(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103053130 A
(43)申请公布日 2013.04.17

(21)申请号 201180042024.8
(22)申请日 2011.07.27
(30)优先权数据
102010040115.3 2010.09.01 DE
(85)PCT申请进入国家阶段日
2013.02.28
(86)PCT申请的申请数据
PCT/EP2011/062906 2011.07.27
(87)PCT申请的公布数据
WO2012/028391 DE 2012.03.08
(71)申请人 罗伯特·博世有限公司
地址 德国斯图加特
(72)发明人 M. 格布哈特 G. 莫尔冈 N. 特雷西
S. 布林德 N. 罗尔费 D. 赖希勒
A. 施泰纳特 T. 赖希 P. 奥斯丁
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 丁永凡 王忠忠
(51)Int.Cl.
*H04L 9/06*(2006.01)

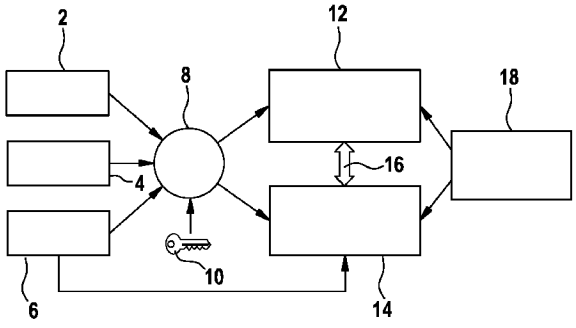
权利要求书 1 页 说明书 6 页 附图 3 页

(54)发明名称

用于为控制设备提供信息的方法

(57)摘要

本发明涉及一种用于提供信息的方法，所述信息被设置用于驱动汽车的控制设备并且被存储在至少一个原始文件(2,4,6)中，其中将从所述至少一个原始文件(2,4,6)中所选择的至少一个信息加密，并且其中使从所述至少一个原始文件中所选择的至少一个信息(34)保持未被加密，使得提供至少一个部分加密的文件(12,14)。




CN 103053130 A

1. 一种用于提供信息(32,34,35)的方法,所述信息(32,34,35)被设置用于驱动汽车的控制设备(36)并且被存储在至少一个原始文件(2,4,6,30)中,其中将从所述至少一个原始文件(2,4,6,30)中所选择的至少一个信息(32)加密,并且其中使从所述至少一个原始文件(2,4,6,30)中所选择的至少一个信息(34)保持未被加密,使得提供至少一个部分加密的文件(32,34,52),所述至少一个部分加密的文件(12,14,50)具有至少一个被加密的信息(52)和至少一个未被加密的信息(34)。

2. 根据权利要求 1 所述的方法,其中至少一个要加密的信息(32)通过至少一个列表(42)来选择。

3. 根据权利要求 1 或 2 所述的方法,其中将所述至少一个要加密的信息(32)的名称加密。

4. 根据上述权利要求之一所述的方法,其中所述至少一个至少部分被加密的文件(12,14,50)设置有签名。

5. 根据上述权利要求之一所述的方法,其中所述至少一个被加密的信息(52)嵌入所述至少一个部分被加密的文件(12,14,50)中。

6. 根据上述权利要求之一所述的方法,其中所述至少一个部分被加密的文件(12,14,50)与至少一个另外的文件(2,4,6,12,14,30,50)链接。

7. 根据权利要求 6 所述的方法,其中将所述至少一个另外的文件(12,14,50)同样部分地加密。

8. 一种用于提供信息(32,34,35)的装置,所述信息(32,34,35)被设置用于驱动汽车的控制设备(36)并且存储在至少一个原始文件(2,4,6,30)中,其中所述装置(28)包括计算单元(29),所述计算单元(29)带有加密工具(8,40),所述加密工具(8,40)将从所述至少一个原始文件(2,4,6,30)中所选择的至少一个信息(32)加密,并且使从所述至少一个原始文件(2,4,6,30)中所选择的至少一个信息(34)保持未被加密,使得提供至少一个部分加密的文件(32,34,52)。

9. 根据权利要求 8 所述的装置,所述装置包括解密工具(18,38),所述解密工具(18,38)将来自所述至少一个部分被加密的文件(12,14,50)的至少一个被加密的信息(52)解密。

