利用基于模型的系统工程探索演进的量子密钥分发网络架构

Hayato Ishida*‡, Amal Elsokary*‡, Maria Aslam*, Catherine White†
, Michael J. de C. Henshaw*, *Member*, IEEE, Siyuan Ji*, *Member*, IEEE
*Loughborough Quantum Systems Research Group, Loughborough University,
Loughborough, UK, {h.ishida, a.elsokary, m.aslam, m.j.d.henshaw, s.ji}@lboro.ac.uk
†BT Research, Ipswich, UK, catherine.white@bt.com
‡Both authors contributed equally

摘要—量子技术实现传感器、计算、计时和通信能力的重大进步，取决于将量子设备集成到现有经典基础设施中的高复杂系统工程。采用系统工程方法来应对日益增长的需要，即克服成熟量子计算对加密构成的威胁，以实现量子安全电信。本研究探讨了现有的未来量子通信网络，特别是量子密钥分发网络提案，以建模和展示量子密钥分发网络架构的发展。利用正交可变性建模和系统建模语言作为候选建模语言，该研究创建了可追溯的工件，促进模块化架构的发展，这些架构可以用于未来的研究。我们提出了一种基于变化驱动的框架来管理快速发展的网络架构，以满足利益相关者日益增长的期望。结果有助于量子密钥分发网络的系统性发展，并支持对更广泛的量子系统工程背景下的类似集成挑战进行研究。

***Index Terms*—基于模型的系统工程，正交变分模型，量子系统工程**

I. 介绍

自 2012 年以来，英国已投资超过 10 亿英镑用于量子技术，并承诺在未来十年内再投入 25 亿英镑 [1]。如果能够克服重大挑战，量子技术将带来巨大的能力提升和投资机会。一个主要的挑战是从实验室演示过渡到实用设备和系统；这将是未来投资的重点，而系统工程师在管理伴随而来的复杂性方面的作用不容小觑。在这篇论文中，我们提出了一种方法，通过这种方法可以将基于模型的系统工程（MBSE）应用于当代量子应用，以阐明系统中量子力学元素的功能和接口，从而为非专家提供一个易于理解的高层次视图。

This work was partly supported by the Innovate UK [grant number 10102791]

量子密钥分发（QKD）网络系统利用诸如叠加和纠缠等量子原理，使分布式节点间的信息传输安全。QKD 网络的一个主要应用场景是提供一种能够抵御量子计算机攻击的通信系统。原则上，QKD 系统提供了无条件的安全缓解措施，而未来的量子通信网络（QCN）预计将实现量子计算机之间的量子信息传输。利用集成了量子和经典信道的统一通信基础设施来实现组合功能，可以支持广泛的应用场景，例如在需要两者结合的 QKD 协议中。实施过程中甚至可能涉及物理共性，如在通信介质上同时传播量子和经典加密，这可能会降低成本但同时也存在从经典信道到量子信道交叉干扰的风险 [2]。

已公认将量子技术整合到现有的通信基础设施中面临巨大的挑战 [3]，部分原因是由于量子子系统的技术复杂性，包括其控制以及与所运行的经典环境接口的管理。这导致提出了采取定制化的系统工程方法来管理这种复杂性的建议 [4]，后来这种方法演变成为一个独特的跨学科领域，称为量子系统工程（QSE）[5]。然而，直到最近这一学科才获得了足够的动力，承认需要采用一种结构化的方法来解决已识别的工程挑战 [6]。在 QSE 中的一个特定研究方向是探讨 MBSE 如何支持管理量子系统的复杂性，就像它已经被成功应用于其他复杂系统（例如国防和航空航天领域）一样。鉴于量子物理学家和工程师用专业语言和图纸 [7]–[11] 提出他们的量子密钥分发网络架构提案，这些很可能无法被广泛的利益相关者所理解，特别是所有系统工程师，这自然激发了应用一种标准化和通用建模语言（如系统模型语言 SysML）来捕捉这种提案的想法。

此类调查中遇到了几个重大挑战。首先，建模一个 QKD 网络架构提案所需的努力可能非常大，因为所需的知識超出了单一学科的范畴，即量子物理、网络架构和 MBSE，至少可以说如此。其次，这些提案明显显示了重复模式。然而，在没有整体且量身定制的方法来识别和建模这些特定于量子系统的模式的情况下，从一个架构到另一个架构复用模型元素需要大量的人工努力。最后，大多数这些架构并不是针对明确的利益相关者需求设计的。事实上，创新往往在于详细设计层面，而不是在架构级别。这使得标准的自上而下的系统构架方法不合适。本工作的目标是解决这一挑战并分享我们的发现。

本工作的贡献可以概括为一个经过验证的框架，该框架可用于有效建模各种 QKD 网络架构，以促进模块化架构的可重用性、针对利益相关者需求组合新架构的灵活性以及向不同利益相关者有效地传达架构的效果。

本文结构如下。第 II节介绍了本工作的基本背景。然后在第 III节中介绍框架，并在第 IV节中对框架进行验证，该节还包括对该框架所提出方法的实际性、适应性和可扩展性的讨论。最后两节分别讨论相关工作并给出结论。

