# Merify安全验证模块的语言支持分析

## 支持语言

Merify合约安全验证模块能够支持的合约语言包括Solidity源代码，及EVM字节码。对于Solidity源代码输入，需要保证代码能够被solc编译器正确编译为EVM字节码，对于具体Solidity语言元素的使用、编码模式、API使用，没有具体限制。而对于EVM字节码输入的合约，没有具体限制要求。

## 具体说明

Merify的验证引擎基于Ethereum黄皮书中定义的EVM虚拟机指令集语义，对所有类型指令都提供验证支持，并实现完整EVM架构（stack, memory, storage）。

具体而言，支持的指令类型包括以下大类：

* 0s: Stop/Arithmetic，停止及算数运算指令
* 10s: Comparison/Logic，比较及逻辑运算指令
* 20s: Sha3，椭圆加密指令
* 30s: Environment，区块链运行时环境信息
* 40s: Block，区块数据相关指令
* 50s: Stack/Memory/Storage/Flow，栈、内存、存储操作指令及控制流指令
* 60s&70s: Push，压栈指令
* 80s: Duplication，栈复制操作指令
* 90s: Exchange，栈交换操作指令
* f0s: System，系统相关操作指令

其中，面向安全验证分析需求，部分指令提供特殊支持（涉及跨合约及数据操作），即生成符号化变量进行统一分析，以保证该操作能够保证不产生漏报。

* CALL/CALLCODE/DELEGATECALL：返回符号化远端合约的具体执行结果
* EXTCODECOPY：返回符号化远端代码
* EXTCODESIZE：返回符号化远端代码大小
* RETURNDATACOPY：返回远端函数调用返回值返回符号化结果
* RETURNDATASIZE：返回符号化返回值大小结果
* CREATE：返回一个符号化创建合约地址
* SLOAD：创建符号化storage字典入口数据。