Industry News & Events | TDL Integration | Useful Resources

TDL Technology

6 Tactical Data Link Interoperability Testing
Compelling reasons to act now

12 Gordon Welchman
Father of TDLs

14 Airborne Early Warning (AEW)
Evolving the mission

Published by SyntheSys for the Tactical Data Links Community

Issue 10
Spring 2020

www.synthesys-defence.co.uk

SyntheSys DEFENCE

DATA LINK MANAGER
INTERFACE CONTROL OFFICER

2020 TRAINING DATES

LEARN HOW TO PLAN, DESIGN, MANAGE AND ANALYSE A MULTI-TDL NETWORK

Portugal, 4-22 May | The Netherlands, 29 June - 17 July
The Netherlands, 14 September - 2 October

For more information, including a detailed overview of how you will benefit from attending this course, plus booking information, visit:
https://bit.ly/2w9LxLv

SyntheSys DEFENCE

Letter from the MD

Editorial

Editor: Sarah Thomas
Email: sarah_thomas@synthesys.co.uk

Copy Editor: Penny Morgan
Email: penny_morgan@synthesys.co.uk

Contributors:
John S Hartas, Mark Hudspeth, Tony Castle
John Miller, Dan Quixote, Michael Morgan

With Special Thanks to:
Athanasios Chouliaras (Hellenic Air Force Colonel (Veteran), Aerospace & Defense Consultant, Airborne ISR-C2BM Platforms & EW Systems Evaluator.)
Thomas Withington (Armada International)

Printing:
Illustrated Stationery Ltd

Cover photo: Bletchley Park

Spring 2020 : Issue 10

To subscribe:
www.tdl-technology.com

Ten out of Ten for TDL Technology

Dr J S Hartas Managing Director

A proud milestone has been reached with the publication of this bumper tenth edition of TDL Technology magazine. To mark the occasion, I would like to look back at some of the most notable features throughout the last 10 issues and I would like to start by mentioning the invaluable contributions we receive from esteemed members of the Tactical Data Link (TDL) and wider community. I've continually reinforced that TDL Technology is built on an ethos of collaboration and knowledge sharing, and whilst we naturally share our own insights, we designed TDL Technology to benefit the community and we rely on a range of different views to achieve that.

With this sentiment in mind, special thanks go to all the organisations who have featured in TDL Technology as follows: Swedish Defence Material Administration (FMV) – Issue 1; Daronmont Technologies - Issue 2; Engility (SAIC) – Issue 3; Diginext – Issue 3; Lt Cdr Richard Lewis QVRM MCGI RNR (UK MOD) – Issue 3; Cobham – Issue 4; Viasat – Issue 4 / 6 / 9; Mass – Issue 4; Lt. Col. Volker Schaaf (Bundeswehr) – Issue 5; IT Insider – Issue 5; Maj Aaron Spreacher & Maj Sameek Parsa (United States Air Force) – Issue 8.

For this latest issue, we feature an article from Athanasios Chouliaras via Armada International (Page 14) which examines how the electronic support mission performed by Airborne Early Warning (AEW) aircraft is often overlooked and how this mission could be evolved.

Testing has been a regular theme throughout all 10 magazines; this is because we believe that TDL Testing is an area which requires much more attention throughout the community. As such, we have included a testing article with a slightly different approach on Page 6 of this issue. We also invite readers to perhaps re-visit some of the previous issues for further insights around TDL Testing.

We've had fun producing our 'Free Resources'. Some may have downloaded our Introduction to TDL Guide, the TDL Reference Guide, Quick Look TDL Comparison Table, TDL Interoperability Test Initiative Help Sheet, TDL Glossary of Terms, or our Guide to Choosing a TDL. All of these assets are still available for download via the SyntheSys Defence Community Portal, which is free to access. Sign up here: https://bit.ly/3a3L7VR

After a trip down memory lane, I would sincerely like to thank our readers and subscribers for continued support of the magazine and hope that Issue 10 proves to be entertaining and useful.

Very best regards

John S Hartas

Contents

News & Industry Events

5 SyntheSys News
The latest news from us

15 Industry Events
Dates for your diary

16 2020 Training Schedule
SyntheSys' Tactical Data Link (TDL) training courses open for enrolment

Technical Knowledge Bank

6 TDL Interoperability Testing
A 'stick' or 'carrot' approach?

10 Demystifying Tactical Data Links
Link 22 under the spotlight

Guest Articles

14 Best Supporting Actor
Evolving the Airborne Early Warning (AEW) mission

Features

8 Requirements Engineering
Using the scientific method

12 Father of TDLs
Homage to Gordon Welchman

SyntheSys News

SyntheSys Opens Additional Client Engagement Office in the Heart of Team Valley, Gateshead

In an exciting time of expansion, SyntheSys establishes a satellite base in Gateshead's Team Valley.