II. 背景

本节提供了本工作的基本背景知识。

A. 量子密钥分发

量子密钥分发（QKD），最初由 Bennett 和 Brassard 于 1984 年提出 [12]，作为 BB84 协议，一直是量子信息领域最活跃的研究方向之一。此后开发了一系列的协议，特别是 Ekert 基于纠缠的方案（E91）[13] 和测量设备独立（MDI）QKD [14]，每个都解决了之前协议中的不同安全和实施挑战。

对于任何 QKD 协议，都遵循以下步骤：

1) **量子传输**：合法各方（Alice 和 Bob）交换量子态。
2) **筛分**：经典元数据（例如编码和测量基）的公共比较会产生一个相关的原始密钥。
3) **后处理**：经典程序如纠错和隐私放大产生一个相同的密钥。

虽然总体框架是通用的，但各个协议在状态准备程序、测量方法以及后处理期间应用的校准技术上有所不同。QKD 利用量子力学定律来实现两个用户之间的密钥分发。由于安全性依赖于基本的量子定律，主要是不可克隆定理和情境性，QKD 提供了信息论意义上的安全加密。相比之下，RSA 作为最常用的经典加密协议之一，是计算安全的，这意味着它的安全性取决于计算难度假设。任何窃听尝试必然会引起可检测的扰动，使通信双方能够检测到窃听者的存在，并在信道受到破坏时中止协议。

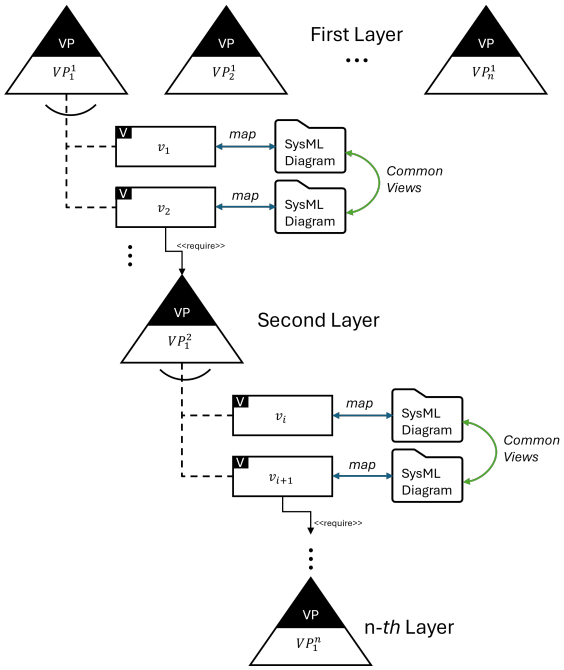


图 1: 一个不包含量子特定内容的分层 OVM+SysML 模型结构。

B. 基于模型的系统工程

基于模型的系统工程（MBSE）通过正式模型而不是叙述性文档来表达工程数据 [15]。这种方法增强了可追溯性，支持明确管理依赖性和接口，并减少了跨学科团队内部的误解——这一能力对量子技术尤为重要。MBSE 的另一个好处是其模块化：每个子系统都被表示为一个独立的模块，可以重复使用或进化，对邻近模块的影响最小。这种“分而治之”的方法允许工程师先掌握单个模块，然后再处理系统级交互，从而降低整体复杂性。

系统建模语言（SysML）是 MBSE 的主导标准。本研究中所有模型均使用 SysML 1.7 开发；随着建模工具的成熟，预计最近发布的 SysML v2 的采用率将增长。

C. 正交变异建模

正交变异性建模（OVM）在产品线工程中广泛使用，捕捉变异点、相关变体及其相互关系 [16]。变异点表示一个系统特性，该特性存在多种实现选项。因此，OVM 非常适合 QKD 网络，在这种网络中必须表示多个协议选择及其相应的架构影响。此外，该方法可以描绘预期配置，从而支持对替代系统演进的前瞻性分析。

III. 框架

A. 模型开发过程

为了探索不断发展的 QKD 网络架构并组织在架构设计中观察到的复杂性，受到 [17] 所述基于模型的产品线工程（MBPLE）和 [18] 所述变异实现机制启发，在本节中我们提出了一个基于模型的 QKD 网络架构探索框架。为了避免混淆，我们强调该框架不是一个典型的架构框架（例如统一架构框架），而是概述了一种方法，即将一系列已知的提议或实现的 QKD 网络架构实体通过结合 OVM 和 SysML 进行建模的方法，以支持对 QKD 网络系统的研究和未来发展。

B. 模型结构

框架的第一部分是一个非量子特定的模型结构，该结构在图 1中进行了开发和展示。如所示，在一个标准的多层分层 OVM [16] 内，对于 OVM 中的每个变体，都会开发出一种基于 SysML 的图表来提供对该变体的模型化规范。这会在 OVM 与基于 SysML 的模型之间创建一对一的映射关系。然后，对于一个变异点下的变体

