Applying the Layered Enterprise Data Safety Model



The Glade of Light memorial opened in 2022 to commemorate the victims of the Manchester Arena bombing of 2017, one of the deadliest terrorist attacks in the UK. Nick Hales examines how the Layered Enterprise Data Safety Model (LEDSM) and supportive techniques can provide insights into how to prevent the worst aspects of an attack of this nature and in managing the sharing of information in its aftermath.

The Manchester Arena suicide bombing was an example of how badly emergency services safety communication can fail the public, despite the fact that the multi-agency integrated emergency management process is statutory under the Civil Contingencies Act 2004 and is referred to as a Local Resilience Forum. The report from the Public Enquiry highlighted that duties of the responders include "*to cooperate; to share information; to assess risks in their area; to plan for emergencies".* Unfortunately, it is clear the emergency services failed in these four areas because they assumed:

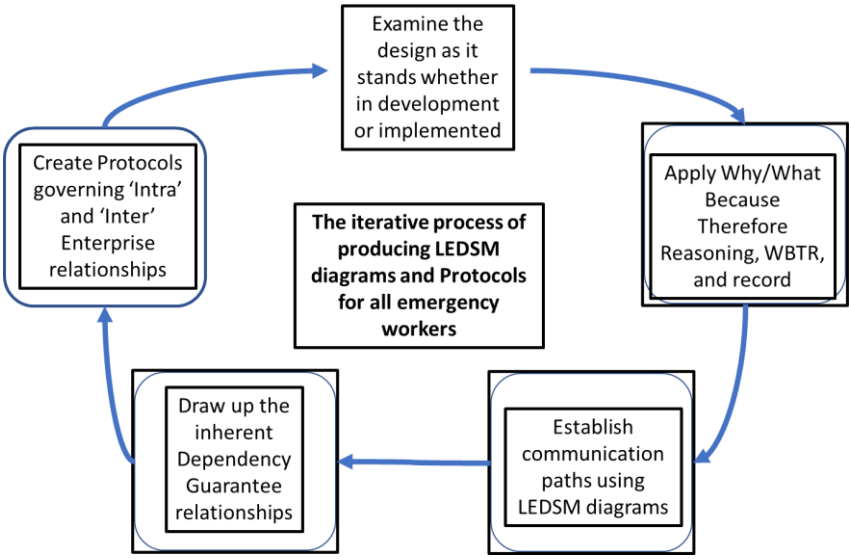
- the cooperating and sharing of information had been thought through in planning
- cooperating and sharing information would be simple
- risks had been assessed by someone and mitigated
- the granularity of analyses would enable effective action and all would know what to do

It is for those reasons that the incident has been chosen to illustrate how the LEDSM [1] process can effectively prepare the communication network for emergencies. The importance of communication is illustrated by examining the Joint Emergency Service Interoperability Principles, (JESIP), which feature in the inquiry report and are listed here with annotations by the author:

- Co-location (to improve communication)
- Communication (that is what this article is about)
- Coordination (facilitated by effective communication)
- Joint Understanding of Risk (one big risk being poor communication)
- Shared Situational Awareness (facilitated by reliable and available communication networks)

Brief Recap on LEDSM

- The term LEDSM is used because not all important, independent nodes of a network are necessarily organisations. Just like businesses, Enterprises can be one person or many, and this is reflected in the many to one and one to many relationships involved in LEDSM planning. The flexibility and granularity of LEDSM diagrams means that communication from a multi-level LEDSM can connect with one person who owns their own single level Enterprise.
- In electronics, a seven layer model has been used to establish most communication between machines, the Open Systems Interconnection (OSI). It is considered that a seven layer model at maximum for any enterprise in a network should be adequate for emergency communication planning. Although somewhat arbitrary, it is considered that anything larger than the number of levels complex electronics manages with, would become cumbersome and begin therefore to make successful communication less likely.
- The process of LEDSM analysis including associated techniques is illustrated in the figure below (See [1] for further information and diagrams)



Detail relevant to the Manchester Arena concert bombing is given later in the text. Any Enterprise may have many links from various layers but the use of LEDSM diagram enables appropriate granularity so that those connections to Enterprises not involved in the problem being addressed may be omitted, even down to individuals being offered their own LEDSM diagram with just the connections they need to make shown.

