May, 2024 | Beijing

Organizational Code Quality Improving
组织级软件质量提升

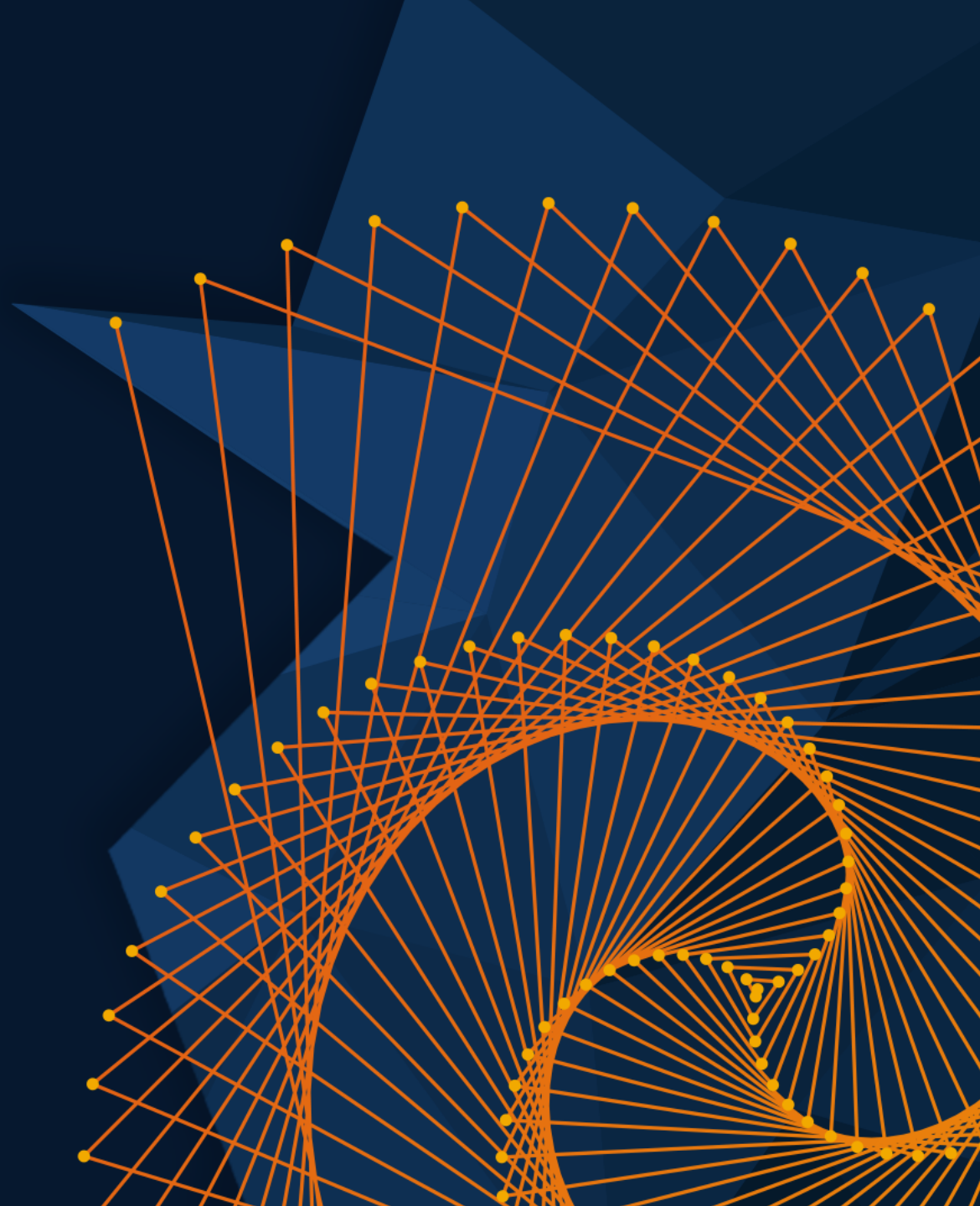
Yujian Chen - Lotus

MATLAB EXPO

MATLAB EXPO

大纲

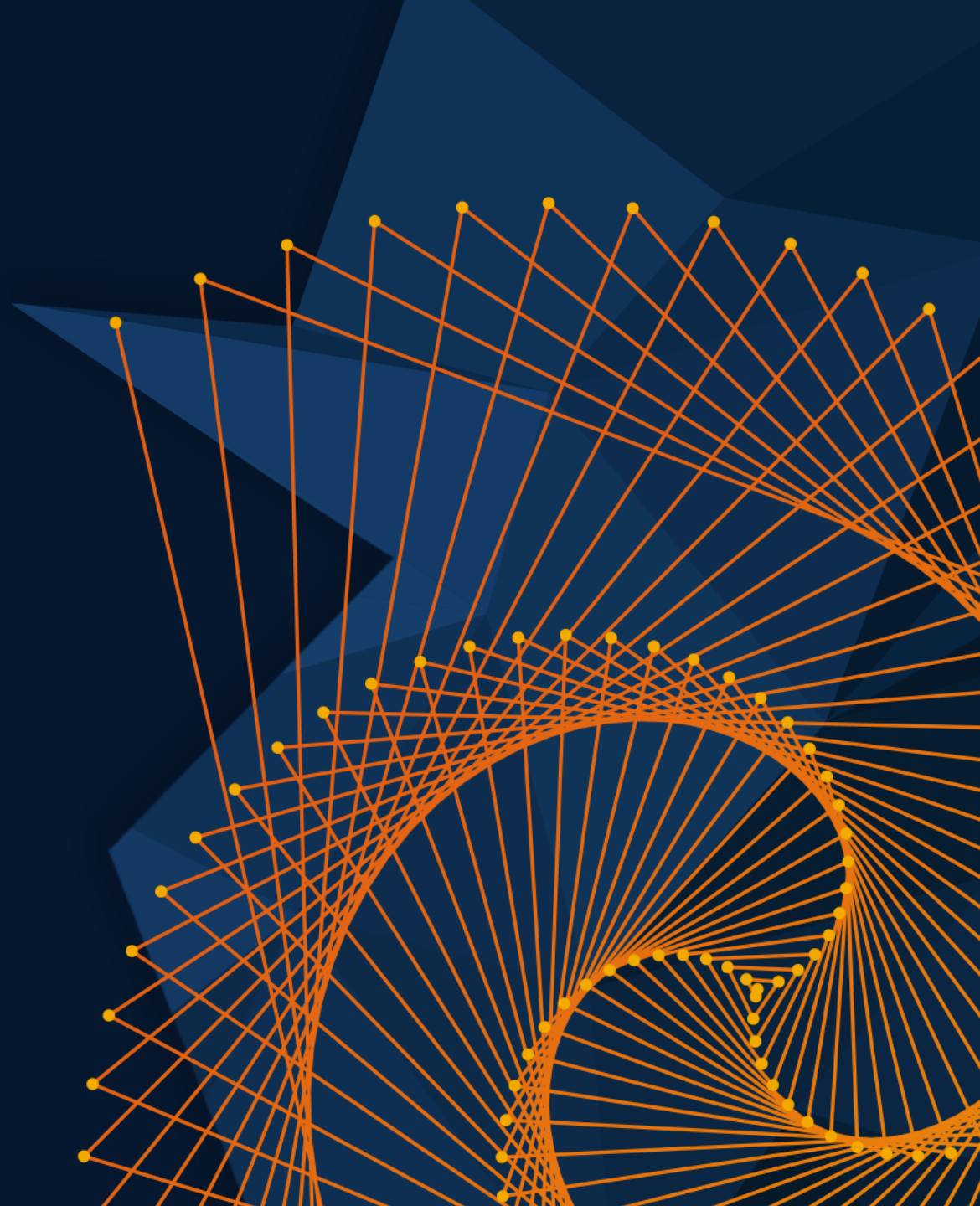
- About US
- 方法论：控制组织代码质量
- IT 实现与质量实践



MATLAB EXPO

大纲

- About US
- 方法论：控制组织代码质量
- IT 实现与质量实践

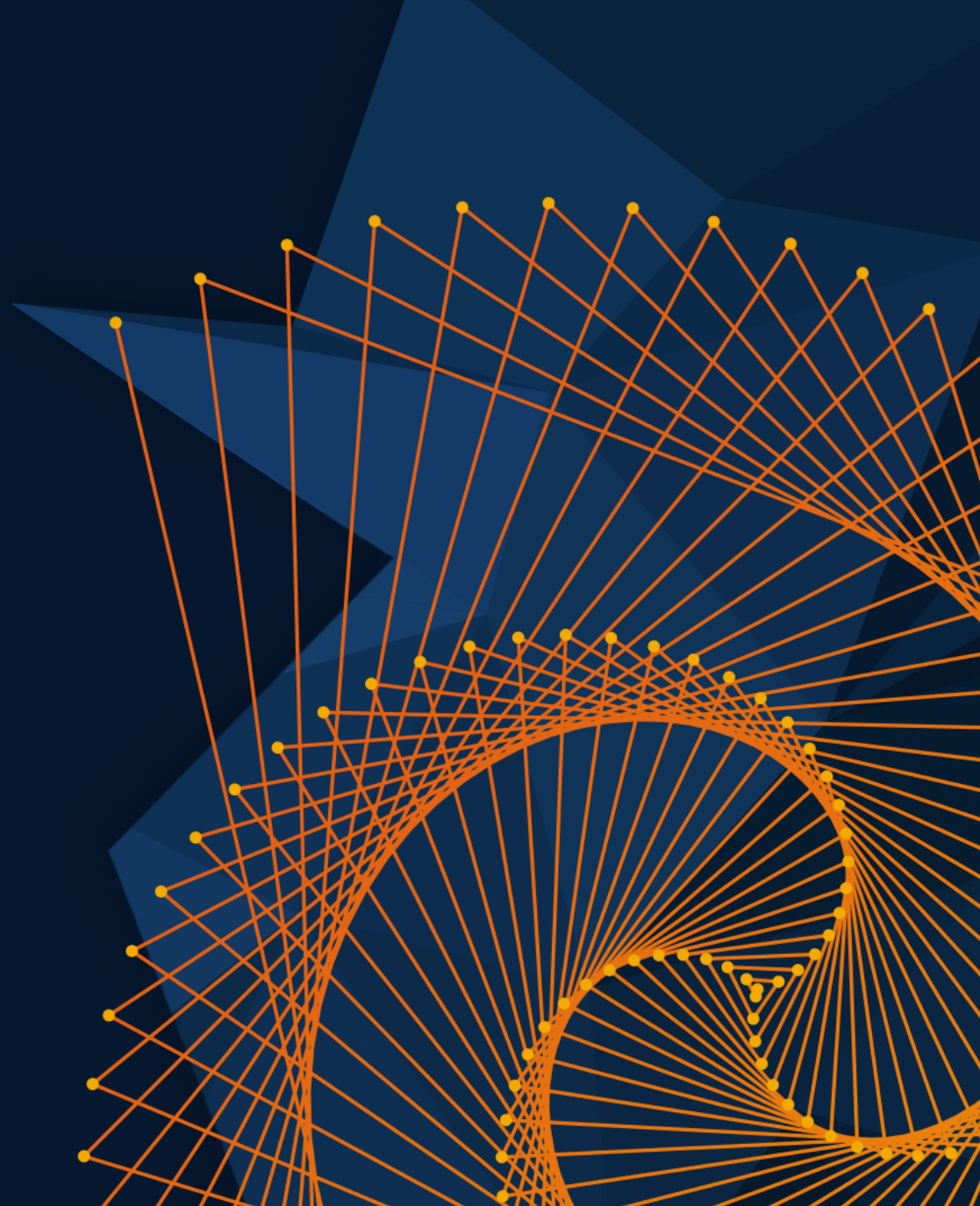


About US

MATLAB EXPO

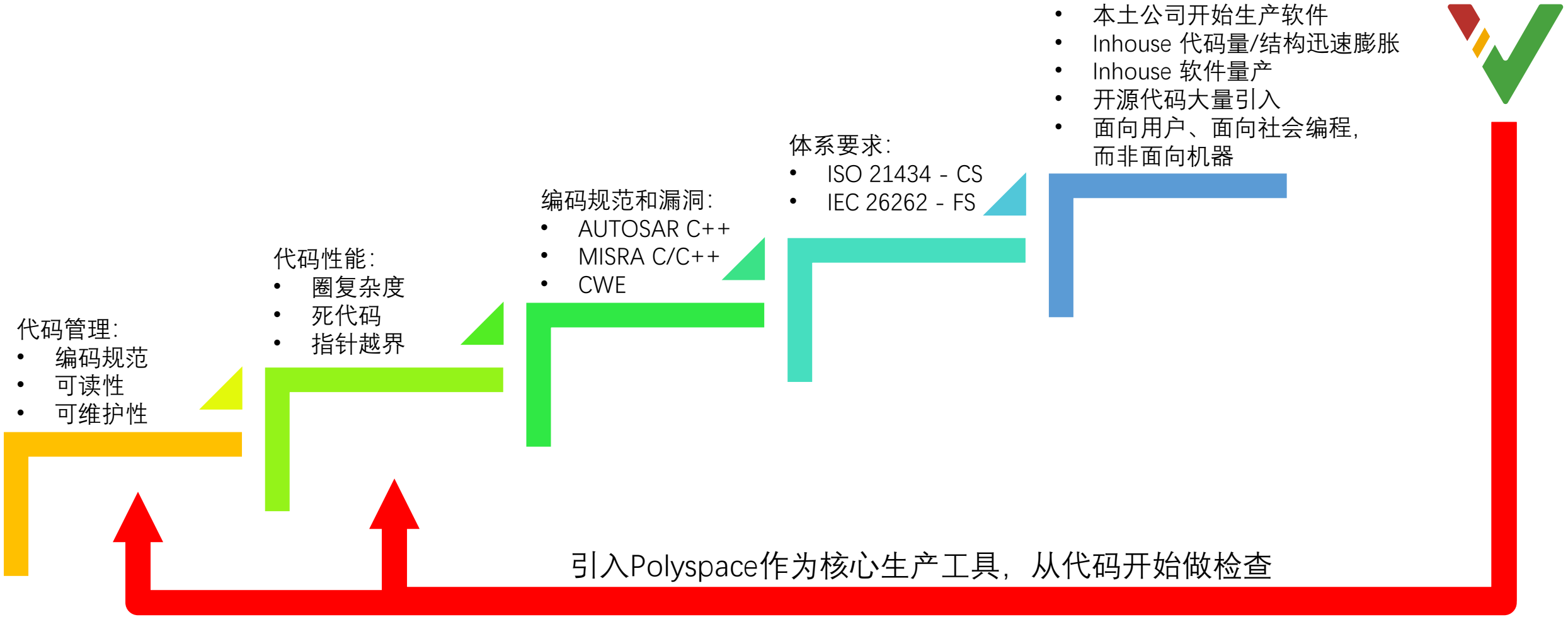
大纲

- About US
- 方法论：控制组织代码质量
- IT 实现与质量实践



在合适的时机引入代码质量

我们认识软件工程的阶梯：



重建软件项目过程

BeaconTower

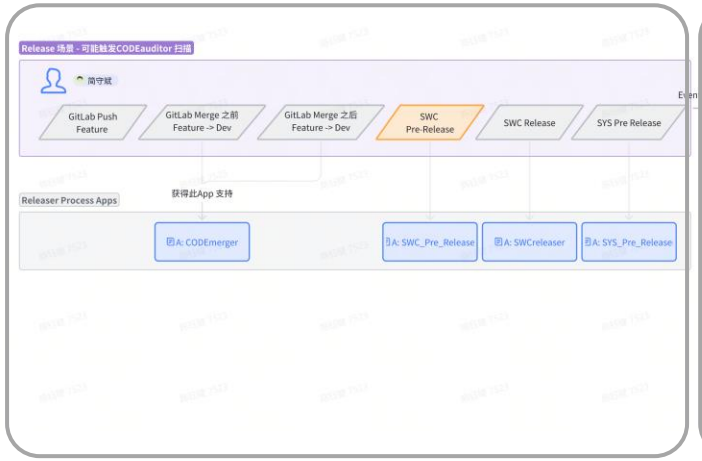
CODEmerge

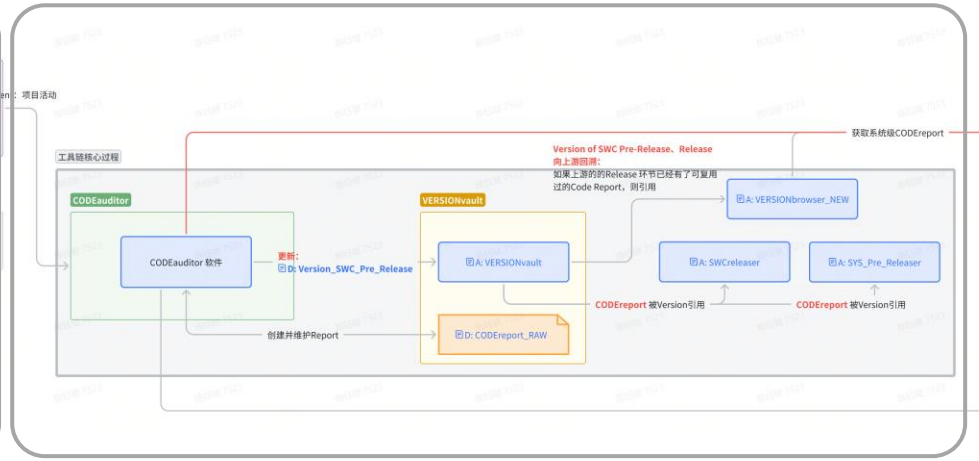
VERSIONreleaser

VERSIONvault

VERSIONbrowser

CODEauditor



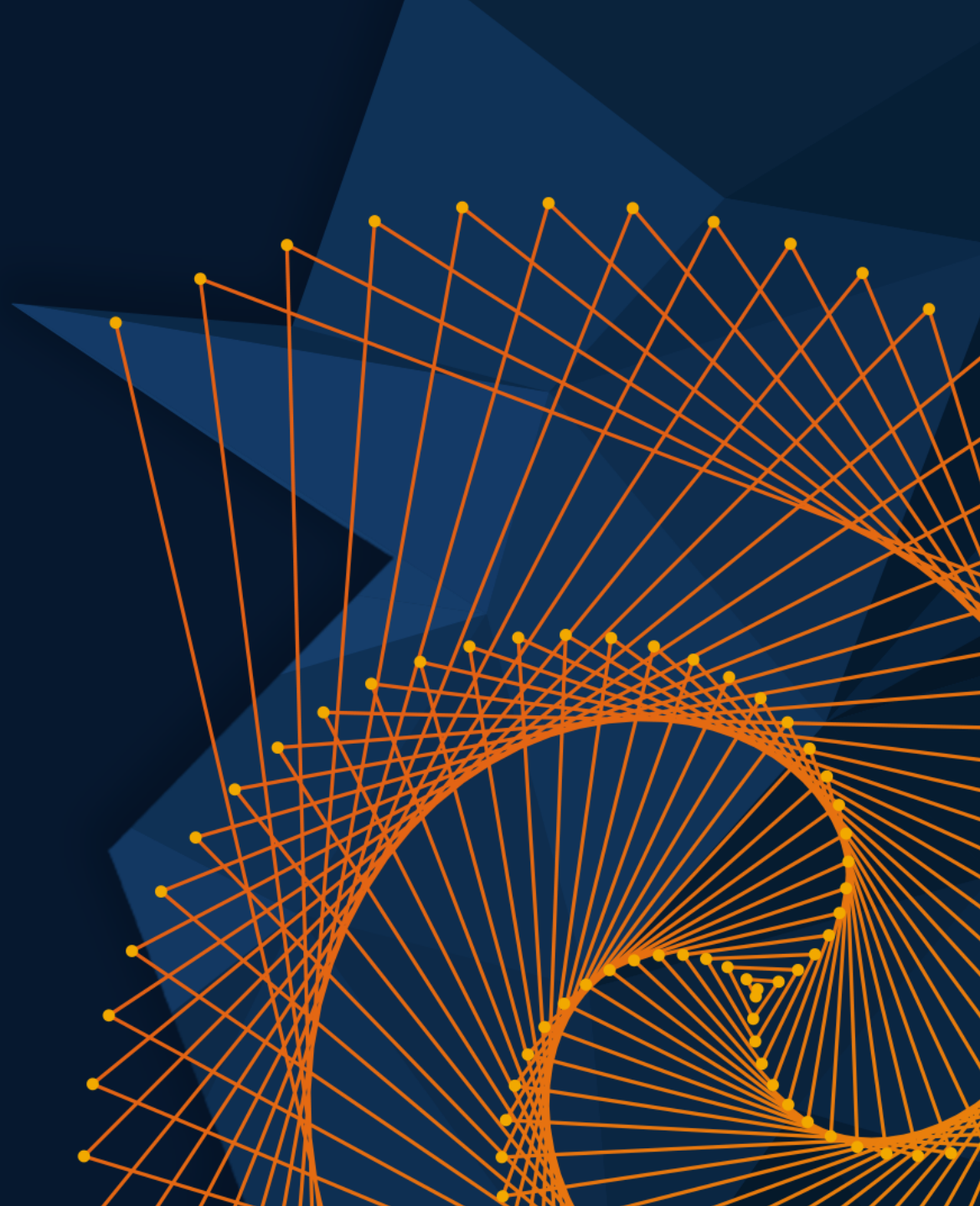


组织痛点　　代码、软件Release 活动　　代码扫描、版本信息入库　　质量改善活动

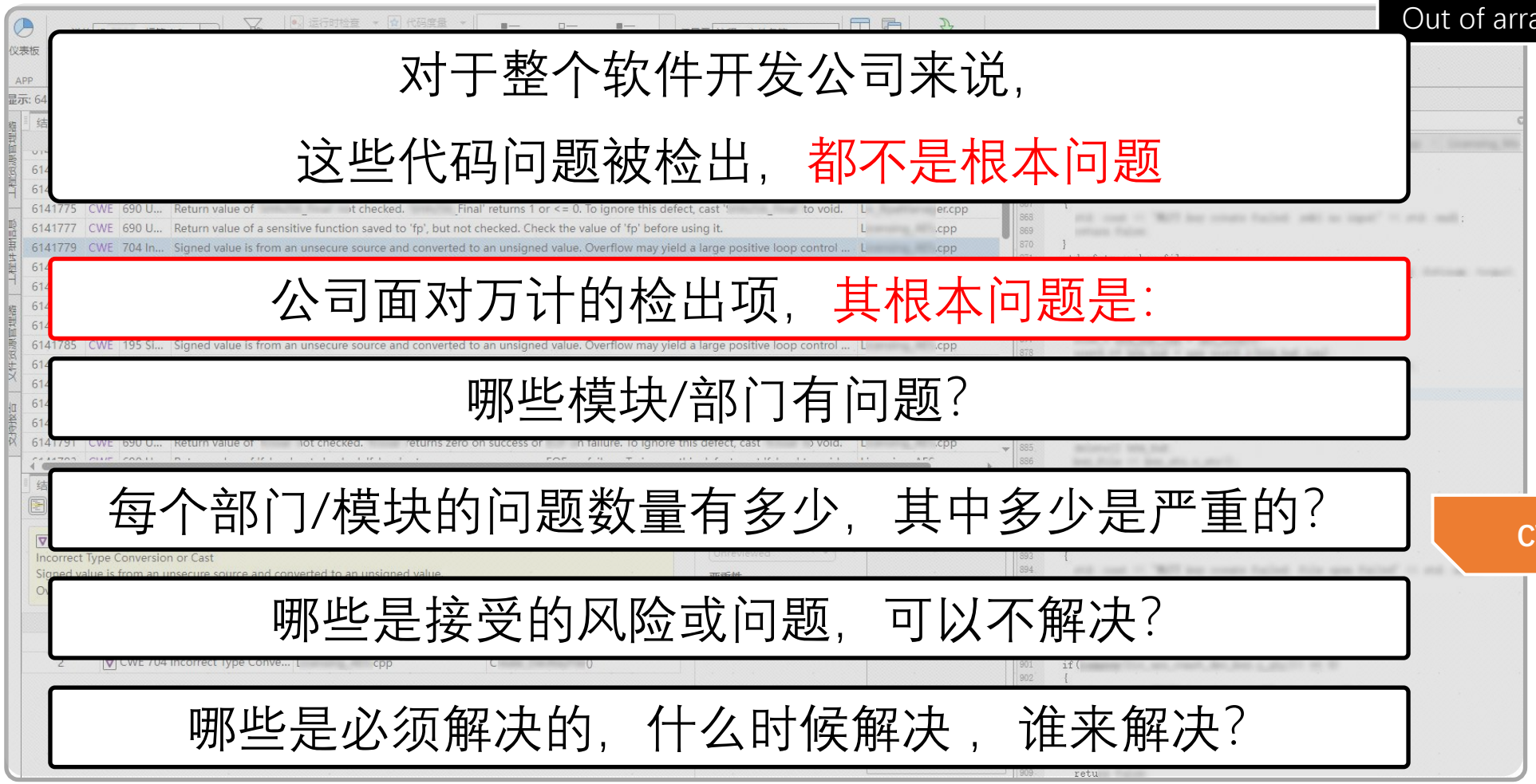
MATLAB EXPO

大纲

- About US
- 方法论：控制组织代码质量
