Technical Note

对嵌入式系统软件可靠性设计的一些看法

嵌入式系统

V1.00 Date:2010/03/18 工程技术笔记

类别	内容
关键词	嵌入式系统 软件 可靠性
摘 要	本文分析了 嵌入式系统软件的复杂度、可靠性与稳定性之间的关系，本给出了增加嵌入式系统可靠性的一般方法。

修订历史

版本	日期	原因
V1.00	2010/03/18	创建文档

销售与服务网络（一）

广州周立功单片机发展有限公司

地址：广州市天河北路 689 号光大银行大厦 12 楼 F4
邮编：510630
电话：(020)38730916　38730917　38730972　38730976　38730977
传真：(020)38730925
网址：www.zlgmcu.com

广州专卖店

地址：广州市天河区新赛格电子城 203-204 室
电话：(020)87578634　87569917
传真：(020)87578842

南京周立功

地址：南京市珠江路 280 号珠江大厦 2006 室
电话：(025)83613221　83613271　83603500
传真：(025)83613271

北京周立功

地址：北京市海淀区知春路 113 号银网中心 A 座 1207-1208 室（中发电子市场斜对面）
电话：(010)62536178　62536179　82628073
传真：(010)82614433

重庆周立功

地址：重庆市石桥铺科园一路二号大西洋国际大厦（赛格电子市场）1611 室
电话：(023)68796438　68796439
传真：(023)68796439

杭州周立功

地址：杭州市天目山路 217 号江南电子大厦 502 室
电话：(0571) 28139611　28139612　28139613
28139615　28139616　28139618
传真：(0571) 28139621

成都周立功

地址：成都市一环路南二段 1 号数码同人港 401 室（磨子桥立交西北角）
电话：(028)85439836　85437446
传真：(028)85437896

深圳周立功

地址：深圳市深南中路 2070 号电子科技大厦 C 座 4 楼 D 室
电话：(0755)83781788（5 线）
传真：(0755)83793285

武汉周立功

地址：武汉市洪山区广埠屯珞瑜路 158 号 12128 室（华中电脑数码市场）
电话：(027)87168497　87168297　87168397
传真：(027)87163755

上海周立功

地址：上海市北京东路 668 号科技京城东座 7E 室
电话：(021)53083452　53083453　53083496
传真：(021)53083491

西安办事处

地址：西安市长安北路 54 号太平洋大厦 1201 室
电话：(029)87881296　83063000　87881295
传真：(029)87880865

销售与服务网络（二）

广州致远电子有限公司

地址：广州市天河区车陂路黄洲工业区 3 栋 2 楼
邮编：510660
传真：(020)38601859
网址：www.embedtools.com （嵌入式系统事业部）
www.embedcontrol.com （工控网络事业部）
www.ecardsys.com （楼宇自动化事业部）

技术支持：

CAN-bus：

电话：(020)22644381 22644382 22644253
邮箱：can.support@embedcontrol.com

iCAN 及数据采集：

电话：(020)28872344 22644373
邮箱：ican@embedcontrol.com

MiniARM：

电话：(020)28872684 28267813
邮箱：miniarm.support@embedtools.com

以太网：

电话：(020)22644380 22644385
邮箱：ethernet.support@embedcontrol.com

无线通讯：

电话：(020) 22644386
邮箱：wireless@embedcontrol.com

串行通讯：

电话：(020)28267800 22644385
邮箱：serial@embedcontrol.com

编程器：

电话：(020)22644371
邮箱：programmer@embedtools.com

分析仪器：

电话：(020)22644375 28872624 28872345
邮箱：tools@embedtools.com

ARM 嵌入式系统：

电话：(020)28872347 28872377 22644383 22644384
邮箱：arm.support@zlgmcu.com

楼宇自动化：

电话：(020)22644376 22644389 28267806
邮箱：mjs.support@ecardsys.com
mifare.support@zlgmcu.com

销售：

电话：(020)22644249 22644399 22644372 22644261 28872524
28872342 28872349 28872569 28872573 38601786

维修：

电话：(020)22644245

目　录

1. 概述

自从40多年前嵌入式系统诞生以来，随着技术的发展和需求的变化，嵌入式系统软件就在嵌入式系统中越来越重要。现在，甚至一些嵌入式系统硬件一模一样，仅仅是软件不同，就是不一样的产品（如交换机和路由器）。

嵌入式系统应用领域千差万别、他们对嵌入式系统的要求和侧重点不尽相同，（如工业控制特别强调可靠性），但基本要求嵌入式系统功能强大、性能稳定、工作可靠。但这3点不是相辅相成的，而是互相之间有矛盾的。