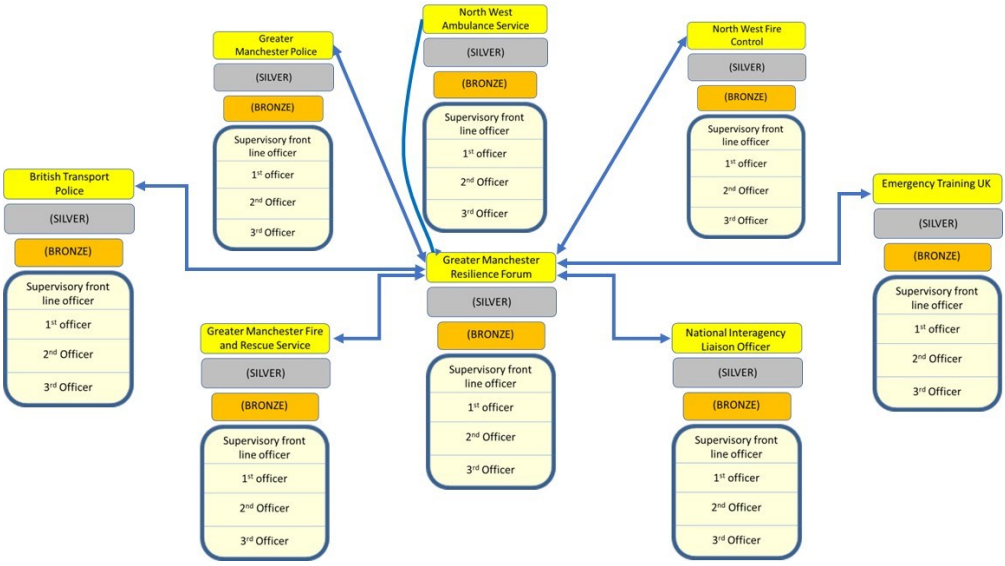
Identification of Partner Organisations

This article does not go in depth into the identification of partner Enterprises though that is an important part of de-risking any safety critical event or process as that is a choice of the organisations involved. Here the Enterprises that were involved are simply shown below in a LEDSM maximum configuration diagram, (i.e. with seven layers that not each Enterprise may eventually use but is always a useful starting point).

The lower levels are equivalent to the electronic checking levels in the OSI model. They represent those operatives who may or may not currently be involved in the creation of Protocols, suggestions for other Enterprises to be involved, the development of Dependency-Guarantee relationships, or links to higher and lower ranking persons that full analysis of potential emergency events may prove to be potentially beneficial.

The links shown are simply those between the Gold or in LEDSM terms Enterprise level and the Resilience Forum as complex relationships at a top level abstraction are not possible unless on very large sheets of paper.

The convention of referring to the top three levels as Gold, Silver and Bronze, as used by the Manchester Resilience Forum is used throughout to ensure the Inquiry Report terminology and this paper are easily understood.



Timeline of Events

Having established the primary Enterprises involved in an Emergency in Manchester, those involved would move to the next stage and then go through the cyclical process, as illustrated in the first figure.

To show the effectiveness of LEDSM, and how it would reduce risk, a timeline of events is used which is given in the following table. It shows a few of the problems in the first ten minutes of the incident and comments indicating more detail of the failures. Only a subset of the full plethora of problems that occurred in the golden hour immediately after the bomb, in which lives can generally be saved, can practically be reproduced in this article. Indeed, even the problems of first ten minutes, as given by the Inquiry Report [2] had to be reduced to some of the most significant.