- IT 实现与质量实践



基本技术工具：Polyspace



对于整个软件开发公司来说，

这些代码问题被检出，都不是根本问题

公司面对万计的检出项，其根本问题是：

哪些模块/部门有问题？

每个部门/模块的问题数量有多少，其中多少是严重的？

哪些是接受的风险或问题，可以不解决？

哪些是必须解决的，什么时候解决，谁来解决？

数组越界
Out of array bound

空指针
NULL pointer

边界值保护
Boundary value protect

内存泄漏
Memory leak

变量未初始化
Non-init

CWE 80+

CERT 160+

AUTOSAR 10+

惯性思维：代码质量就是自动化检查、门禁

一个典型的代码质量检查自动化过程

The process of automatic verification of code quality

能否解决这些问题 – 更加务实的“根本问题”：

- 质量经理（QA）怎么告诉开发人员代码有缺陷？How QA report defects to developers?
  - 哪个项目、哪个分支、哪个Commit、哪个文件？ - 而且很严重，必须修正！
- 一个系统包含50个GitLab项目，如何透视整个系统的代码缺陷? What is overview of defects in a project?
  - 例如CWE-125 Out-of-bounds Read 一共命中多少次，分别是哪些软件模块，哪些部门负责？
- 如何向公司管理层汇报? How to report to managers?
  - 50个GitLab项目分别有共计多少个命中项？
  - 那么这些信息呢：重要Level 缺陷的命中数、分别分布在哪些部门

组织级 IT Solution

灵魂拷问：我们公司是否按这种流程生产软件并质检？你中意咩?