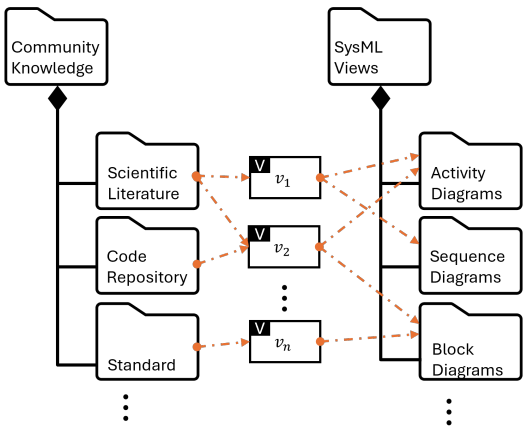


图 2: 示例模型开发过程（仅步骤 1 和步骤 2）使用量子特定知识。

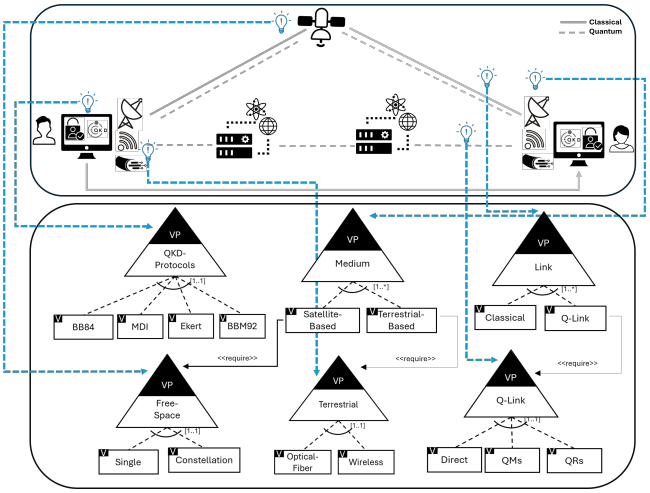


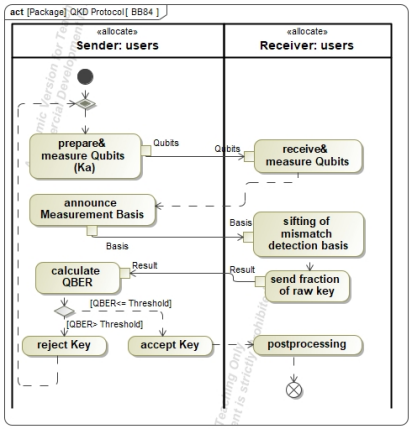
图 3: 来自领域特定知识的 OVM 骨干结构

组，会使用最适合该变异点概念的一种特定类型的图表（例如活动图）来对这些变体进行建模。这样可以使变体共享一种“共同”的视图，具有相似的结构，从而使得利益相关者可以探索这些变体之间的差异而无需调查其他变异点。我们强调，本框架提出的方法与 Li [17] 提出的方法相反，在他的方法中，变异点和变体是从基于 SysML 的系统模型推导出来的。在我们的框架中，则是在定义了变异点和变体之后再开发基于 SysML 的模型。这种做法得到了以下事实的支持：不同于软件、汽车和航空航天领域，在这些领域中由于工业化采用模型驱动的发展和 MBSE（基于模型的系统工程），系统模型往往非常丰富，而在相关工作部分回顾的研究表明，在基于模型的 QSE（量子系统工程）方面的工作却非常有限。

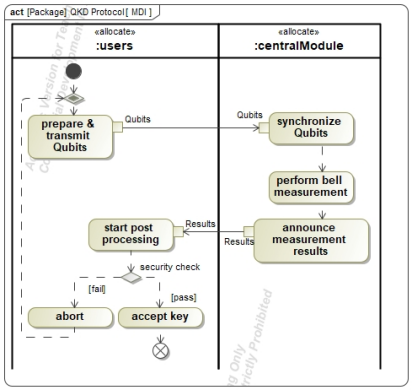
框架的第二部分是一个流程，如图 2所示，该流程能够开发一个基线模型，其中包括 OVM 主干和一组映射到 OVM 变体的 SysML 图表。这部分是量子特定的。

遵循框架模型结构的构建，人们自然会通过定义 OVM 主干开始模型开发，采用自上而下的方法，其中识别并指定第一层变异点及其相关变体。随后，按照图 1向下完成层级，直到达到足够的工程细节水平。然而，初步调查表明这种直观的自上而下方法效果不佳。这主要是因为量子技术的发展发现是由组件层面而不是系统层面的突破所驱动的，例如，量子存储设备 [19]。因此，我们提出了一种迭代、实验性的自下而上的过程来开发 OVM+SysML 模型。

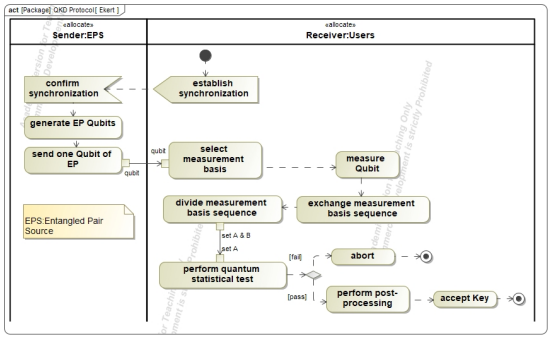
步骤 1 - 知识收集阶段: 此步骤涉及收集关于 QKD



(a) BB84 量子密钥分发



(b) MDI-QKD



(c) Ekert-QKD (E91)

