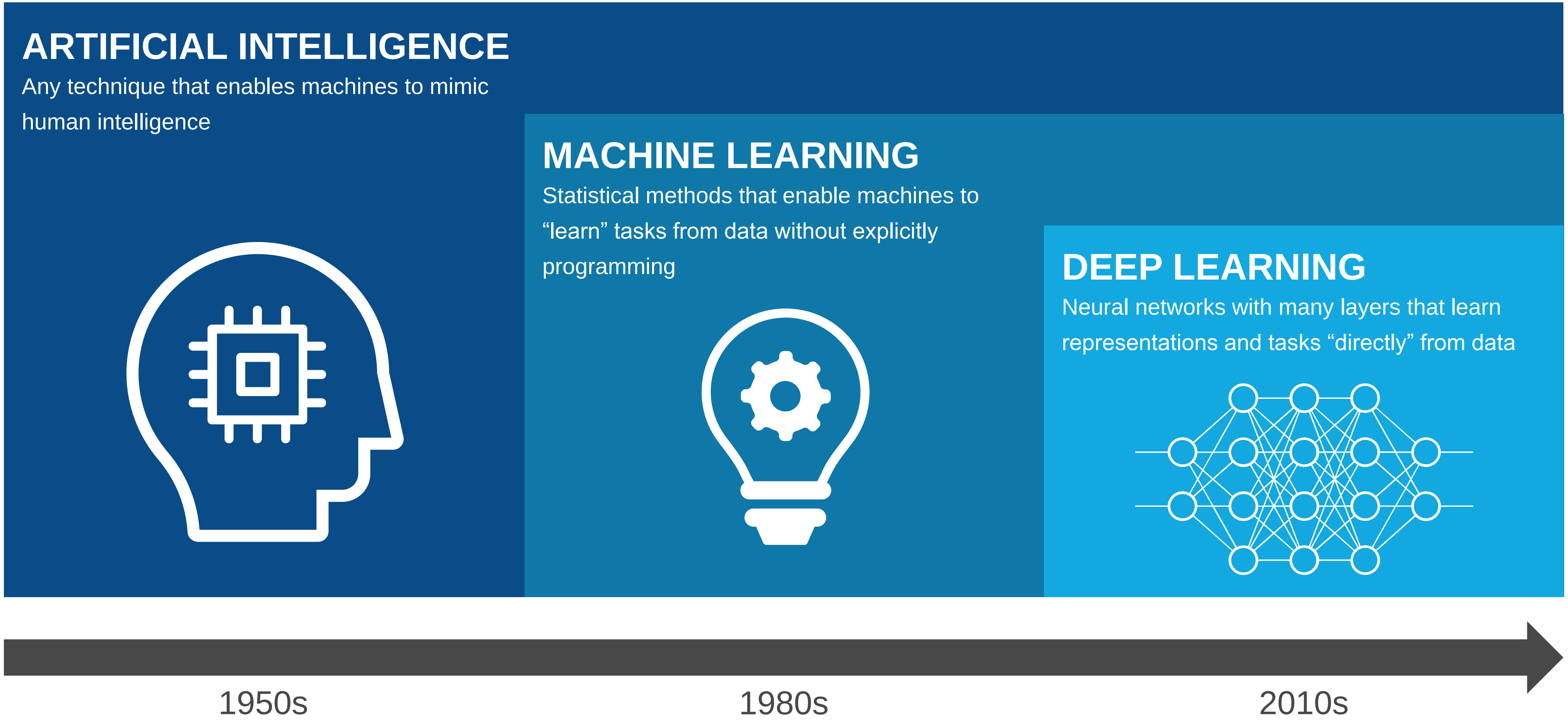
2024 MathWorks
中国汽车年会

面向 ASPICE 4.0 的 AI V&V 工作流

陈建平, MathWorks 中国

MathWorks

深度学习是推动人工智能大趋势的关键技术



ARTIFICIAL INTELLIGENCE

Any technique that enables machines to mimic human intelligence

MACHINE LEARNING

Statistical methods that enable machines to “learn” tasks from data without explicitly programming