If yes：先实现这个流程，

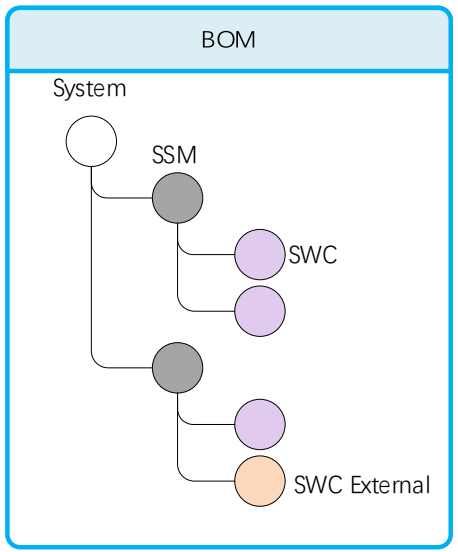
然后考虑才流程/企业外部的声音：ASPICE、客户流程审计

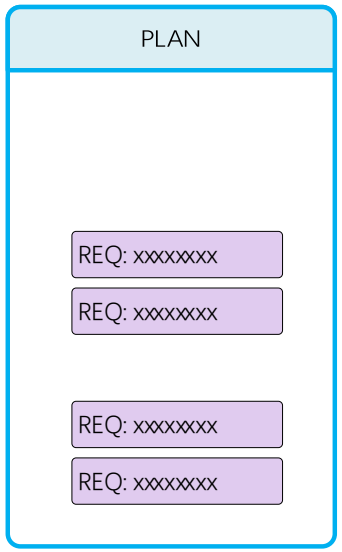
DevOps +
System Architecture

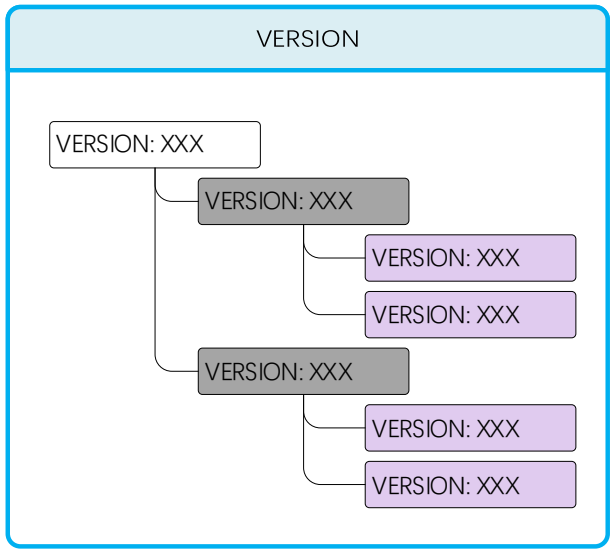
PM

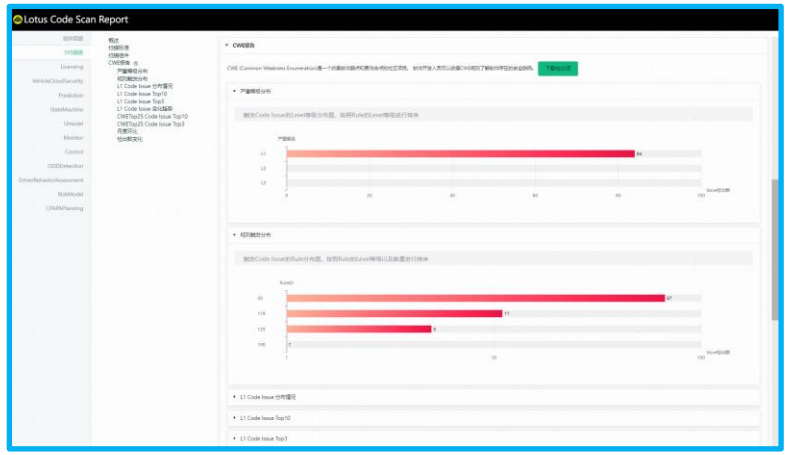
Coder

QA









组织/系统级组件范围、架构
- SW Object ID、Name
- GitLab Source

某一次迭代范围、内容
- SW Object
- REQs

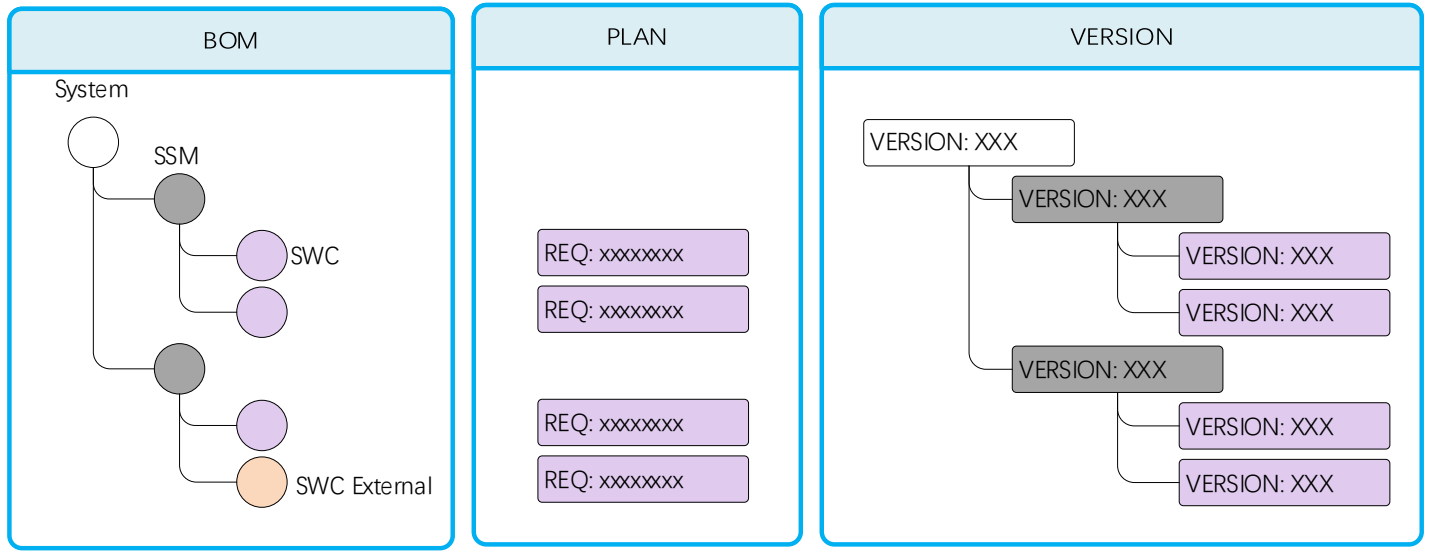
系统迭代的软件成果
- System、Subsystem、SWC
- Version Code、Bin、Source

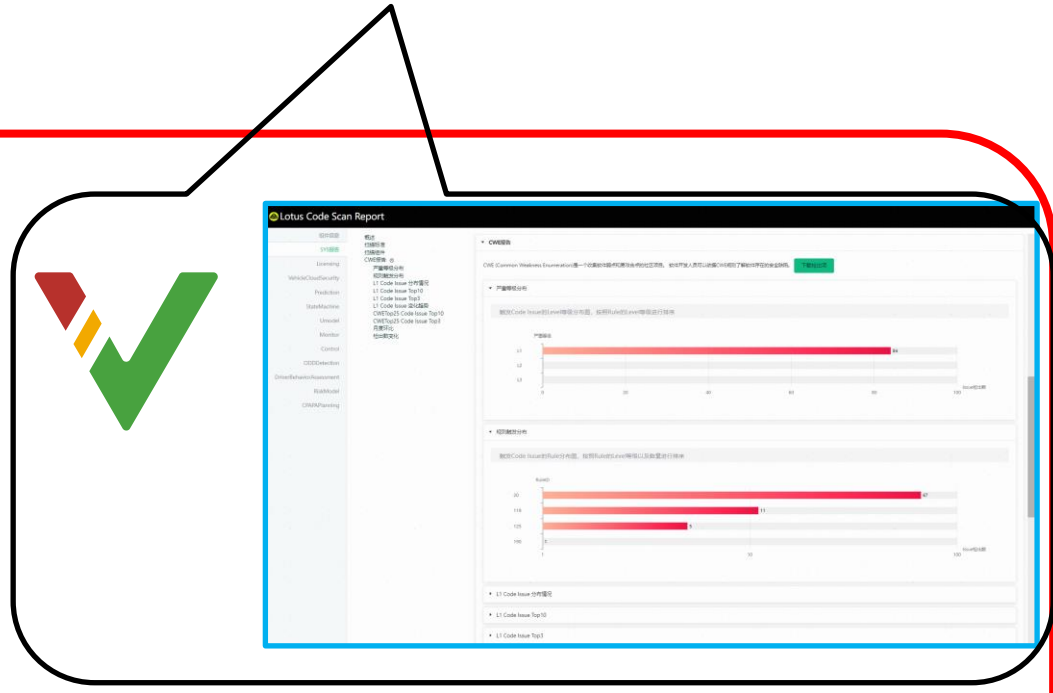
系统扫描的结果
- 具体的Version、SWC
- 文件路径
- 扫描统计

组织级 IT Solution

BeaconTower

CODEauditor





组织级IT Solution – BOM based SW Engineering

BOM

项目要得到的最终交付内容：**软件内容**

项目得到最终交付的途径：计划、构建、集成

基于软件项目过程Key Process 举例说明：

System AD → 软件开发的架构内容 → PM → 某次迭代的开发计划 → Dev Team

BOM	ID	Name	Owner Dept	Owner	Inhouse	GitLab Project URL
SYS-1	SYS_0001	AD_SYS_LTS	架构	xxx	yes	
SYS-2	SSM_0001	ADMC_SOC	集成	xxx	yes	
SYS-3	SWC_0001	Planning	算法		yes	xxxx/xxx/xxxxxxxx
SYS-3	SWC_0002	Control	算法		no	
SYS-2	SSM_0002	ADSC_SOC	集成		yes	
SYS-3	SWC_0003	DriverTakeOver	功能		yes	xxxx/xxx/xxxxxxxx
SYS-2	SSM_0003	MCU	集成		yes	
SYS-3	SWC_0004	Arbitration	ADAS		yes	xxxx/xxx/xxxxxxxx
SYS-3	SWC_0005	LDW	ADAS		no	

Version Plan of System	新版本?	需求类别	需求明细	Legacy Version
SYS-1	yes			
SYS-2	yes			
SYS-3	yes	E2E	1. xxxx, 2. xxxx	
SYS-3	no			xxxx.xxxx.xxxx.xxxx
SYS-2	yes			
SYS-3		E2E	1. xxxx, 2. xxxx, 3. xxxx, 4. xxxx	
SYS-2	yes			xxxx.xxxx.xxxx.xxxx
SYS-3	yes	FUSA	1. xxxx, 2. xxxx, 3. xxxx	xxxx.xxxx.xxxx.xxxx
SYS-3	yes	FUSA	1. xxxx	xxxx.xxxx.xxxx.xxxx

Version	Version Code	Binary File	Test Report	Code Audit Report
SYS-1	xxxx.xxxx.xxx.xxxx	File 1, File 2, File 3, File 4	Report 1, Report 2, Report 3	Audit Report
SYS-2	xxxx.xxxx.xxx.xxxx	File 1	Report 1	Audit Report
SYS-3	xxxx.xxxx.xxx.xxxx	File 1, File 2	Report 1	Audit Report
SYS-3	未集成			
SYS-2	xxxx.xxxx.xxx.xxxx			Audit Report
SYS-3	xxxx.xxxx.xxx.xxxx			Audit Report
SYS-2	xxxx.xxxx.xxx.xxxx			Audit Report
SYS-3	xxxx.xxxx.xxx.xxxx			Audit Report
SYS-3	未集成			