嵌入式系统的功能、稳定性、可靠应与嵌入式系统的硬件、软件都有关系。本文仅讨论版嵌入式系统软件的可靠性设计问题，因此假设嵌入式系统的硬件是稳定可靠的。尽管一些应用可以在不可靠的硬件上通过软件设计获得可靠的产品（如U盘，NAND FLASH是一个不可靠的存储介质，但通过软件设计，可以得到可靠的存储设备。硬盘更是如此。），但这不在本文的讨论范围之内。

2. 可靠性与稳定性之间的关系

2.1 定律 1：越简单的东西越容易做得可靠

相对锤子来说，机械手表足够复杂。如果让一个锤子和一个机械手表都从10层楼高处掉到普通水泥地面，哪个损坏的可能性更大？当然，如果花费大的代价，如使用最好的材料，并增减减震系统，机械手表甚至可以做到锤子摔坏了而手表不坏。不相信？飞行员从几万米高空掉下来不受伤的比比皆是（当然有降落伞啦）。

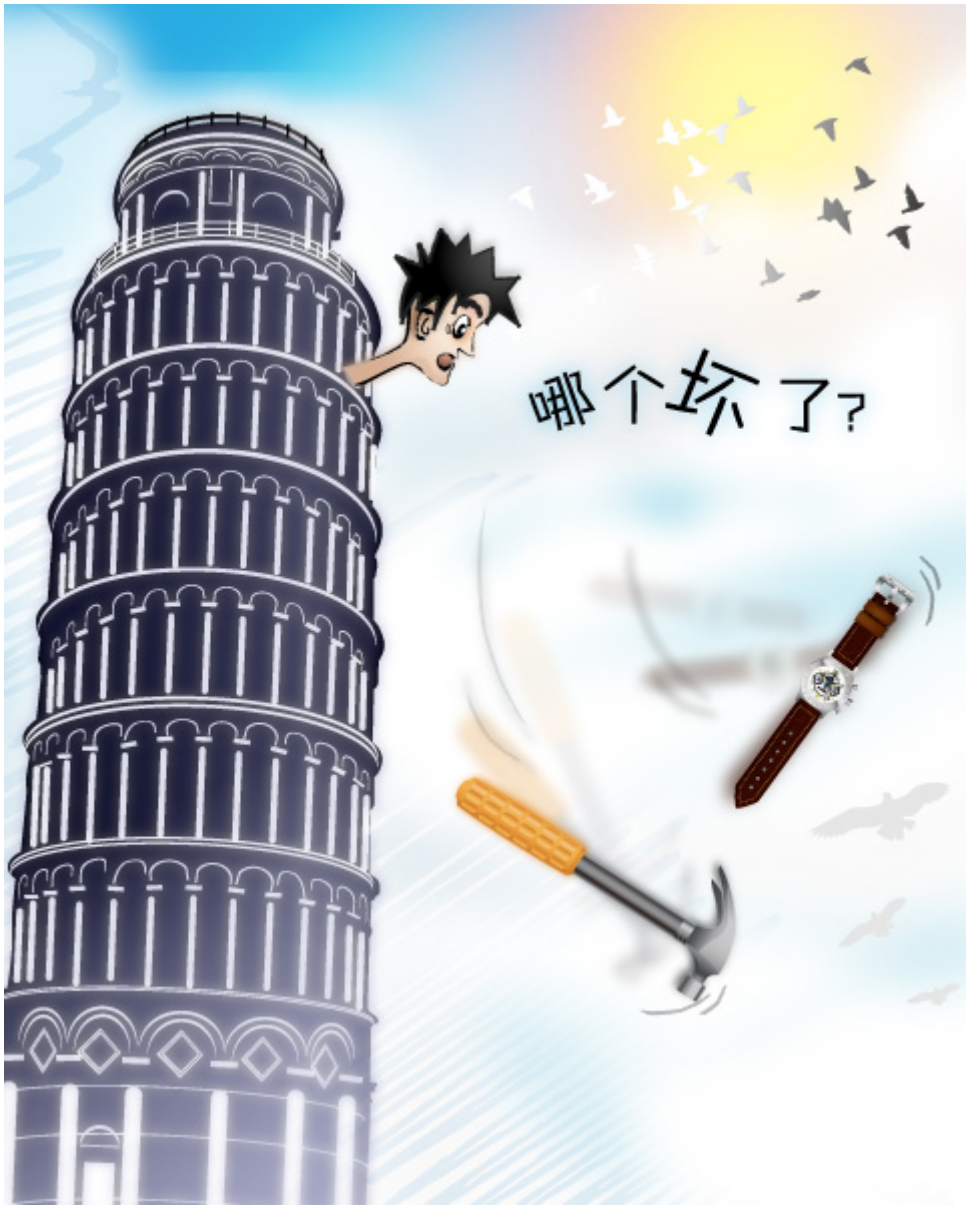

图 2.1 那个坏了?

