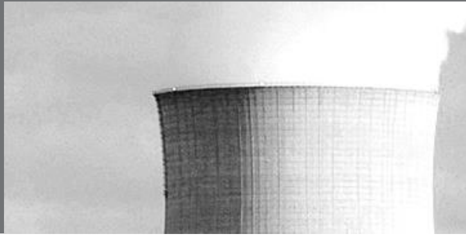
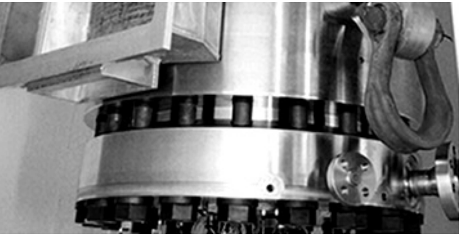
Best Practices for Protecting the Supply Chain

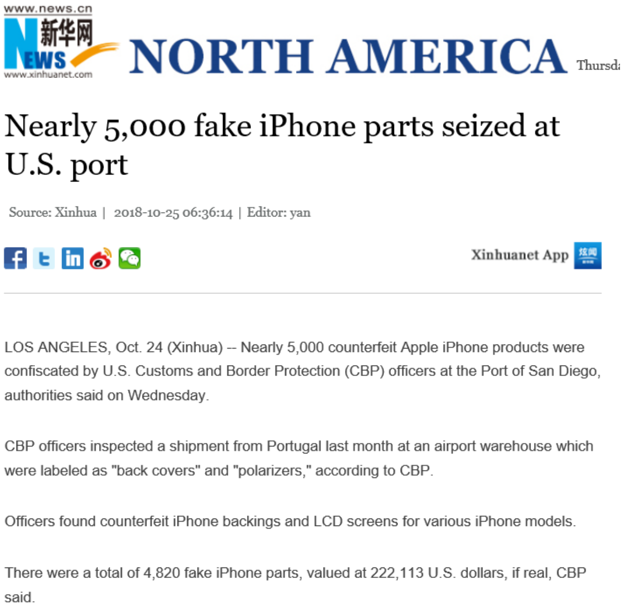
Steve Edwards, Curtiss-Wright Defense Solutions





TRUSTED
PROVEN
LEADER

Counterfeit Parts are a Threat to All



www.news.cn 新华网 News www.xinhuanet.com **NORTH AMERICA** Thursd

Nearly 5,000 fake iPhone parts seized at U.S. port

Source: Xinhua | 2018-10-25 06:36:14 | Editor: yan

Xinhuanet App

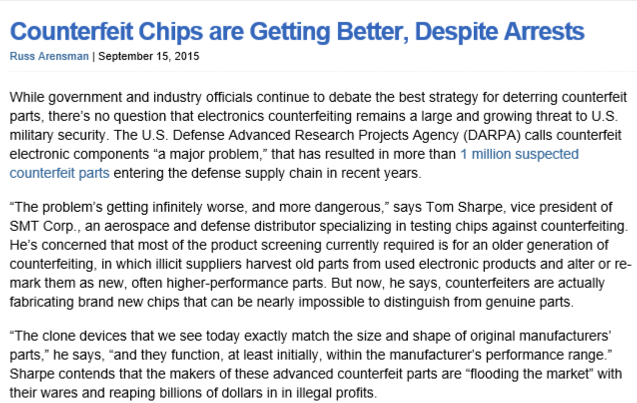
LOS ANGELES, Oct. 24 (Xinhua) -- Nearly 5,000 counterfeit Apple iPhone products were confiscated by U.S. Customs and Border Protection (CBP) officers at the Port of San Diego, authorities said on Wednesday.

CBP officers inspected a shipment from Portugal last month at an airport warehouse which were labeled as "back covers" and "polarizers," according to CBP.

Officers found counterfeit iPhone backings and LCD screens for various iPhone models.

There were a total of 4,820 fake iPhone parts, valued at 222,113 U.S. dollars, if real, CBP said.

