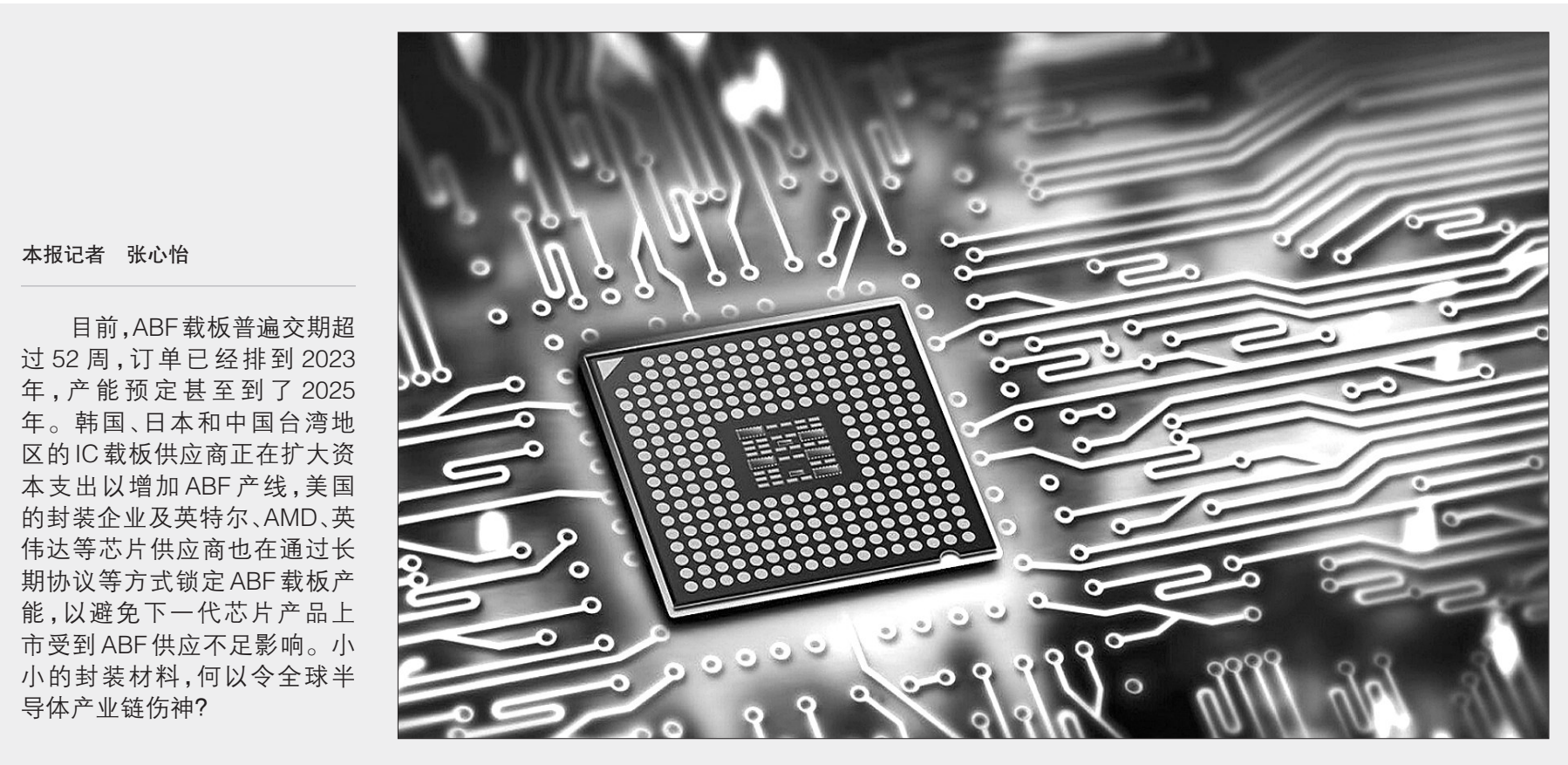


小小ABF载板，何以“梗阻”芯片供应链？



本报记者 张心怡

目前,ABF载板普遍交期超过52周,订单已经排到2023年,产能预定甚至到了2025年。韩国、日本和中国台湾地区的IC载板供应商正在扩大资本支出以增加ABF产线,美国的封装企业及英特尔、AMD、英伟达等芯片供应商也在通过长期协议等方式锁定ABF载板产能,以避免下一代芯片产品上市受到ABF供应不足影响。小小的封装材料,何以令全球半导体产业链伤神?