从上述说明可知，简单的东西很容易做得高可靠，但复杂的东西要做高可靠花费的代价就高多了。这是普遍原则，对于嵌入式软件也适用。既然如此，哪为什么人们还要做复杂的东西呢？这就涉及第二定律了。

2.2 定律 2：越复杂的东西越容易做得稳定

记得大学刚入学时有军训，最后一项是打靶。本班奉命在打靶的前一天下午擦拭打靶用得半自动步枪，具体型号记不得了，但肯定是中国建国后早期生产的。在擦拭前教官给我们讲注意事项，其中有一句是这样的：“一个人擦一把枪，不要把零件搞混，否则装不上的。”也就是说，同样型号的两把枪，同一个零件不能互换！只是因为建国初期的枪都是使用简单的工具制造的，零件的尺寸、质量都不稳定，而一把枪上一些零件间的公差要求较小，只好用人工的方法筛选能够互相配合的零件组装成成品。这样，由于产品的零件的不稳定，造成了同一个型号的产品的零件互不通用。再看一些现在的枪支，不同型号的枪支60%零件可以互换是很正常的，这有设计的原因，同时也要归功于制造工具足够精密复杂，足以制造尺寸质量足够稳定的零件。

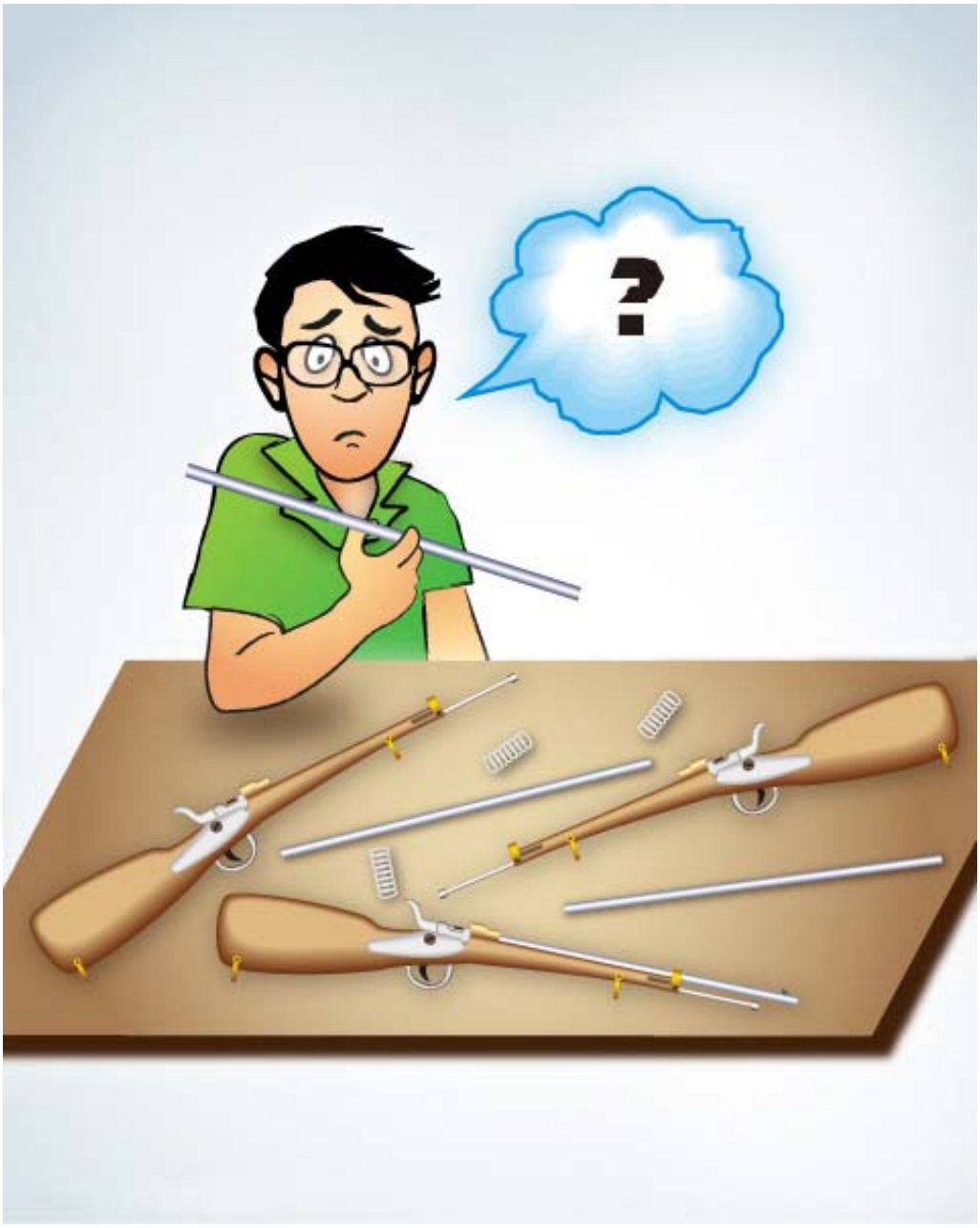

图 2.2　安装到哪里？

嵌入式系统软件也是这样。我们的代码越写越大，越写越复杂，很大程度不就是让软件在各种情况下都能够稳定运行吗？

2.3 定律 3：每个系统有一个最小的复杂度

一般普通的锤子必须有一个锤柄和一个锤体，锤柄最简单估计是圆柱体了，锤体也一样。似乎最简单的锤子就是由两个圆柱体组成了，笔者想象不出更简单的锤子。而要把锤子做复杂一些很容易，方法很多，例如在锤子上铸龙雕凤。

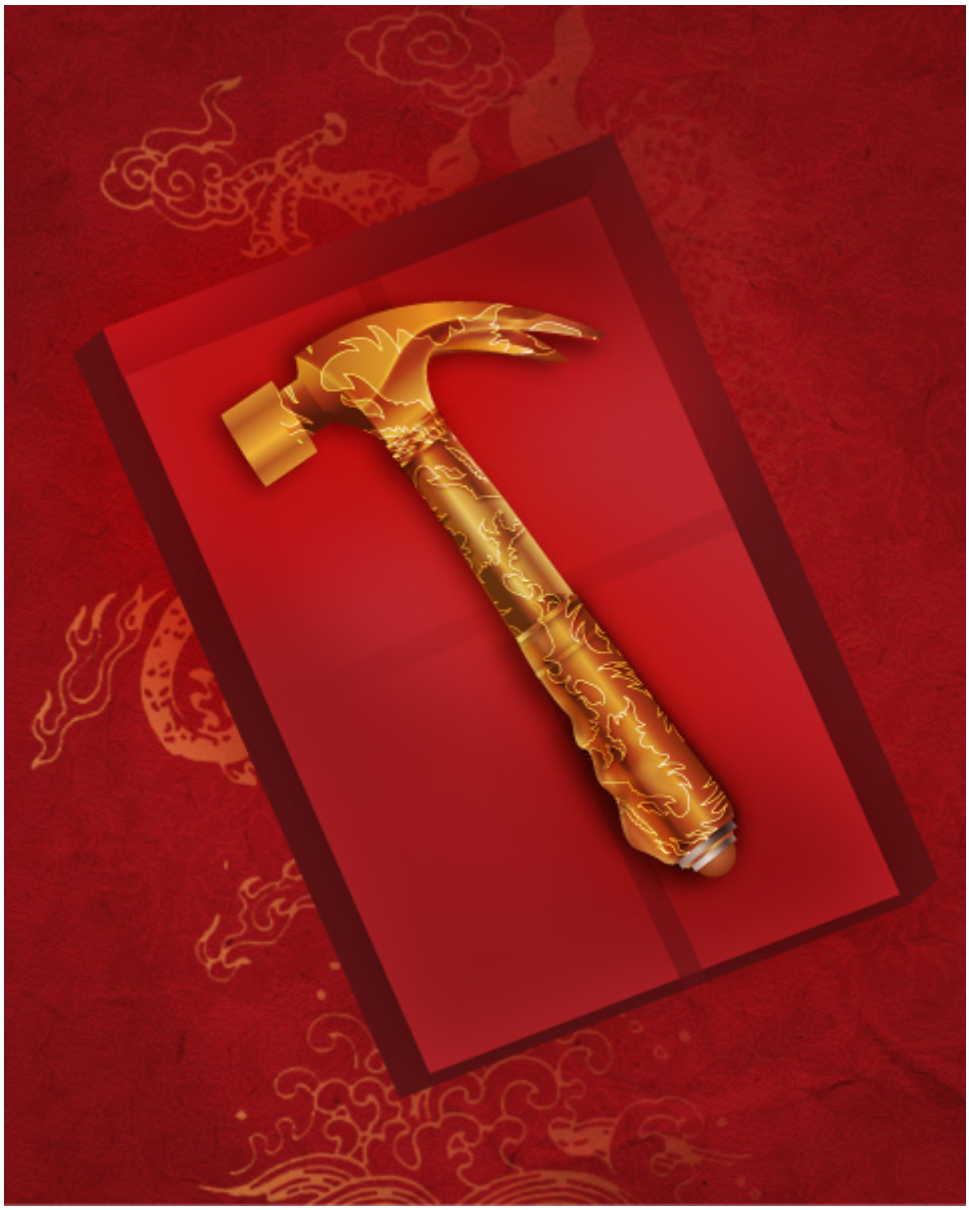

图 2.3 礼品锤？

也就是说，在相同的功能与稳定性的前提下，每个系统有一个最小的复杂度。锤子的功能是敲打东西，仅仅是这个功能的话，仅需要一个垂体即可，但那样容易伤到人的手（稳定性不好），所以需要一个锤柄。嵌入式系统软件也是如此。