SyntheSys' headquarters will remain in Whitby, North Yorkshire, but the new office location will bring further opportunity for growth and will enhance the relationships the company has worked hard to forge over the past 30 years. Team Valley is just five miles from Newcastle City Centre and benefits from easy access by car, rail or air travel.

SyntheSys' Managing Director, John Hartas comments: ''We are proud of our heritage as a company born and bred in North Yorkshire, and the Whitby office will remain our headquarters. That being said, we are already feeling the benefits of having an office location which provides more convenient access to our national and international customers and we feel this is an opportunity for us to expand the business through access to a larger pool of professional talent.''

For more information about SyntheSys, including our portfolio of services and office addresses please visit: www.synthesys.co.uk.

If your organisation is based in the Team Valley or surrounding areas, we would love to grow our network and meet with you, contact us via: info@synthesys.co.uk or call: +44(0)1947 821464.

SyntheSys Technologies Maintains IBM® Gold Business Partner Status

Two years ago, we announced that we had achieved the prestigious 'Gold' partner status through the IBM® business partner certification programme and today we are thrilled to announce that we continue to maintain our IBM® Gold Business Partner Status.

Achieving the Gold Status is no mean feat and is something we are extremely proud of, having gone through a series of stages and assessments: to demonstrate our expert knowledge of IBM® tools; to confirm the satisfaction of our IBM® licence customers, and to demonstrate our ability to reach new customers.

We are expert providers of IBM® Engineering Lifecycle Management tools and have been using the powerful toolset as part of our Collaborative Engineering Management offering, which describes SyntheSys' approach to Engineering Management with expert personnel, process advice and tool support. We have helped many organisations increase their competitiveness through advice on processes, training and the introduction of software tools.

For more information about the work we have been doing with a range of engineering organisations in industries such as aerospace, defence, automotive, transportation and energy please visit: www.synthesys-technologies.co.uk or call: +44(0)1947 821464.

IBM Gold Business Partner™

What happens if you don't test interoperability.....
should we 'dangle a carrot' or 'beat you with a stick'?

Mark Hudspeth
Programme Director
SyntheSys Defence

When I was asked to write this article, I was asked to think of it from a different angle – "stick rather than carrot" I think was the phrase.

Anyway, it got me thinking (and those that know me may find that hard to believe!).

We, in the Tactical Data Link (TDL) industry (or industry in general), have a tendency to frame our business in a positive manner, it's all about 'features and benefits' and 'return on investment'.

Whilst it is obviously important to understand what you may get from product investment, or by undertaking some no doubt expensive work, it is also important to understand what the consequences are if you don't invest. Here is my article doing just that.

I have been involved in testing and trials just about continuously since 1993. My first trial was when I was in the Royal Air Force (RAF) and tasked with testing a Link 11 ground station (a Racal system if my memory serves me). Suffice it to say, the system failed the trial (which ironically in my view was a trial success!). What would have happened if we hadn't tested it?….well, it simply wouldn't have worked operationally as intended, the full effects of this are, of course, unknown.

Move forward 25 years, and with more modern TDL systems it may not be as clear cut as that simplistic example. The majority of intended functionality may support operational use, but failure of individual functions reduces capability, not just at platform level, but increasingly at force level.

More and more it is necessary to perform interoperability testing with coalition partners focusing on force level functions, not just against other national platforms. Answering the question 'what happens if you don't test interoperability?' is a challenge, so I have decided the best way to answer the question is to give a number of real-world examples of interoperability issues that I have observed.

Whilst I can't be specific about the platforms in the following examples, these are some examples of my experiences supporting platforms integrated into a coalition test environment over secure Wide Area Networks (WAN):

- There are many issues with digital aircraft control, reducing the effectiveness of being able to assign missions digitally without resorting to voice procedures, resulting in the operational community being unable to rely on the process consistently and therefore stopping using it / forgetting how to;

- A platform unable to process command orders dependent upon the population of the Friendly Weapon System data field. This would cause delays in executing the command, with the transmitting platform having to resort to voice procedures once the operator realises there is a digital issue.

- A data forwarding platform failing to forward command orders from Link 16 to Joint Range Extension Application Protocol Type C (JREAP C). JREAP platforms therefore unable to respond and failure of the digital function, resulting in delays in executing the command, and reversion back to voice procedures.

- A data forwarding platform failing to forward Precise Participant Location and Identification (PPLI) between Link 16 and JREAP C, resulting in loss of Situational Awareness (SA) and, more importantly, potential for more serious fratricide consequences;

- A platform making a fundamental decision to not process globally addressed messages. Relatively low impact in some situations but loss of SA and potential need to revert to voice if the transmitting platform even realises the platform hasn't received the information.