图 4: 量子密钥分发协议过程。

网络的初始领域知识，细节足够丰富以支持下一步骤，但不需要详尽无遗。例如，这将包括实现量子行为的最新实验结果，这些行为有望具备商业可行性、经过验证的 GitHub 存储库，提供量子设备的数字孪生，以及社区认可的标准，用作基准衡量量子技术。

步骤 2 - 模型开发: 使用收集到的知识作为基础，我们随后推导出一个初始的非分组“变体”列表，这些变体代表了关键的量子特性，例如量子隐形传态。然后，对于每个变体，我们使用不同的 SysML 图来捕捉该变体的核心概念。在初步开发了一套视图（SysML 图）之后，我们再整体分析变体和视图：

1) 识别变体之间的结构和行为共性。
2) 将组变体相应地分组以定义泛化概念的变异点。
3) 对每个变异点进行视图规范化，使得在整个变体组中一致使用单一的 SysML 图表。

步骤 3 - 迭代: 承认可以有多种方式将知识组织成 OVM 主干结构，这会导致对变体进行 SysML 图规范化的方法不同。因此，第 3 步是关于尝试不同的 OVM 主干结构，并可能添加捕捉最近量子技术发展突破的知识。此步骤主要以试错为主，具有迭代开发过程的特征。虽然优化 OVM 主干结构可能会很困难，但我们建议定义并使用实验原则来推动这一步骤。例如，分组应该在对量子物理学家有意义且便于系统工程师用 SysML 建模之间找到平衡。

步骤 4 - 配置: 一旦完成 OVM+SysML 模型，配置可以根据利益相关者的需求进行组合。具体来说，对于任何给定的利益相关者需求，系统工程师可以与量子工程师合作，通过选择一组变体快速组成一个有意义的配置，而不是从头开始开发 QKD 网络架构。然后，初始的体系结构描述将是相应 SysML 图集的组合。我们强调，这个组成的体系结构描述不会完全代表现实中的 QKD 网络。这是因为 OVM+SysML 模型结构没有处理变体之间的相互作用。因此，这一步骤还需要对单个 SysML 图进行必要的修改，以确保视图之间的一致性，并创建特定于配置的接口定义。

IV. 验证

框架在本节中得到验证，以展示其适用性和可扩展性。首先，在上一节提出的框架指导下开发了一个基准的 OVM+SysML 模型。接下来是一个案例研究，展示了如何快速组成一个初始架构来解决高层次的利益相关者需求。最后通过讨论所提出框架的优势和局限性来结束本节。

A. OVM 主干和 SysML 视图

首先，根据广泛的文献综述定义了初始变体列表，例如 Refs [8]–[10], [20]。这些变体显示在图 3中。变体的分组定义了变异点（VP）及其层级结构，在图表中也

有展示。例如，不同类型的通信介质被归类为一个“介质”VP，不同的卫星排列则被归类为一个“自由空间”VP。这两个 VP 通过“基于卫星”的介质变体进行层级链接，表明如果选择了“基于卫星”的介质变体，则需要进一步指定卫星排列。为了使读者理解这些 VP 的意义，在 OVM 主干之上绘制了一个示意图，展示了 VP 试图抽象的内容。在到达这个最终版本之前，根据利益相关者的反馈导出了许多中间的 OVM 主干结构但都被舍弃了，这遵循了过程中的第 3 步指导原则。值得注意的是，并非所有的 VP 和变体都是量子特定的。这使得在平衡不同利益相关者观点的基础上决定最终 OVM 主干结构变得具有挑战性。

步骤 2 中的另一项并行活动涉及为变体开发 SysML 视图。同样，我们不展示所开发的中间视图，而只展示最终的、与 OVM 主干对齐的标准视图。

在图 4中，QKD 协议，BB84（图 4(a)）、MDI-QKD（图 4(b)）和 Ekert（图 4(c)）使用 SysML 活动图进行建模。序列图在之前的迭代中也被测试为可能的候选者（过程的第 3 步）。然而，选择了活动图为最终类型，因为复杂协议（如 Ekert）的交互机制可能导致一个冗长的序列图，使其难以与更简单的协议（如 BB84）进行规范化。活动图的内容限于操作流程，而不是显示行为细节。

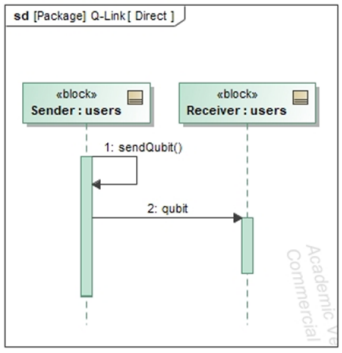
图 5说明了 Q 链接（量子链路）VP，并突出了不同的通信路径，其中图 5（a）描绘了两个用户之间的直接量子信道，即发送方和接收方。然而，直接的 Q 链接仅在短距离内实用。另一个序列图展示了如何通过使用量子中继器 [21], [22] 来建立长距离通信，这是一种更先进的量子通信技术，尚未完全实现。该序列图被认为是用于此 VP 的最合适的图表类型，因为链路机制旨在描述信息是如何交换的，而作为交互图的序列图正是用来建模信息交换的。