DEEP LEARNING

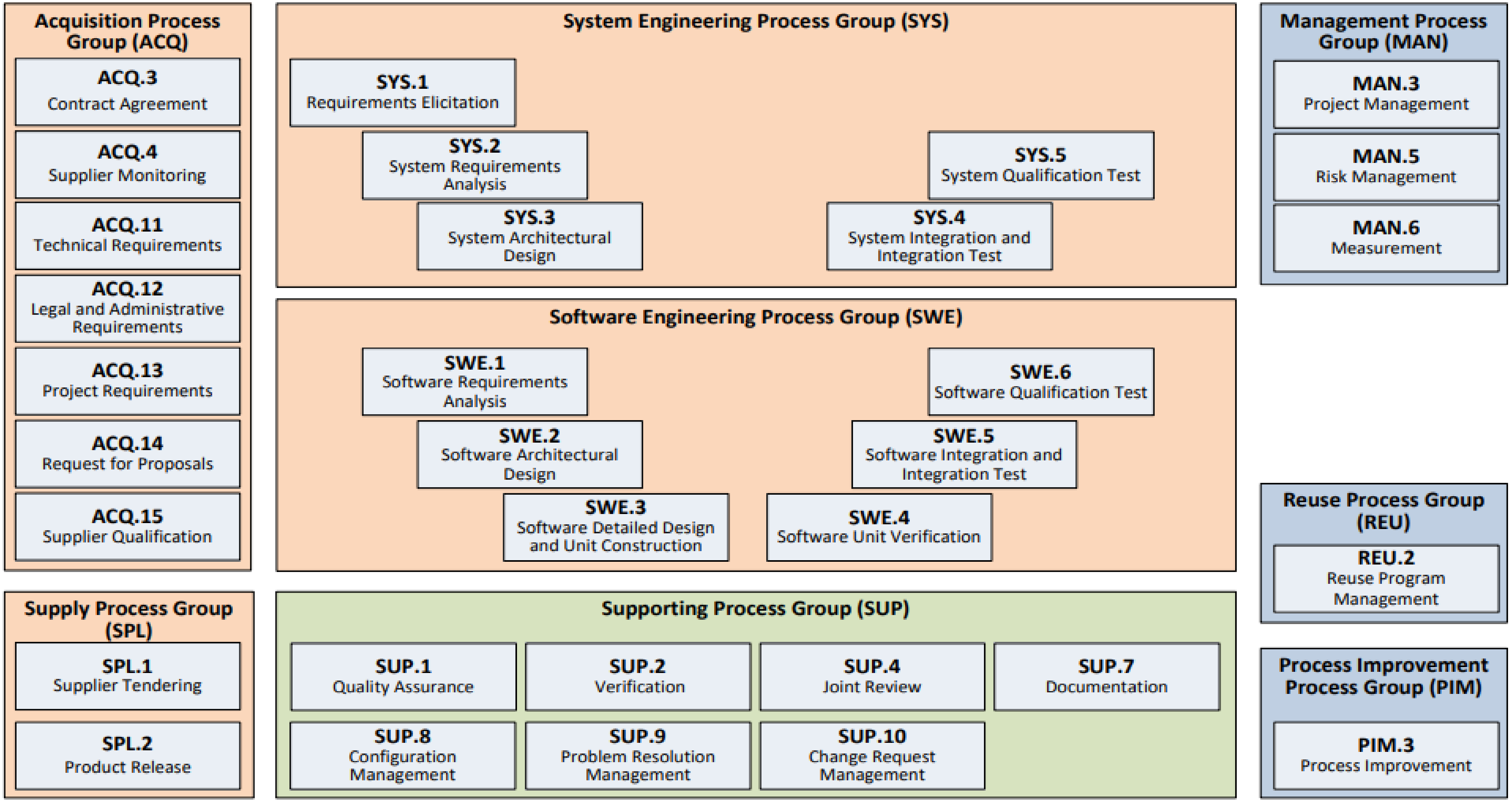
Neural networks with many layers that learn representations and tasks “directly” from data

1950s

1980s

2010s

ASPICE 3.x 过程参考模型



Acquisition Process Group (ACQ)

- **ACQ.3** Contract Agreement
- **ACQ.4** Supplier Monitoring
- **ACQ.11** Technical Requirements
- **ACQ.12** Legal and Administrative Requirements
- **ACQ.13** Project Requirements
- **ACQ.14** Request for Proposals
- **ACQ.15** Supplier Qualification

System Engineering Process Group (SYS)

- **SYS.1** Requirements Elicitation
- **SYS.2** System Requirements Analysis
- **SYS.3** System Architectural Design
- **SYS.4** System Integration and Integration Test
- **SYS.5** System Qualification Test

Software Engineering Process Group (SWE)

- **SWE.1** Software Requirements Analysis
- **SWE.2** Software Architectural Design
- **SWE.3** Software Detailed Design and Unit Construction
- **SWE.4** Software Unit Verification
- **SWE.5** Software Integration and Integration Test
- **SWE.6** Software Qualification Test

Management Process Group (MAN)

- **MAN.3** Project Management
- **MAN.5** Risk Management
- **MAN.6** Measurement

Reuse Process Group (REU)

- **REU.2** Reuse Program Management

Process Improvement Process Group (PIM)

- **PIM.3** Process Improvement

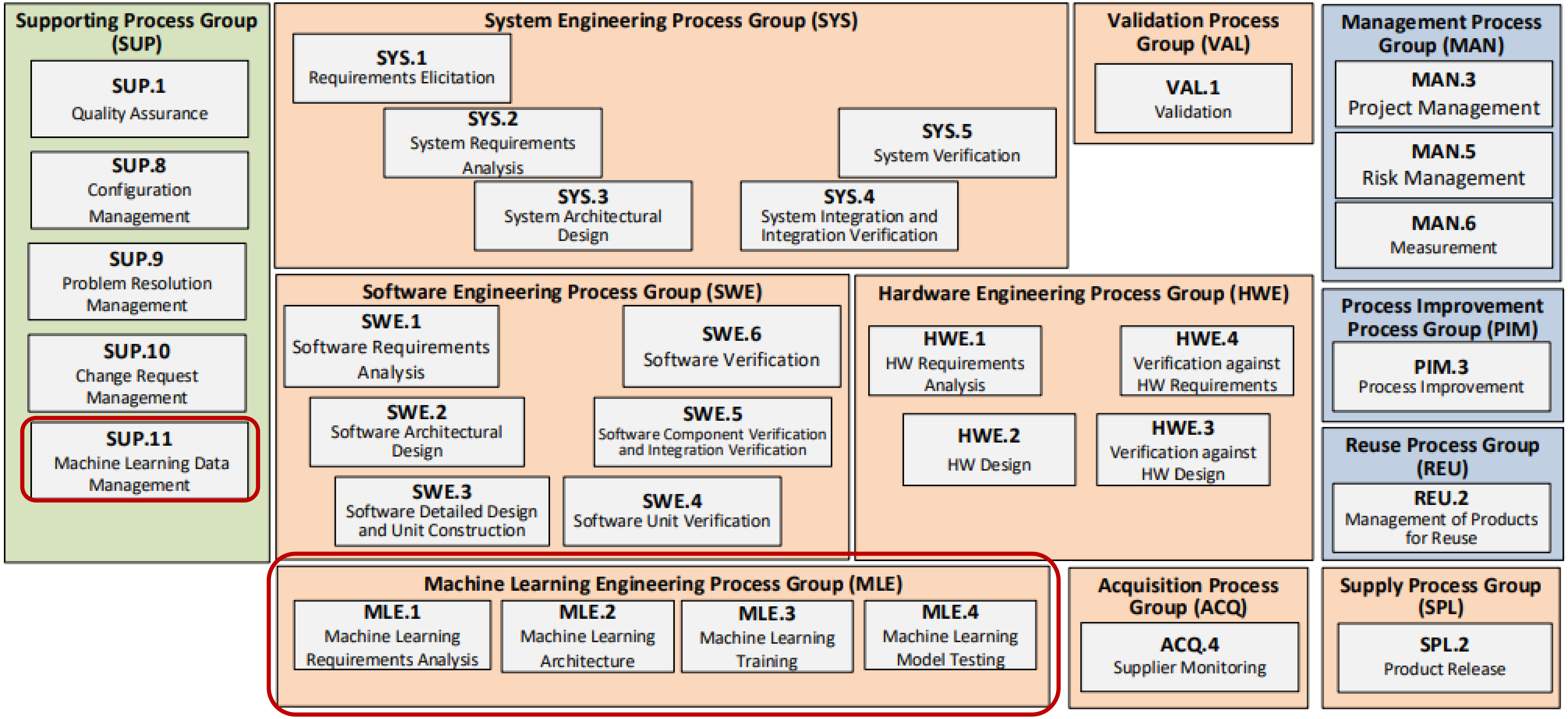
Supply Process Group (SPL)