TIME	ACTION	COMMENT
22.31	Bomb goes off	
22.32	NWAS should have contacted their Hazardous Area Response Team (HART)	It took until 22.39 for Tactical Commander Annemarie Rooney to tell the GMP HART to employ their specialist skills at the bombing site.
22.34	GMP control duty officer Inspector Sexton	Takes Gold and Silver GMP roles as well as both Tactical and Strategic Firearms Commander roles
22.35	Inspector Sexton should have declared a "MAJOR INCIDENT"	Total failure of training. As Gold Commander he must take total responsibility for this.
22.36	NWFC control should have mobilised GMFRS	In the absence of LEDSM protocols, NWFC supervisor prevents mobilisation insisting that a National Interagency Liaison Officer (NILO) must be consulted first.
22.36	BTP officers at the site of the bomb fail to declare a MAJOR INCIDENT and fail to send a METHANE message	LEDSM protocols carried with officers detailing their expected behaviour would have ensured the required messages were passed on.
22.36	NWAS control tries to Contact GMP but has to wait in a queue for 2 minues	LEDSM analysis would have shown a reserved radio channel was an essential fall back measure for lack of telephone communication as would multiple telephone options including land-line and mobiles.
22.36	GMP Inspector Michael Smith declared a Rendezvous Point (RVP) to GMP control	In the event the message was only passed to NWFC in reasonable time 22.40 but other organisations did not get it or got it an hour later, (GMFRS at 23.54).
22.37	ETUK personnel did not pass on a METHANE message to NWAS as ther training instructed them to do.	The LEDSM analyses would have identified this as a protocol and a Dependency-Guarantee relationship established that would and should be a high priority and wold have been know to be such by ETUK staff
22.37	Incident log at BTP records inability to contact GMP	LEDSM analysis would have shown the need for multiple channels of communication between the Enterprises.

What/Why Because Therefore Reasoning, (WBTR)

LEDSM applied to any system, whether it is human only, human and machine or machine to machine communication, is firstly about one loss, the 'loss of correct communication'. 'Correct' being used here as a term that encompasses timeliness, availability and accuracy among other qualitative terminology. Secondly, it is about capturing concerns visually. Hence, in the WBTR stage, conversations may take place such as the hypothetical one given here in dialogue involving a Front Line Officer, (FLO) and a BRONZE Commander, (BC):

FLO:- If I am first at the scene WHAT do I or my team members need to do to inform others of the scene?

BC:- One of you will need to send a METHANE message. The question is WHAT could go wrong?

FLO:- I might get injured or killed.

BC:- OK, then we need all your team trained to send the METHANE message.

These conversations can then be gathered into formal decisions as to what must happen, as below.

WHY/WHAT	**BECAUSE**	**THEREFORE**
What to do if first at scene	METHANE messages are priority	Need appropriate comms and training
What if dedicated METHANE officer cannot send	There may be hazards that injure or at worst kill the officer	Other trained and equipped personnel needed
Why might the METHANE message not get through	Jammed lines or problem broadcasts like interference	Extra diverse communication needed
Why does everyone need two channels	All need to know the METHANE message and one channel may fail	Diverse comms needed for all involved
What Enterprises need METHANE messages	All Resilience Forum members need METHANE data	Have group phone number and a common radio channel
What if mobile and radio channels are down	The METHANE message and others agreed are essential	Declare METHANE as text message and move position until it is sent by the mobile

When WBTR is used, one can start with a picture of an envisaged system or one may have to start with something only understood in verbal terms at the outset. This is why the Manchester Arena bombing is a good example to describe here as it is only one of many scenarios the emergency services may get caught up in, e.g. a plane crash as at Lockerbie, or a pub blast, none of which can be pictured particularly well in the initial analysis because of the variety of locations at which an emergency can occur.

As can be seen, the problems in communication should not have occurred if this formal methodology had been used as they are plain to see and moreover, in the next sections the development of the LEDSM diagram can be shown to produce an easily understood (and adjustable if necessary) picture of who should be contacting which role in which Enterprise.

The Initial Internal LEDSM Block

A meeting will need to be called at this point for the first iteration of the cyclic LEDSM process introduced earlier. This meeting is best facilitated by Suitably Qualified and Experienced Personnel, (SQEP). It would be only a matter of guessing what partner stakeholder Enterprises require and may supply in terms of data. Therefore, it is important to establish a LEDSM Block of one's Enterprise to provide an opening gambit for the subsequent meeting with other stakeholder Enterprises, members of the Resilience Forum in this case.

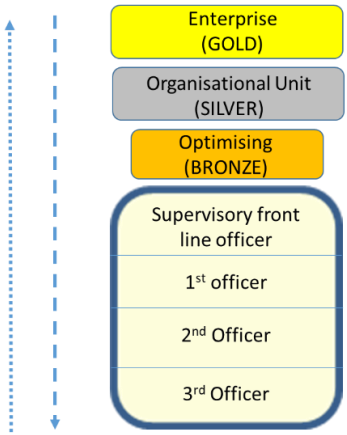
Some negotiation of positions on necessary LEDSM levels and who communicates to whom will be required internally, prior to the negotiations on positions in other Enterprises. The fundamental of this phase, is to establish the protocols that define the data that will be passed up and down internally in the Enterprise, the intra-communication as shown in next figure that shows the (up to 7) levels in an Enterprise between each of which protocols will exist.