图 6显示了介质 VP 的建模，利用 SysML 块定义图以比较的方式捕获层次结构。选择块定义图是直截了当的，因为它是捕捉系统层次最方便的图表类型。

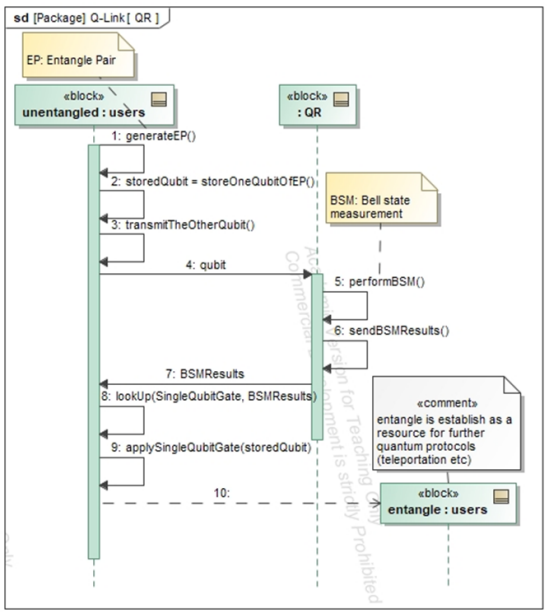
为了展示从 OVM+SysML 模型组成初始架构描述的有效性，我们进行了以下案例研究。

B. 案例研究：长距离通信

一个综合的利益相关者用例被制定如下：需要一个安全的网络来进行远程通信。该网络还必须具有韧性；

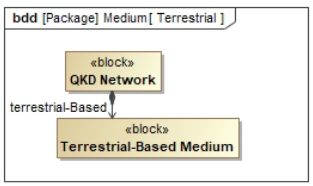


(a) 直接 Q 链接

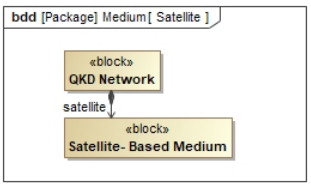


(b) 基于纠缠交换的 Q-链接

图 5: 量子链路变异性



(a) 基于陆地的中等范围



(b) 基于卫星的介质。

图 6: 量子密钥分发网络介质。

因此，它应该具备冗余性，以确保在网络的一个通道受到攻击时，网络仍能继续安全运行。QKD 是首选的技术来测试可行性。

在与量子系统工程师的讨论中，这些利益相关者的需求导致选择了以下变体：

- 对于中等 VP，选择了卫星和地面两种变体以确保网络在其中一个信道故障或受到攻击时仍然可用：
  - 对于所需的空间自由 VP，选择了“单一”变体，即一颗卫星
  - 对于所需的地面 vp，选择了光纤变体
- 对于 QKD 协议 VP，选择了 BB84 协议
- 对于 Q-Link VP，QR 被选中是因为直接量子链接无法实现系统保真度

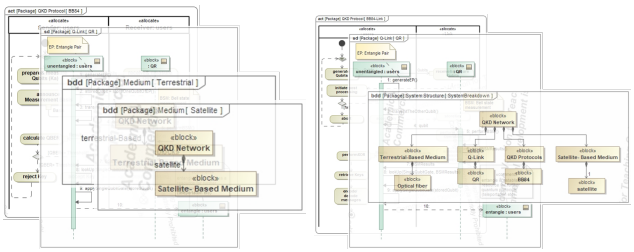
图 7和图 8展示了执行过程第四步所获得的结果。选定变体相关的视图组成如图 7 (a) 所示。这些视图随后被修改为一组新视图，以增强一致性，如下图 7 (b) 所示，服务于该配置的初始行为和结构架构描述。修订后的模型最终使这个特定 QKD 网络架构的接口定义成为可能。此接口定义使用内部块定义图来捕捉，如图 8所示。

C. 讨论

实用性- 框架指导下的 OVM+SysML 模型的成功开发，以及案例研究的成功完成，证明了框架在探索 QKD 网络架构方面的实用性。然而，也很清楚，为了演示目的，模型和案例研究都是简单的验证。更全面的验证需要进行多个具有不同利益相关者需求的案例研究，这些需求导致不同的配置。在将框架部署用于工业级研究之前，这样的验证是必要的。

有人可能会认为，为了增强框架的实际应用性，尽管这超出了本研究的范围，但评估架构是否符合利益相关者需求的能力对于未来版本来说是可取的。

适应性- 尽管该框架是专门为 QKD 网络架构的探索而开发的，但观察到该框架可以适应利用不同量子技术的其他类型系统，并且可能成为领域无关的。这是因为在框架中提出的模型结构如图 1所示是非特定于量子



(a) 组成的 SysML 视图 (b) 修改后的 SysML 视图

图 7: 初始量子密钥分发网络架构描述。

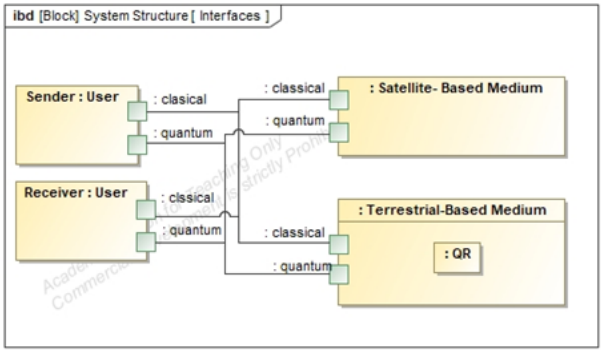


图 8: 组成配置的接口定义。

的，这意味着原则上可以按照在 [23] 中讨论的保持结构范式将任何知识解释为其中的一部分。

然而，在反思框架过程时，我们强调该框架对于系统架构已经相当成熟的领域来说实用性较低，例如使用喷气发动机的飞机。这是因为该框架的主要能力是通过自下而上的方法来探索尚未实现的系统架构。