NAVY
NEW DEVELOPMENTS
TWITTER
FAKE PARTS PUTTING U.S. TROOPS AT RISK
Senate: More than a million bogus parts in military equipment
CNN
Arkansas primary may pose challenge for Obama
DOW -1.67
CNN



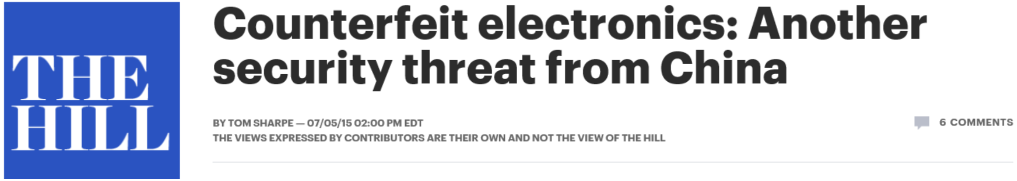
Counterfeit Chips are Getting Better, Despite Arrests

Russ Arensman | September 15, 2015

While government and industry officials continue to debate the best strategy for deterring counterfeit parts, there's no question that electronics counterfeiting remains a large and growing threat to U.S. military security. The U.S. Defense Advanced Research Projects Agency (DARPA) calls counterfeit electronic components "a major problem," that has resulted in more than 1 million suspected counterfeit parts entering the defense supply chain in recent years.

"The problem's getting infinitely worse, and more dangerous," says Tom Sharpe, vice president of SMT Corp., an aerospace and defense distributor specializing in testing chips against counterfeiting. He's concerned that most of the product screening currently required is for an older generation of counterfeiting, in which illicit suppliers harvest old parts from used electronic products and alter or re-mark them as new, often higher-performance parts. But now, he says, counterfeiters are actually fabricating brand new chips that can be nearly impossible to distinguish from genuine parts.

"The clone devices that we see today exactly match the size and shape of original manufacturers' parts," he says, "and they function, at least initially, within the manufacturer's performance range." Sharpe contends that the makers of these advanced counterfeit parts are "flooding the market" with their wares and reaping billions of dollars in in illegal profits.



THE HILL

Counterfeit electronics: Another security threat from China

BY TOM SHARPE — 07/05/15 02:00 PM EDT
THE VIEWS EXPRESSED BY CONTRIBUTORS ARE THEIR OWN AND NOT THE VIEW OF THE HILL

6 COMMENTS

Trust, But Verify

Establishing and maintaining a Trusted Supply Chain:

- Key watchwords: Vigilance and Visibility

  An old adage made popular by President Ronald Reagan remains words to the wise: "Trust, But Verify"

- For example, trust in your supplier's certification, but verify their performance to ensure that they (and any brokers and distributors they use) have demonstrated their commitment and adherence to counterfeit mitigation and prevention

Trusted Supply Chain Components

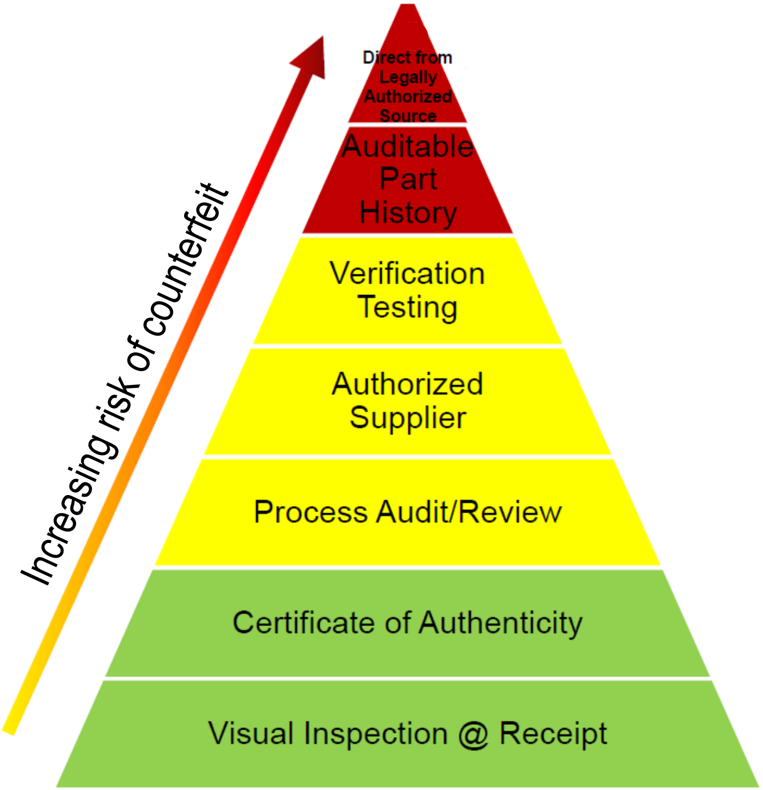
- **For years, COTS vendors such as Curtiss-Wright have taken a leadership role in establishing state-of-the-art Trusted Computing processes for open architecture rugged modules used by the embedded COTS industry**
- **These processes are designed to:**
  - Reduce risk
  - Mitigate malicious threats against hardware or data.