ABF载板景气狂飙

IC载板是IC封装中用于连接芯片与PCB motherboard的重要材料,主要功能包括为芯片提供保护、固定支撑及散热等。从封装材料成本端来看,高端倒装芯片IC载板的成本占比高达70%~80%,已经成为封装工艺价值最高的材料。

今年以来,IC载板量价齐涨,提升了PCB类供应商的营收表现。全球IC载板最大供应商欣兴电子的营收和毛利率已经连续三个季度呈现增长,1—9月份累计毛利较去年增长58%。在2021年前三季度,IC载板对于欣兴电子的营业贡献高达53%,占比相较于去年同期上涨了5个百分点。三星电机2021年第三季度营收同比增长21%,其中载板部门营收年增28%,台式机所需的低压CPU拉动FC-BGA(倒装芯片球栅阵列)封装所需载板用量持续增长。

依据基板材料分类,ABF载板(基材为日本味之素堆积膜的载板)和BT载板是IC载板的两大分支。其中ABF载板主要用于CPU、GPU、FPGA、ASIC等高运算性能IC。ABF基材匹配半导体先进制程,以满足其细线路、细线宽的要求。目前,ABF载板已经成为FC-BGA封装的标配。高性能计算应用以及PC、处理器等芯片,都对FC-BGA封装存在需

求。据悉,苹果公司自研的M1芯片就采用了FC-BGA封装,其ABF载板由三星电机供应。

受惠于5G、AI云端运算、大数据分析等应用带动高效能运算芯片需求,加上“宅经济”、远距离工作等场景推动CPU、GPU等LSI芯片用量倍增,FC-BGA基板需求大增,ABF载板景气上涨。香港线路板协会表示,2020年下半年起,ABF载板与BT载板价格分别上涨了30%~50%和20%。高盛证券预计2021年ABF载板将涨价15%,2022年再涨10%。

供给端是少数者的游戏

本轮ABF载板愈发严重的缺货行情,已经成为芯片供应链的主要“堵点”。

“ABF载板缺货将拖累高性能处理器芯片封装周期,提高相关上下游企业回款周期,大幅增加相关企业的运营压力。”芯谋研究高级分析师张彬磊向《中国电子报》指出。

从供应端来看,ABF缺货的主要原因是缺少ABF基材,而ABF基材供应受限,是因为其产能几乎集中在一家公司——日本味之素。据悉,日本味之素公司在1996年就开展了ABF的技术立项,仅用4个月的时间就完成了原型和样品开发,但寻求市场化却用了3年左右的时间,

在1999年之后才逐步推动ABF载板被芯片制造产业接受。在找不到市场的3年,日本味之素公司依旧看好ABF的市场前景,构建知识产权保护体系,不断提升技术壁垒,使得味之素在ABF产业构建了霸主地位,并保持至今。有产业链人士称,目前味之素的ABF产能已经跟不上市场需求,且扩产态度较为谨慎。

“味之素的ABF基材产能供不应求,是ABF载板缺货的根本原因。另外,全球能够量产ABF载板的企业数量较少,也限制了产能的释放。”开源证券副所长、电子行业首席分析师刘翔向《中国电子报》记者表示。

国内IC载板供应商兴森科技在3月12日投资者关系活动上表示,IC载板行业本来就是少数企业的游戏,在2019年之前因为PC、手机行业景气度较低,市场需求没有真正起来,行业主要参与者经营状况不佳,没有实施扩产,导致行业供给受限。