- **SPL.1** Supplier Tendering
- **SPL.2** Product Release

Supporting Process Group (SUP)

- **SUP.1** Quality Assurance
- **SUP.2** Verification
- **SUP.4** Joint Review
- **SUP.7** Documentation
- **SUP.8** Configuration Management
- **SUP.9** Problem Resolution Management
- **SUP.10** Change Request Management

ASPICE 4.0 过程参考模型



Supporting Process Group (SUP)

- **SUP.1** Quality Assurance
- **SUP.8** Configuration Management
- **SUP.9** Problem Resolution Management
- **SUP.10** Change Request Management
- **SUP.11** Machine Learning Data Management

System Engineering Process Group (SYS)

- **SYS.1** Requirements Elicitation
- **SYS.2** System Requirements Analysis
- **SYS.3** System Architectural Design
- **SYS.4** System Integration and Integration Verification
- **SYS.5** System Verification

Validation Process Group (VAL)

- **VAL.1** Validation

Management Process Group (MAN)

- **MAN.3** Project Management
- **MAN.5** Risk Management
- **MAN.6** Measurement

Software Engineering Process Group (SWE)

- **SWE.1** Software Requirements Analysis
- **SWE.2** Software Architectural Design
- **SWE.3** Software Detailed Design and Unit Construction
- **SWE.4** Software Unit Verification
- **SWE.5** Software Component Verification and Integration Verification
- **SWE.6** Software Verification

Hardware Engineering Process Group (HWE)

- **HWE.1** HW Requirements Analysis
- **HWE.2** HW Design
- **HWE.3** Verification against HW Design
- **HWE.4** Verification against HW Requirements

Process Improvement Process Group (PIM)

- **PIM.3** Process Improvement

Reuse Process Group (REU)

- **REU.2** Management of Products for Reuse

Machine Learning Engineering Process Group (MLE)

- **MLE.1** Machine Learning Requirements Analysis
- **MLE.2** Machine Learning Architecture
- **MLE.3** Machine Learning Training
- **MLE.4** Machine Learning Model Testing

Acquisition Process Group (ACQ)

