This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/

Ministry of Defence

JSP 886
DEFENCE LOGISTICS SUPPORT CHAIN MANUAL

VOLUME 7
SUPPORTABILITY ENGINEERING

PART 05.01
MANAGEMENT AND EXPLOITATION OF AUTOMATICALLY GENERATED LOGISTIC INFORMATION

VERSION RECORD		
Version Number	**Version Date**	**Version Description**
1.0	02 Aug 11	Interim Published Version.
2.0	30 Jan 12	Policy Rewritten.
2.1	14 Feb 13	Minor Changes to Format and POC.

This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/

Contents

This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/

CHAPTER 1: MANAGEMENT AND EXPLOITATION OF AUTOMATICALLY GENERATED LOGISTIC INFORMATION

CONTEXT

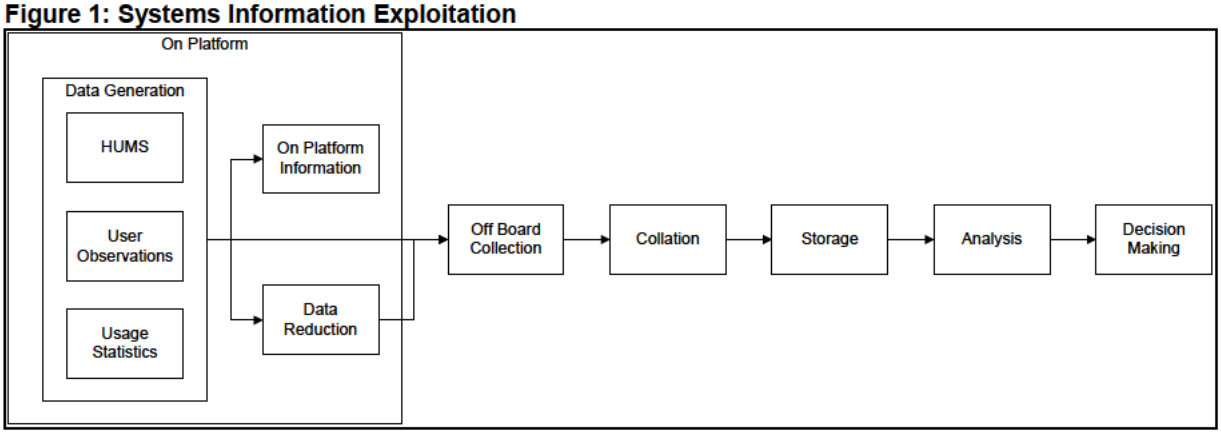
1. The aim of this document is to give the joint service policy on the management and exploitation of logistic information that is automatically generated by equipment.

2. The policy is derived from the need for automatically generated logistic information to be managed and exploited according to the Defence Logistic Information Strategy (DLIS)[1]. The strategy highlights the need to provide the Logistic Decision Support (LDS) processes with accurate and timely information of sufficient quality and governance to enable it to be quickly and simply exploited by skilled personnel.

3. Information automatically generated by equipment may not only be the outputs produced by electronic Health and Usage Monitoring Systems (HUMS) but can also includes the result of data directly entered into the equipment by users as observations, or result from other usage statistics. The information will frequently cover the maintenance aspects of equipment's health and usage, associated logistic areas such as consumption, safety and configuration, and areas of business intelligence[2], such as demand trends, performance and usage patterns.

4. However the generation of information alone is not enough, it must be exploited. It is this exploitation (also know as Systems Information Exploitation (SIE)) that enables the LDS process to achieve the agreed levels of system operational availability. Therefore, the scope of this policy covers not only the automatic generation of the information, but also it's off board collection, collation, storage and analysis. (See Figure 1).

Figure 1: Systems Information Exploitation



POLICY

5. It is MOD policy as directed by Director Joint Support Chain (DJSC) that the following procedures and processes are applied to all MOD projects:

a. Project Team (PT) Leaders shall appoint staff responsible for developing equipment Through Life Management Plans with their associated information plans.

---

[1] ACDS (Log OPS) Defence Logistic Information Interim Strategy dated 17 Oct 11.

[2] Business Intelligence – Information that is collected and processed to aid the targeting of service, system and network improvements based on demand trends and patterns of use.

