information Strategy [2], a DoD strategy for Network Centric Defence was developed in response to these emerging theories of war. The SA DoD adopts and defines Network Centric Defence as “the capability inherent in the Defence Information and Communication Infrastructure to store, process and move essential data in planning, directing, coordinating and executing operations in digital format. It is all the normal functions of defence that can be done in a digital format”.

#### Why Tactical Data Links?

Voice communications via radio frequency (RF) communications systems has been the primary means of communications on the military battlefield since World War II. Furthermore Pike and Sherman [3] describe how World War II sparked the development of components and equipment that first allowed very high frequency (VHF) and ultra high frequency (UHF) communication systems. These voice communications did however impose severe limitations when coherent and detailed battlespace information needed to be conveyed. Voice communications proved to be slow and prone to misunderstanding, thus adding inefficiencies in the execution of the OODA loop.

Tactical Data Links (TDL) evolved from combining digitisation and RF communications technology in order to meet a growing defence requirement for systems that can exchange more information, faster and without ambiguity [4]. In this sense, TDLs are an enabler for Network Enabled

Defence and therefore a required Network Enabling Capability (NEC).

TDLs allow the exchange of digital information between command and control (C<sup>2</sup>) systems and weapons platforms. The types of information to be exchanged include platform positions, battlefield surveillance and intelligence, and mission management information. This exchange of information is required to allow defence forces to effectively manage the situational awareness, planning, tasking and control of their forces in the context of battlefield C<sup>2</sup> albeit it for conventional warfare or Operations Other Than War (OOTW).

### SOUTH AFRICAN TDL HISTORY

The requirement for TDLs in the SANDF was highlighted with the South African Strategic Defence Procurement Packages (SDPP) in 1999. South Africa embarked on the development of an indigenous South African TDL standard, now known as Link-ZA.

Most SDPPs were contracted with requirements for a Link-ZA capability. Platforms that would be Link-ZA compliant included fighter aircraft, Lead In Fighter Trainer (LIFT) aircraft, maritime helicopters, submarines as well as frigates. Subsequently Link-ZA became a requirement for most new systems in the SANDF and is pursued as part of achieving a Network Enabled Defence capability.

Delivery of the SDPP's started in 2005 with frigates and submarines and was followed by the LIFT aircraft in 2006, maritime helicopters in 2007 and fighter aircraft in 2009.

The impression by many was that Link-ZA compliance by the SDPP acquisition projects would imply message exchange interoperability between all these platforms. Disappointingly it was found that most platforms could only exchange information between similar type platforms.

Some of the reasons for interoperability inconsistencies are discussed below.

*No interoperability strategy.* In the requirements, specifications and development philosophies of SDPP platforms no consideration was given to utilising platforms as an integrated joint capability, thus concluding that no clear strategy or owner was driving crosscutting project capability requirements for Network Enabled Defence.

*Standard evolution.* It was assumed that using a single standard would ensure interoperability between platforms.

\* Interoperability Development Environment, Council for Scientific and Industrial Research, Pretoria, South Africa.