- A platform unable to process a received pointer message unless it's Source Track Number is in the first address field. The receiving platform will therefore lose SA, but the transmitting platform will not be aware that all of the intended recipients did not get the message, so may not resort to other procedures.

Rather ironically if we did not test interoperability, we would not have observed these issues and subsequently not been able to report and address them.

So, testing costs and it unveils issues that cost some more; cheaper not to, so let's not bother. Much better to ignore blue on blue engagements, air collisions and enemy fire and pin our hopes on it just not happening. After all we generally have work-arounds for these issues, such as revert to voice, it's good to talk, right?

Well I don't believe the previous paragraph any more than you do but we have to address the issues before they bite us in an operational environment.

So, what factors allow them to happen? It is a complex conundrum that platform integrators and platform teams responsible for a TDL-equipped platform continue to grapple with. I therefore leave you with some thoughts and conversation points on the possible causes:

- Funding and affordability is always a problem that platform teams struggle with, despite their best efforts to do the right thing;
- Pressure to get the platform into service and avoid requirements creep resulting in a 'fix it later' attitude. Does this really happen?
- Lack of knowledge / training. I once read a TDL requirement that simply stated that the platform shall be interoperable, which was accepted by the integrator. I still have the bruises from my head hitting the brick wall repeatedly.
- Are coordinated changes necessary, and how does that work programmatically? Can we ignore Information Exchange Requirements (IERs)? Or can we just do that when we think someone else should pay?
- How do you coordinate resolution of issues across different platforms? An even more complex issue between nations.
- Classification of data will always have a stranglehold on what we can do (for some very good reasons!). Interoperability, however, could be considered as the continued battle between the need to exchange information and the need to keep things to ourselves.

National governance may seek to give guidance and direction to platform teams, but without the funding, collaboration and coordination between platforms, and ultimately nations, I can only see that issues will continue to remain and be discovered, and so a detailed understanding of them is necessary to allow for their mitigation. Ultimately, testing is important and apart from giving me the excuse to allow my sarcastic juices to flow in this article, it is fundamental as the first step in finding and informing on information exchange between TDL-equipped platforms.

I would love to hear your views on this article and the discussion points, but remember, only if your grammar and punctuation is correct or my system will discard your communication and we will have to revert to voice. *(Tongue firmly in cheek.)*

Requirements Engineering

It's well known that the implementation and testing of Tactical Data Links and associated military platforms is high cost.

The application of proven requirements engineering methods provides systems engineers with a robust method for fulfilling operator, policy and other stakeholder requirements. But, getting users to articulate their needs can often be a challenging process. No process can pull information out of the void when it doesn't exist, but systems engineering takes a robust and scientific approach to requirements management that cleanly and specifically identifies ambiguities and gaps in stated stakeholder needs.

The best way to get a straight answer is to ask a straight question, and the systems engineering process is very good at generating straight questions.

Working with vague or incomplete requirements doesn't just lead to a risk of building the wrong product: it can also risk building the right product badly. Effective projects run individual management tasks rigorously and efficiently, and the ability to follow a rigorous process is severely hindered by a lack of robust inputs. Problems that arise in this way only multiply over time as knock-on effects are generated and start introducing chaos of their own.

The process begins by identifying what users want in terms of a problem that they need to solve, or an opportunity that they want to pursue. Without yet looking to specific solutions, the first step is to develop the 'operational concept': what users want the system to do. The context and environment for the system – its basic inputs and outputs – should be understood as clearly as possible while the system as a whole is still being treated as a black box. It is important even at this stage to look past acquisition, towards deployment, configuration management, support and retirement.

In a systems engineering process, only then do you start to formally investigate the sorts of systems which could solve the user's problem. This should begin by generating as many ideas as possible about what should go in the black box, and at this stage should not progress beyond identifying a preferred class of solutions. It has been a long-standing maxim in organisational psychology that the most efficient way to solve a problem is to discuss it for as long as possible before proposing solutions; systems engineering embraces this as a philosophy for the stakeholder relationship.

The next step is to identify as wide a set of stakeholders for the system as possible, and talk to users as directly as you can about what their needs for the system will be. If the low priority or impracticality of these needs isn't trivially obvious, this analysis generally falls into a later stage.

In other words, getting stakeholder needs begins by being as open-minded as you can, in as broad a conversation as possible. From there, the job of the systems engineer becomes that of turning these needs into formalised requirements.

Using the Scientific Method for Requirements

The philosopher of science Karl Popper famously said that for a statement to be considered scientific, it must be falsifiable: you have to be able to tell the difference between a world in which the statement is true and a world in which its false. Similarly, systems engineers work towards requirements by which it is possible to tell the difference between a system that achieves them and one that doesn't.

