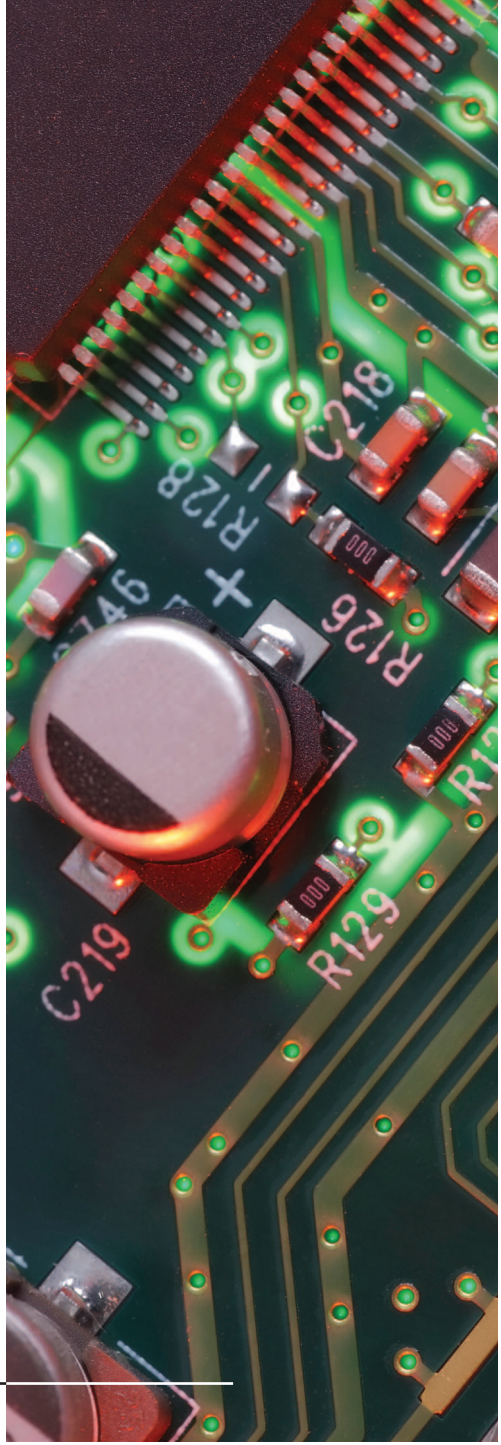
The Counterfeit Electronic Components Minefield

Version 2 – Revised and updated - incorporating the "Date Code Minefield" booklet.

A Guide to Understanding, Detecting, Avoiding Purchasing and Using Counterfeit Electronic Components



Published by the Component Obsolescence Group
Unit 3, Curo Park, Frogmore, St Albans, Hertfordshire AL2 2DD
Tel: 01727 876029 **Fax:** 01727 871336
email: admin@cog.org.uk **Web:** www.cog.org.uk

Price £15 $22 €18

Contents:

Dedication

To all those who have been or will be "stung" or injured by Counterfeit Electronic Components but especially, for all those who do not even recognise the problem - yet!!

Handbook written for the Component Obsolescence Group by Charles Battersby

The Counterfeit Electronic Components Minefield, now in its second edition, has been updated and revised. As noted in the first edition, in overcoming the difficulties posed by Counterfeit Components, we are all working against a "moving target" hence there has been the addition of new material in an attempt to keep this document up to date.

Since we are all "shooting at this moving target", future effective action planning becomes rather difficult to predict with any degree of accuracy – therefore E&OE.

This booklet was written by Charles Battersby in co-operation with members of the Publications and Standardisation Group (formally the External Liaison Group) of the Components Obsolescence Group (COG) and thanks for the valuable help and comments of other members of COG.

This publication is one of a series of booklets published by the Components Obsolescence Group, all of which are recommended as essential reading for organisations or individuals tasked with obsolescence management. This growing series includes:

The Obsolescence Minefield
The Obsolescence Minefield – Senior Executive Edition
The Date Coding Minefield
The Supply Chain Minefield
The Long-Term Storage Minefield
The Pb-Free Minefield
The Redundant Stock Minefield
The Hardware Design Minefield
The Emulation and Substitution Minefield
The Software Obsolescence Minefield
The Obsolescence Tools Minefield

Dedication

To all those who have been or will be "stung" or injured by Counterfeit Electronic Components but especially, for all those who do not even recognise the problem - yet!!