同时,新冠肺炎疫情和载板厂火灾等非人力原因所导致的偶然性停产,也加剧了ABF载板的短缺情况。

扩产的关键是人才

为了提升ABF载板的供应能力,日、韩、中国台湾地区的IC载板供应商纷纷投资扩建ABF载板产能。中国台湾地区

的欣兴电子、景硕等一线厂商都在加大力度扩张ABF载板的产能,新建或者改造部分BT载板产线,力求更进一步绑定海外大客户。韩国厂商方面,三星电机将投资1万亿韩元提升高端半导体基板供应能力,并集中在ABF载板。大德电子将在ABF载板方面投入4000亿韩元。日本Ibiden、Shinko也在扩建ABF载板产线。同时,英特尔、AMD、英伟达等芯片厂商正在寻求与IC载板供应商签订长期供应合同,以避免下一代CPU、GPU、HPC的生产因为载板供应不足而受到影响。

目前来看,ABF的产能补充至少要到2024年左右才能落实。

“IC载板横跨传统的印刷电路板以及半导体行业,扩产顺利也需要2年以上才能开出产能,而且现在设备的交期都大幅延长,所以虽然多家厂商都在积极扩产,但能否在2024年大量开出产能也很难说。”张彬磊说。

ABF的技术难点在于ABF基材和细线宽的制造工艺,技术门槛较高,扩产的关键在于能否招募足够的技术人才。

“ABF产能建设的关键不是资金,而是人才,因为ABF载板除了ABF基材之外,对高多层、细间距线路工艺要求极高。比如高端ABF载板层数已经高达20层,线路线宽进入6μm~7μm,考验厂商的技术研发和人才储备能力。”刘翔说。

英伟达Q3营收增长50% 重“安培”降“挖矿”展望元宇宙

本报记者 张心怡

北京时间11月18日,英伟达公布了截至2021年10月31日的第三季度财报。信息显示,本季度营收71亿美元,较去年同期增长50%,较上一季度增长9%,游戏、数据中心和专业视觉市场收入创历史新高。财报发布后,英伟达盘后股价涨幅超过5%。

“安培”成为增长主力

本财季,英伟达的游戏、数据中心、专业视觉业务均取得创纪录的营收。游戏部门营收达32.2亿美元,同比增长42%,季增5%;数据中心营收29.4亿美元,同比增长55%,季增24%;专业视觉营收5.77亿美元,同比增长144%,季增11%。

三个业务平台年、季双增的背后,是安培架构的市场穿透力走强。安培是英伟达于2020年5月发布的GPU架构,面向专业市场和消费市场分别采用了台积电7nm和三星8nm工艺。英伟达CFO Colette Kress表示,本季度游戏平台的收入增长受益于安培架构产品在假日季需求旺盛,专业视觉的增长主要来自安培架构在桌面和笔记本工作站的部署,数据中心的增长也主要受到安培架构的驱动。

“安培架构的销售额主要来自自然语言处理、深度推荐模型以及垂直行业等云计算和工作负载领域的大规模数据中心用户,驱动了数据中心业务的增长。”Colette Kress在财报解读中指出。

汽车和“挖矿”季减

英伟达的汽车和“OEM与其他”业务虽然也实现了同比增长,但分别出现了11%和43%的环比下降。

其中,汽车部门受益于英伟达自动驾驶项目启动,实现了8%的同比增长,但受限于整车企业的供应问题,营收出现季减。

而“OEM与其他”业务的季减,是由于加密货币的利润贡献降低。本季度英伟达出货的桌面级GeForce GPU基本都是限制哈希率的版本,以降低对于“挖矿”从业者的吸引力,确保更多显卡能够被游戏玩家购买。

对元宇宙寄予厚望

在财报发布中,英伟达CEO黄仁勋对虚拟协作平台Omniverse的发展寄予厚望。他表示,Omniverse的开发历时5年,能够与其他数字平台连接。英伟达的构想是未来工程师、设计师甚至自动化机器都可以连接到Omniverse,创造数字孪生和用于产业的元宇宙。

目前,Omniverse已经推出了用于生成交互式AI虚拟形象的平台Omniverse Avatar和合成数据生成引擎Omniverse Replicator,前者可以连接英伟达在语音AI、计算机视觉、自然语言理解、推荐引擎和模拟方面的技术,后者可生成用于训练深度神经网络的物理模拟合成数据。黄仁勋表示,Omniverse将用于协作设计、客户服务虚拟形象和视频会议,以及工厂、加工厂乃至整座城市的数字孪生。Omniverse汇集了英伟达在AI、模拟、图形和计算基础架构方面的专业知识,而这些也只是未来的冰山一角。