10. 根据权利要求 9 所述的装置,其中利用控制设备(38)实施所述解密工具(18,38)。

# 用于为控制设备提供信息的方法

## 技术领域

[0001] 本发明涉及一种用于为汽车中的控制设备提供信息的方法。

## 背景技术

[0002] 控制设备软件使用还包括工作参数的文件来驱动汽车的控制设备。这种文件例如以 A2L 格式存在并且由文件的创建者提供给客户，用于作为汽车的组成部分使用在控制设备中。

[0003] 在目前的方式中，文件通常被减少了对于部件保护或技术秘密保护有关的量。被减少的文件被递送给客户以及可能的 SW 共享伙伴。通过去除关键量不仅保证了部件保护而且保证了技术秘密。与此同时，然而通过在客户方使用所谓的标签数据库需要提供包含所有量的文件，尤其是 A2L 文件。

[0004] 通常，所谓的 ZIP 格式用于压缩文件。为了密码加密，可以使用对称的加密方法如 AES（高级加密标准）。为了将二进制文件转换成 ASCII 格式，例如可以使用 Base64 并且因此使用用于对 8 位二进制数据编码的方法。

[0005] 在此背景下介绍了一种具有独立权利要求的特征的方法和装置。本发明的其他扩展方案从从属权利要求和说明书中得到。

[0006] 在扩展方案中，本发明涉及对文件的加密功能的应用，其被设置用于驱动技术设备的控制设备例如汽车的控制设备，以及应用措施如通过加密功能能够实现的部分加密。通常，这样的文件(或 Files)被整体加密，然而这会使这种文件整体不可用。尽管为了获得可使用的文件，仅加密数据内的各项并且因此仅加密数据内的各信息。这种被部分加密的文件可以用于标签数据库的运行，其中在文件内加密至少一个信息并且至少一个信息未被加密。通过已进行的部分加密，可以支持标签数据库或标识数据库，并且同时仍然保证了技术密码和部件保护。

[0007] 该方法在扩展方案中适于构建为 A2L 文件的文件。A2L 文件是通过 ASAM 群组标准化的文件，其包含关于确定的控制设备软件版本的周详信息。而用于实施应用系统的控制设备软件如 INCA、CANape 等需要这些信息。在 A2L 文件中，对于每个测量和调节量作为信息将相应的存储地址存储在微控制器（μc）中。可以是原装设备制造商(Original-Equipment-Maunufacturer,OEM)的客户通常要求提供完整 A2L 文件，在其中包含所有存在的量。在此，A2L 文件可以包含非常多的值得保护的信息例如参数，其在错误参数化的情况下会导致控制设备(ECU，electronic control unit（电子控制单元))的损毁。利用所设想的发明尤其可以保护这种信息并且

因此也保护控制设备以及被控制设备控制的部件。

[0008] 部分 A2L 加密的使用因此适于控制设备的应用工具(或 Applikationstools)，譬如 ETAS 公司的 INCA、Vector 公司的 CANape 或 RA-Consulting 的 Diagra。

[0009] 用于将调节量定义为信息的 A2L 文件的一部分可以如下地构建：

/begin CHARACTERISTIC（起始特征）-> 参数的例子

tLOCK_P.OSC_SVPWM_Dyc2PWM.OSC_SVPWM.OSC_Output

SignalsCalculation（信号计算）-> Funktionsbeschreibung（功能描述）

"Lock Time (in μS)"（锁定时间(单位为 μS)）-> 参数的描述

VALUE（值）-> 参数值 / 特征曲线 / 表格

0x801 C540E -> 控制设备软件中的地址

STANDARD_VALUE_U8（标准 _ 值 _U8）-> 数据类型

0.0

Ct_50ns s -> 物理折算

0.5 -> 最小可调节的值 10.0 -> 最大可调节的值 / 结束 特征

用于将测量量定义为信息的 A2L 文件的一部分可以如下地构建 :