2.4 结论

由上面3条定律可知，系统的稳定和可靠之间有一定的矛盾：提高稳定性容易实现的方式是降低系统的复杂度，这又往往降低了系统的稳定系。同样，提高系统的稳定性又容易降低系统的可靠性。要稳定和可靠都高就需要花费比较大的代价。

3. 功能与可靠性、稳定性之间的关系

由2节可知，系统的功能与可靠性、稳定性之间不是孤立的，是互相联系互相制约的，下面详细分析。

3.1 定律 1：功能的增加是依靠复杂度的增加而增加的

大家知道，普通的锤子只能锤东西，现在需要增加拔钉子的功能，锤体的一端需要改变形状，很显然更难制造了（复杂度增加了）。锤子功能增加了，可是也更难使用也更容易损毁了（锤子拿反了，用拔钉子的一面锤东西……）。

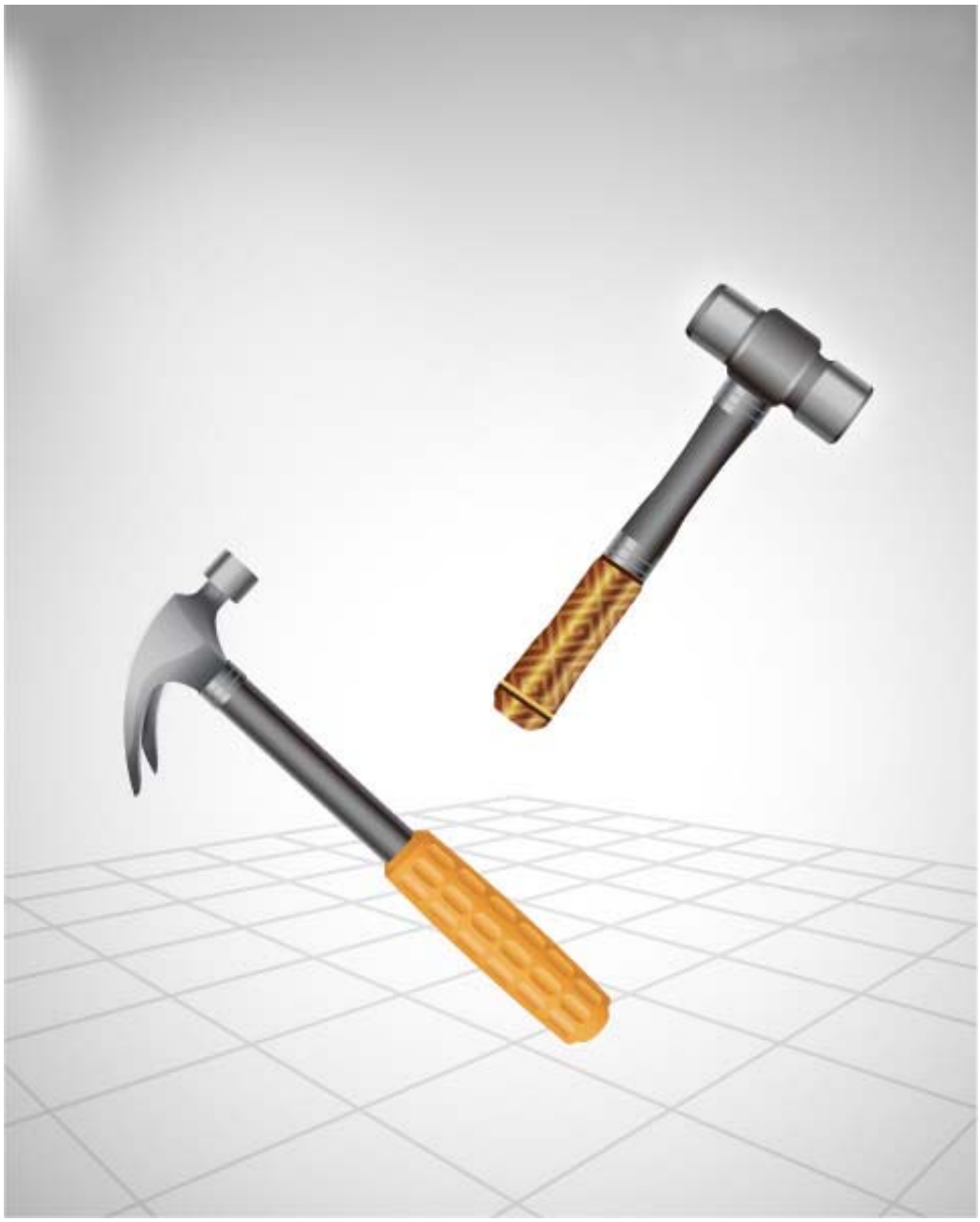

图 3.1 普通锤子与多功能锤子

由2.1小节可知，复杂度增加了，要保证同样的可靠性就需要花费更多的代价。显然功能和可靠性也是一对矛盾。

图 3.2　不是这样钉钉子的

3.2　定律 2：功能的增加可能造成单个功能的复杂度的减少

大家可以找一个目前市场上可以买到的最好的拍照手机，和一个普通的数码相机，比较它们的拍照效果。可以肯定，数码相机的效果更好。原因是拍照手机由于种种限制，不很把其集成的数码相机功能做得与普通数码相机一样复杂（镜头不够精密、闪光灯只能用LED或低挡的氖灯、感光元件也只能用简单的），当然稳定性要差一些了。对于嵌入式软件也是如此，受限于存储空间的大小、人机接口等，嵌入式软件的往往只能简化各个功能代码才能把它们集成在一起。