对于第四财季,英伟达预计收入将达到74亿美元,上下浮动2%。

(上接第1版)

根据IDC研究,随着云计算、大数据、移动互联网、物联网、5G等技术广泛应用到企业信息化建设和业务发展中,远程办公、业务协同、分支互联等业务需求快速发展,企业的员工、设备、合作伙伴以及客户需要通过多种方式灵活接入企业业务系统,企业原有的网络边界逐渐泛化。这导致基于边界的传统安全架构不再可靠,零信任成为一个必选项。

腾讯企业IT安全架构师蔡东赞在接受《中国电子报》记者采访时分析称:“从安全趋势上看,内网安全基于边界的安全已经不是那么牢不可破,数字化办公发展导致没有边界内网。核心的爆发点还是来自于疫情带来的物理隔离,大家远程办公,这是最基本的适用场景,人们已经不得不使用这种架构。”

同时,云计算业务天然需要零信任。云计算的快速发展和普及应用,包括应用云化、基础架构的异构化和混合化,业务的数字化生态化以及接入网络及设备多元化等因素,推动了更多企业开始通过部署零信任架构来建立能够适应云时代的全新安全体系。

Forrester高级顾问谷丰指出,从最初的原型概念向主流网络安全技术架构演进,从最初的网络控制平面的微分段向涵盖云边端的访问控制与网络防护全场景演进,零信任如今已经成为新一代安全架构的标准。零信任的兴起不能简单看作是某种技术、产品的扩展,而是对固有安全思路的改变,这是它的核心价值点。

中国零信任市场 尚未发育成熟

得益于云计算、大数据等技术的蓬勃发展,美国最早提出了零信任概念,且花费了大力气投入布局。从国家层面来看,美国国防

零信任：网络安全产业下一轮爆发点

部在零信任概念成型之前就已开始相关研究。2021年5月,美国政府发布的14028号行政命令《改善国家网络安全》,宣布要将联邦政府迁移到零信任架构。随后,《联邦零信任战略》《零信任成熟度模型》《云安全技术参考架构》相继出台,组成了联邦各级机构的网络安全架构路线。如今美国最大的安全公司不是防火墙类传统公司,而是零信任SaaS公司。典型的零信任公司Okta市值达333.51亿美元,远超传统安全公司。

Okta发布的《2021零信任安全态势》白皮书指出,2021年有82%的欧洲企业增加了在零信任建设方面的预算。另一家网络安全厂商Gigamon的调研结果显示,超过2/3的欧洲组织已采用或计划采用零信任框架,以应对不断变化的威胁形势。

而在国外已经实现规模化应用的零信任,在中国落地时似乎有点“水土不服”。尽管工信部2019年发布的《关于促进网络安全的指导意见(征求意见稿)》已将“零信任安全”列入需要“着力突破的网络安全关键技术”。但目前来看,零信任市场发展成熟度仍有不足。

“相较于欧美国家,国内在零信任方面仍处于起步阶段。”谷丰分析称,从技术及解决方案来看,国内零信任产品本身在功能以及技术方面仍处于发展过程中,能够提供零信任全面解决方案的厂商较为缺乏;从企业接受度来看,更多的企业处于初始的引入阶段,只有少部分企业已经部署了零信任产品和服务,并在进行优化和完善。

对于企业自身而言,零信任的实现并非

易事。邬怡指出:“一方面,老旧设备改造比较麻烦。零信任不是传统的网络安全,它还深入到应用安全和数据安全层面,需要对设备进行改造和升级,工程量较大。另一方面,零信任的实施成本相对较高。数据层面、应用层面都要做到防护,控制措施越多越细,投入也会越高,并且零信任还要对任何试图建立访问的人或物进行持续验证,成本会继续上升。”