Examples of Trusted Supply Chain

- **Best practices for protecting the supply chain must address:**
  - Physical Security
  - Manufacturing Security
  - Component Supply Chain Integrity
  - Secure Handling and Chain of Custody Protection
  - Product Reliability
  - Counterfeit Parts Mitigation and Parts Inspection

Secure Supply Chain

- When possible, buy directly from
  - OEM
  - Authorized distribution
- Flow down requirements
- More risk requires more countermeasures


Direct from Legally Authorized Source
Auditable Part History
Verification Testing
Authorized Supplier
Process Audit/Review
Certificate of Authenticity
Visual Inspection @ Receipt
Increasing risk of counterfeit

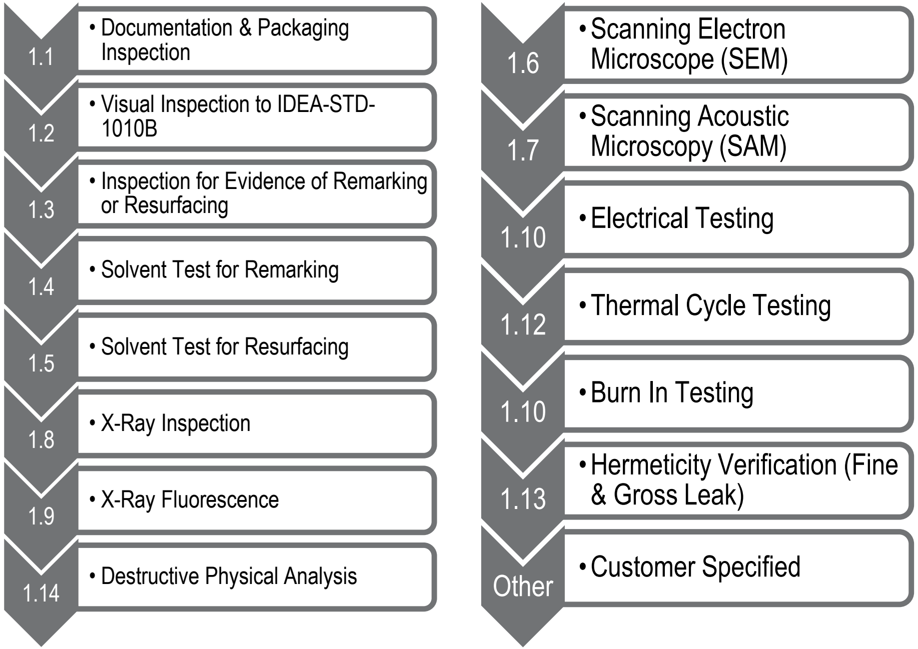
Adapted from www.dla.mil/Portals/104/Documents/LandAndMaritime/V/VA/PSMC/Apr12/LM_5AntiCounterfeiting_151030.pdf

Obsolescence and the Supply Chain

- **Mitigate obsolescence through**
  - Footprint and I/O compatible replacements through authorized source
  - Last Time Buy through authorized source
    - Extends product life
    - No need to procure obsolete parts from brokers