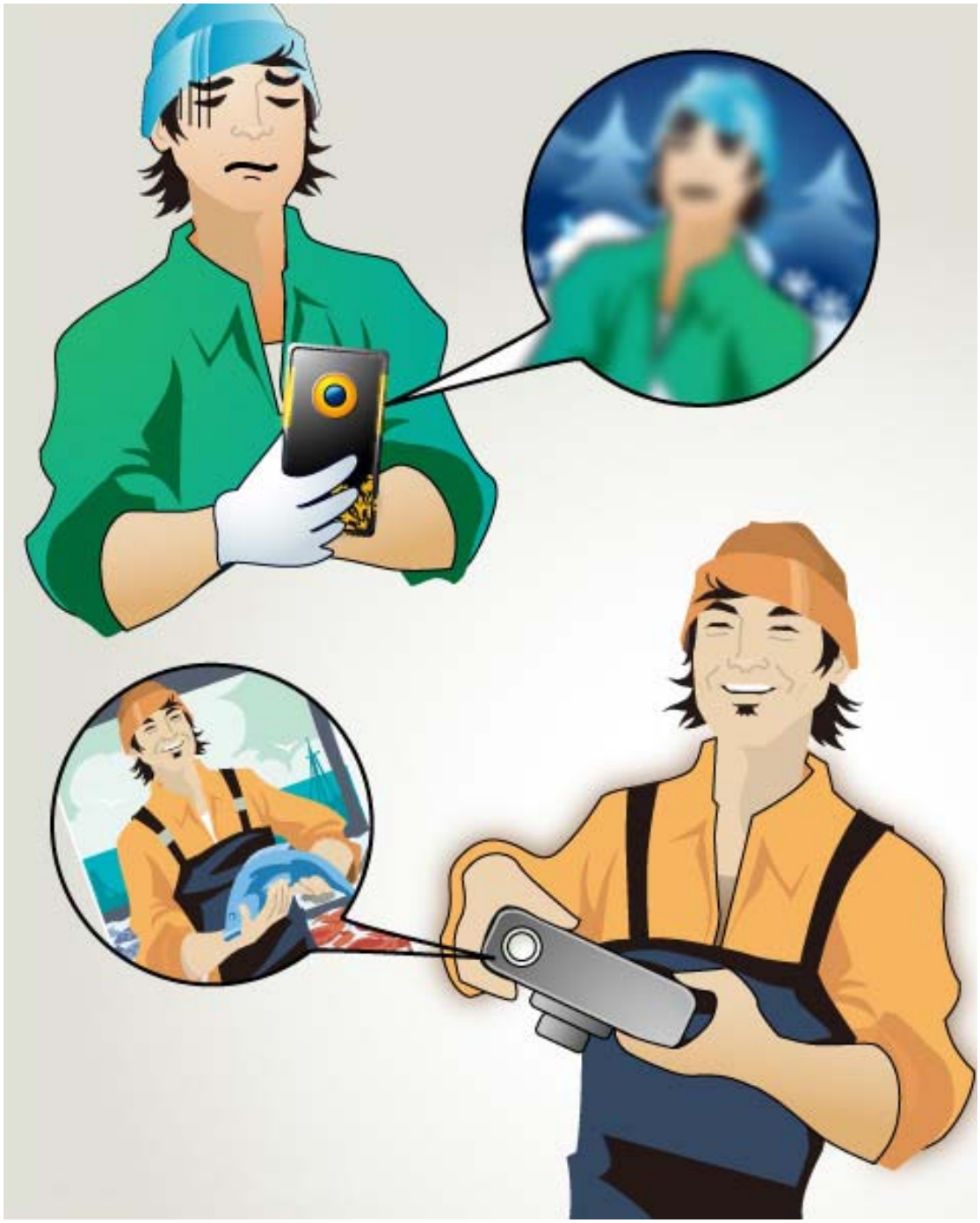

图 3.3　不比不知道

由2.2小节可知，复杂度降低了，要保证同样的稳定性是就需要花费更多的代价，根据2.3小节，保证同样的稳定性甚至是不可能完成的任务。显然功能和稳定性也是一对矛盾。

3.3　结论

由上面2条定律可知，系统的功能和系统的稳定、可靠之间有一定的矛盾。要功能多又要稳定可靠就需要花费比较大的代价。

4. 增加嵌入式系统软件的可靠性和稳定性的有效方法

4.1 优化系统框架设计可以提高系统的稳定系和可靠性

在一定的稳定性和可靠性的基础上，一个系统有一个理论上最小的最小复杂度，但在实际上要达到这个最小复杂度是不可能的。在实际工作中，往往如在锤子上雕花一样，增加了复杂度，不但不会提高系统的稳定性，如果做得不好，反而会降低系统的稳定性。系统的复杂度的增加，要保持原有的可靠性更困难，对提高系统可靠性没有任何帮助。

想要花费比较小的代价提高系统的稳定性和可靠性，比较好的办法就是减少系统不必要的复杂度。而对系统复杂度影响最大的就是系统框架，一个好的系统框架能够抑制系统复杂度的不必要的增加，并且在系统功能变化时对已存在的功能模块的影响降到最低。这样，提高系统的稳定性和可靠性所花费的代价就较低，间接提高了系统的稳定性和可靠性。

图 4.1　还是三角形稳定

4.2　稳定可靠来源于严格的测试

人永远不能完全了解世界，因此设计系统时不可能把所有的情况都考虑到。因此，稳定可靠不是嘴说出来的，也不能仅够通过分析系统设计而来确定。

提高稳定性的第二步来自严格的测试，包括先期的设计人员自己测试和中后期的第三方测试。在测试中发现了问题就必须修改设计并重新测试。如此反复，直到在一定的时间内测试不出问题。

4.3 稳定可靠来有赖于时间的检验

产品经过严格的内部测试和小批量试产并提供给友好顾客使用后（外部测试），终于大批量上市了。但即使这样，世界级的大公司也会出现产品大规模召回的现象，为什么？

前面说过，人永远不能完全了解世界，因此再严格的测试也不肯能模拟出实际使用过程中的所有情况。这样，用户使用的环境与方法与测试的环境与方法不一致时，产品潜在的不稳定点或不可靠点被暴露出来。如果这些不稳定点或不可靠点是致命的，产品必须被召回。如果不是致命的，也需要改进设计，提高系统的稳定性和可靠性。如此反复。如果系统大量和长时间的使用而不需要改进，说明是稳定可靠的。