These protocols will define information from the Managerial level downwards (dashed), and personnel offering suggestions upwards to change their protocol (dotted). The top three levels may be considered equivalent to the Gold, Silver and Bronze levels in the current command and control structures.

In the case used here, British Transport Police (BTP) are to contact Greater Manchester Police (GMP) with a METHANE message, which stands for:

- **M**ajor Incident?
- **E**xact location?
- **T**ype of incident?
- **H**azards?
- **A**ccessibility?
- **N**umbers of casualties?
- **E**mergency services attending?

The relevant instruction among all the protocol instructions from the GOLD Enterprise level downward in this Inter-Enterprise protocol creation phase, would be simply to "Complete a METHANE message and send to all other Enterprises requiring it".



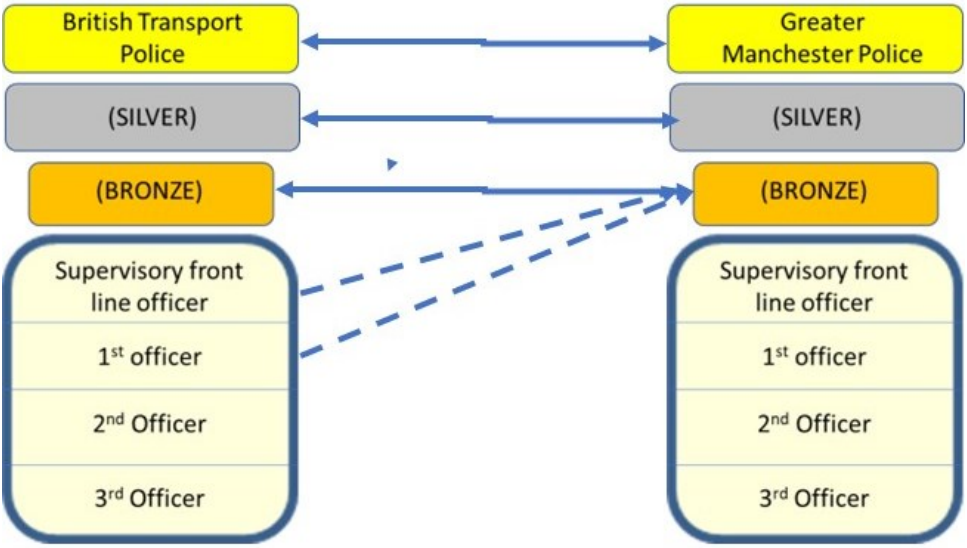
This is passed down through SILVER and BRONZE levels who may add to the protocol created at the GOLD level for additional requirements they need of the staff assigned to deal with the incident.

Also at this stage, initial Dependency Guarantee Relationships (DGRs) need to be proposed. One such could be for instance, a BTP officer, who may get there first, stating that he or she will require a guarantee that a message will be received, (a dependency), "*A Rendezvous Point notification within 4 minutes of arrival at the scene*" and guarantee to "*Send a METHANE message within 3 minutes of arrival at the scene*".

That officer has then created both a "Dependency Relationship" and a "Guarantee Relationship" for future negotiations with other Enterprises which the senior personnel in the officer's Enterprise will be aware of and agreed to.

A first meeting with partner Enterprises

The next figure shows an example of the finer detail for the links between GMP and BTP, which relate to the event shown at 22.36 in Timeline of Events table. At that point in time and subsequently, a METHANE message should have been sent but was not in the actual incident.