Broker by Approval ONLY

Tested to industry-standard validation methods



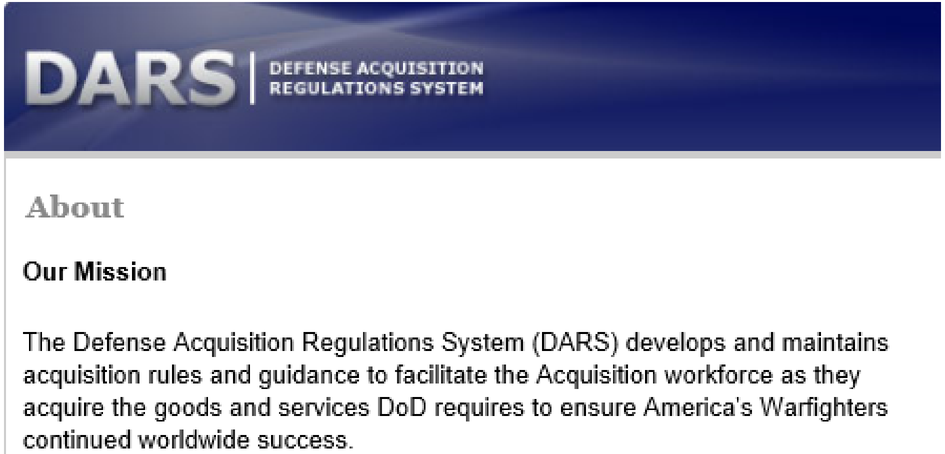
- 1.1 • Documentation & Packaging Inspection
- 1.2 • Visual Inspection to IDEA-STD-1010B
- 1.3 • Inspection for Evidence of Remarking or Resurfacing
- 1.4 • Solvent Test for Remarking
- 1.5 • Solvent Test for Resurfacing
- 1.8 • X-Ray Inspection
- 1.9 • X-Ray Fluorescence
- 1.14 • Destructive Physical Analysis
- 1.6 • Scanning Electron Microscope (SEM)
- 1.7 • Scanning Acoustic Microscopy (SAM)
- 1.10 • Electrical Testing
- 1.12 • Thermal Cycle Testing
- 1.10 • Burn In Testing
- 1.13 • Hermeticity Verification (Fine & Gross Leak)
- Other • Customer Specified

AS5553B/ARP 6328 process

Standards & Regulations

- Help shape the regulatory landscape of the defense industry
- Stay up to date with evolving standards
- Comply with DoD acquisition regulations

SAE INTERNATIONAL™



DARS | DEFENSE ACQUISITION REGULATIONS SYSTEM

About

Our Mission

The Defense Acquisition Regulations System (DARS) develops and maintains acquisition rules and guidance to facilitate the Acquisition workforce as they acquire the goods and services DoD requires to ensure America's Warfighters continued worldwide success.

Examples of Systems with Counterfeit Parts

THAAD

C-17

P-8A

The failure of a single electronic part can leave a soldier, sailor, airman, or Marine vulnerable at the worst possible time

~ 2012 Senate Armed Services Committee Report

Understand Counterfeiting “State of the Art”