/ 起始 测量 -> 测量量 CIF_B_rq_rscobd_diag -> 量的名字

"原设备管理 OBD 故障存储器和环境条件(停帧)"。该信号包含至相关副设备的状态信息,该副设备恰好曾要求擦除 OBD 故障存储器。相关 " -> 功能描述 UBYTE -> 数据类型

ident -> 物理折算式

110001

BIT_MASK 0x1

ECU_ADDRESS 0xD0003920 -> 在 SG 软件中的地址 / 结束 测量。

## 发明内容

[0010] 在本发明的一个扩展方案中,通过至少一个列表、通常为白列表(肯定列表)或黑列表(否定列表),定义哪些测量或调节量作为信息可从要提供给客户的文件中读取而哪些不能。工具(Werkzeug)基于至少一个所述的列表对未发布的信息例如测量和调节量进行过滤。在 A2L 文件中包含的并且值得保护的未发布的信息即其名称例如名字、描述、单位、式子的名字等等以及因此通常未发布的量要么通过加密方法来保护,要么通过加密哈希函数来保护。在此,在扩展方案中,要加密的信息的名称被加密。未发布的量因此对于使用者例如信息提供商的客户而言不可读。未发布的量的名字可以在所有软件版本上都保持不变。因此,在软件制造(Software-Make)或者软件编程时相对量的简单串行编号进行划界。

[0011] 如果要通过加密函数来进行保护,则未发布的量在此情况下利用常用的并且足够可靠的加密方法例如 RSA、AES、DES、RC5 等和密码来加密。被加密的量及其名称接着例如可以利用统一的前缀(在此为 :"Crypt_"表示为被加密的量。

[0012] 如果量的原始名字和因此原始名称例如为 B_k115,则在加密时产生的该量的被加密的名字以及因此被加密的名称可以为 Crypt_WL57RJVYW44GZRM2AJXLK3YXM。被加密的量和被加密的名称在此情况下可以用正确的密码又被解密。不需要用于将原始名字与被加密的名字关联的列表。这些名字可以根据所使用的加密和接着的编码而长度不同。

[0013] 如果设置通过哈希函数或控制值函数进行保护,则每个未发布的量通过加密哈希函数例如 MD5、SHA 等关联有唯一的哈希值并且用作量的名字。哈希值接着同样可以用统一的前缀表示并且因此标志为具有被加密的名称的被加密的量,在此 :"Crypt_"。如果原始名字为 B_k115,则借助哈希函数例如可以为所产生的被加密的名称,在此被加密的名字为 Crypt_c43437d52489a345133159fe48aacfaf。在此,所有量作为名称例如具有相同名字长

度，因为哈希函数产生固定数目的符号。密码在此情况下并不一定是必要的，被加密的量的被加密的名称的关联通常通过列表来进行。

[0014] 在所描述的扩展方案中得到的是，在作为 A2L 文件存在的文件中作为信息包含所有量。对于客户而言未发布的信息不可读，使得不可能回推出信息的函数。对于敏感信息而言整体上保证了技术秘密。

[0015] 部件保护的确保尤其通过构建为量的信息的改变的名称来改善，因为客户可能并非无意识地改变完全无意义的量，而在解释名字时不允许改变名字的引诱明显变得更大。尽管在本发明的范围中对文件进行部分加密，客户能够对由控制设备控制的量执行测量，但这些量对客户而言不可读，因为为此设置的控制设备可以进行控制设备内的解密。此外可以相应地调节确定的量，而该客户对此不必已知其他技术秘密。

[0016] 在其他扩展方案中，用于解密 A2L 文件的函数可以集成在(例如用于应用系统、控制设备的)应用程序中。该应用程序通常也构建用于对量进行测量、校准、诊断和 / 或存储。利用该应用程序，在输入对此所需的密码之后才显示被加密的信息的相应明文名字。因此，典型地可以使用部分加密的 A2L 文件。疏忽传送未加密的 A2L 文件的危险明显降低。此外，可以将解密函数集成在测量数据观察器或用于测量数据的显示设备中。接着在分析时又可以使被客户一同测量的不可读的量不可读，这能够实现测量数据分析的简化。

[0017] 在本发明的范围中，因此可以设置对数据至少部分加密。该措施可以包括名称的部分加密并且因此也可以包括名称的改变，即原始文件的一些信息的描述、变量、参数等等的部分加密和改变。

[0018] 相应地，通常，A2L 文件的部分即至少一个信息被加密。加密可以进行使得被加密的部分在不解密的情况下在客户处不能被使用。代替地，需要特殊工具，其能够利用相关的密钥解密并且使用 A2L 文件的被加密的部分。

[0019] 可替选地，在 A2L 文件中的项可以被部分加密，使得其也可以在没有事先解密的情况下并且在没有特殊工具的情况下被直接使用。只有被加密的信息的变量和参数的名字和描述通过该加密来改变，使得客户由此不能获得关于所基于的软件的技术秘密。