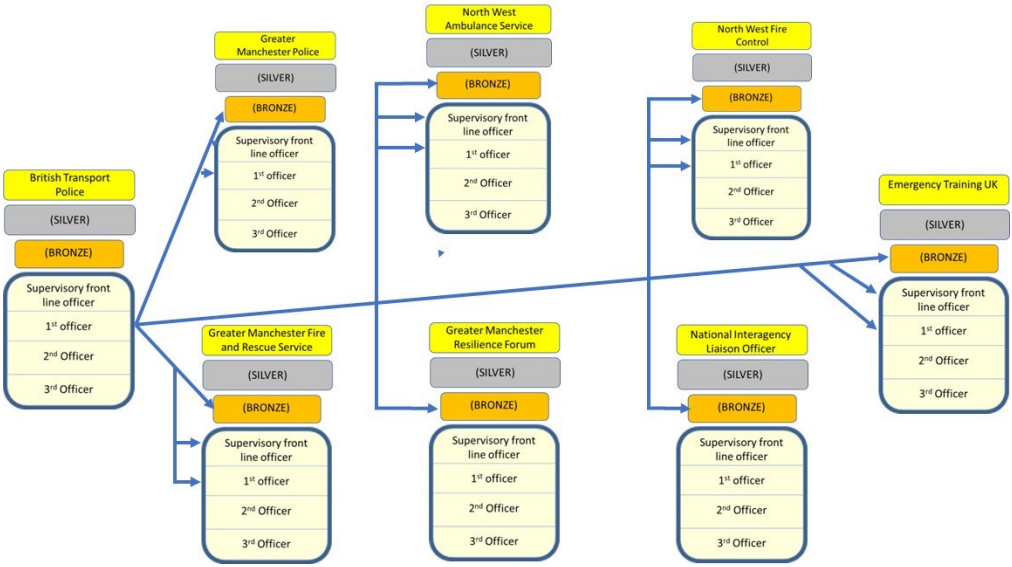
Even with this simple example, it is apparent from a brief look at the diagram that if the personnel (connected by dashed lines) upon whom duties fell had:

- a personal card indicating who should be contacted
- listed protocols dictating what information should be conveyed when contacting
- the results of a prior analysis showing what spare communication device should be provided
- DGRs stating the priority order of communications both to and from the individual that should occur
- A LEDSM diagram of their Enterprise and the roles in other Enterprises that they must contact.

then the METHANE message required would almost certainly have been sent. All that was required was two officers present with different communication devices, (e.g mobile phone and radio), which a well conducted LEDSM study would have plainly shown were required.

The 'granularity', 'getting down in the weeds', or 'the devil is in the detail', whatever expression one wishes to use as a description, is where most failures will occur. Therefore that is the area that needs to be approached more cautiously using the techniques here than the current basic overconfident assumption that the command levels will have perfectly organised their Enterprises.

The diagram above shows a LEDSM interpretation of communication the official report describes. However, after a LEDSM cycle show in the first figure had been completed a much better picture emerges. It could have been agreed at the Resilience Forum that any officer may send a METHANE message if they know their immediate superior front-line officer, who would normally send the message, is incapacitated. This is little different from the questioning by the ambulance service of a random member of the public calling about the emergency so it is perfectly acceptable to delegate the task. The next diagram shows the hypothetical situation of the front-line supervisory officer being incapacitated and the METHANE message being sent by the 1st Officer. Everyone involved at the front needs to know so the flow of data from the 1st Officer may be something similar to that shown.



Establishing the Necessary Communication Systems

The systems that will be required to communicate may need a deep analysis as certain environmental conditions that may occur and the uniqueness of internal communication processes and systems could make it impossible to communicate with other organisations.

Any system used in the internal network or that is intended to be used in communication with external organisations needs to be reviewed. Typical environmental conditions affecting communication may be the difficulty of getting signals from other systems in the network, such as when in high rise towers, as well as problems due to mobile phone networks having trouble with the volume of traffic that can grow exponentially in an emergency situation, dedicated lines being a necessary fallback where common public communication systems fail.

Generally, for emergency communications, a minimum of two paths should be available for information to flow within an Enterprise or across to other Enterprises. Each Enterprise needs to be clear about what systems they intend to use for internal and external Enterprise relationships and have confidence that they are compatible with other Enterprises.

Development of the LEDSM diagram to include other Stakeholders

The next stage of the development of the Protocols and DGRs is to include in the LEDSM diagram the other Enterprises. In a computerised system, (yet to be developed), the LEDSM diagrams, with associated protocols and DGRs would all be available to any depth or granularity as required from a single screen by zooming in and zooming out.

Print-outs so individuals have with them a LEDSM picture of their connections, protocols to adhere to and DGRs that are expected to be fulfilled would also be possible but it is simple to do that on paper for individuals, the complete computerised picture will be much more complex but, importantly, verifiable.

