Counterfeit Parts Prevention Toolkit

Guidance for suppliers

Background

Counterfeit parts — from electronics to raw materials — are more than quality risks. They are also cybersecurity risks to our products. Threat actors can use counterfeit parts, which have been detected across many supply chains, as attack vectors, allowing them to insert malicious code or disrupt operations.

What Is a Counterfeit Part?

A counterfeit part is an unauthorized copy, imitation, substitute, or modified part (e.g., material, part, component), which is knowingly misrepresented as a specified genuine part of an original or authorized manufacturer, according to AS9110. NOTE: Examples of a counterfeit part can include, but are not limited to, the false identification of marking or labeling, grade, serial number, date code, documentation, or performance characteristics, also according to AS9110.

What Are the Risks?

Risks stemming from the use of counterfeit parts include:

- **Product safety and reliability:** A counterfeit part could affect the performance or lifecycle of a product or system.
- **Cybersecurity:** Counterfeit parts could be modified to inject malicious code or contain intentional back doors that allow unauthorized users access to a system.
- **Reputation:** Use of counterfeit parts could lessen a customer's trust in a company's products.
- **Cost:** Use of counterfeit parts, and any resulting investigations, could increase costs due to manufacturing downtime or needed part replacement. Revenue could also be lost if a product must be pulled from service.
- **Regulatory compliance:** A company found to be non-compliant with standards related to counterfeit parts could lose or cease business.

Strategies to Prevent Use of Counterfeit Parts

Suppliers must ensure that they are obtaining authentic parts and that they can detect counterfeit parts before use. Ways to prevent the use of counterfeit parts include:

1. Source from trusted suppliers (original equipment manufacturers and authorized distributers). The most likely way a counterfeit part enters the supply chain is through unauthorized suppliers, or the "gray market."

2. Adopt a parts provenance program to ensure the traceability of a part throughout its lifecycle. For example, a parts provenance program could include serializing certain parts and relevant paperwork.
3. Apply robust inspection methods to check parts and relevant paperwork. Always ensure that these inspections and paperwork are tied to a planned shipment.
4. Monitor sites such as **EASA** or the **Federal Aviation Administration (FAA)** for the latest information on counterfeit or suspect unapproved part activity and investigations.
5. Create and deploy employee training on counterfeit parts risks and best practices to ensure parts are authentic. For example, a counterfeit part could still be a conforming part, and therefore difficult to detect; employees who handle parts should be trained to recognize a potential counterfeit part.
6. Use tamper-evident packaging, labels, etc. This will make it easier for those handling the materials to detect a potential counterfeit part.
7. Implement anti-counterfeit technologies to aid in parts provenance or to provide assurance in authentic parts. Examples include utilizing RFID tags or applying an unclonable feature to a product.
8. Use obsolescence management tools. “Obsolescence” means that a part, supplier, or service is obsolete and no longer available. Poor obsolescence management increases the risk of sourcing parts from an unknown alternative supplier.

If Rolls-Royce Suppliers Discover Counterfeit Parts, What Are You Required to Do?

Per SABRe, suppliers should begin their containment process: segregate the counterfeit parts and store them in a secure location.

Notify Rolls-Royce via the Notice of Escape process.

Check to see if industry standard reporting requirements apply to you (including but not limited to: **GIDEP**, **EASA**, or **FAA**).

Additional resources

1 ISO 9001:2015 Standard – Section 8.1 - Operational planning and control

2 AS9100:2018 - Section 8 Operation - 8.1.4 Prevention of Counterfeit Parts

3 AS9110:2015 - Section 8 Operation - 8.1.4 Prevention of Counterfeit Parts

4 AS5553D: Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition - SAE International

5 AS6081: Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors Counterfeit Electronic Parts; Avoidance Protocol, Distributors - SAE International

6 DFARS 252.246-7007 and DFARS 252.246-7008 (US Department of Defense)

7 AC 21-29D - Detecting and Reporting Suspected Unapproved Parts (FAA)

8 CAA/EASA Part 145 (UK and Europe) Guidance for Part 145 approval holders - UK Civil Aviation Authority

9 NIST SP 800-53 SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations - CSRC

10 Supply Chain Security and the Gray Market

11 AC 21-29D - Detecting and Reporting Suspected Unapproved Parts (CISA/FAA)

SUPPLIER COMMUNICATION | Rolls-Royce's Global Supplier Portal is your first stop for information and documents, such as Notices to Suppliers (NTS). Go to suppliers.rolls-royce.com for more.