Monitor counterfeit reporting bodies

elecTech

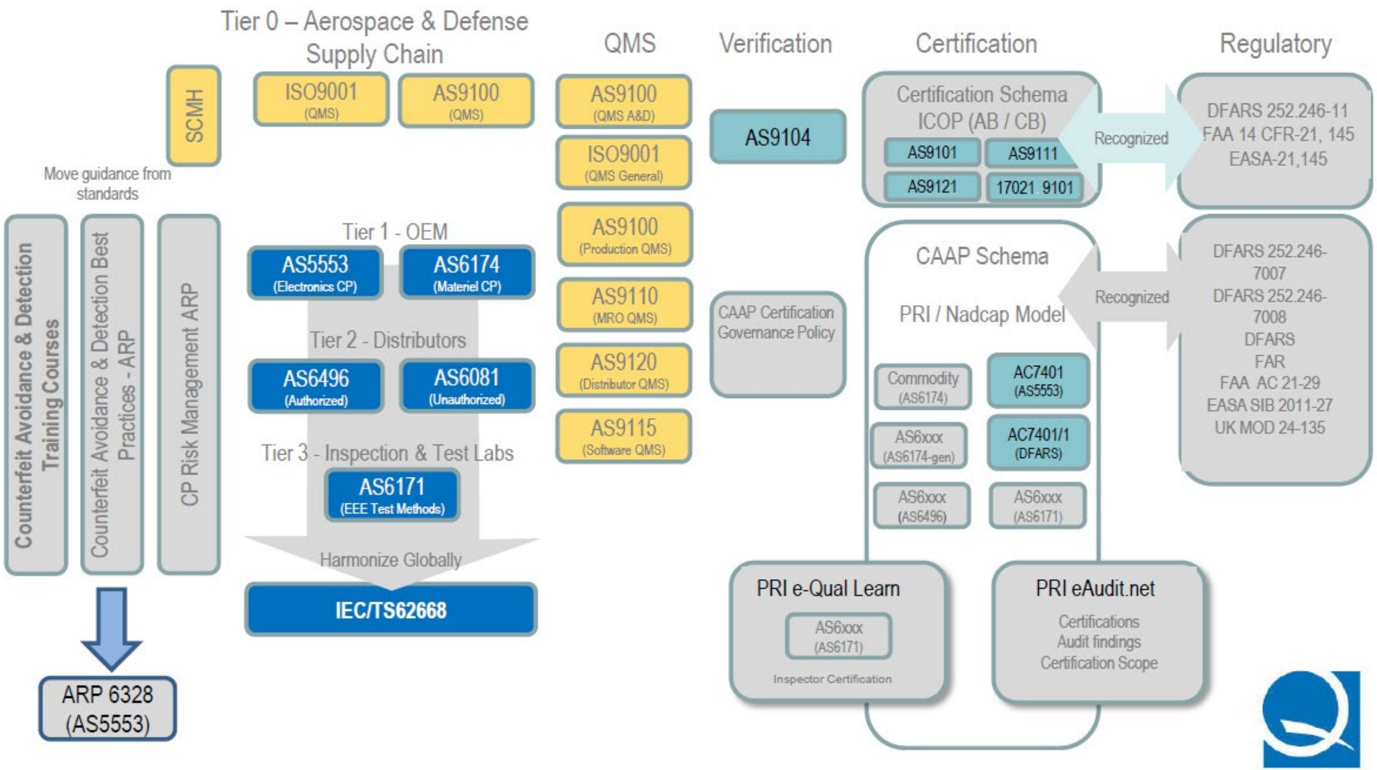
GOVERNMENT-INDUSTRY

GIDEP

DATA EXCHANGE PROGRAM

erai

Know your Supplier's Certifications



Tier 0 – Aerospace & Defense Supply Chain

ISO9001 (QMS)

AS9100 (QMS)

SCMH

Move guidance from standards

Counterfeit Avoidance & Detection Training Courses

Counterfeit Avoidance & Detection Best Practices - ARP

CP Risk Management ARP

ARP 6328 (AS5553)

Tier 1 - OEM

AS5553 (Electronics CP)

AS6174 (Materiel CP)

Tier 2 - Distributors

AS6496 (Authorized)

AS6081 (Unauthorized)

Tier 3 - Inspection & Test Labs

AS6171 (EEE Test Methods)

Harmonize Globally

IEC/TS62668

QMS

AS9100 (QMS A&D)

ISO9001 (QMS General)

AS9100 (Production QMS)

AS9110 (MRO QMS)

AS9120 (Distributor QMS)

AS9115 (Software QMS)

Verification

AS9104

CAAP Certification Governance Policy

Certification

Certification Schema ICOP (AB / CB)

AS9101

AS9111

AS9121

17021 9101

Recognized

CAAP Schema

PRI / Nadcap Model

Commodity (AS6174)

AC7401 (AS5553)

AS6xxx (AS6174-gen)

AC7401/1 (DFARS)

AS6xxx (AS6496)

AS6xxx (AS6171)

PRI e-Qual Learn

AS6xxx (AS6171)

Inspector Certification

PRI eAudit.net

Certifications
Audit findings
Certification Scope

Regulatory

DFARS 252.246-11
FAA 14 CFR-21, 145
EASA-21,145

Recognized

DFARS 252.246-7007
DFARS 252.246-7008
DFARS
FAR
FAA AC 21-29
EASA SIB 2011-27
UK MOD 24-135

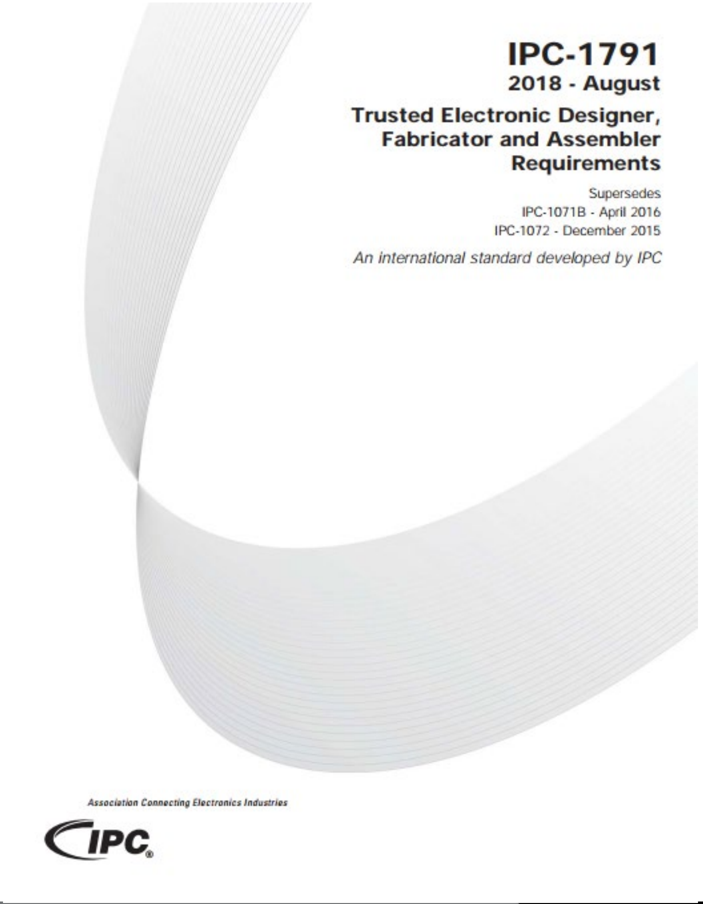
A standards based approach for DFARS compliance