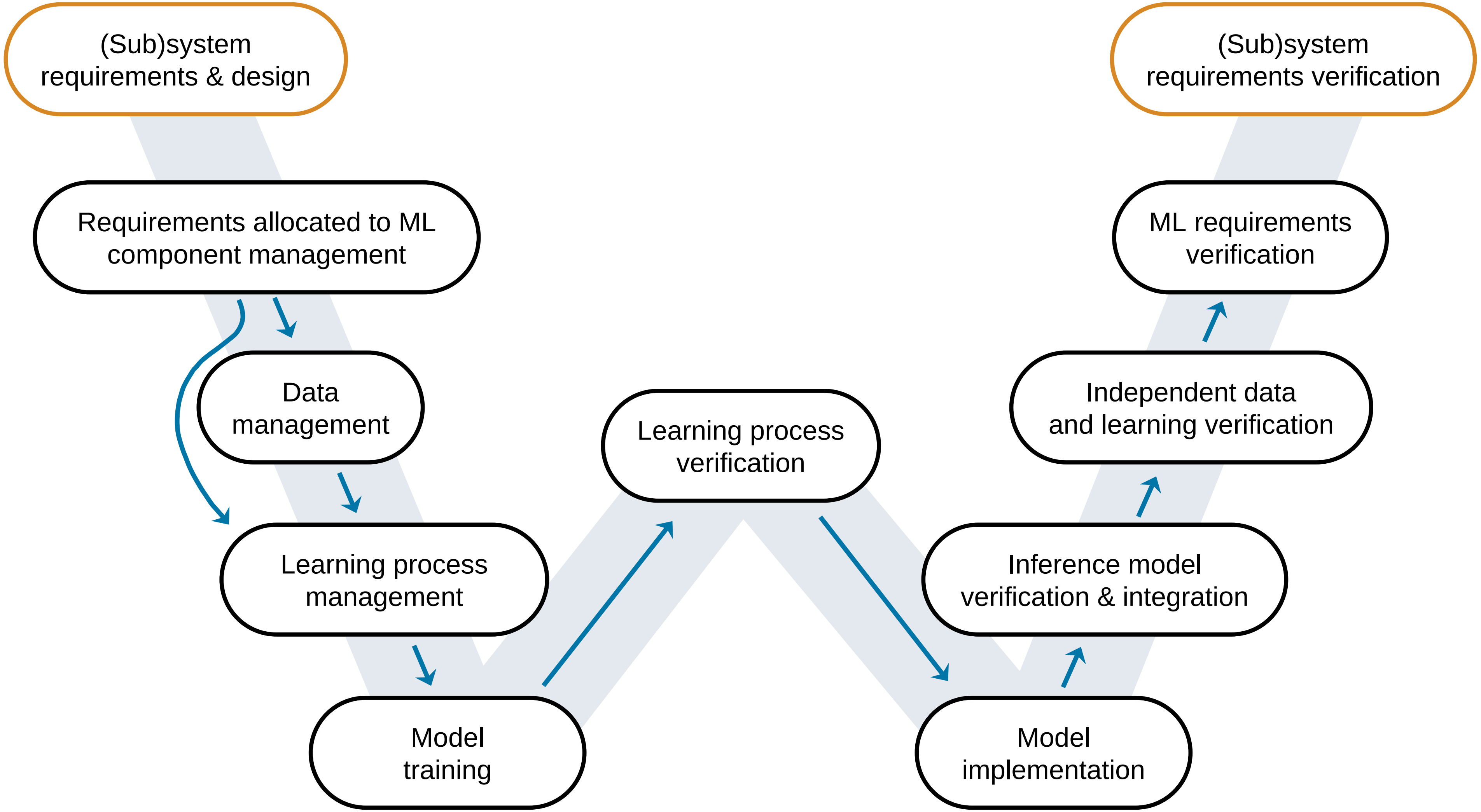
- **ACQ.4** Supplier Monitoring

Supply Process Group (SPL)

- **SPL.2** Product Release

W 开发过程模型

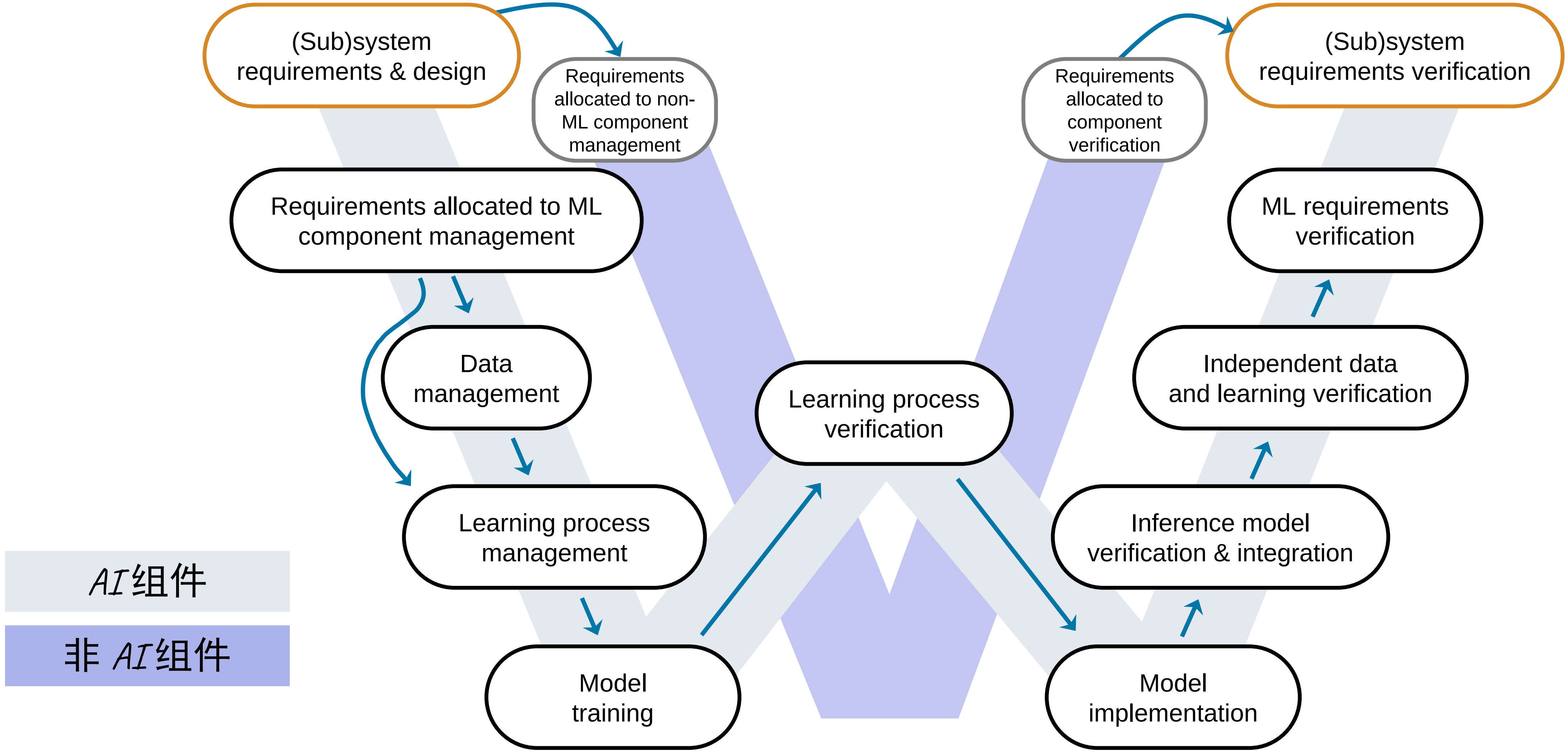
将经典的 V 形开发过程扩展至 AI


(Sub)system requirements & design
Requirements allocated to ML component management
Data management
Learning process management
Model training
Learning process verification
Model implementation
Inference model verification & integration
Independent data and learning verification
ML requirements verification
(Sub)system requirements verification