Specifically, this means all requirements have to be individually:

- **Clear** (concise, limited to one idea, impossible to misinterpret);
- **Verifiable** (related to a specific, identifiable test of success);
- **Functional** (describe what is to be done, not how it is to be done);
- **Feasible** (technically achievable, with acceptable research risks);
- **Compliant** (compatible with regulatory and governance constraints);
- **Traceable** (related to specific higher-level requirements and ultimately stakeholder needs);
- **Unique** (not replicating other requirements); and
- **Minimal** (describe only "must haves", not "nice to haves"); and taken together they must be:
    - **Complete** (define the system in its entirety); and
    - **Consistent** (not contradicting one another, including not contradicting cost and time requirements).

By forcing requirements to be specified in this way, systems engineers can be thoroughly robust and scientific in developing a system model, and can identify in specific terms the straight questions that need to be asked of stakeholders to define the system properly.

Systems engineers also take a comparably atomised approach to risk: "if [event] then [consequence for stakeholder]". Risk assessment needs to begin at, or before, the requirements phase, and while requirements are being defined the systems engineer must also look to asking what the consequences of the likelihood of failing to meet those requirements would be.

By treating the requirements engineering process like generating a scientific hypothesis, systems engineering can generate sophisticated whole-system models, and enforce robust standards for verification and validation.

We believe this process is the best way to ensure accuracy and quality in any development process.

Demystifying Tactical Data Links (TDLs)

Focus on Link 22

Tony Castle
Defence Business
Group Manager

In the last edition of TDL Technology, in our series on the demystification of TDLs, we provided a general overview of TDL systems in use today.

For this edition we will examine just one of those TDLs which is seen as the 'new kid on the block', Link 22. The article will aim to give a general overview of Link 22 and also focus on what this relatively new system provides, that we don't get from the other systems. Note that this article is very much at an introductory level; we would be pleased to provide more information on request.

Introduction

Due to the lack of Electronic Counter Measures (ECM) resistance provided by Link 11 using an easily jammable single frequency system, and a lack of Beyond Line-Of-Sight (BLOS) capability when using Multifunctional Information Distribution System (MIDS)/Link 16 (without relay), North Atlantic Treaty Organisation (NATO) recognised the need for a new system which could overcome both of these issues. This was particularly important for naval platforms, as MIDS/Link 16 using Ultra High Frequency (UHF) would only provide connectivity for around 20 miles. To achieve Link 16 connectivity over greater distances airborne relay platforms would be desirable, however, not always available. Hence Link 22 was born to overcome these problems, while also providing several other improvements over Link 11. The aims of Link 22 may be described as: to replace Link 11, thereby removing its inherent limitations; to improve allied interoperability; to complement Link 16; and to enhance the commanders' war fighting capability.

Link 22 History

Canada, France, Germany, Italy, Spain, United Kingdom and the United States of America signed a Memorandum of Understanding (MOU) to develop and sustain the core products necessary to meet the NATO requirements for Link 22. These seven nations are referred to as the NILE Nations. The core element of the Link 22 system, the System Network Controller (SNC) has been jointly developed by the NILE nations. The SNC software is only available through the NILE programme office, the aim being to ensure Interoperability (IO) between users who will all be using the same software. The other elements of a complete Link 22 system, the Tactical Data System (TDS), the Data Link Processor (DLP), the SNC, and the radios, are procured as a national responsibility. The final element, the Link Level Communications Security (COMSEC) (LLC) unit has been developed in the United States (US) and is available via US Foreign Military Sales (FMS) procedures.

What does Link 22 Provide for Us?

In the introduction above we have touched on Link 22's ability to provide a jam resistant capability, and also to overcome BLOS issues, but what else is provided?

The major improvements are summarised below:

- High Frequency (HF) and UHF Line-Of-Sight (LOS);
- When using UHF, two operational modes are available: Fixed Frequency (FF), or frequency hopping in the Electronic Protection Measures (EPM) mode, which provides anti-jamming.
- Various waveforms that allow selection of resilience versus throughput to adapt to every propagation condition;
- Automatic relay between all NILE Units (NUs) using available networks without the need of an airborne relay;
- Network Management is highly automated, relatively simple and includes features such as dynamic bandwidth allocation;
- No requirement for a Net Control Station (NCS). Designed with no single point of failure.
- Link 22 messages are part of the J-Series family (specifically F and F/J messages). Link 22 uses the same data dictionary as Link 16 and thus makes translation and forwarding relatively easy compared to Link 11.
- Time Division Multiple Access (TDMA), without the need for a Network Time Reference (NTR);
- Late Network Entry (LNE) capability to allow units to join the network seamlessly after initiation;
- Flexible Addressing techniques, allowing more efficient delivery of data.

To better understand the improvements in the above list, we will now take a more detailed look at each element.

HF and UHF Line-Of-Sight

Link 22 has been designed to use the same HF and UHF frequency bands as Link 11 (UHF 225-400 MHz, HF 2-30 MHz). Therefore Link 11 radios may be re-used for Link 22 fixed frequency operations. UHF radios will provide short range LOS communications, whereas HF provides for BLOS communications. See also the paragraph on Automatic Relay.