[0020] 信息的部分 A2L 加密例如因此可以进行，因为客户为了创建数据需要软件的所有标签或标识。然而，安全相关性和值得保护的信息并不提供给客户。

[0021] 根据本发明的装置构建为执行所介绍的方法的所有步骤。在此，该方法的各个步骤也可以由该装置的各个部件来执行。此外，该装置的功能或该装置的各部件的功能可以转换为该方法的步骤。此外，可能的是，将该方法的步骤实现为该装置的至少一个部件或所有装置的功能。

[0022] 本发明的其他优点和特征从以下说明书和所附的附图中得到。

[0023] 应理解的是，前面所提及的和下面还要阐述的特征不仅可以以响应所说明的组合而且可以以其他组合或者可以单独地应用，而不离开本发明的范围。

## 附图说明

[0024] 图 1 示出了针对根据本发明的方法的第一实施例的第一图表。

[0025] 图 2 以示意图示出了针对根据本发明的方法的第一实施形式的第二图表。

[0026] 图 3 以示意图示出了针对根据本发明的方法的第二实施形式的图表以及根据本

发明的装置的例子。

## 具体实施方式

[0027] 借助附图中的实施形式示意性地示出了本发明并且以下参照附图详细地描述了本发明。

[0028] 对附图予以关联并且全面地描述，相同的附图标记表示相同的部件。

[0029] 根据本发明的方法的第一实施形式借助图 1 和图 2 中的两个图表来描述。在该方法的实施形式中，由用于驱动控制设备的信息的提供商和 / 或制造商将在至少一个文件 2、4、6 内的信息提供给控制设备的客户和 / 或使用者，其中文件 2、4、6 的信息的部分被加密。

[0030] 图 1 中的第一图表表明了根据本发明的方法的第一实施形式的步骤，这些步骤由作为发送方的制造商和 / 或提供商实施。图 2 上的第二图表表明了根据本发明的方法的第一实施形式的步骤，这些步骤由作为接收方的使用者和 / 或客户实施。

[0031] 在发送方存在三个原始文件 2、4、6，其包含要提供给接收方的信息。此外，第一文件 2 包括私有数据，在此情况下包括为发送方的知识产权（intellectual property, IP）的信息。第二文件 4 构建为公共 A2L 文件，其包含其他信息。第三文件 6 包括存储器映射（memory image）并且例如可以作为 Hex 文件等等存在。

[0032] 为了至少部分加密在所述的文件 2、4、6 内的信息，由发送方通过第一加密工具 8 在这里未示出的计算单元中通过使用密钥 10 至少加密来自第一文件 2 中的要保护的私有信息。此外，来自第一文件 2 的所选择的私有信息通过使用密钥 10 被嵌入第二文件 4 中并且因此嵌入 A2L 文件中，其中在本实施形式中也进行加密和 ASCII 加密。在该步骤中，提供具有被保护的信息和签名的第一部分加密的文件 12，其中第一部分加密的文件 12 构建为 A2L 文件。

[0033] 通过使用校验（或 Check）和算法即为存储器映射提供第三文件 6 的签名，其中作为第二部分加密的文件 14 提供存储器映射的 Hex 文件。

[0034] 在对三个原始文件 2、4、6 的所进行的部分加密的情况下，这两个所产生的部分加密的文件 12、14 彼此组合并且因此链接。在另一步骤中，例如基于可以在至少一个列表中的预给定导出何种信息与第二例如作为 Hex 文件存在的文件 14 相关并且与来自第一部分加密的文件 12 的要保护的知识产权组合。可替选地，也可能的是，第一部分加密的文件与未加密的文件和 / 或完全被加密的文件链接。

[0035] 这两个通过链接 16 组合的文件 12、14 发送给接收方 18，使得包含 A2L 标准的一致性。

[0036] 由接收方（图 2 中的图表）进行被签名的并且部分被加密的文件 12、14 的接收 20，文件 12、14 还彼此连接 16。对于接收方而言可以利用文件编辑器读取第一部分加密的文件 12。然而，在此被加密的和因此被保护的信息不可读。修改或编辑签名的尝试会损坏文件 12。

[0037] 然而在本发明的扩展方案中设计的是，接收方调取执行的解密工具 22（其包括密钥并且例如由发送方提供），使得解密工具 22 在未示出的控制设备上执行。利用解密工具 22 可以使用部分加密的文件 12、14。进行解密工具 22 提供了对于解密第一文件 12 的被保护的部分（IP）所需的正确密钥并且校验签名。如果签名的校验不可能，则这暗示第一部分