BOM - 控制所有过程、数据资产的结构：
- 系统包含的软件内容：子系统、模块
- 软件内容的静态支持要素：Git 项目、是否外包
- 系统对应的人员组织：责任人、责任部门

Version Plan - 控制一轮系统迭代的开发内容：
- 基于哪一个系统版本迭代
- 哪些模块更新 – 哪些需求、Bug
- 哪些模块不更新

System Version – 版本发布、系统集成：
- 按BOM 的系统层级逐级提交
- 系统集成全貌：版本号、二进制文件、测试报告

IT 实现 - BOM

BOM协同了软件项目的关键信息

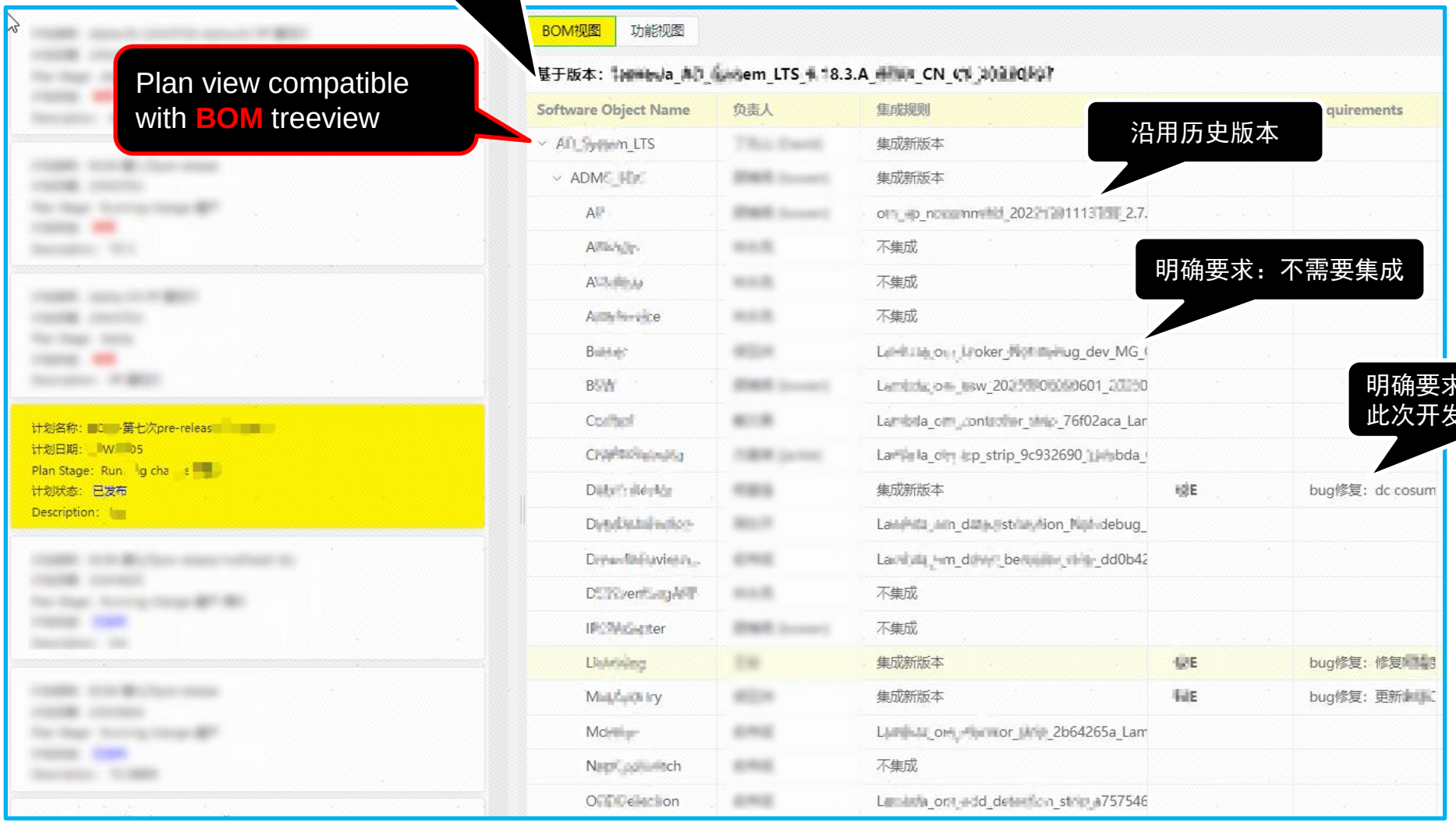
- 软件自身组成、架构
- 软件负责人
- 软件技术信息索引：
  - 版本号
  - 源码
  - 二进制文件
- 版本计划
- 系统集成的过程

IT 实现 – PLAN4version

本计划基于某一个
历史Release版本提出

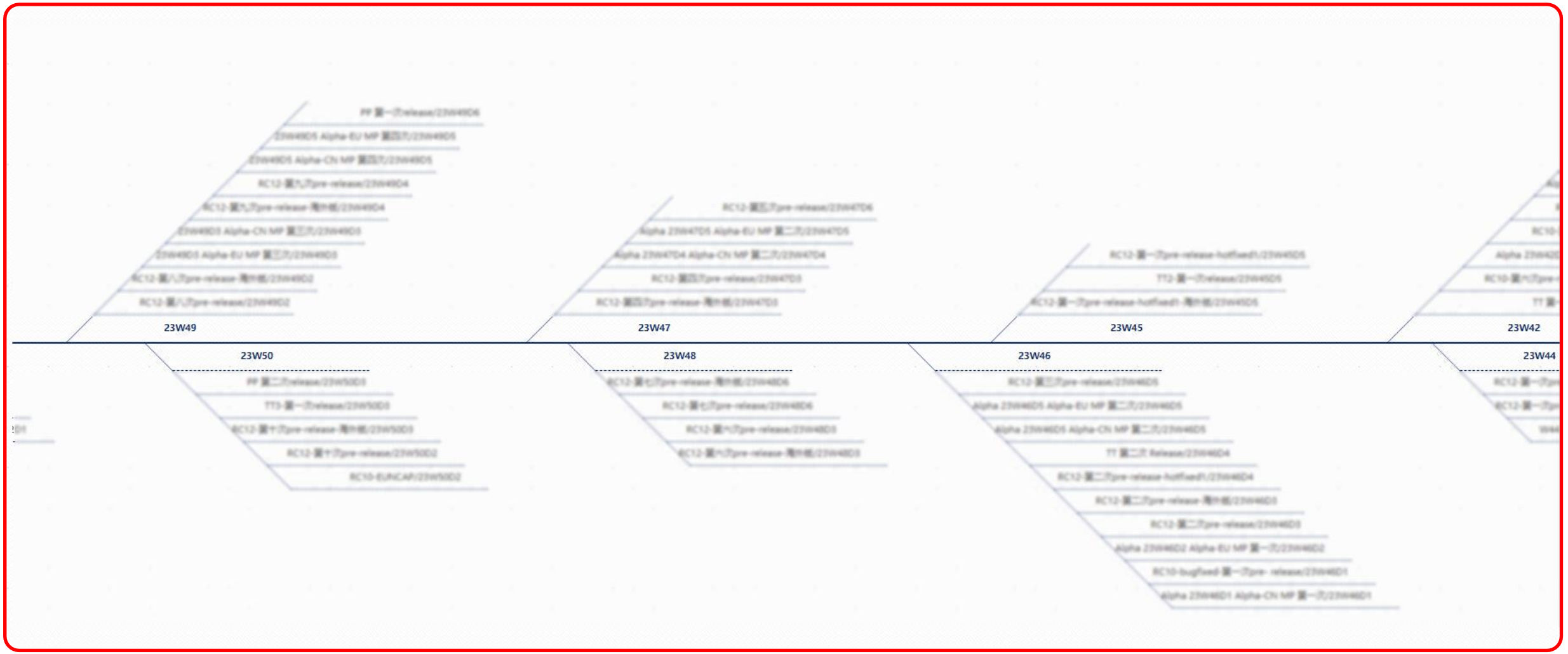
Plan view compatible
with **BOM** treeview