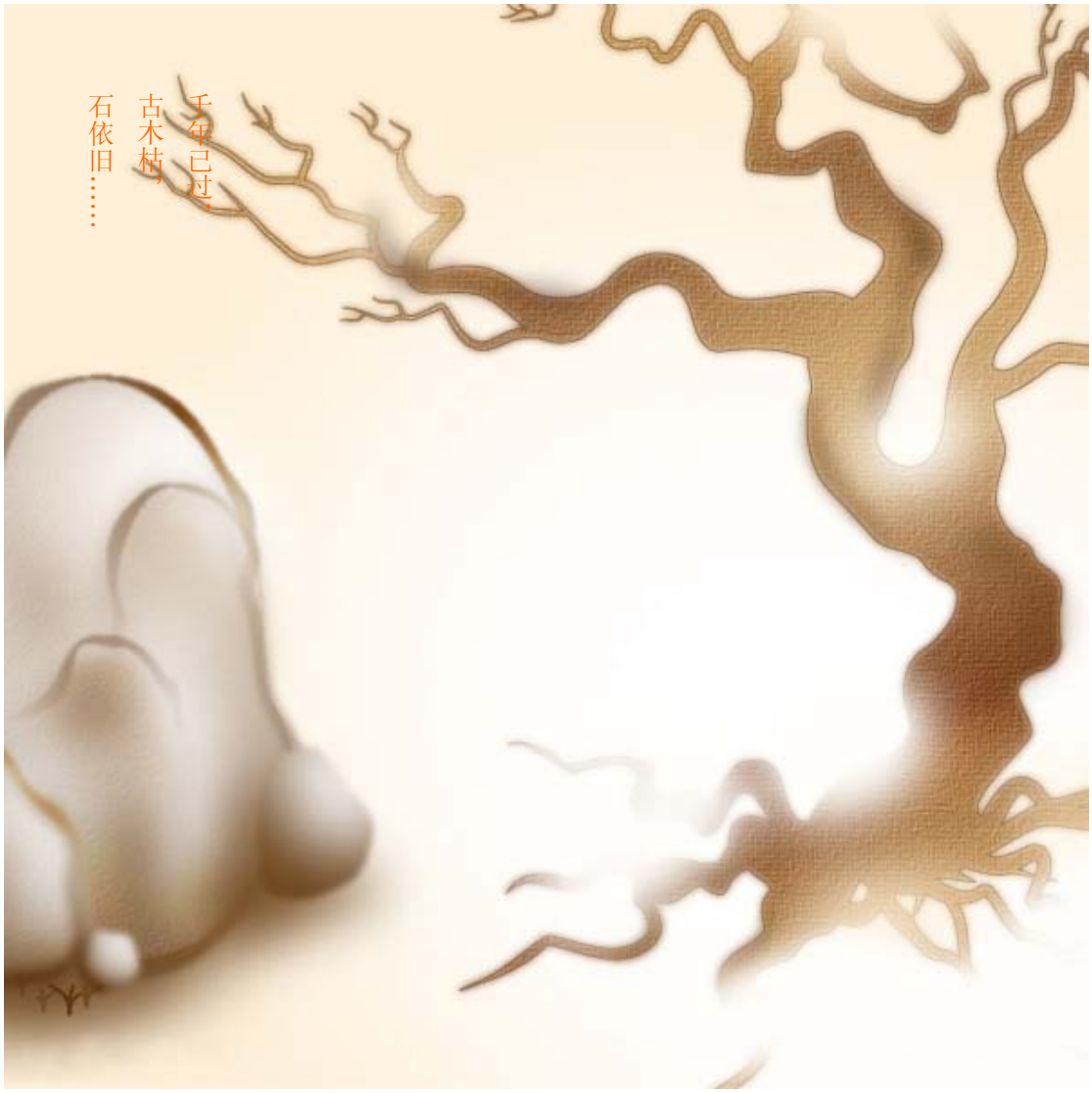

图 4.2　千年已过……

4.4 因为专业所以稳定可靠

在古代，如果您与专业打铁匠做铁锤，谁的产量和质量稳定可靠呢？显然是打铁匠。为是么？因为您是业余的而打铁匠是专业的。

为是么专业会导致稳定可靠？

最重要的原因是他们已经在这个领域花费了很多代价提高系统的稳定和可靠性（否则就不专业了），他们与非专业的已经不在一条起跑线上，非专业的想在短期内超过专业的是不可能的。

其次，是他们对本领域内的情况非常了解，制定的测试方法与实际情况符合度很高，增加了稳定性和可靠性。

第三，是他们可以利用已经经过时间检验的系统作为新系统的基础，甚至直接使用老系统，不可控的复杂度增加有限，只要花费较小的代价就可以保证系统的稳定性和可靠性。

5. 结论：专业分工合作是提高嵌入式系统软件的最快最省方法

随着技术的发展和社会的进步，现在用户要求嵌入式系统功能强大、性能稳定、工作可靠。一个系统功能强大、稳定的系统有的比较高的复杂度，但不是所有的复杂度都对系统的可靠性有大的负面影响。一个经过时间检验的可靠模块对系统可靠性的负面影响很小。

但一个强大的系统往往涉及多方面的知识，很多往往还不是自己的专业范围内，自己研发要做到可靠要花费的代价太大，甚至超过收益。此时，寻找专业的合作伙伴提供稳定可靠的模块集成到自己的系统中，自己只做自己专业内的部分，这样，复杂度的各个部分对可靠性的负面影响都较少，同时整体复杂度也容易控制，产品可以较快的上市。