被加密的文件 12 曾被进行篡改。在此情况下，在文件内的信息的进一步执行可以通过解密工具 22 中断。然而，如果签名的校验是可能的，则被加密的信息可以进行解密，使得现在被解密的信息作为附加信息通过解密工具 22 提供，以便为接收方提供扩展信息。

[0038] 利用所描述的本发明的第一实施形式可能的是，参与该方法的发送方以及接收方(其可以为原装设备制造商(OEM))交换文件 12、14。在此情况下，信息例如作为 A2L 文件存在并且作为存储器映射以 Hex 格式存在，其中这种 A2L 文件包括发送方的部分知识产权，其应该对于接收方不可得到。当然，接收方只有利用解密工具 22 才能利用被加密的信息。

[0039] 因此，由发送方为接收方提供作为信息的软件，其可以通过解密工具 22 来校验和发现。在此情况下，当已知软件的内部信息时，可以向接收方更好地显现该软件特性。利用第二部分加密的文件 14 可能的是公开仅仅确定的、所选择的信息，然而确定的信息作为知识产权(IP)加密和保护。

[0040] 然而利用解密工具 22 也可能的是，解密文件 12 的被保护的部分并且利用其中包含的信息来驱动控制设备，该控制设备包括解密工具 22。部分加密的文件 12、14 在本实施形式中附加地签以签名，其中该签名可以基于所述文件 12、14 的内容。该签名通过工具 8、22 来认证。因此，可以阻止尤其是部分加密的数据 12、14 的不允许的混淆以及其不允许的改变。

[0041] 根据本发明的方法的第二实施形式通过图 3 的图表来阐明。在此，图 3 示出了根据本发明的装置 28 的实施形式，该装置 28 具有计算单元 29，利用该计算单元 29 来执行作为软件的解密工具 40。此外，图 3 示出了作为数据包含多个原始信息 32、34 的原始文件 30。在控制设备 36 作为装置 28 的其他部件工作时，利用该控制设备 36 执行软件 38，其中使用这种文件 30 的信息 32、34。

[0042] 在根据本发明的方法的该实施形式中，至少一个所选择的信息(在此为第一信息 32)利用加密工具 40 来加密，该加密工具具有密钥并且在计算设备 28 上执行。而，至少一个所选择的信息(在此为第二信息 34)在文件 30 总并未被加密。通过至少一个列表 42 预给定要加密至少哪一个信息 32 和至少哪一个信息 34 要保持不加密。

[0043] 因此，根据进所行的部分加密，从原始文件 30 在通过加密工具 40 处理之后提供部分加密的文件 50。在部分被加密的文件 50 内，在所进行的部分加密之后，第一被加密的信息 52 源自原始文件 30 的第一信息 32。此外，部分加密的文件 50 也包含来自原始文件 30 的未加密的第二信息。

[0044] 部分加密的文件 50 可以在根据本发明的方法的另一步骤中还通过控制设备 36 来执行。为此，控制设备 36 包括作为软件 38 的软件部件的解密工具 54。解密工具 54 可以利用密钥在控制设备内解密被加密的第一信息 52，使得可以利用控制设备 36 执行基于加密的第一信息 30 的第一功能 56。在考虑第二未加密的信息 34 的情况下来执行控制设备 36 的第二功能 58。所述功能 56、58 通常适于控制并且因此适于控制和 / 或调节设置有控制设备 36 的汽车的至少一个部件。

[0045] 在根据第一要加密的信息 32 产生第一加密的信息 52 时，在所描述的本方法的实施形式中，也可以加密第一信息 32 的名称并且在此利用新符号顺序占用，其对于客户而言不可读。因此，加密的名称提供第一加密的信息 52，其根据所进行的加密源于原始第一信息 32，不提供对加密的信息以及原始信息 32、50 的说明。在此，现在被加密的第一信息 52 的

新加密的名称可以具有附加部例如前缀并且因此具有合适的标志，其在加密名称时为该名称添加并且标志这样的被加密的第一信息 52。如果对部分被加密的文件 50 进行解密，则第一加密的信息 52 的被加密的名称也被解密。在此，带有其原始名称的原始第一信息 32 又源自第一加密的信息 52。