This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/

The purpose of the information plan is to capture the agreement between the PT, its industrial partners and other stakeholders on the flow and use of information.

b. As part of each Information plan, a sub section covering the need for automatically generated information and its exploitation shall be developed that is in line with theatre plans or constraints for data management. The sub section shall be fully coherent with and driven by the logistic requirements for information such as safety, maintenance planning, the needs of CLS, the supporting analysis of the level of repair, and the demand trends and usage patterns applicable to business intelligence and LDS.

c. As part of the assurance process, the information plan and its sub section shall be addressed at both Initial Gate and Main Gate, and be regularly reviewed in-service.

PRECEDENCE AND AUTHORITY

6. Ownership of Logistics policy in support of the Logistics Process falls to the Assistant Chief of Defence Staff Logistics Operations (ACDS Log Ops) as Chief of Defence Materiel (CDM)'s Process Architect[3]. This role is exercised by the Defence Logistics Policy Working Group (DLPWG) and the Defence Logistics Steering Group (DLSG) reporting up to the Defence Logistics Board (DLB). It is against this governance framework that the Defence Logistic Information Strategy has been published by ACDS Log Ops and the subsequent sponsorship[4] for policy delegated to Hd JSC SCM.

MANDATED REQUIREMENTS

7. To meet MOD's Duty of Care obligations and other legal responsibilities[5], it is a requirement that the operating and maintenance authorities have accurate and accessible records of the material state of key engineering components and systems. The generation of automatic information from equipment is an important means of providing this information, and will thus form an essential part of ensuring safe operations.

PROCESS

8. The process for providing the equipment information and its subsequent exploitation shall be developed according to JSP 886 Volume 7 Part 2: ILS Management and according to JSP 886 Volume 7 Part 05: Management of Support Information. The process forms an important part of providing logistic support, in particular maintenance, where the timely provision of information may improve safety and equipment availability and thus justify its cost and complexity.

9. The process of determining what automatic information is required is driven from the start by the logistic capabilities required, the decisions that need to be made to support the equipment and the business intelligence needed to support better logistic investment decision-making. These decisions dictate the information requirements and the data fields required. They also decide when the data is required and how it is best provided.

---

[3] JSP899: Logistics Process – Roles and responsibilities.

[4] Sponsor - The Post responsible for the content, currency and publication of a JSP (as per letter of delegation). Responsibility established through Letters of Delegation (LoD), issued through the DLPWG chair and exercised through Terms of Reference.

[5] Health and Safety at Work Act 1974 ,Airworthiness respons bilities, Maritime Seaworthiness obligations, roadworthiness etc

This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/

10. Further processes for the collaborative use of electronic information are identified in the AOF Commercial Tool Kit in the e-business overview, and further guidance is contained in associated standards. (See references).

REQUIREMENTS AND CONSTRAINTS

Requirements

11. The automatic Information system shall be designed to meet the needs of the user. The system and the data it generates are to be managed to ensure that the quality and the provenance of the data is maintained through life.

Constraints

12. The design of any new information system shall take into consideration the constraints imposed by other logistic systems fielded in similar operational areas to ensure the consistency of approach and interoperability as required by the Defence Logistic Information Strategy. The design should also take into account the SOSA approach as directed by D S&E. The electronic information is to be handled in accordance with Log NEC guidelines. (See references).

KEY PRINCIPLES

13. For new equipments, the capabilities and the information required from an automatic information system must be considered early in the design cycle.

14. When setting requirements for automatically generated logistic and business intelligence information, the key principles are:

a. A calculated and informed balance must always be struck between the cost/complexity of obtaining information automatically from a system and the benefit that can be derived for business intelligence and LDS. The capabilities required of the automatic Information system shall consider first the top level asset management requirements and subsequently work down to the item level needs. The capabilities shall be prioritised as necessary.

b. Recognise that the equipment information is only one part of the overall information system. The system or platform information plan adopted must be coherent with the other end-to-end logistic and operational information elements, including data links.

c. When considering the specific capabilities required, consideration shall be given to all uses of the data. These can include:

(1) Upholding safety.

(2) Improving availability.

(3) Reducing through life costs.

(4) Reporting mission logistic capability.

(5) Monitoring consumables.

This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/

(6) Recording events or parameters that influence maintenance intervals.

(7) Predicting maintenance requirements and the issue of warnings of early failure. The advantages (timeliness and reductions in data) of using prediction algorithms should however be weighed against the costs of additional complexity and the need for the prediction algorithms to work in changing environments.