可扩展性- 对于系统工程中的任何基于模型的方法，其可扩展性是面对不断增加的系统复杂性的典型关注点。这是因为随着系统规模的增长，模型元素（包括关系）的数量会迅速增加。依赖手动过程的方法不太可能具有可扩展性。我们认为我们的框架在 OVM 主干可以通过随时添加更多 VP 或变体来扩展方面提供了可扩展性，以应对新的突破。这是从使用 OVM 构建产品线模型中继承的特性。将 OVM 进行扩展面临的挑战可能在于需要一个全新的主干结构，这可能是由于颠覆性的技术突破导致遗留变体出现空白。

不可扩展的部分是配置过程。随着 VP 和变体数量的增长，为保持一致性而需要的手动干预可能会变得不可行。为了应对这一挑战，作为未来可能的工作方向，可以开发一种自动化机制以实现视图 [24] 的同步。该自动化机制可以考虑扩展 OVM 基础结构以包括变体之间的依赖关系，从而使配置空间大小的增长可控 [25]。

V. 相关工作

A. 量子系统工程

在量子系统或技术开发中需要采用系统工程方法这一点已经在此前 [4], [5], [26] 中讨论过，这些研究主要针对 QSE 必须解决的挑战。QSE 不同于直接将系统工程应用于量子系统的做法。这不仅仅是一个把熟悉的方法扩展到更复杂系统或技术的问题：量子技术在完全

不同的物理法则下运行，在这里叠加、纠缠和量子测量取代了经典系统中假设的确定性行为。由于量子领域独有的特性，特别是纠缠，量子系统工程面临着各种挑战。Everitt 等人 [5] 识别出两个主要挑战：接口问题和建模问题。接口问题是由于纠缠造成的，这使得不能将子系统视为孤立存在，阻碍了清晰界定边界、界面和需求。量子系统存在于希尔伯特空间中，并且张量积组合导致系统的自由度呈指数级增长，复杂化了建模与仿真。建模问题也源于量子系统模拟复杂性的指数级增长 [27], [28]。第三大障碍是环境耦合，引入了一个额外的挑战：不可避免地与周围环境相互作用会导致退相干，并模糊经典工程赖以实现模块化设计的系统边界 [26]。还有关于测试和可扩展性的其他挑战。此外，Henshaw 等人 [4] 的工作将这些量子系统工程中的挑战及问题映射到 ISO/IEC/IEEE 15288:2015 标准定义的技术流程上 [29]。他们的映射显示在需求捕获、架构定义、集成、验证和确认等过程中，当这些过程面对量子现象时存在特定的不足之处。因此，在术语上的挑战对于系统工程社区来说是熟悉的。

B. 量子系统的 UML 和 SysML

若干先前的研究已探讨了建模量子系统所面临的挑战。尽管量子软件工程与量子系统工程（QSE）有所不同，但它们共享统一建模语言（UML）和系统建模语言（SysML）等基础概念。Silverman 和 Jiron [30] 提出了使用 MBSE 和 SysML 对量子系统进行建模的方法，重点在于量子计算和架构。将 UML 应用于量子软件的研究比 QSE 方面的研究更为广泛。先前的研究已使用 UML 来建模量子软件或算法 [31], [32]。这些研究集中在量子电路级模型上，这可能无法扩展到未来量子计算机所预期的数千个量子比特。Pérez-Castillo 和 Piattini 的工作 [31] 扩展了用于量子软件的 UML；然而，这种扩展不能直接应用于包括硬件元素在内的更广泛的量子系统。

尽管之前的研究所致力于建模量子系统，但先前的努力并未完全解决 Everitt 等人 [5] 指出的挑战。这一结果并不令人意外，因为引用的研究关注的是量子软件而非完整的量子系统。因此，仍存在重大的研究空白。本文解决了量子系统中 SysML 建模的一些挑战；然而，对独特量子特征（如纠缠）进行精确的 SysML 表示仍然是未来工作的主题。

C. 基于模型的产品线工程

量子密钥分发网络系统很复杂，因为它们集成了经典和量子组件，并且 QKD 协议及其架构的种类不断扩展。为了管理这种复杂性和变异性，本研究调查了 MBPLE，即通过将 MBSE 系统的全范围可追溯性与 PLE 的变体管理结合起来的方法。MBSE 为工程师提供了一个清晰、一致的整体系统模型，但它对变异点的支持有限；因此，当需要许多产品变体时，工程师经常复制模型 [17]。相反，PLE 通过功能或选项模型来捕获变异性，但缺乏从每个选择到行为、结构和验证工件的显式可追溯性 [33]。结合这两种方法可以生成一个单一的可追踪系统模型，同时允许安全地选择和重用变体 [18]。