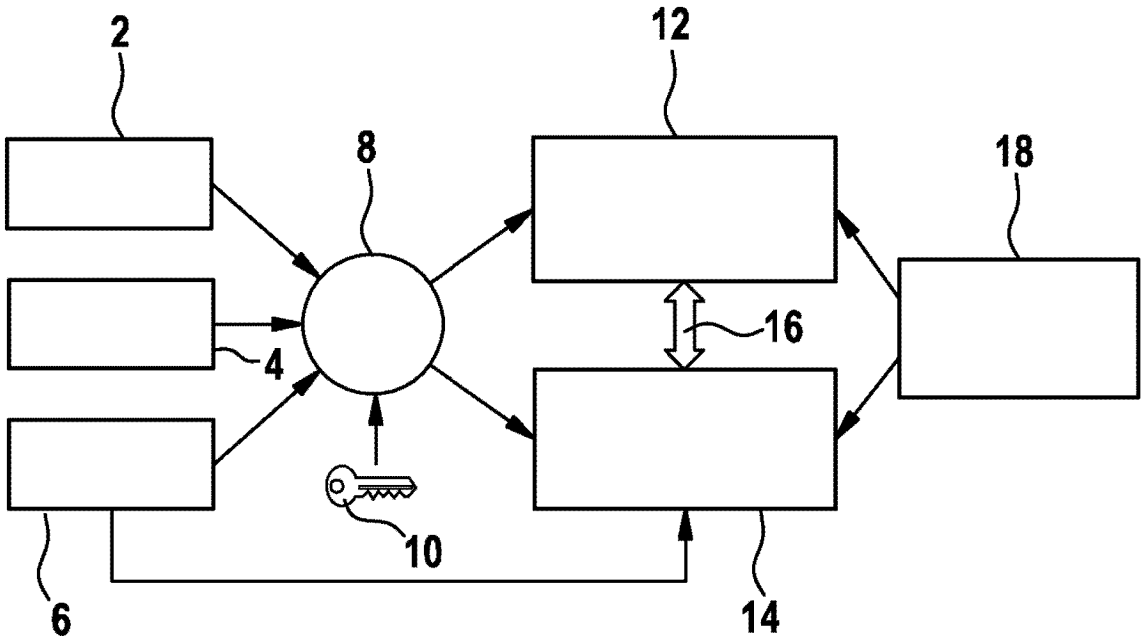



图 1

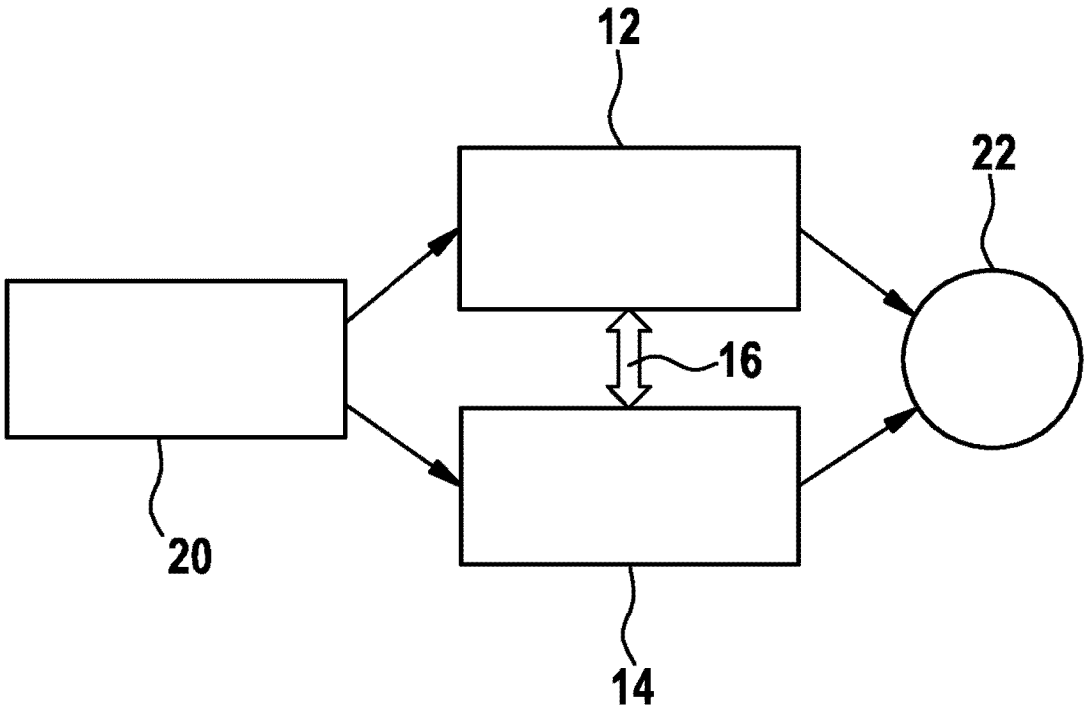