UHF EPM

An anti-jamming capability can be achieved when using UHF by utilising frequency hopping radios. This capability was also originally planned for HF, but the development of frequency hopping HF radios for Link 22 appears to have been shelved. UHF EPM radios will hop within the same band as utilised by the fixed frequency system. EPM radios will require a Time Of Day (TOD) input to achieve synchronisation with their peer systems.

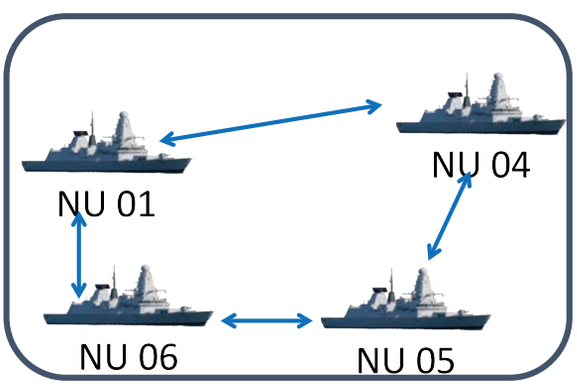
Waveforms

The selection of differing waveforms allows Link 22 to provide reliable data exchange in poor conditions, and also to optimise the media for operations in good conditions. However, optimisation of the media to achieve best reliability, will generally result in a reduction of throughput.

When using HF, or UHF EPM, a parameter known as the Media Setting Number (MSN) will determine the reliability versus throughput selection. When initialising a Link 22 network, it is possible to utilise a function known as Probing, which allows the selected frequency to be tested using various MSNs before selecting the preferred option. A further function known as Fragmentation Rate, which determines how data is fragmented before transmission is also available, and will further affect the throughput and robustness of transmissions.

Automatic Relay

To overcome the UHF LOS issue, and to assist where HF propagation does not achieve the desired connectivity, automatic relay may be employed. Units carrying out the relay function do not require specific transmission capacity for relay (like Link 16), they will simply utilise their existing capacity to relay appropriate messages. The SNC will determine the most efficient relay path based on connectivity information shared between active units. In the diagram below, if NU01 needs to send data to NU05, 2 relay paths are available (via NU04 or NU06). The SNC will determine the most efficient path to use.



Network Management

Network Management (NM) is a mainly automated function, vastly decreasing the requirement for operator interaction. This is achieved through the use of system generated NM messages. The management of the Link 22 network is designated through 2 duties, the Super Network Management Unit (SNMU) who is responsible for the whole architecture (which may comprise of up to 8 individual networks), and a Network Management Unit (NMU) who is responsible for their own network, reporting upwards to the SNMU.

Net Control Station

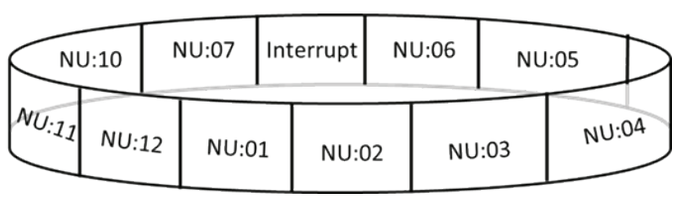
Link 22 has been designed to operate as a non-nodal system without any single point of failure. Time synchronisation for frequency hopping radios, and transmission opportunities is provided by the TOD input. The NM duties of SNMU and NMU may be handed over to a standby unit automatically if no transmission is received from those units after a specified period of time. Where automatic relay is being used, the system will recognise units leaving the network, and will automatically route data via other available paths.

Link 22 Messages

Link 22 utilises a combination of F and FJ-Series messages to pass tactical data. These messages are part of the J-Series message family, and as such are planned for development for the foreseeable future. FJ messages are replicas of their Link 16 J- Series counterparts, whereas F messages are unique to Link 22. Due to their transmission characteristics these messages provide for a more efficient use of the available bandwidth. For example, in Link 22 the Identification Friend or Foe (IFF) message can be sent without the associated track update message, however, in Link 16 to achieve the same update both initial and continuation words of a track message would need to be sent. Link 22 also uses a separate set of variable format technical messages for NM and other network maintenance functions.

Time Division Multiple Access

Link 22 transmission capacity is divided amongst users based on their requirements. Each transmitting unit is allocated an Assignment Slot, the size of which will be based on their required transmission capacity. Time synchronisation for the assignment slots is provided by the TOD. Once the network is established, Dynamic TDMA may be used to reallocate capacity between users. This dynamic reallocation is carried out automatically between units; its use will be enabled and disabled by the NMU using a technical message. An Interrupt slot may also be provided allowing units to transmit high priority messages outside their Assignment Slot.