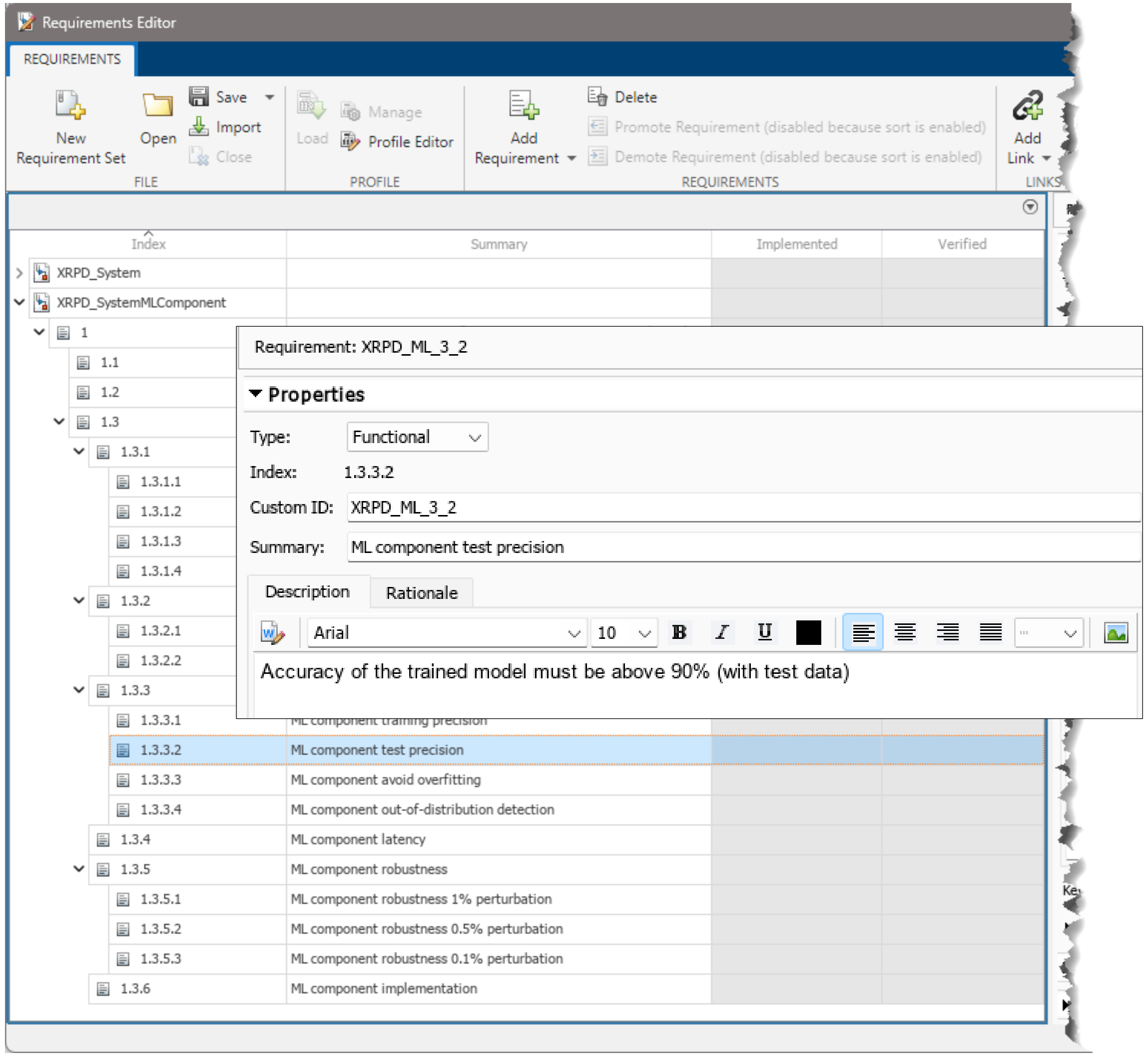
Credit: EASA, Daedalean

W 开发过程模型

与 V 模型共存


(Sub)system requirements & design
Requirements allocated to non-ML component management
Requirements allocated to ML component management
Data management
Learning process management
Model training
Learning process verification
Model implementation
Inference model verification & integration
Independent data and learning verification
ML requirements verification
Requirements allocated to component verification
(Sub)system requirements verification
AI组件
非 AI组件

汇集分配给 ML 组件的需求



Index	Summary	Implemented	Verified
XRPD_System			
XRPD_SystemMLComponent			
1			
1.1			
1.2			
1.3			
1.3.1			
1.3.1.1			
1.3.1.2			
1.3.1.3			
1.3.1.4			
1.3.2			
1.3.2.1			
1.3.2.2			
1.3.3			
1.3.3.1	ML component training precision		
1.3.3.2	ML component test precision		
1.3.3.3	ML component avoid overfitting		
1.3.3.4	ML component out-of-distribution detection		
1.3.4	ML component latency		
1.3.5	ML component robustness		
1.3.5.1	ML component robustness 1% perturbation		
1.3.5.2	ML component robustness 0.5% perturbation		
1.3.5.3	ML component robustness 0.1% perturbation		
1.3.6	ML component implementation		