历次计划列表

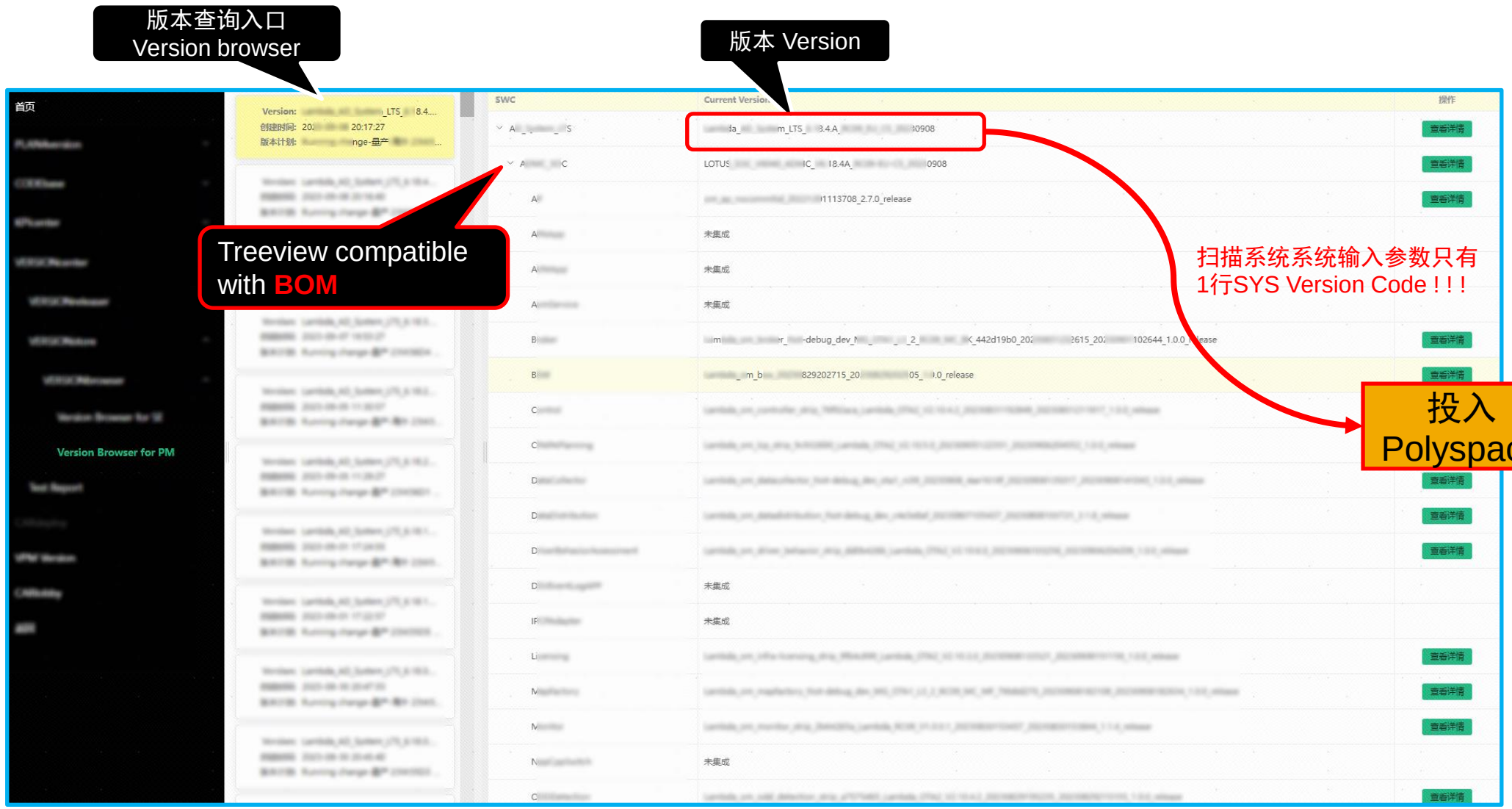


IT 实现 – PLAN4version

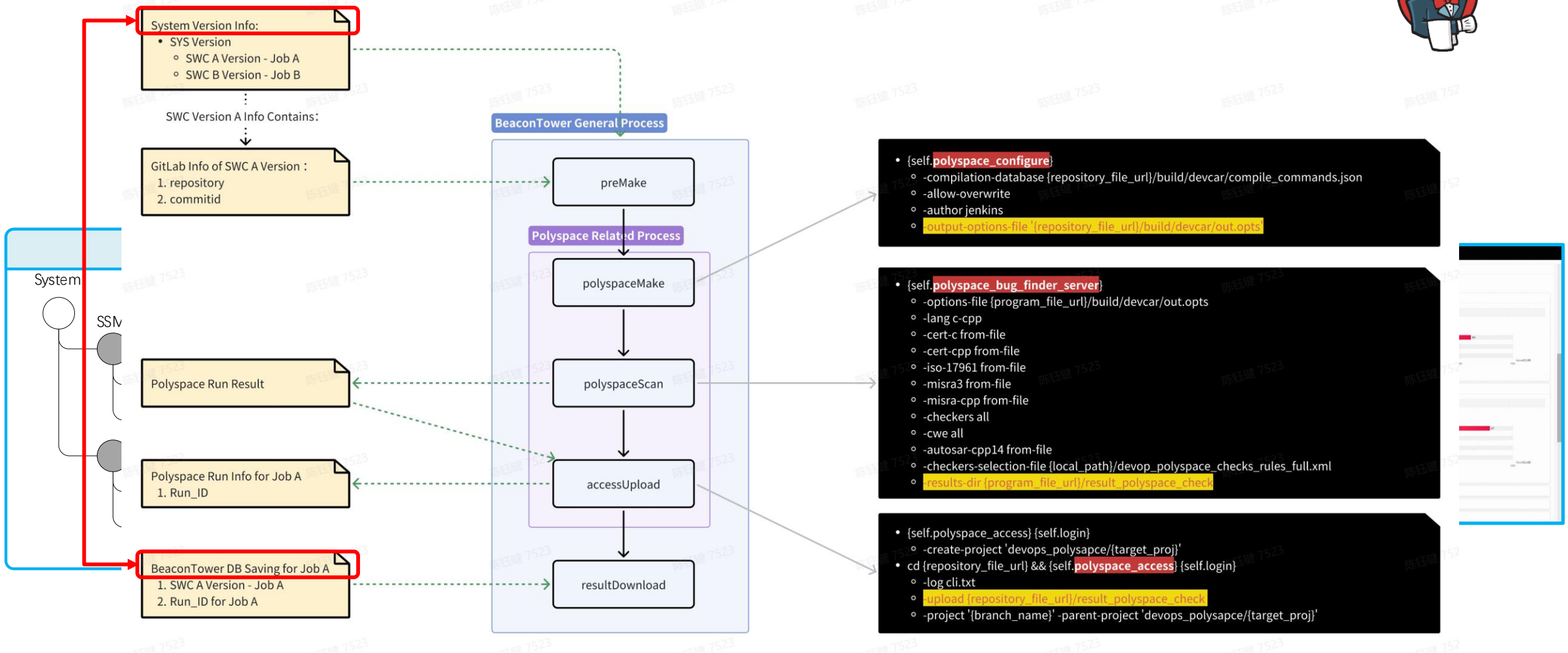
SYS Version Plan
另一种系统计划的透视管理



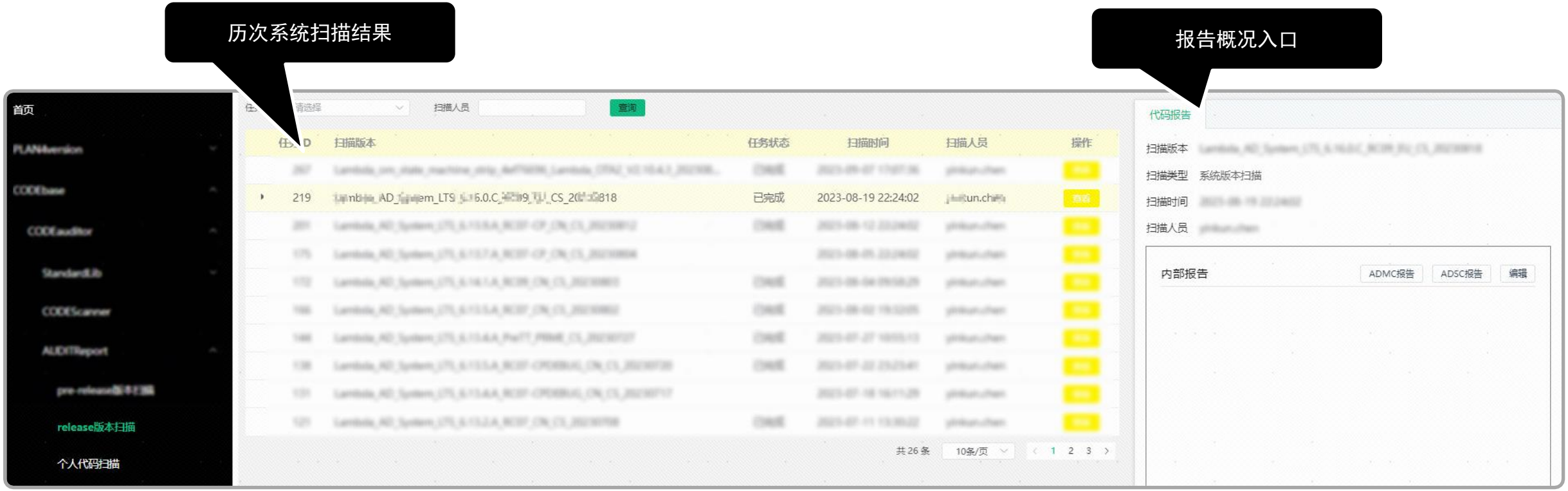
IT 实现 – System Version to audit



IT 实现 – CODEauditor core with Polyspace



IT 实现 – 报告获取


历次系统扫描结果
报告概况入口
首页
release版本扫描
个人代码扫描
扫描人员
查询
扫描版本
任务状态
扫描时间
扫描人员
操作
219
已完成
2023-08-19 22:24:02
共 26 条
10条/页
代码报告
扫描版本
扫描类型
系统版本扫描
扫描时间
扫描人员
内部报告
ADMC报告
ADSC报告
编辑