在 Schäfer 等人编目中的变异性实现机制 [18] 中，有三种机制特别适用于 QKD 网络产品线：

- 模块替换使工程师能够在不修改基线经典控制模型的情况下，替换成特定协议的设备（例如，诱骗态光源或纠缠光子探测器）。
- 条件编译在单一的超规格 SysML 模型中保留了可选的安全原语，并在构建时选择合适的原语。
- 多态性将不同的密钥管理算法与一个通用接口关联起来，保持了更高层次的编排。

补充这些设计时策略，Li 等人在需求层面的变体建模将功能选择从利益相关者的需求传播到功能性、逻辑性和物理性视图中，保持端到端的可追溯性——这是安全认证 QKD 部署的关键属性 [17]。变异点在需求视图中指定一次，然后传播到块图、行为图和参数图中，保持可追溯性而不增加图表混乱 [17]。

对于一个 QKD 网络，如前所述的部分所示，诸如协议族和量子链路等变体选择可以一次性指定并通过功能、逻辑和物理 SysML 层自动传播，从而在每个网络变体 [17] 中保持一致性和可追溯性。

VI. 结论与未来工作

本工作提出了一种基于模型的框架，用于探索快速演进的 QKD 网络架构并满足利益相关者的期望。该方法使利益相关者能够在不完全开发需求和架构的情况下研究采用量子技术对其系统的影响。通过利用 OVM，该框架能够实现配置的快速创建和评估。

目前，QKD 网络技术仍处于早期发展阶段，实际应用较少。随着量子通信网络的成熟，这一框架将作为

有价值的工具，指导其融入经典基础设施。为了完全实现这种预期的能力，一个自然的发展方向是扩展当前的 OVM+SysML 模型，纳入更广泛的架构实体，使得能够高效地组成更为复杂的配置。这些模型可以通过拉夫堡量子系统工程 GitHub 仓库 [34] 访问。

除了第 IV-C节讨论中强调的未来工作之外，我们还突出一个额外的机会：调查利用 SysMLv2 功能来增强框架的可能性，包括开发支持量子设备及其行为精确建模的全面模型配置文件或库。

致谢

C. White、M. Henshaw 和 S. Ji 感谢 QAssure 项目的资助，该项目由英国创新署（Innovate UK）支持，并且是英国国家量子技术计划中的量子挑战的一部分。

CRediT 作者贡献声明

石田隼人： 调查、方法论、可视化、写作 - 原始草稿。**阿马尔·埃尔索卡里：** 调查、方法论、可视化、写作 - 原始草稿。**玛丽亚·阿斯拉姆：** 写作 - 审阅和编辑。**凯瑟琳·怀特：** 验证、写作 - 审阅和编辑。**迈克尔·J·德·C·亨肖：** 监督、写作 - 审阅和编辑。**司元积：** 概念化，监督，撰写 - 原稿，写作 - 审核和编辑。

参考文献

[1] S. Wilkes, S. Brawley, S. Benjamin, S. Brierley, W. Chalupczak, D. Cielecki, T. Cubitt, M. Haji, A. Hammond, J. Hance *et al.*, "Quantum computing, sensing, and communications," *POSTnote*, 2025.

[2] P. Tan, T. Wang, H. Zhao, Z. Tan, P. Huang, and G. Zeng, "Simultaneous quantum and classical communication via multiparameter modulation," *Physical Review A*, vol. 109, no. 3, p. 032621, 2024.

[3] A. Orieux and E. Diamanti, "Recent advances on integrated quantum communications," *Journal of Optics*, vol. 18, no. 8, p. 083002, 2016.

[4] M. J. d. C. Henshaw, M. J. Everitt, V. M. Dwyer, J. Lemon, and S. C. Jones, "The challenges for systems engineers of non-classical quantum technologies," *arXiv preprint arXiv:1710.05643*, 2017.

[5] M. J. Everitt, J. D. C. Michael, and V. M. Dwyer, "Quantum systems engineering: A structured approach to accelerating the development of a quantum technology industry," in *2016 18th International Conference on Transparent Optical Networks (ICTON)*. IEEE, 2016, pp. 1–4.

[6] R. Claridge, R. Hancock, D. Harvey, G. Marshall, T. Rabbets, J. Vovrosh, and P. Yates. (2024) Quantum technologies: a new frontier for systems engineering? The Institution of Engineering and Technology (IET). Accessed 16 June 2025. [Online]. Available: https://www.theiet.org/impact-society/policy-and-public-affairs/digital-futures-policy/reports-and-papers/quantum-technologies-a-new-frontier-for-systems-engineering

[7] W. Chen, Z.-F. Han, T. Zhang, H. Wen, Z.-Q. Yin, F.-X. Xu, Q.-L. Wu, Y. Liu, Y. Zhang, X.-F. Mo *et al.*, "Field experiment on a "star type" metropolitan quantum key distribution network," *IEEE Photonics Technology Letters*, vol. 21, no. 9, pp. 575–577, 2009.

[8] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes *et al.*, "The secoqc quantum key distribution network in vienna," *New journal of physics*, vol. 11, no. 7, p. 075001, 2009.

[9] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, "Field test of quantum key distribution in the tokyo qkd network," *Optics express*, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[10] C. Huang, R. Guan, X. Liu, S. Li, W. He, H. Liang, Z. Luo, Z. Zhang, W. Li, and K. Wei, "Fully connected twin-field quantum key distribution network," *arXiv e-prints*, pp. arXiv–2504, 2025.