(8) Providing a Business Intelligence capability through an ability to direct, collect, process and disseminate relevant data and information.

d. The data set shall be minimised in order to avoid the duplication of similar information being recorded elsewhere by other systems on the same platform.

15. When designing systems for automatically generating logistic and business information, the key principles are:

a. For every logistic decision requirement the information requirements shall be determined and demonstrated to be understood by the purchaser and the supplier. It should be established that the information requirements are capable of being achieved and can be transferred to the logistic information system before these are finalised.

b. It shall be clear where the original data is to be processed or interpreted into information.

c. Consideration is to be given to how the information can be used in the processing of Business Intelligence based on demand trends and use patterns and to how the information can be used particularly in the maintenance and repair decision making process.

d. Consideration should be given to minimising data transfer requirements. The design of the data transfer requirements should consider:

(1) The likely limitations of the bearer networks, to ensure that the system will function properly in its operational role.

(2) The pre-processing of data to reduce data transfer requirements from the platform either automatically or by human intervention.

(3) The data flow paths and the effect of discontinuous communications.

(4) The need for reversionary data requirement modes including transfer by other means.

e. The information shall be made available to the person required to make the required intervention, e.g. the operator, the forward maintainer or the maintenance manager, in sufficient time for it to be acted upon.

f. The need for controlling data accuracy and authenticity, cleansing, validation and verification should be planned for and enabled.

g. The information shall be made available in a format that can be used by a third party Business Intelligence system or network.

This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/

16. When managing automatically generated logistic and business intelligence information, the key principles to follow are:

a. There shall be a process of information validation and governance put in place by the stakeholders who require the capability, in order to ensure data quality.

b. Reporting and resolution procedures shall be in place and implemented, where necessary, for any problems with the information system.

c. It shall be clear where the information is to be kept, who owns it, and how long it is to be retained. Information and data records shall be maintained in accordance with JSP 747: Defence Information Management Policy.

d. Security requirements for the information should be clear and in accordance with JSP 440, in particular, it should be clear what information is to be separated for sensitivity or security reasons. Any restrictions on use of the information must be clearly published to all stakeholders.

e. The need for information should be routinely reviewed.

17. When exploiting automatically generated logistic and business intelligence information, the key principles are:

a. It should be clear which stakeholder requires which particular information, who is responsible for taking any action and by when it is required.

b. Where possible the method of initiating action such as trigger points or threshold levels should be predetermined.

c. If an analysis of the information in accordance with an agreed algorithm or trigger point suggests a particular action and it is not taken then it should be recorded in an appropriate place, who has decided not to take the action and why.

d. The consequences of not taking any such action resulting from an analysis (such as safety) must be clear and must be disseminated to all concerned stakeholders.

e. Where possible the data and information should be made available to successor projects.

ASSOCIATED STANDARDS AND GUIDANCE

18. Associated Standards and Publications are:

a. JSP 329: Information Coherence for Defence.

b. JSP 440: Manual of Defence Security.

c. JSP 602: 1006 leaflets: Information Coherence Directions and Guidance – Tactical Data Links.

d. JSP 604: Network Joining Rules.

e. JSP 747: Defence Information Management Policy.

**This document, JSP 886:
The Defence Logistics Support Chain Manual, has been archived.
For Logistics policy, please refer to the Defence Logistics Framework (DLF)
via www.defencegateway.mod.uk/**

f. JSP 817: Condition Monitoring and Condition Based Maintenance Policy.

g. JSP 886 Volume 7 Part 2: ILS Management.

h. JSP 886 Volume 7 Part 5: Management of Support Information.

i. JSP 886 Volume 7 Part 8: Conduct and Record Maintenance.

j. Support Solutions Envelope (SSE): KSA GP4.1 (HUMS, LOG IP). GP4.2 (LCIA, IER).

k. AOF Commercial Tool Kit e business collaborative working.

l. ISO 8000: Data Quality.

m. DEFSTAN 23-09: Generic Vehicle Architecture.

OWNERSHIP AND POINTS OF CONTACT

19. The policy for Management and Exploitation of Equipment Generated System Information is sponsored by DES JSC SCM-Eng. Contact details are as follows:

a. Document sponsor and SME:

DES JSC SCM-EngTLS-Rel1d
Tel: Mil: 9679 Ext 35355, Civ: 030 679 35355.

b. Document Editor:

DES JSC SCM-SCPol-ET Editorial Team
Tel: Mil: 9679 Ext 80953 Civ: 030 679 80953.