Link 22 TDMA Example

Late Network Entry

Link 22 provides this facility which allows units who were not able to join the network at start-up to join an established network. The LNE protocol, will be operator initiated, but will generally then be automatic. The joining unit will be provided with all the parameters required and will be instructed which network(s) it may then join. Transmission capacity will also be allocated via this protocol.

Flexible Addressing

Link 22 provides various addressing capabilities designed to make best use of the available bandwidth. The capabilities are:

- **Totalcast**
  Where all units in a Super Network are addressed;
- **Neighbourcast**
  Where all units within RF range are addressed;
- **Mission Area Sub Network (MASN)**
  Messages will be addressed to a specified group of units with a shared operational interest (e.g. Electronic Warfare) who may or may not be in the same Network. MASNs may be predefined, or created / altered during operations, on order of SNMU.
- **Dynamic List**
  A non pre-defined list of between 2 and 5 units to which messages will be sent;
- **Point to Point**
  A single unit is addressed.

Summary

This article has been created with the aim of providing a high-level overview of some of the functionality provided by Link 22, and how it has been designed to make the most efficient use of the system. We will welcome any observations or questions.

Father of Tactical Data Links

Gordon Welchman

World War Two (WW2) codebreaking ace Gordon Welchman can justifiably be described as one of the founding fathers of modern-day Tactical Data Links. Although subsequently overshadowed by the fame of Bletchley Park colleague Alan Turing, Cambridge University maths genius Welchman was Turing's equal in the cracking of the Nazi Enigma code which led to the Allies being able to read most of the key German military's secret messages during the worldwide conflict.

German Enigma Machine

And unlike Turing, after the war had ended, Welchman emigrated to America and was responsible for helping to develop the Joint Tactical Information Distribution System (JTIDS) – the military communications TDL system still in use today in the United States (US) and with North Atlantic Treaty Organisation (NATO) forces. This supports data communications principally in air, surface and land situational awareness and command control utilising Link 16, one of the most popular tactical data links.

Just before the outbreak of WW2 in 1939, Welchman was contacted by Commander Alastair Denniston and invited to join the Government Code and Cypher School (GCCS). GCCS had established a "Station X" centre for the decryption and analysis of mostly German encrypted messages at Bletchley Park (BP), a country mansion conveniently situated between the Oxford and Cambridge universities which supplied many of its codebreaking recruits.

Welchman was one of four key early recruits to BP, along with Alan Turing, Hugh Alexander, and Stuart Milner-Barry. Ultimately, Turing became the most famous of these, but all the others made major contributions to the work. They were also the four signatories to an urgent letter to Prime Minister Winston Churchill in October 1941, pleading for more resources for the vital code-breaking work at BP. Churchill immediately recognised the importance of the work and responded with one of his famous 'Action This Day' written comments, subsequently giving the code breakers all the resources they required.

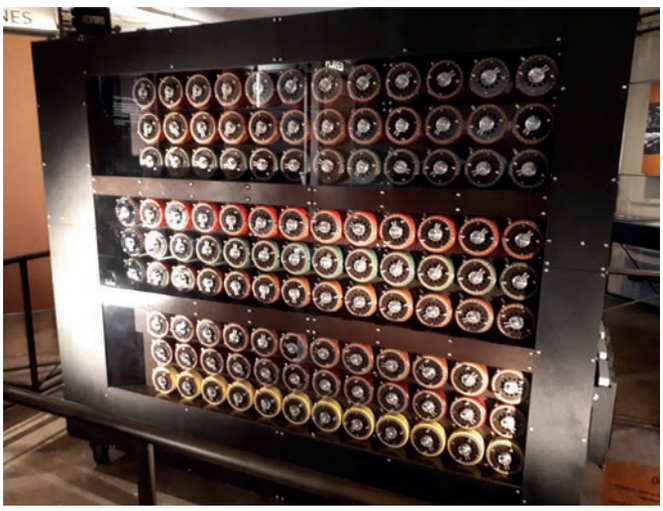
So important was the secret work carried out, that the intelligence gleaned was regarded as above even Top Secret, being designated as 'Ultra' Secret; Churchill ordered that it was to remain classified at all cost. Much of Welchman's work at Bletchley was in developing 'traffic analysis' of encrypted German communications. This involved the interception and analysis of data detailing which enemy units sent and received messages. The places and timings were also recorded. This complex, meticulous analysis and pattern matching revealed a plethora of information about enemy organisation, movements and activities, even though the messages themselves remained unbroken.

Welchman is acknowledged for creating this technique which became adopted into common use, and is still utilised by US and NATO forces, even today. However, like Turing, Welchman's main contributions were in the process of breaking the now famous and crucial German Enigma machine cipher.