嵌入式系统软件更加适合这种模式。这是因为软件是一种容易复制的东西，复制品的可靠性、稳定性和复杂度都不会改变。专业公司的软件模块一般已经被多个公司在完全不同的环境使用，其功能、稳定性、可靠性都经过严格的检验，不会对自己的系统带来大的负面影响。多个公司使用也分担软件研发的费用，直接使用成本较低。同时，专业公司对自己所属的领域非常了解，他们可以协助用户开发，更进一步降低用户成本。

所以说专业分工合作是提高嵌入式系统软件的最快最省方法。

6. 免责声明

1、 此文档著作权归广州致远电子有限公司所有，任何个人或者是单位，未经本公司同意，私自使用此文档进行商业往来，导致或产生的任何第三方主张的索赔、要求或损失，均与广州致远电子有限公司及其合作公司、关联公司无关。

2、 广州致远电子有限公司不保证本文档的正确性。除非特别声明，使用此文档所造成的任何后果由使用者自行承担。广州致远电子有限公司会不断修正文档中发现的问题。

3、 广州致远电子有限公司保留任何时候在不事先声明的情况下，对 AnyWhere 系统相关产品文档的修改的权力。

4、 本免责声明不断更新，如有未列出声明，以最新声明为准。

5、 本公司有修改任何一条“免责声明”之权利，以上声明之解释权归广州致远电子有限公司所有。