Requirement: XRPD_ML_3_2

Properties

Type: Functional

Index: 1.3.3.2

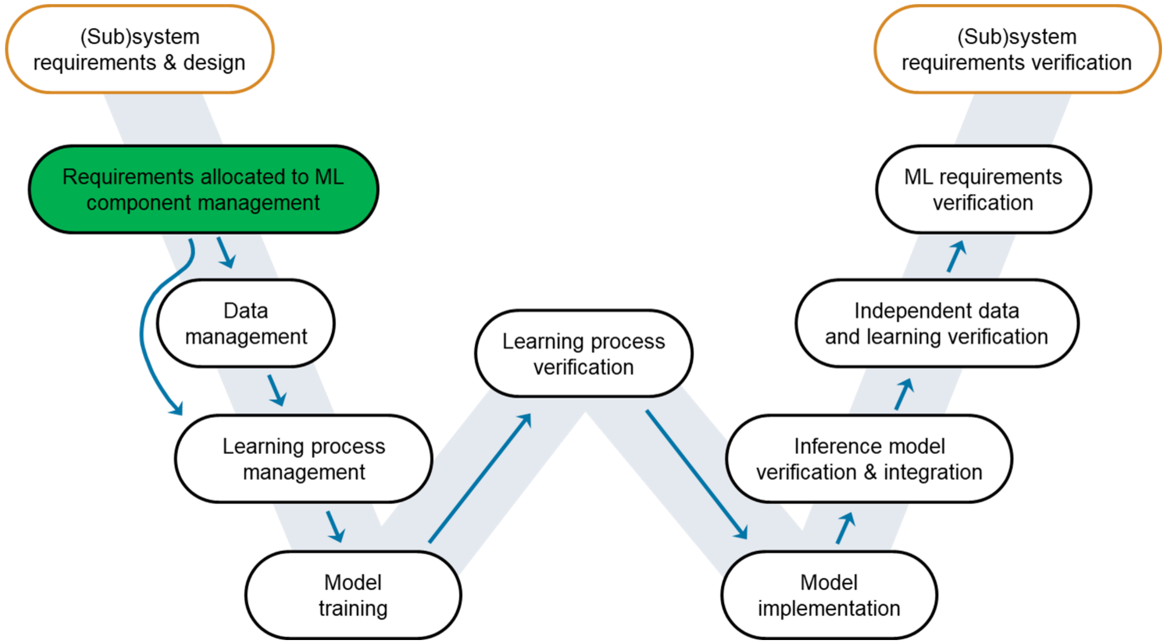
Custom ID: XRPD_ML_3_2

Summary: ML component test precision

Description | Rationale

Arial 10

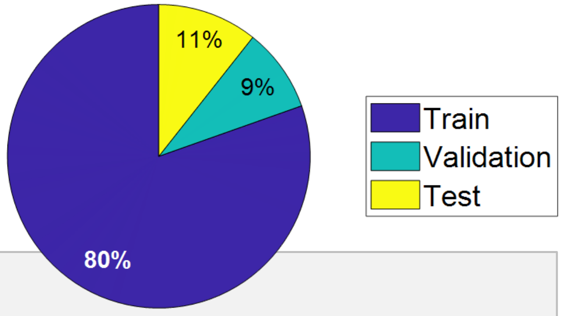
Accuracy of the trained model must be above 90% (with test data)


(Sub)system requirements & design
Requirements allocated to ML component management
Data management
Learning process management
Model training
Learning process verification
Model implementation
Inference model verification & integration
Independent data and learning verification
ML requirements verification
(Sub)system requirements verification

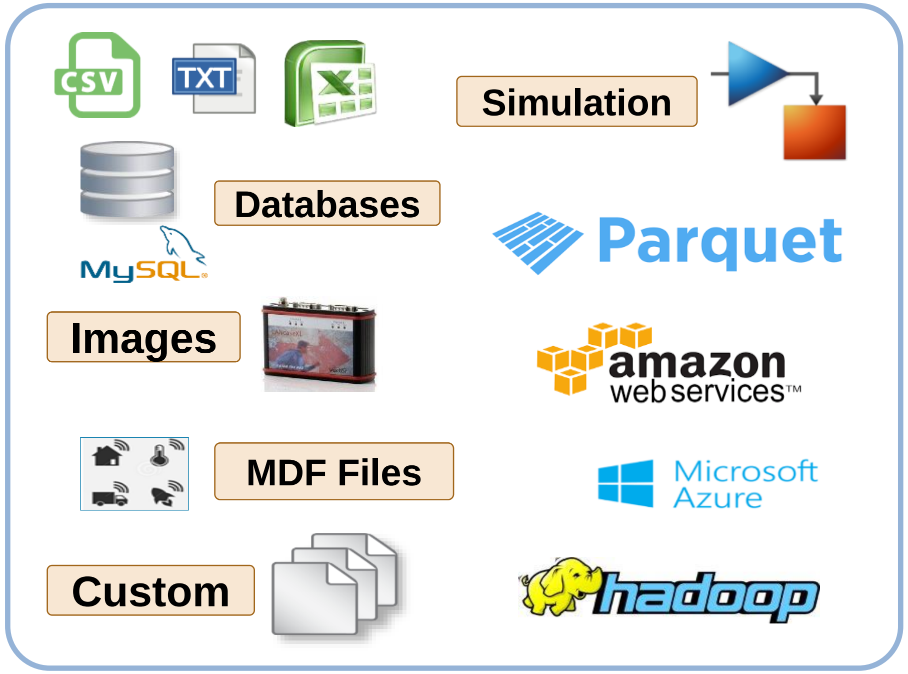
Machine Learning Engineering Process Group (MLE)