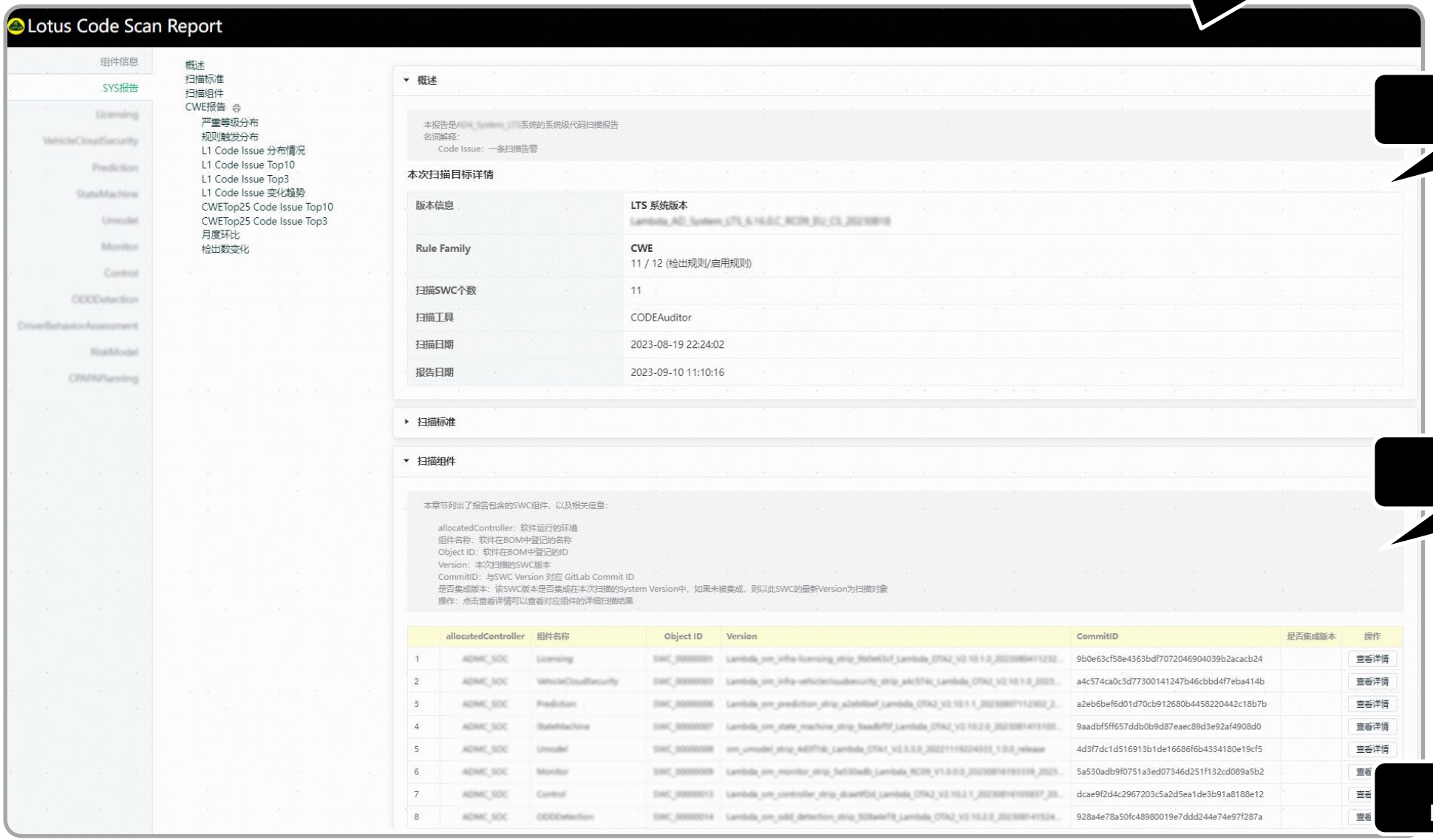
IT 实现 – System Code Audit Report

针对整个系统的扫描结果概述

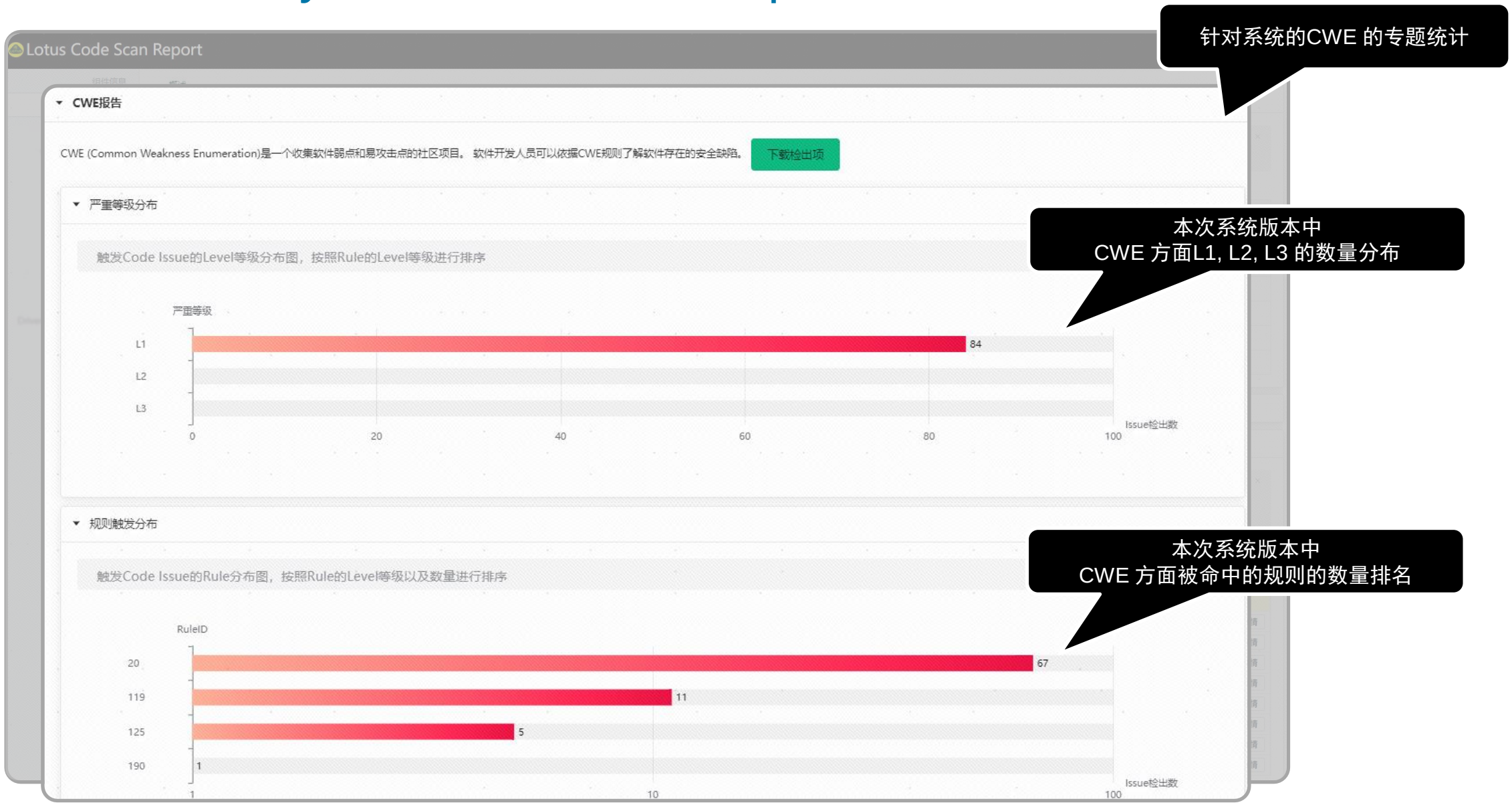
扫描任务自身信息

被扫描的对象

下面还有很多，例如：
L1 统计信息、Top 10 统计



IT 实现 – System Code Audit Report

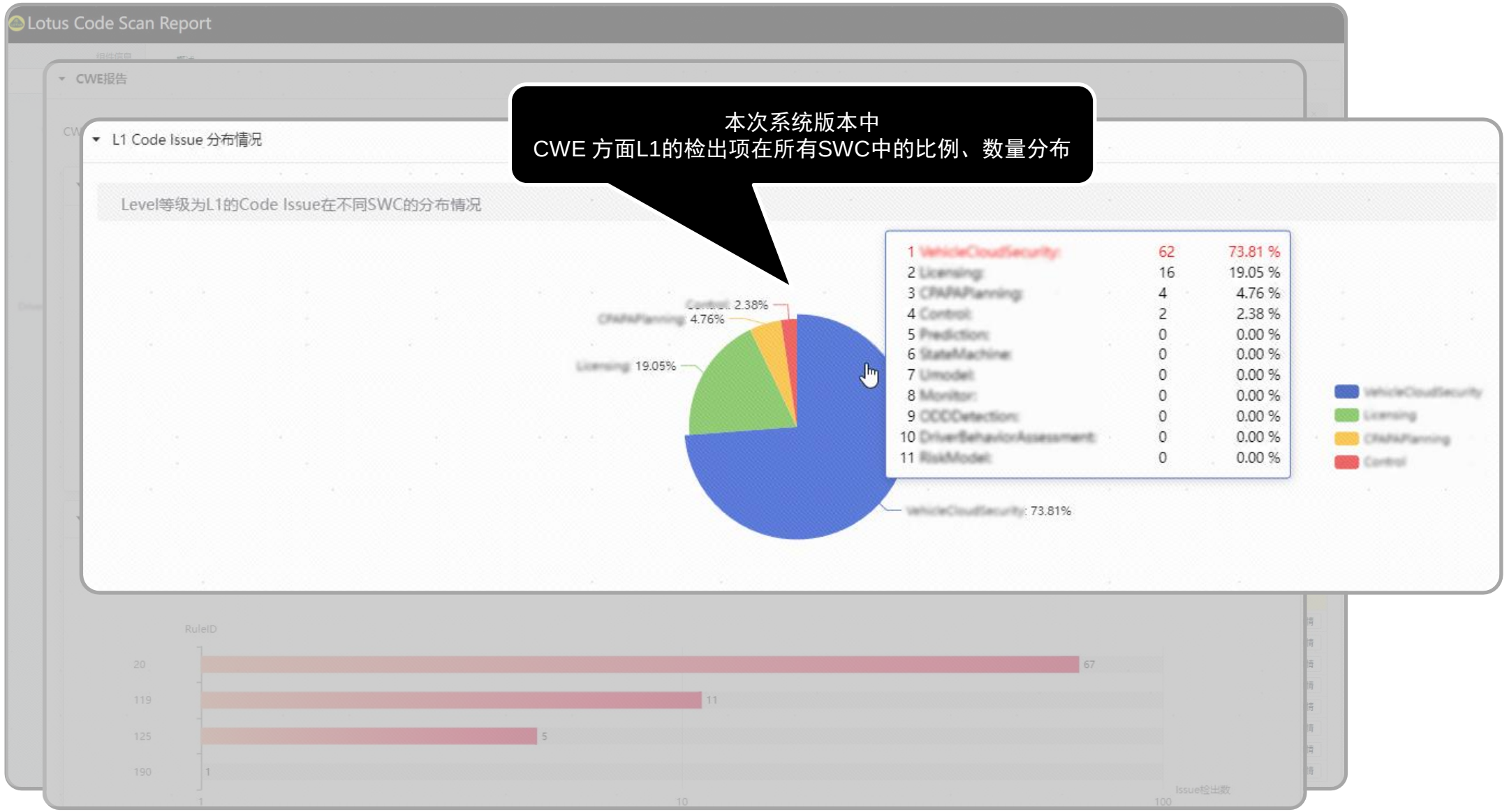


针对系统的CWE 的专题统计

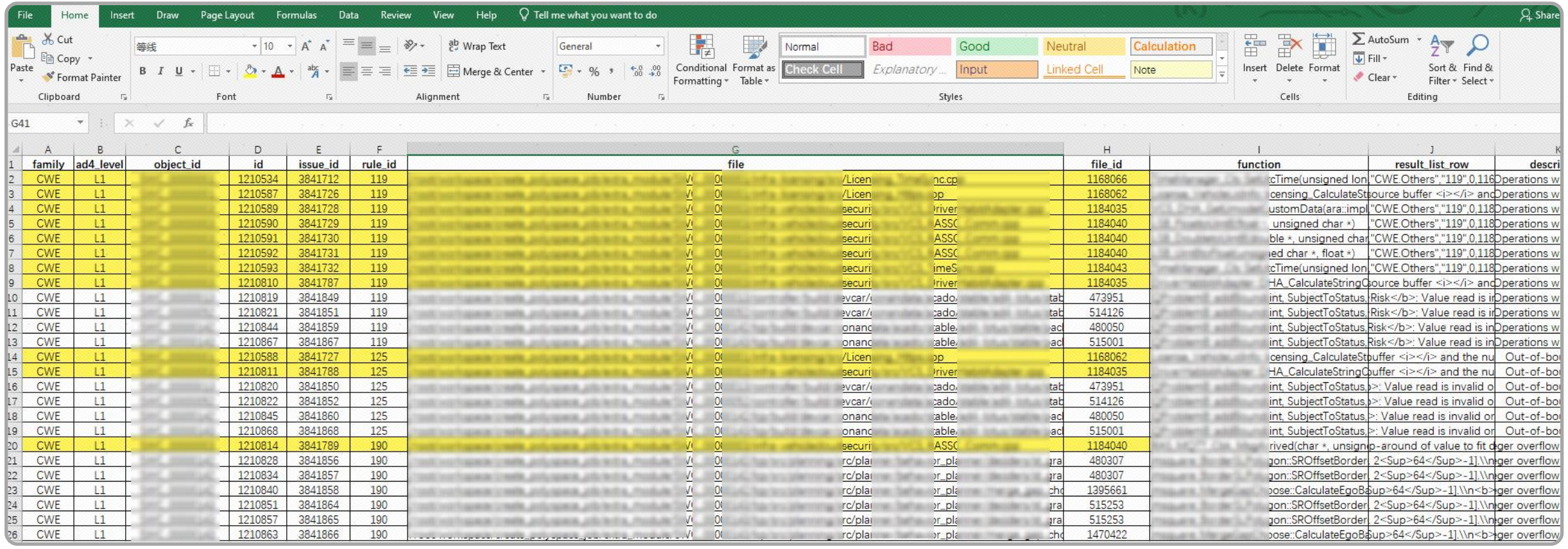
本次系统版本中
CWE 方面L1, L2, L3 的数量分布

本次系统版本中
CWE 方面被命中的规则的数量排名

IT 实现 – System Code Audit Report



IT 实现 + 改善活动 – 代码改善督导



family	ad4_level	object_id	id	issue_id	rule_id	file	file_id	function	result_list_row	descri
CWE	L1		1210534	3841712	119	/Licen nc.cp	1168066	cTime(unsigned lon	"CWE.Others","119",0,116	Operations w
CWE	L1		1210587	3841726	119	/Licen pp	1168062	censing_CalculateSt	ource buffer and	Operations w
CWE	L1		1210589	3841728	119	securi river	1184035	ustomData(ara::impl	"CWE.Others","119",0,118	Operations w
CWE	L1		1210590	3841729	119	securi ASSC	1184040	unsigned char *)	"CWE.Others","119",0,118	Operations w
CWE	L1		1210591	3841730	119	securi ASSC	1184040	ble *, unsigned char	"CWE.Others","119",0,118	Operations w
CWE	L1		1210592	3841731	119	securi ASSC	1184040	ed char *, float *)	"CWE.Others","119",0,118	Operations w
CWE	L1		1210593	3841732	119	securi imeS	1184043	cTime(unsigned lon	"CWE.Others","119",0,118	Operations w
CWE	L1		1210810	3841787	119	securi river	1184035	HA_CalculateStringC	ource buffer and	Operations w
CWE	L1		1210819	3841849	119	evcar/ cado tab	473951	int, SubjectToStatus,	Risk: Value read is in	Operations w
CWE	L1		1210821	3841851	119	evcar/ cado tab	514126	int, SubjectToStatus,	Risk: Value read is in	Operations w
CWE	L1		1210844	3841859	119	onanc table act	480050	int, SubjectToStatus,	Risk: Value read is in	Operations w
CWE	L1		1210867	3841867	119	onanc table act	515001	int, SubjectToStatus,	Risk: Value read is in	Operations w
CWE	L1		1210588	3841727	125	/Licen pp	1168062	censing_CalculateSt	buffer and the nu	Out-of-bo
CWE	L1		1210811	3841788	125	securi river	1184035	HA_CalculateStringC	buffer and the nu	Out-of-bo
CWE	L1		1210820	3841850	125	evcar/ cado tab	473951	int, SubjectToStatus,	>: Value read is invalid o	Out-of-bo
CWE	L1		1210822	3841852	125	evcar/ cado tab	514126	int, SubjectToStatus,	>: Value read is invalid o	Out-of-bo
CWE	L1		1210845	3841860	125	onanc table act	480050	int, SubjectToStatus,	>: Value read is invalid or	Out-of-bo
CWE	L1		1210868	3841868	125	onanc table act	515001	int, SubjectToStatus,	>: Value read is invalid or	Out-of-bo
CWE	L1		1210814	3841789	190	securi ASSC	1184040	rived(char *, unsign	p-around of value to fit d	ger overflow
CWE	L1		1210828	3841856	190	rc/pla r_pla gra	480307	gon::SROffsetBorder	2⁶⁴-1].\\n	ger overflow
CWE	L1		1210834	3841857	190	rc/pla r_pla gra	480307	gon::SROffsetBorder	2⁶⁴-1].\\n	ger overflow
CWE	L1		1210840	3841858	190	rc/pla r_pla cho	1395661	oose::CalculateEgoB	up>64</Sup>-1].\\n	ger overflow
CWE	L1		1210851	3841864	190	rc/pla r_pla gra	515253	gon::SROffsetBorder	2⁶⁴-1].\\n	ger overflow
CWE	L1		1210857	3841865	190	rc/pla r_pla gra	515253	gon::SROffsetBorder	2⁶⁴-1].\\n	ger overflow
CWE	L1		1210863	3841866	190	rc/pla r_pla cho	1470422	oose::CalculateEgoB	up>64</Sup>-1].\\n	ger overflow