The Second and Subsequent Meetings to agree the LEDSM model, Protocols and DGRs

Before each subsequent meeting of, in this case The Resilience Forum, each Enterprise will go through the LEDSM cycle. All improvements and changes required to communication protocols should be taken to the Resilience Forum. Requests alone should be considered insufficient as each change should have a rationale that, it is patently obvious to the other Enterprises, is an improvement to the overall intention of saving lives. Suggested DGRs should be negotiated because one Enterprise's idea of how quickly they need information may be unrealistic to the supplying Enterprise. Ultimately the best possible functioning of the emergency services will emerge.

Declaration of the Refined Communication Protocols and Dependency Guarantee Relationships with Necessary Training

When the LEDSM has been developed through sufficient iterative use of the process cycle, both within an Enterprise and at, in this case, the resilience forum, there will be greater confidence among the Enterprises and especially those personnel working for the Enterprise at the front line levels, that communication associated with any emergency situation will be adequate and certainly at a much lower risk of failure at any point in the rescue mission.

The output should include declaration of

- appropriate communication devices in both type and numbers
- protocols acting as instructions to cope with all anticipated problems
- protocols derived generically for unanticipated problems for each level in the Enterprise
- DGRs on the critical aspects of the Protocols concerning information that should be supplied within certain time frames
- LEDSM diagrams, at both the macro level for the management of Enterprises, and micro level, to graphically illustrate the communication links the front line personnel should have.

A Protocol for the BTP Officer

PART OF A LEDSM PROTOCOL FOR A BRITISH TRANSPORT ENTERPRISE SUPERVISORY OFFICER

- Call for back-up assistance from other BTP officers and request First Aid equipment be brought including items from for pain relief from secured cabinets.
- Within 2 minutes of arrival at scene that can be described as a <Major Incident>, declare the Major Incident text message to all Enterprises in the Emergency Response WhatsApp group using your Major Incident mobile phone
- Within 4 minutes of arrival at a scene that can be described as a <Major Incident> send a METHANE text message to all Enterprises in the Emergency Response WhatsApp group using your Major Incident mobile phone.
- If no Enterprise acknowledges either message within 1 minute of sending, use your standard radio to establish contact with either the BTP Bronze Level Officer or a Bronze Level Officer in another Enterprise and ask them to send the two messages and request confirmation that acknowledgements have been received.
- In the event of all emergency communication systems failing, send a colleague to report the event by any means available including personal attendance at a coordinating response centre or use of public phones.
- When communications established and METHANE and <Major Incident> messages sent try to assist injured and wait for the declaration of Rendezvous Point, (RVP), by the NWAS, in order to direct anybody helping with evacuation of casualties to the NWAS RVP.
- If no RVP received from NWAS within 4 minutes of successful METHANE and <Major Incident> communication, request another Enterprise declares the best RVP for all parties using the whatever communications are available but preferably the Emergency Response WhatsApp group.

Above is what a Protocol may look like, though this is drawn up for illustrative purposes and is only part of the duties expected.

Conclusion

It is suggested that, just as safety-critical software requires a degree of formality in requirements capture and design, data communication requirements prepared for emergency situations should be developed more formally than is currently practiced. If LEDSM and associated techniques are used by a Resilience Forum, or indeed by any group of organisations planning for emergencies and safety critical control, the overall response may be better, and may improve the outcomes for some of the victims.

Image Attribution
front picture: Tomasz Kozlowski licensed under creative commons BY-SA v4.0

References

[1] The Layered Enterprise Data Safety Model (LEDSM) - A Framework for Assuring Safety-critical Communications – Nicholas Hales - [SCSC-176] Safety-Critical Systems eJournal vol.1 no.2 Summer Issue 2022

[2] Manchester Arena Inquiry -Volume 2: Emergency Response Volume 2-I Report of the Public Inquiry into the Attack on Manchester Arena on 22nd May 2017 - Chairman: The Hon Sir John Saunders - November 2022

Nicholas Hales

Nicholas is a retired engineer who as a student worked in communications with Royal Naval Reserve. He has a degree in Computer and Control Systems and Masters degrees in Modern Electronics and Quality Improvement and Systems Engineering. He has been involved in software safety and numerous projects involving safety critical avionics for the MoD. He is a member of the IET.