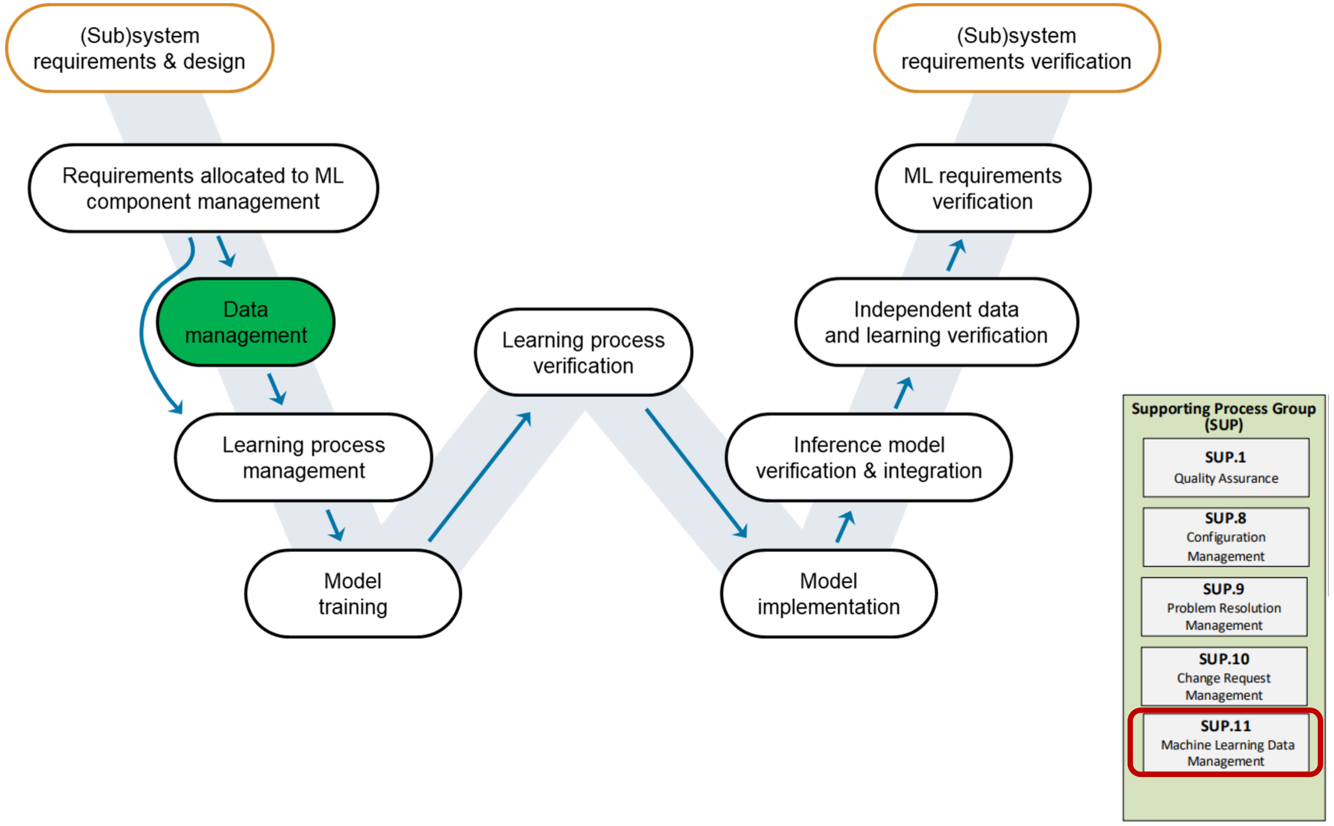
MLE.1	MLE.2	MLE.3	MLE.4
Machine Learning Requirements Analysis	Machine Learning Architecture	Machine Learning Training	Machine Learning Model Testing

便利地管理大数据



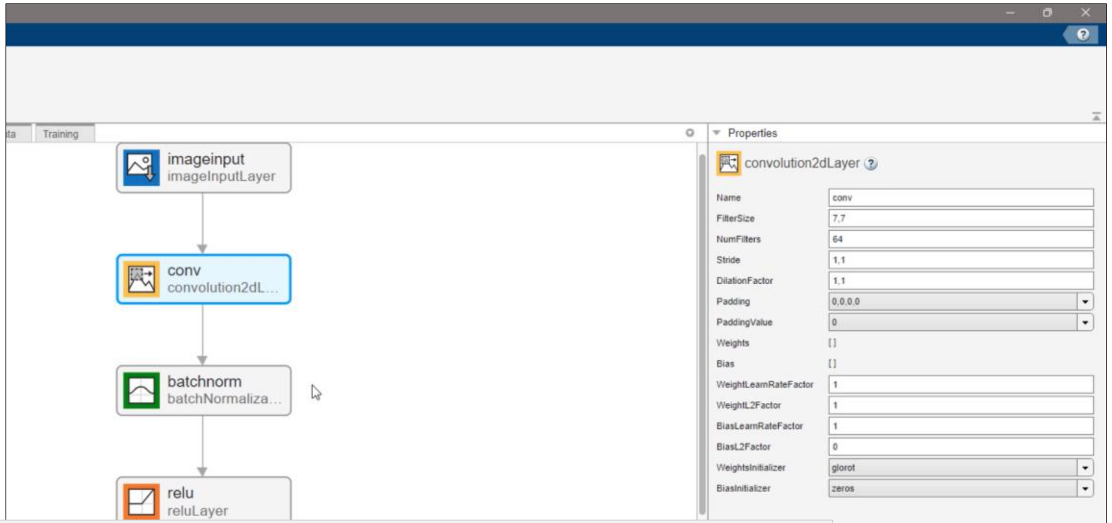
```
trainingDataFolder = “trafficsign\Train";
imdsTrain = imageDatastore(trainingDataFolder,IncludeSubfolders=true,LabelSource="foldernames");
```




(Sub)system requirements & design
Requirements allocated to ML component management
Data management
Learning process management
Model training
Learning process verification
Model implementation
Inference model verification & integration
Independent data and learning verification
ML requirements verification
(Sub)system requirements verification
Supporting Process Group (SUP)
SUP.1 Quality Assurance
SUP.8 Configuration Management
SUP.9 Problem Resolution Management
SUP.10 Change Request Management
SUP.11 Machine Learning Data Management

直观地创建网络加快设计速度

Machine Learning Engineering Process Group (MLE)			
MLE.1 Machine Learning Requirements Analysis	MLE.2 Machine Learning Architecture	MLE.3 Machine Learning Training	MLE.4 Machine Learning Model Testing