ASQ

asq.org/asd/2018/04/quality-control/an-industry-standards-approach-to-counterfeit-prevention-compliance.pdf

Secure Manufacturing

IPC-1791 provides guidance on establishing trust in the manufacturing & assembly process



IPC-1791
2018 - August

Trusted Electronic Designer, Fabricator and Assembler Requirements

Supersedes
IPC-1071B - April 2016
IPC-1072 - December 2015

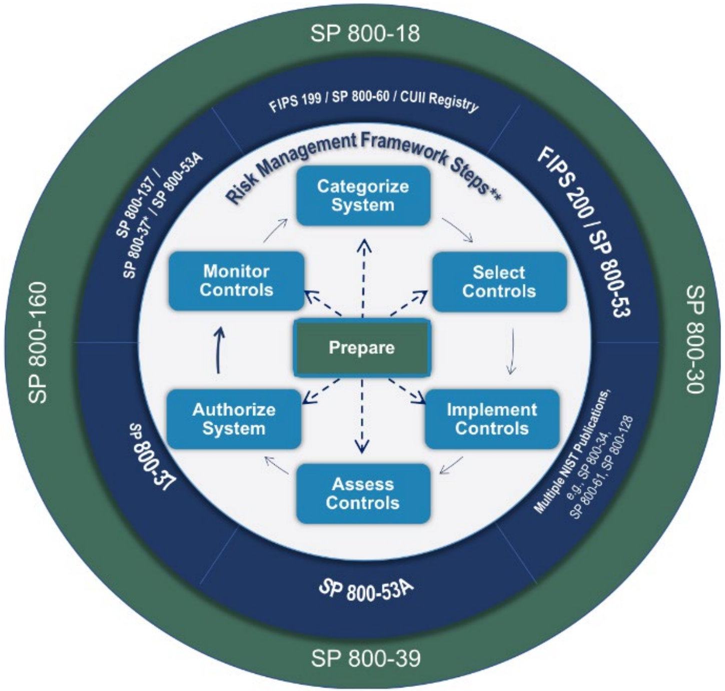
An international standard developed by IPC

Association Connecting Electronics Industries

IPC®

Design Integrity

Risk Management Framwork (RMF) provides controls to mitigate against unauthorized access, modification, loss, or theft of critical design information



Curtiss-Wright’s Total LifeCycle Management Services

Total LifeCycle Management

AL Dedicated Curtiss-Wright care team, including a team of lifecycle experts

Custom industry-leading TLCM platform

Free on-site component storage

Component Health Analysis

AL Obsolescence reporting on semiconductor devices

Forward-looking availability predictions

Risk mitigation strategies for DMS parts

Test Infrastructure Investments

L Test hardware maintenance

Procurement of test item (cables, jigs, test cards, etc.)

Operator training

Active equipment maintenance

Product Configuration Controls

AL Fit, form, function DMS replacements

Operational enhancements

Non fit, form, function DMS solutions

Service Notifications

AL Early Alert LTB notification

LTB component quotations

Service renewals

Push email system for services portal

TLCM Partnerships

A Have an active voice in change approval

Make calculated risk assessments in order to secure forecasts

Reduce cost and risk of supply with early identification

Increase operational readiness

L Common goal to support a fixed forecast or fielded units

Extension of your program with the preferred COTS vendor

LTB parts buys sustain a fixed configuration

🟦 Active

🟥 Longevity

Summary

- Don’t underestimate the threat
- Adopt industry standard best practices
- Security in all areas
  - Components
  - Manufacturing
  - Design
- Protect your systems throughout the entire lifecycle

Thank You

CURTISS - WRIGHT

For more information about system security from the COTS perspective please contact us at ds@curtisswright.com.

[redacted]

TRUSTED
PROVEN
LEADER

www.curtisswrightds.com