Welchman was one of the two main key codebreakers with Turing and he became head of Hut Six, the section at BP that had the responsibility for breaking German Army and Air Force Enigma ciphers. In the run up to the outbreak of war, Polish cryptanalysts had developed what they called the Bomba, an electromechanical device which could find the Enigma settings used by German operators. This was smuggled to Britain where Turing painstakingly improved the Polish design. However, Welchman then made an astounding breakthrough. He invented the Diagonal Board, an addition to the British Bombe, which made it immensely more powerful. The Diagonal Board enabled the Bombe to solve the Enigma plugboard setting separately from the wheel setting with which the Germans randomly programmed their Enigma machines. In plain language, Welchman's brainwave reduced the time needed to find the complete setting from days to hours.

As head of Hut Six, Welchman was also closely involved in other work which resulted in breaks into Enigma by identifying German operational lapses. Amazingly, these were quite extensive, and Welchman's experience in this field helped guide his later US work on making military communications secure.

Welchman was a brilliant organiser and these instinctive abilities were instrumental in making Bletchley Park the most efficient code cracking centre of the entire war. He left Hut Six in 1943, to become Assistant Director for Mechanisation with responsibilities including the construction, deployment, and operation of more Bombes. By the end of the war, a multitude of Bombes were in use at BP and other locations in the United Kingdom (UK). Welchman also had responsibility for cryptographic liaison with the US, which built and used many additional Bombes. He was also responsible for making sure that the British and American Bombes' operators were not wasting time by working on the same keys, and that all solutions were reported to the other group.



Bombe Machine

But a key interest at this time also was the development of similar machines for cracking even more advanced German ciphers, such as the Geheimschrieber used by the German High Command. Welchman's contribution and the overall codebreaking activities at Bletchley Park are considered to have shortened the length of the war by a matter of years – a crucial result for the Allies.

Welchman was awarded the Order of the British Empire (OBE) in the 1944 King's Birthday Honours list. The London Gazette described him at the time as "William Gordon Welchman, Esq., employed in a Department of the Foreign Office" in a ruse to hide his true secret activities. The codebreaking at Bletchley Park, famously known as Ultra, was kept Top Secret during the war, and for many years afterwards those involved were forbidden to talk about their vital work.

After the end of the war, Welchman became Director of Research for the John Lewis Partnership. In 1948, he emigrated to the US where he taught the first computer science course. Afterwards he was employed by Remington Rand and Ferranti. He became a US citizen in 1962 and joined the MITRE Corporation, working on what became known as secure JTIDS communications systems for the US military. He retired in 1971 but was retained as a consultant. He led a team specifically developing the Time Division Multiple Access (TDMA) algorithms for frequency hopping and cypher protection. JTIDS began with an advanced planning study sponsored by the Air Force Electronic Systems Division (ESD) Advanced Plans (XR) at L.G. Hanscom Field.

Welchman later caused a storm by writing a book called 'The Hut Six Story' which described his clandestine wartime activities in detail and contained some information about his work at MITRE. The US National Security Agency strongly disapproved, as the book went into too much detail. The book was not banned, but Welchman lost his security clearance and his consultancy with MITRE and was forbidden to discuss either the book or his wartime work.
It was a stinging rebuke for such a towering wartime hero.

He died in 1985. His final conclusions and corrections to the story of wartime code breaking were published posthumously in 1986 in the paper 'From Polish Bomba to British Bombe: the Birth of Ultra' in Intelligence & National Security, Vol 1, No 1. The paper was also included in a revised edition of 'The Hut Six Story' published in 1997 by M & M Baldwin.

As the years slipped by, he gradually became the forgotten genius of Bletchley Park, until an acclaimed biography and TV documentary reminded the nation of his heroic efforts to defeat the Nazi war machine in the dark days of WW2.
Today many agree that he ranks as an equal to Alan Turing in the now famous and no longer clandestine Ultra secret story.

Sources:
Bletchley Park remembers forgotten genius Gordon Welchman by Alexander J. Martin 2015.
Gordon Welchman Post exhibition Bletchley Park.
Gordon Welchman Crypto Museum.
Gordon Welchman Sparticus Educational.
Gordon Welchman 1906 – 1985 mathshistory standrews.ac.uk
Wikipedia

Best Supporting Actor

Athanasios Chouliaras believes that AEW ESMs must grow in capability to meet emerging threats; an increasingly contested and congested electromagnetic environment and the need to share signals intelligence with other users.

The electronic support mission performed by Airborne Early Warning (AEW) aircraft is often overlooked. AEW and tactical data links expert Athanasios Chouliaras shares his thoughts on how this mission could evolve.

AEW aircraft use Electronic Support Measures (ESMs) to detect, locate and identify friendly and hostile ground-based, naval and airborne radars to associate them with specific platforms. This not only helps to build an accurate electronic Order-of-Battle (ORBAT) of friendly and hostile forces, but enables the early detection of threats.