Coder

QA

IT 实现 + 改善活动 – 组织级活动干预

代码质量做到QA，是否够了？

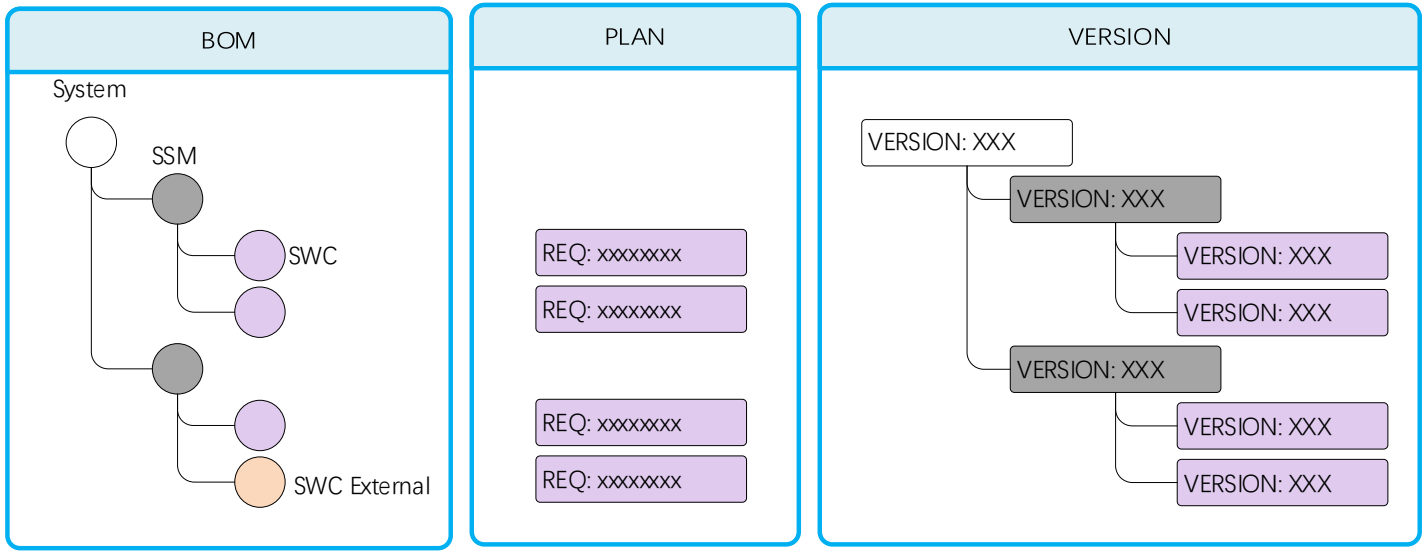
IT 实现 + 改善活动 – 组织级活动干预

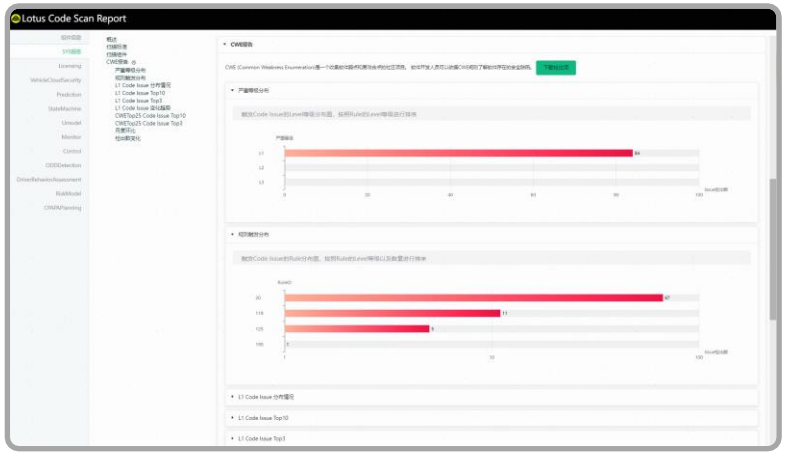
DevOps +
System Architecture

PM

Coder

QA





组织/系统级组件范围、架构
- SW Object ID、Name
- GitLab Source

某一次迭代范围、内容
- SW Object
- REQs

系统迭代的软件成果
- System、Subsystem、SWC
- Version Code、Bin、Source

系统扫描的结果
- 具体的Version、SWC
- 文件路径
- 扫描统计

IT 实现 + 改善活动 – 组织级活动干预

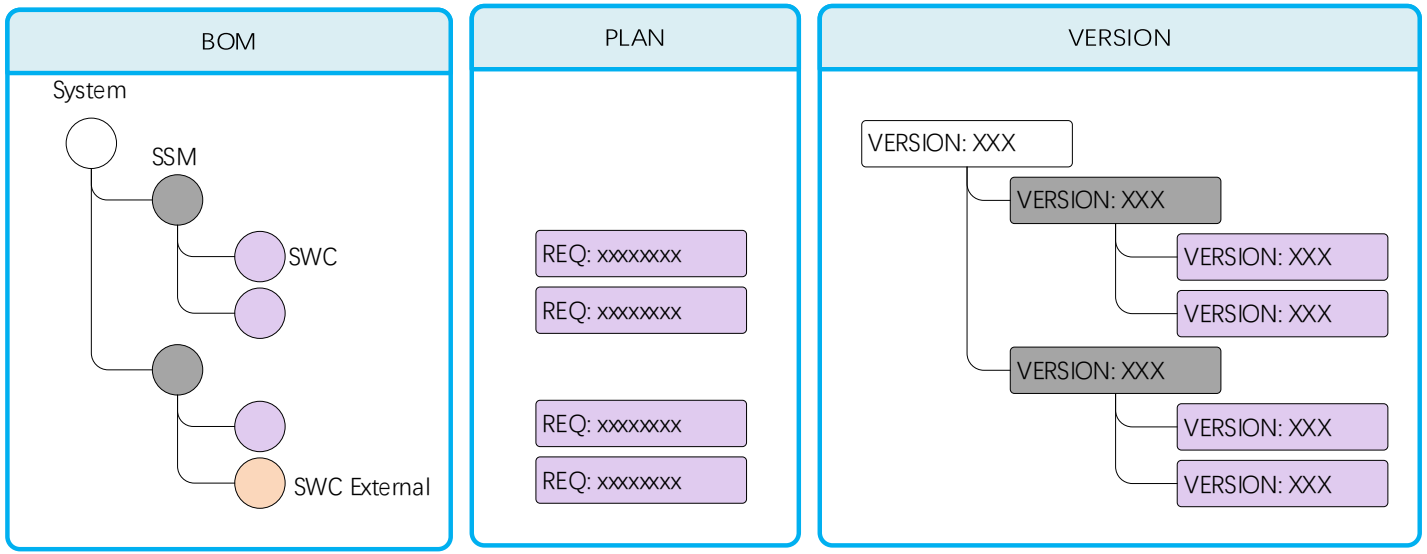
DevOps +
System Architecture

PM

Coder

QA

Management



组织/系统级组件范围、架构
- SW Object ID、Name
- GitLab Source

某一次迭代范围、内容
- SW Object
- REQs

系统迭代的软件成果
- System、Subsystem、SWC
- Version Code、Bin、Source

系统扫描的结果
- 具体的Version、SWC
- 文件路径
- 扫描统计

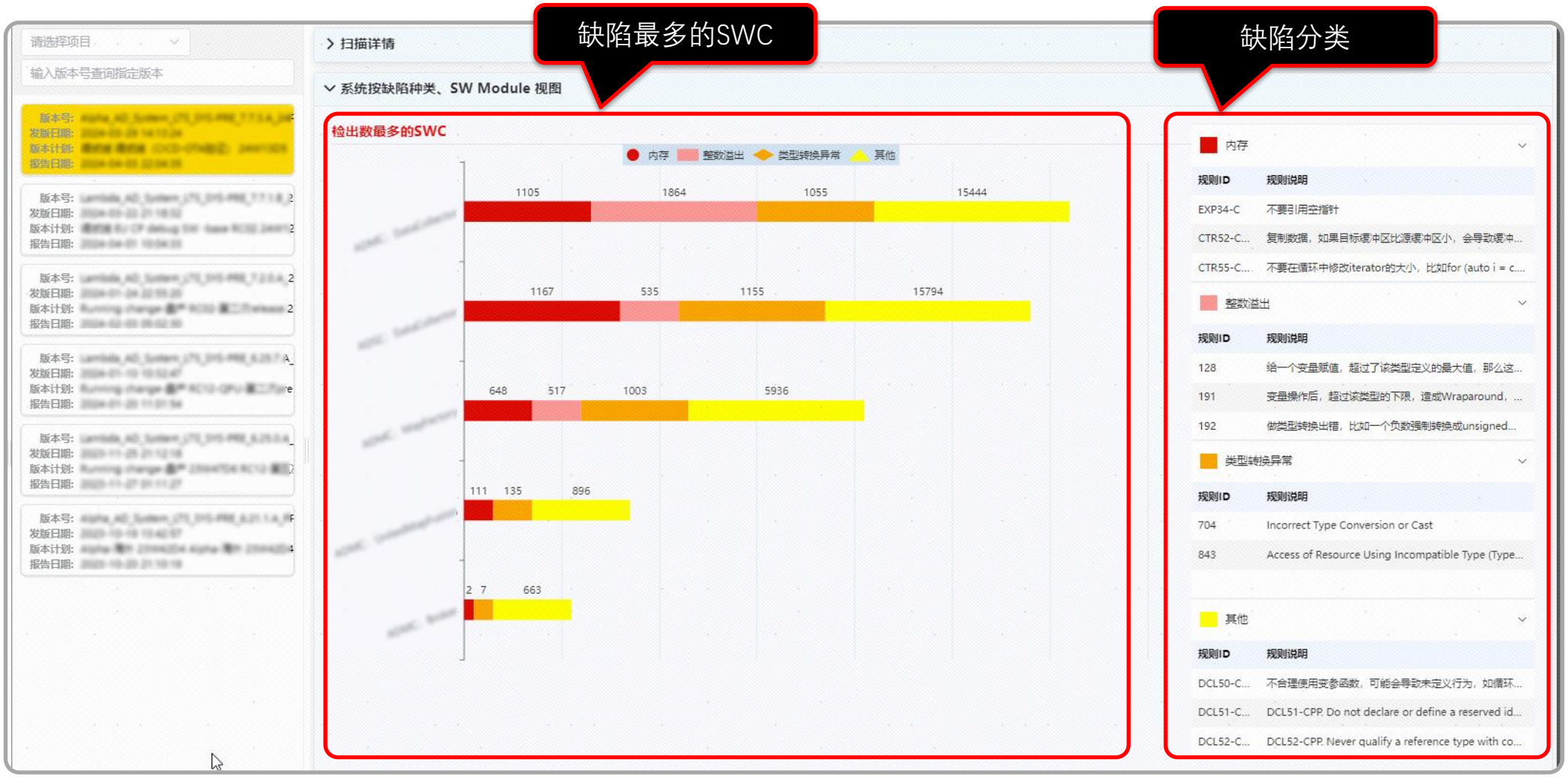
组织代码质量透视
- 最好、最差的部门
- 当前Highlight 代码缺陷

IT 实现 + 改善活动 – 组织级活动干预

组织专家意见

	A	B	C	K	L
1	规则族 Family	规则ID Rule_ID	规则概述 Summary	AD4专家分类 AD4_Expert_Category	AD4专家解释 AD4_Expert_Explain
2	CERT	DCL50-CPP	DCL50-CPP. Do not define a C-style variadic function	输入参数未验证	不合理使用变参函数，可能会导致未定义行为，如循环处理变参直到遇到0，但是输入的变参可能没有0
19	CERT	EXP53-CPP	EXP53-CPP. Do not read uninitialized memory	变量未初始化	引用空指针
26	CERT	EXP60-CPP	EXP60-CPP. Do not pass a nonstandard-layout type object across execution boundaries	不安全的外部函数调用	不要跨文件调用nonstandard-layout type object，否则可能会引发未定义行为。如virtual函数
30	CERT	EXP34-C	EXP34-C. Do not dereference null pointers	内存	不要引用空指针
49	CERT	CTR52-CPP	CTR52-CPP. Guarantee that library functions do not overflow	内存	复制数据，如果目标缓冲区比源缓冲区小，会导致缓冲区溢出
52	CERT	CTR55-CPP	CTR55-CPP. Do not use an additive operator on an iterator if the result would overflow	内存	不要在循环中修改iterator的大小，比如for (auto i = c.begin(), e = i + 20; i != e; ++i) {...}中，修改了iterator e的大小，可能会导致内存溢出
58	CERT	ARR38-C	ARR38-C. Guarantee that library functions do not form invalid pointers	内存	一些标准函数库入参是指针和缓冲区大小，需要保证入参指针是有效指针，缓冲区大小正确。如memcopy、memset
60	CERT	STR50-CPP	STR50-CPP. Guarantee that storage for strings has sufficient space for character data and the null terminator	内存	保证存储字符串的缓冲区有足够的空间（包含尾部的空字符串）
61	CERT	STR51-CPP	STR51-CPP. Do not attempt to create a std::string from a null pointer	内存	不要给std:string赋值空指针
65	CERT	STR31-C	STR31-C. Guarantee that storage for strings has sufficient space for character data and the null terminator	内存	保证存储字符的缓冲区有足够的空间（包含尾部的空字符串）
66	CERT	STR32-C	STR32-C. Do not pass a non-null-terminated character sequence to a library function that expects a string	内存	有些标准函数传入的字符串需要以空字符串结尾
69	CERT	STR38-C	STR38-C. Do not confuse narrow and wide character strings and functions	内存	使用strncpy和malloc等函数时不能忽略输入字符串最后的空字符，否则会导致缓存溢出
70	CERT	MEM50-CPP	MEM50-CPP. Do not access freed memory	内存	访问已释放的空指针
71	CERT	MEM51-CPP	MEM51-CPP. Properly deallocate dynamically allocated resources	内存	分配内存和释放内存的函数要匹配
72	CERT	MEM52-CPP	MEM52-CPP. Detect and handle memory allocation errors	内存	如果分配内存失败，合理处理异常或者返回的空指针
73	CERT	MEM53-CPP	MEM53-CPP. Explicitly construct and destruct objects when manually managing object lifetime	内存	如果给对象手动分配了内存，那么用完对象之后，需要手动释放
74	CERT	MEM54-CPP	MEM54-CPP. Provide placement new with properly aligned pointers to sufficient storage capacity	内存	使用new函数给变量分配内存，分配的内存要足够
1387	CWE	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	内存	软件对内存缓冲区的操作，可能超过缓冲区允许的地址范围 - 某些语言（例如C/C++）允许直接访问内存，对内存的访问如果没有限定地址范围的话，代码可能读取期望的缓冲区之外的内存。 访问此处获取更多专业信息：CWE-119：Improper Restriction of Operations within the Bounds of a Memory Buffer
1388	CWE	120	Buffer Copy without Checking Size of Input (Classic Buffer Overflow)	内存	缓冲区溢出，输入可能大于写入的缓冲区
1389	CWE	121	Stack-based Buffer Overflow	内存	缓冲区溢出 - 基于Stack。如本地变量溢出、递归函数循环次数过多。
1390	CWE	122	Heap-based Buffer Overflow	内存	堆（Heap）溢出，例如：过多调用malloc函数导致溢出
1392	CWE	124	Buffer Underwrite (Buffer Underflow)	内存	引用缓冲区之外的内存地址，如a[-1]
1393	CWE	125	Out-of-bounds Read	内存	引用缓冲区之外的内存地址，如a[-1] a[a.lenth]
1394	CWE	126	Buffer Over-read	内存	读取缓冲区上限之外的地址，如数组a的长度是10，但是代码中有a[20]的操作，可能导致敏感数据泄露和系统崩溃
1395	CWE	127	Buffer Under-read	内存	读取缓冲区上限之外的地址，如代码中有a[-2]的操作，可能导致敏感数据泄露和系统崩溃