图 2

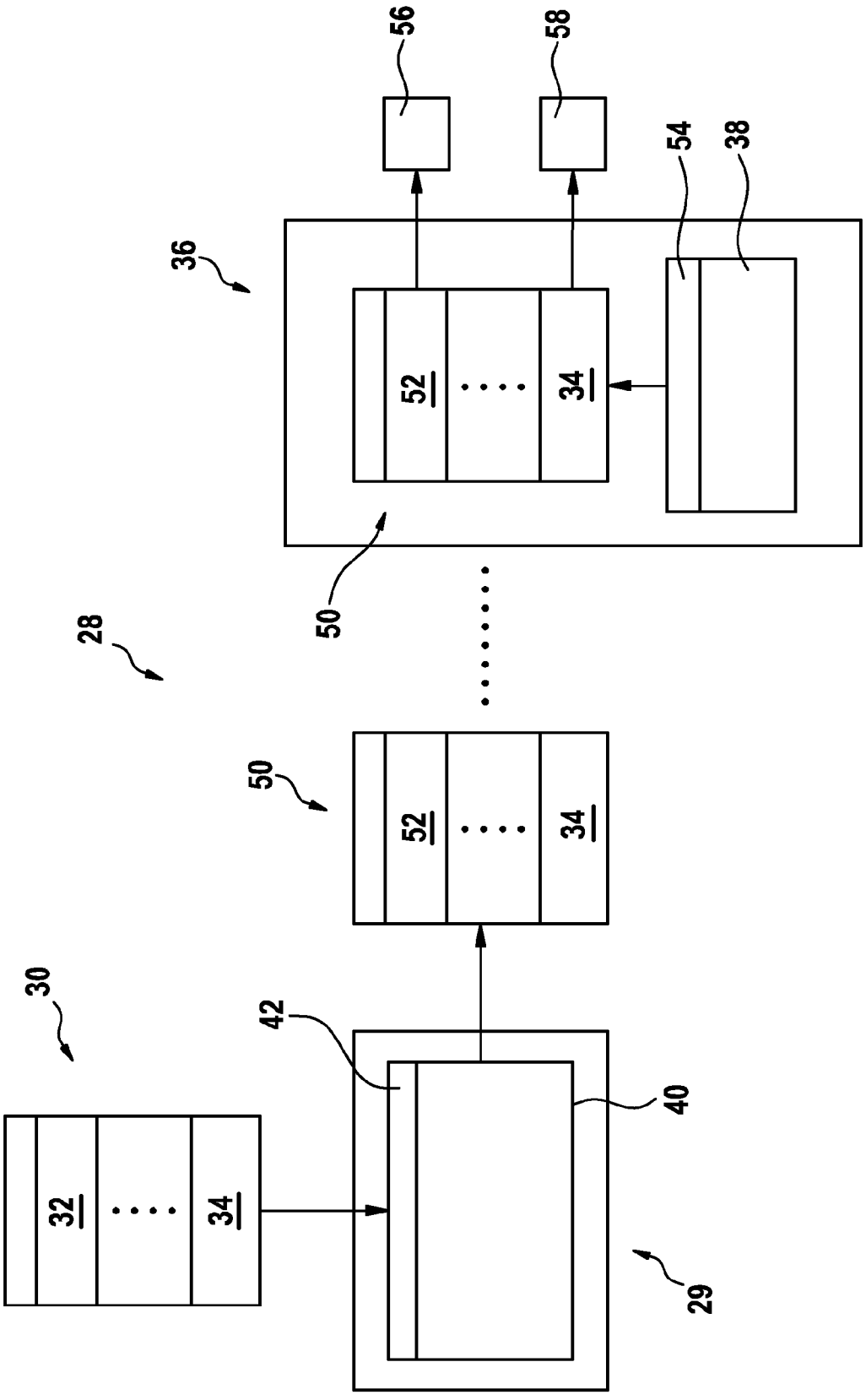



图 3