This Handbook is dedicated to three groups of individuals:-

a those who have already experienced the pain that can come when Counterfeit / Fraudulent or otherwise illegal components enter their supply chain. It could well be that some of their own staff – or worse still, their customers - have experienced the possibly explosive effects of substandard electronic components expiring in their equipment. Such malfunctions can easily cause injury or even - in the worst case - death. The minimum effect on your company will be loss of revenue in the immediate phase plus loss of reputation and hence business opportunities for the future. You will know all about the effects of Counterfeit Electronic Components entering your equipment and certainly have suffered some or many of the consequences.

b those foolish enough to be in denial. You present a public face where you maintain that you have never had a problem with Counterfeit or other similar illegal devices entering your production. If you are a user / buyer of Electronic Components then it is more than likely than not that you have already received and inserted such devices in your equipment. It is almost inevitable that some of these counterfeits will be lying in wait for the most inopportune time to expire exposing you to of losses on many levels – not least of which will be your reputation. There are a very large number of counterfeits out there!

c the most fortunate group of all – those who have never actually been plagued by Counterfeits and have – somehow – managed to stay clear of this problem – congratulations – but you still need to be very vigilant for when the inevitable happens – the dice are most certainly stacked against you!

Beware – even if you try to minimise your risk of receiving Counterfeit Components by avoiding the "Grey Market", you could still be exposed to a lower level of risk by buying directly from the Component Manufacturer or his Franchised Distributor – there still remains a small risk that suspect devices have entered the supply chain.

A few simple questions for anyone involved in the purchase of components for use in their own manufacture, for distributors of components, in fact anyone who relies on the integrity of electronic devices:-

- Have you already been "stung" by the Counterfeiters? Chances are that you may well have received some counterfeit products without even knowing it. Even with tightly controlled supply chains, high volume manufacturers of Computers, White goods etc. have experienced failures due to Counterfeit Devices entering their production lines.
- Do you believe that your Company's reputation is "on the line" if Counterfeits invade your products? Just a few disastrous customer experiences could be critical to your organisations very existence.
- Is the safety of your product (either made by you or used by your organisation) in question should devices fail? This sector ranges from Aircraft systems all the way through to domestic appliances - don't forget - lack of safety here can kill!
- More personally, do you not think that your job would be "on the line" unless you take action against Counterfeits invading your organisation?
- Do you believe that legislation will stamp out counterfeits, think again – it will take a very long time! Those involved in counterfeiting are very bright and will always find ways of "conning" their targets one way or another.
- Do you think that counterfeiting is a temporary problem and will "go away" - wishful thinking! Counterfeiting has been a way of life for many people over all the centuries since time began.
- Do you think that Counterfeiting is restricted to those items that appear to be simple to copy – not so. Even complex Integrated Circuits containing many millions of elements are regularly counterfeited – frequently with deliberately introduced malicious code - just to really make things interesting!
- "It cannot happen to me"? – Oh yes it can!

You may recognise one or more of the above but – more likely - you may well have suffered the consequences of counterfeited or forged products for other completely different reasons.

This Booklet aims to give an insight to the magnitude of the problem, the mechanisms used in the production of fake devices, the mechanisms exploited in the distribution of fakes, possible detection techniques leading through to an action plan to minimise the risk in you becoming a victim of this crime.

The Author also wishes to thank all those who have made valuable contributions to this Handbook – mostly people who have had practical "hands on" experience of the difficulties surrounding Counterfeit Electronic Components and have become their own experts in keeping this problem at bay within their own organisations – Many Thanks.

Disclaimer.

I have endeavoured to ensure that all the facts were correct at the time of writing. However, since no one can be confident that they really know of the size, scale or full impact of piracy, forgeries and counterfeiting within the electronics market, many of the facts have to be regarded as being "Ball Park". It is more than likely that the scale and extent of the problems are somewhat greater than those noted - most unlikely to be less. The origin of counterfeit products will keep moving from region to region and from country to country as will the nature of the counterfeits and the counterfeiters themselves.

The Author has approached all the photograph copyright owners and obtained clearance of use in this document – albeit, sometimes granted only in verbal form.

Note: Most commentators use the word "counterfeit" to cover many various terms such as Piracy, Forgery, Fraud, and Intent to Deceive etc as well as Counterfeit. They also use various other alternative words or phrases. In general, the word counterfeit has been used in this handbook to cover all these different forms of fakery.

Be aware – take action - be safe!

The Counterfeit Electronic Components Minefield

Published by the Component Obsolescence Group

Unit 3, Curo Park, Frogmore, St Albans, Hertfordshire AL2 2DD

Tel: 01727 876029 **Fax:** 01727 871336

email: admin@cog.org.uk **Web:** www.cog.org.uk

ISBN 978-1-907775-00-0

9 781907 775000 52200 >