For comparison: Condor Systems' AN/AYR-1 ESM outfitting the Boeing E-3 Sentry series of AEW aircraft can detect threats transmitting in a two gigahertz/GHz to 18GHz waveband at ranges of circa 300 nautical miles/nm (556 kilometres/km); the E-3 series' Northrop Grumman AN/APY-1/2 S-band (2.3GHz to 2.5GHz/2.7GHz to 3.7GHz) AEW radar meanwhile, has an instrumented range of 216nm (400km). The early warning implications of this ESM's performance are thus clear.

Mr. Chouliaras believes it is essential that AEW ESM technology evolves to ensure it remains abreast of emerging threats. He stresses the need to employ "modern digital receivers" which provide more accurate radar detection, location and identification data compared to some current AEW ESMs. Allied to this is the need for integrated ESMs to perform fast multi-emitter data processing, and intra-pulse analysis. Given that contemporary radars employ a myriad of low probability of detection/identification techniques to mask their transmissions such pulse-by-pulse analysis will help to build a clear picture of a radar's location and identity from seemingly disparate transmissions. Such approaches will be helped in no small measure, Mr. Chouliaras posits, by the employment of powerful processors and spectrum analysers.

AEW ESMs will have to perform these tasks in increasingly dense electromagnetic environments. The global increase expected in civilian and military radar proliferation, not to mention the growing civilian reliance on the spectrum for the carriage of wireless IP (Internet Protocol) traffic provides an ever-increasing deluge of noise in which the signal of interest can hide.

Mr. Chouliaras emphasises that ESMs must be capable of working efficiently in such an environment. He continues that AEW ESMs should also be capable of gathering communications intelligence to separate these emissions from radar signals. This would mean that the ESM can "exploit and record the data separately for each category".

Other imperatives include the ability of ESMs to accurately record data for post-mission analysis; an important consideration when a specific signal has not been programmed into the aircraft's ESM library, and may indicate a new emitter in the aircraft's locale. Equally important is the ability of the electronic support measure to share its tactical information with the AEW aircraft's mission systems and with other airborne and ground-based participants in a Tactical Data Link (TDL) network who depend upon a timely and accurate electronic ORBAT. He states that the ability to clearly visualise emitter characteristics fused with AEW radar track information will improve the situational awareness of the AEW mission systems operators, and participants in the air battle, yet further. All the networked participants should also be able to easily access such information on an integrated network.

Cloud computing may be one mechanism to achieve this, particularly given the data rate limitations of TDLs such as the North Atlantic Treaty Organisation's Link 16. This typically handles data at rates of between 31.6 kilobits-per-second (kbps) and 115.2kbps.

Since AEW aircraft first began to be used en masse with the advent of the US Navy and US Air Force Lockheed EC-121 Warning Star series planes from 1954 onwards, the mission has evolved continuously as technology has increased in sophistication.

Ensuring that the ESMs equipping AEW aircraft are as capable as possible will help this mission to grow in precision, accuracy and relevance in the coming years.

https://armadainternational.com/electronic-warfare/

Reproduced with permission from:

https://armadainternational.com/2019/09/best-supporting-actor/

INDUSTRY EVENTS 2020

23-26 March

23rd NATO TACTICAL DATA LINK SYMPOSIUM (NTDLS) 2020

Calpe, Spain

05 May

International Data Links Society (IDLSoc) UK Chapter Meeting 2020

Lincoln, UK

26-28 May

Tactical Communications Forum (TCF) 2020

Kaunas, Lithuania

26-28 May

Diginext TDL&S Symposium 2020

Aix-en-Provence, France

27-29 October

International Data Link Symposium (IDLS) 2020

Herning, Denmark

TRAINING DATES FOR 2020

10-11 MARCH	LINK 22
24-27 MARCH	VARIABLE MESSAGE FORMAT over COMBAT NET RADIO / JOINT RANGE EXTENSION APPLICATION PROTOCOL (VMF over CNR / JREAP)
4-22 MAY	DATA LINK MANAGER / INTERFACE CONTROL OFFICER (DLM/ICO)
23-24 JUNE	JOINT RANGE EXTENSION APPLICATION PROTOCOL (JREAP)
29 JUNE - 17 JULY	DLM/ICO
4-6 AUGUST	MULTIFUNCTIONAL INFORMATION DISTRIBUTION SYSTEM (MIDS) LINK 16
14 SEPT - 2 OCT	DLM/ICO
13-14 OCTOBER	LINK 22
17-19 NOVEMBER	VMF over CNR
8-9 DECEMBER	JREAP

We take a flexible approach to delivering our training. All of our courses can be held at customer premises globally as required. We tailor our training according to customers' needs and abilities. For more information, please visit: https://bit.ly/2w9LxLv

SyntheSys DEFENCE