此外,在企业选择零信任产品或解决方案时,往往对零信任仍然存在一些顾虑,例如架构过于复杂,内部文化的冲突,会浪费原有的安全资产等。谷丰认为,缺乏掌握零信任的人才以及企业内部的推动者、缺乏提供覆盖端和云安全性的全面解决方案,缺乏成熟的方法论体系、缺乏可借鉴案例等问题都会导致零信任“落地难”。

“从概念走向落地,零信任主要面临平衡安全性,或者说可用性与成本效益之间的挑战。技术不是目前最大的挑战,管理才是。”邬怡认为,零信任的构建需要打破原有管理模式,不仅需要安全团队的加入,还需要协同业务团队等共同建立起良好的沟通机制;同时,零信任建设从本质上讲是“一把手”工程,需要将整体建设深入到业务中去,不能仅存在于安全部门,这将涉及非常多的管理问题,需要长期构建才能真正落地。

“零信任相关技术仍需要持续改进,各技术模块间的集成与协同仍需进一步完善,其 在企业侧落地过程中不免仍将面对技术成熟度、产品和接口标准化,以及人员

配合等方面的问题。”IDC中国研究副总监王军民指出,“向零信任网络的转型,对于几乎所有企业的网络安全体系建设都是一次严峻的挑战。”

零信任架构建设 不是“一键切换”

根据市场研究机构Markets and Markets的报告,全球零信任安全市场规模预计将从2019年的156亿美元增长到2024年的386亿美元,年复合增长率为19.9%。在此基础上,开源证券预测,中性估计2024年我国零信任安全市场规模将达16.7亿美元。零信任有望成为网络安全下一轮爆发点。

要主动把握机遇,但不可盲目追逐浪潮。王军民表示:“零信任架构的建设不是‘一键切换’能够简单实现的,需要长期规划和建设,企业因为零信任建设而降低原有安全防护体系的投入是不明智的选择,特别是

(上接第1版)超高清视频,尤其是8K视频的实时回传,对移动网络的上行链路带宽有非常高的要求。演示所采用的DSUUU帧结构,通过为上行链路分配更多时隙,将现有毫米波技术的上行链路峰值速率提高到了3倍。2021年是5G加速普及的一年。现阶段,5G加速赋能千行百业,5G毫米波正通过增强上行链路的网络容量等优势,有效满足5G垂直行业的业务需求。冰雪体育赛事直

零信任架构建设前期,零信任理念还无法全面覆盖企业所有业务系统和数据。”

他建议,企业在进行了初期的试点应用后,应该充分利用技术提供商及其合作生态的整体方案能力,在零信任网络架构中更多地融入威胁情报、数据安全、网络威胁态势感知等能力,并增强威胁事件的可见性和自动化响应,以有效应对不断涌现的新兴威胁。对于自身网络安全技术能力和研发实力较强的企业,可以考虑在零信任架构未来建设中逐渐增强自研产品和技术的能力,将零信任架构建设成为具备更强自主研发能力的工程,更好地实现网络安全与业务发展的融合。

参照起步较早的国外市场,零信任商业化落地较为成熟,SECaaS(安全即服务)已成为主流交付。国内也已经有很多企业将零信任理念付诸实践,大多数零信任产品交付模式上仍以解决方案为主。蔡东赞认为:“未来,我国零信任交付模式也有望逐渐向SECaaS转变。”

目前全场景的零信任总体框架落地需求一般存在于大型、头部客户之中,例如大型央企、部委、大型银行等,邬怡建议,在统一的规划牵引下,以3~5年为一个周期进行整体的安全架构迁移,将零信任逐步落地到各个业务场景中去。当然,不少企业也选择从一些局部场景切入,例如在远程访问常态化背景下,零信任远程访问能力是不错的切入点。

播是凸显5G毫米波上行增强能力重要性的代表性应用场景之一,但5G毫米波的应用潜力远不限于此。在不远的将来,5G毫米波有望在更多行业应用中大有作为,同时推动各项服务的发展。比如在远程医疗、智慧工厂、智慧港口等多样化场景中,5G毫米波有望实现超高清视频监控多点并发上传、精准远程指导或控制等,为应用领域的拓展铺平了道路。