IT 实现 + 改善活动 – 组织级活动干预

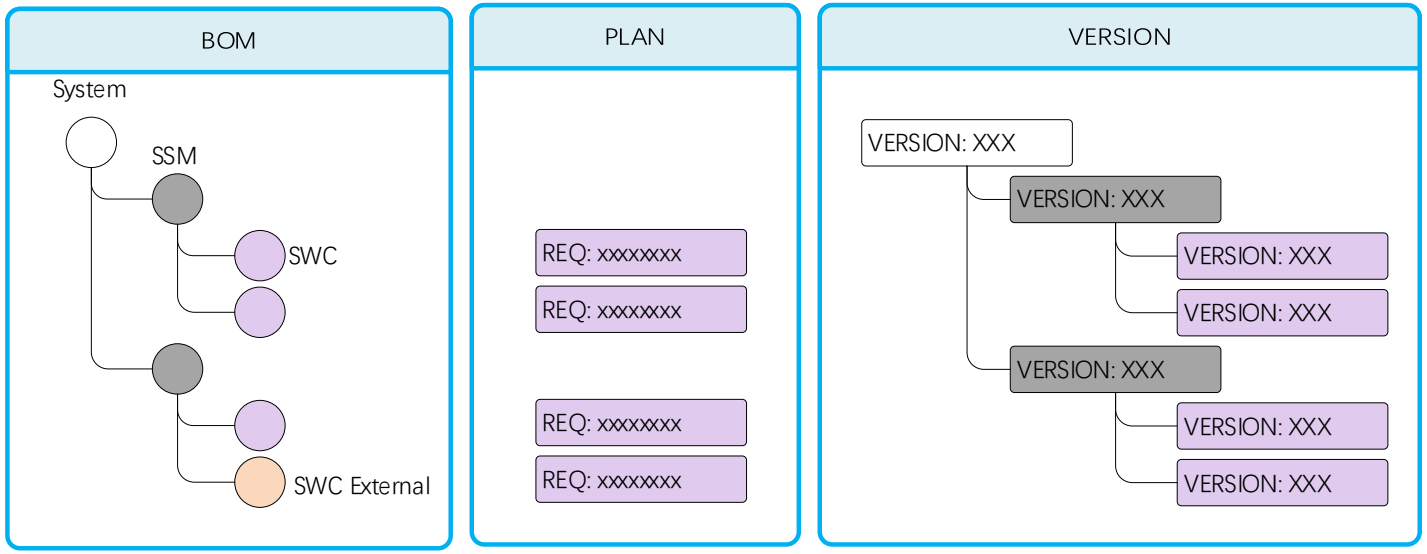


总结：回顾问题、达成目标

- 代码质量人员怎么告诉开发人员？How QA report defects to developers?
  - 哪个项目、哪
- 一个系统包含50个 of defects in a project?
  - 例如CWE-12 哪些部门负责？
- 如何向公司管理层
  - 50个GitLab项目分别有共计多少个命中项？
  - 那么这些信息呢：重要的Level命中数、分别分布在哪些部门

Are we good?

Yes we are good



成果和收益 Results & Benefits

组织流程改善

Process improved

技术体系符合项

Certification passed

代码问题修正

Software defects solved

TÜV NORD

CERTIFICATE

Registered No.:
CER-IND 1102822208018001

This is to certify that the following company comply with the relevant requirements of mentioned safety standards:

Applicant: **Ningbo Lotus Robotics Co.，Ltd.**
Address: Room A101, Building I, No. 7 Zhongchuang 2nd Road, Hangzhou Bay New Area, Ningbo, Zhejiang Province, P.R. China.

Type of Certification: **Functional Safety Product for Intelligent Driving Domain – ADAS (AEB, ACC, ELKA, ERMD, FCTA, HWA, LKA&LDW, RCW, RCTA, EMA) and PAS (APA, RPA, PEB)**

Scope of Certification: Is capable for safety related applications up to **ASIL D**, and meets the applicable requirements listed in the below mentioned standards:
ISO 26262:2018 part 2 - Management of functional safety
- 5 Project dependent safety management
ISO 26262:2018 part 3 - Concept phase
ISO 26262:2018 part 8 - Supporting processes
- 6 Specification and management of safety requirements
- 7 Configuration management

Remark: Base of certification is the report and the tracking list in the valid version.

Mr. Jeffery Fan
Name and Signature

Issued at Shanghai
Place, Stamp

Approval and signed after the first annually surveillance audit:

Approval and signed after the second annually surveillance audit:

TÜV NORD (Hangzhou) Co., Ltd
Room 409, Building 1, No.9 Jiu Huan Road, Shang Cheng District, Hangzhou, Zhejiang Province, 310019 China
SH Branch: No.1, Lane 288 Kangning Road Jingan District, Shanghai 200443, China
Tel: +86-21-33196200 Fax:+86-21-33196334
www.tuv-nord.com/cn

TÜV NORD

CERTIFICATE

Registered No.:
CER-IND 1102822205006001

This is to certify that the following company comply with the relevant requirements of mentioned safety standards:

Applicant: **Ningbo Lotus Robotics Co., Ltd.**
Room A101, Building I, No. 7 Zhong Chuang 2nd Road, Hangzhou Bay New Area, Ningbo, Zhejiang, P.R. China.

Type of Certification: **Functional Safety Development Process**

Scope of Certification: Is capable for safety process related applications up to **ASIL D**, and meets the applicable requirements listed in the below mentioned standards:
ISO 26262:2018 part 2 - Management of functional safety
ISO 26262:2018 part 3 - Concept phase
ISO 26262:2018 part 4 - Product development at the system level
ISO 26262:2018 part 6 - Product development at the software level
ISO 26262:2018 part 8 - Supporting processes
ISO 26262:2018 part 9 - ASIL oriented Analysis - safety Analysis

Remark: Base of certification is the report and the tracking list in the valid version.

Mr. Jeffery Fan
Name and Signature

Issued at Shanghai
Place, Stamp

Approval and signed after the first annually surveillance audit:

Approval and signed after the second annually surveillance audit:

TÜV NORD (Hangzhou) Co., Ltd
Room 409, Building 1, No.9 Jiu Huan Road, Shang Cheng District, Hangzhou, Zhejiang Province, China, 310019
SH Branch: No.1, Lane 288 Kangning Road Jingan District, Shanghai 200443, China
Tel: +86-21-33196200 Fax:+86-21-33196334
www.tuv-nord.com/cn

DNV

CERTIFICATE OF CONFORMITY

Certificate No.:
19003-2022-AUTO-CSM-RGC-DNV

Initial date:
2022-10-27

Valid date:
2025-10-26

This is to certify that the Cybersecurity Management System Process of

Ningbo Lotus Robotics Co., Ltd.

Room A101, Building I, No. 7 Zhong Chuang 2nd Road, Hangzhou Bay New Area, Ningbo, Zhejiang, P.R. China

has been assessed by DNV and found to conform to the standard:

ISO/SAE 21434:2021

This certificate is valid for the following scope:

Organisational and project dependent cybersecurity management, distributed cybersecurity activities, continual cybersecurity activities, as well as cybersecurity activities during concept, product development and post development phases, addressing the requirements of ISO/SAE 21434:2021 clause 5 – 15,except clause 11 and 12.

The validity of this certificate is subjected to the continued maintenance of the Cybersecurity Management System process in accordance with the requirements of the standard as monitored through regular and unannounced surveillance.

Date:
27 October 2022

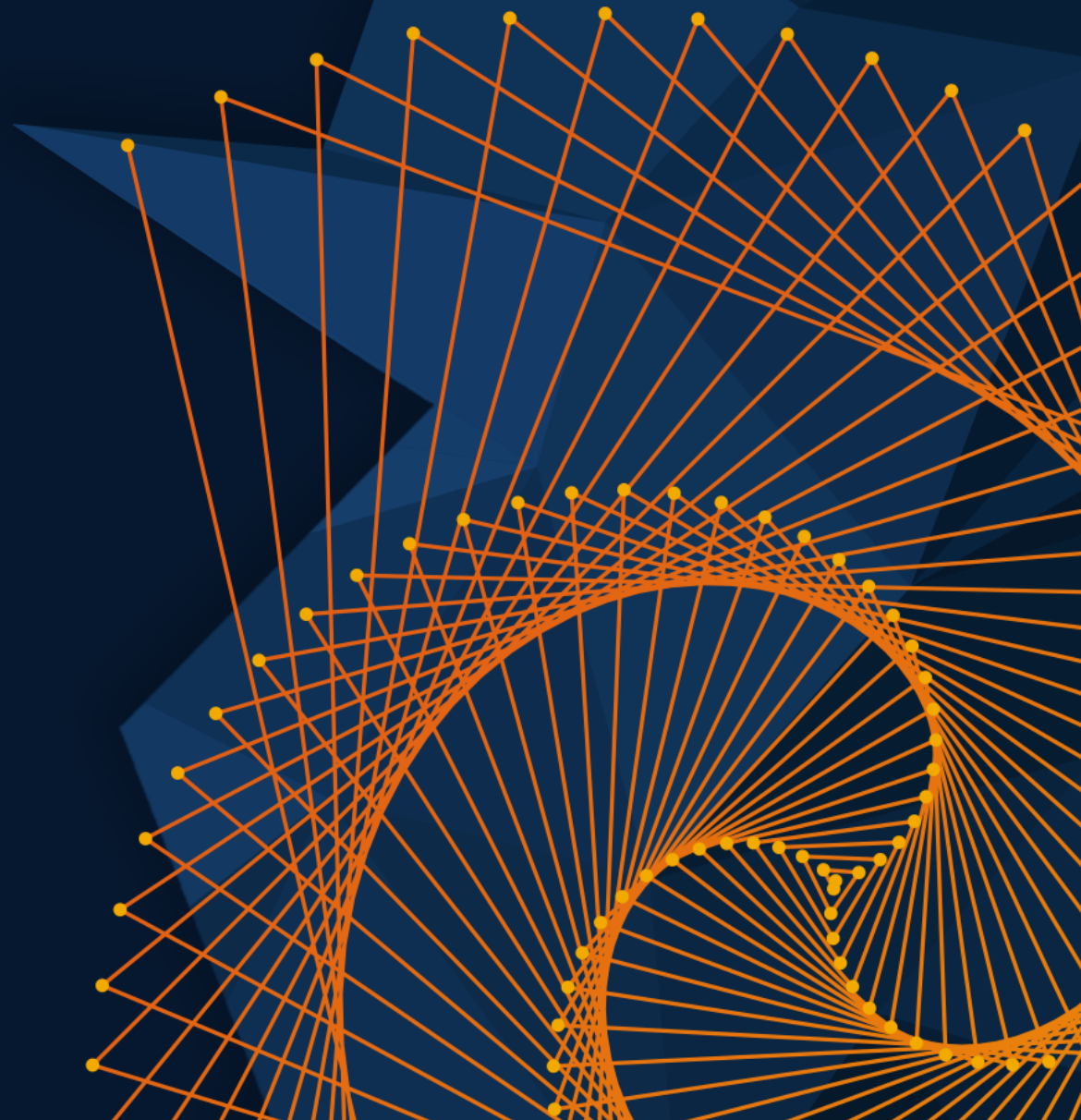
Signed on behalf of DNV

C. K. WONG
Management Representative, SCPA RGC

DNV Headquarters, Veritasveien 1, P.O.Box 300, 1322 Høvik, Norway. Tel: +47 67 57 99 00. www.dnv.com

MATLAB EXPO

Thank you



MathWorks®