[11] M. Dianati, R. Alléaume, M. Gagnaire, and X. Shen, "Architecture and protocols of the future european quantum key distribution network," *Security and Communication Networks*, vol. 1, no. 1, pp. 57–74, 2008.

[12] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems & Signal Processing*. Bangalore, India: IEEE, 1984, pp. 175–179.

[13] A. K. Ekert, "Quantum cryptography based on bell' s theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[14] H. K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, 3 2012.

[15] *ISO/IEC/IEEE 15288:2023 — Systems and software engineering — System life cycle processes*, https://www.iso.org/standard/78832.html, ISO/IEC/IEEE Std., 2023, standard published jointly by ISO, IEC and IEEE.

[16] M. Hause and J. Hummell, "Model-based product line engineering–enabling product families with variants," *INSIGHT*, vol. 22, no. 2, pp. 43–48, 2019.

[17] M. Li, F. Batmaz, L. Guan, A. Grigg, M. Ingham, and P. Bull, "Model-based systems engineering with requirements variability for embedded real-time systems," in *2015 IEEE International Model-Driven Requirements Engineering Workshop (MoDRE)*. IEEE, 2015, pp. 1–10.

[18] A. Schäfer, M. Becker, M. Andres, T. Kistenfeger, and F. Rohlf, "Variability realization in model-based system engineering using software product line techniques: an industrial perspective," in *Proceedings of the 25th ACM International Systems and Software Product Line Conference-Volume A*, 2021, pp. 25–34.

[19] S. A. Moiseev, M. M. Minnegaliev, K. I. Gerasimov, E. S. Moiseev, A. D. Deev, and Y. Y. Balega, "Optical quantum memory in atomic ensembles: physical principles, experiments, and potential of application in a quantum repeater," *Uspekhi Fizicheskikh Nauk*, vol. 195, no. 5, pp. 455–477, 2025.

[20] F. Granelli, R. Bassoli, J. Nötzel, F. H. Fitzek, H. Boche, and N. L. da Fonseca, "A novel architecture for future classical-quantum communication networks," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 3770994, 2022.

[21] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, "Quantum repeaters: From quantum networks to the quantum internet," *Reviews of Modern Physics*, vol. 95, no. 4, p. 045006, 2023.

[22] C. Liorni, H. Kampermann, and D. Bruß, "Quantum repeaters in space," *New Journal of Physics*, vol. 23, no. 5, p. 053021, 2021.

[23] S. Ji, M. Wilkinson, and C. E. Dickerson, "Structure preserving transformations for practical model-based systems engineering," in *2022 IEEE International Symposium on Systems Engineering (ISSE)*. IEEE, 2022, pp. 1–8.

[24] S. Ji, C. E. Dickerson, and M. Wilkinson, "Requirements rationalization and synthesis enabled by model synchronization," *IEEE Open Journal of Systems Engineering*, vol. 1, pp. 26–37, 2023.

[25] M. Li, A. Grigg, C. Dickerson, L. Guan, and S. Ji, "A product line systems engineering process for variability identification and reduction," *IEEE Systems Journal*, vol. 13, no. 4, pp. 3663–3674, 2019.

[26] K. Bjergstrom, "Quantum systems engineering," Ph.D. dissertation, Loughborough University, 2020.

[27] R. P. Feynman, "Simulating physics with computers," Tech. Rep., 1982.

[28] M. Troyer and U. J. Wiese, "Computational complexity and fundamental limitations to fermionic quantum monte carlo simulations," *Physical Review Letters*, vol. 94, 5 2005.

[29] *ISO/IEC/IEEE 15288:2015 — Systems and software engineering — System life cycle processes*, https://www.iso.org/standard/63711.html, ISO/IEC/IEEE Std., 2015, standard published jointly by ISO, IEC and IEEE.

[30] S. J. Silverman and T. Jiron, "Quantum mbse and quantum sysml," in *MILCOM 2023 - 2023 IEEE Military Communications Conference: Communications Supporting Military Operations in a Contested Environment*. Institute of Electrical and Electronics Engineers Inc., 2023, pp. 95–99.

[31] R. Pérez-Castillo and M. Piattini, "Design of classical-quantum systems with uml," *Computing*, vol. 104, no. 11, pp. 2375–2403, 2022.

[32] X. Guo, S. Saito, and J. Zhao, "Quanuml: Towards a modeling language for model-driven quantum software development," *arXiv preprint arXiv:2506.04639*, 2025.

[33] C. Dumitrescu, P. Tessier, C. Salinesi, S. Gerard, A. Dauron, and R. Mazo, "Capturing variability in model based systems engineering," in *Complex Systems Design & Management: Proceedings of the Fourth International Conference on Complex Systems Design & Management CSD&M 2013*, 2014, pp. 125–139.

[34] H. Ishida and A. Elsokary, "Sysml v1 models for quantum-key-distribution (qkd) use-cases," Loughborough Quantum Systems Engineering Research Group, 2025, gitHub repository, accessed 13 June 2025. [Online]. Available: https://github.com/Loughborough-Quantum-System-Engineering/QCN-models