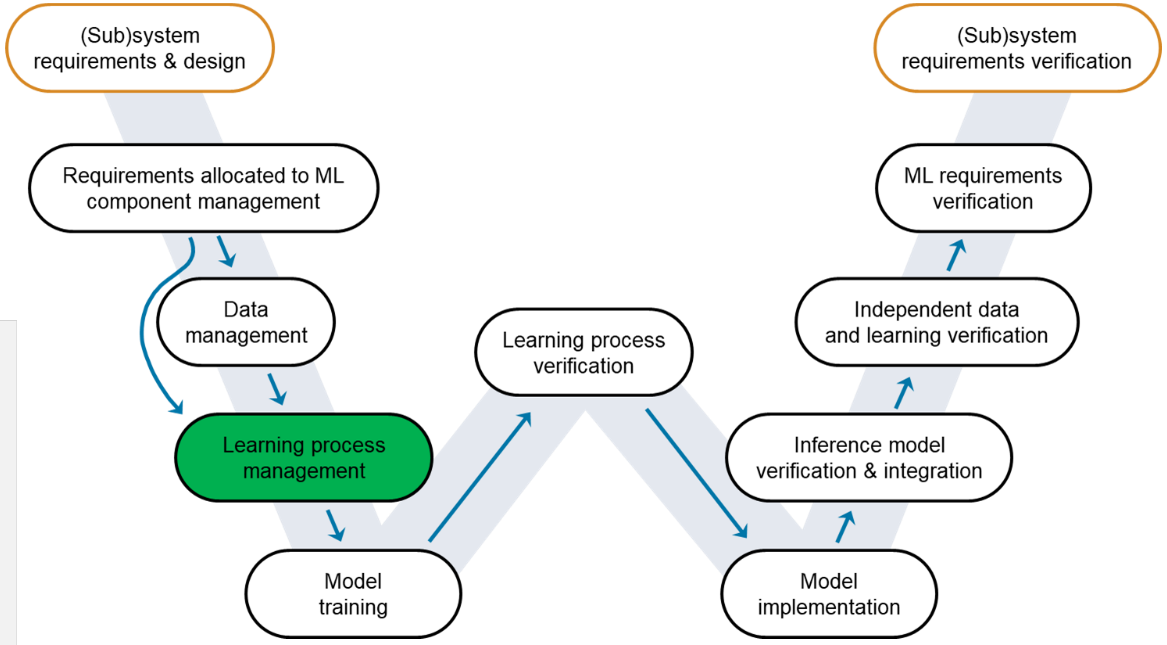


convolution2dLayer

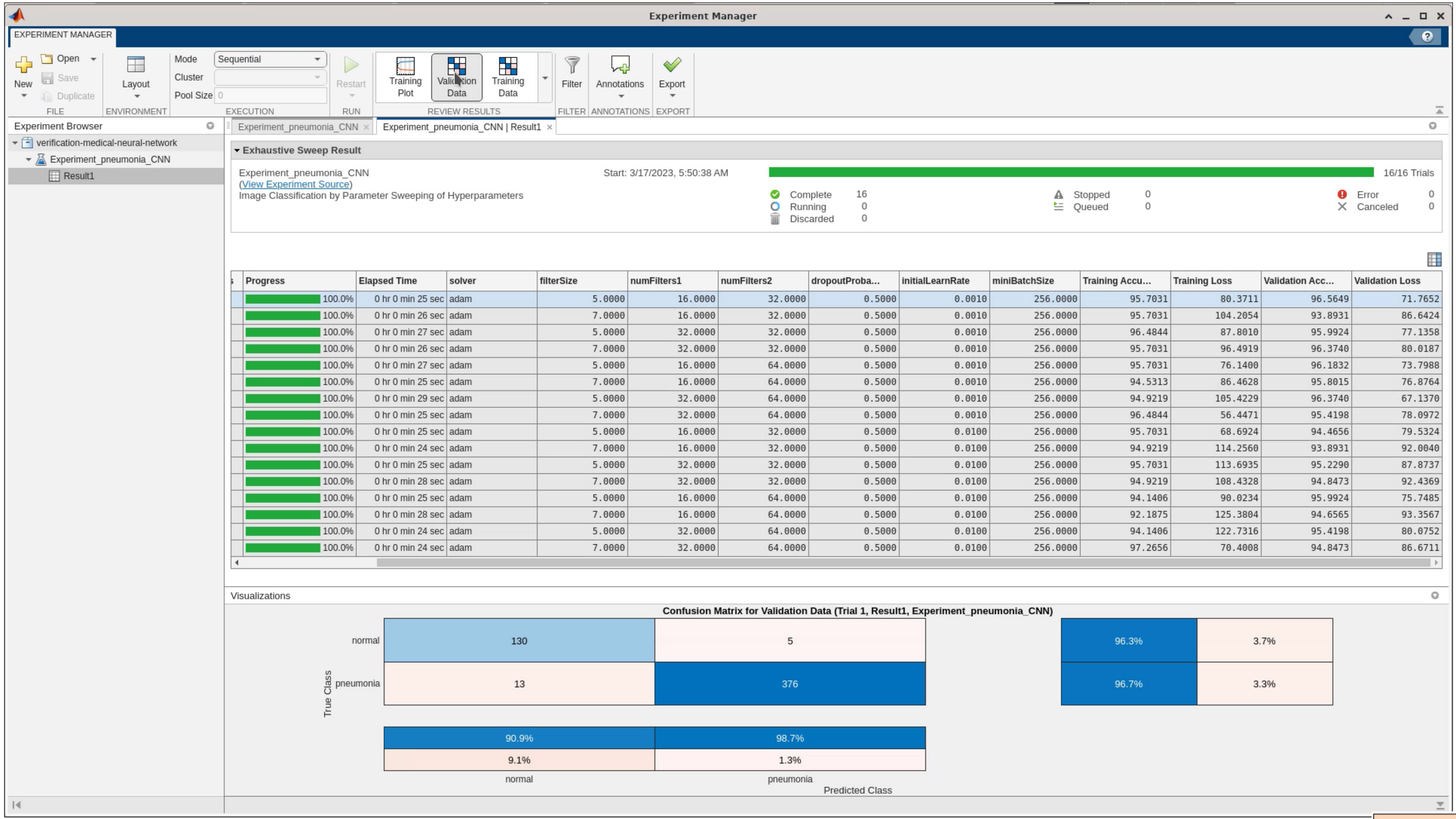
Name	conv
FilterSize	7,7
NumFilters	64
Stride	1,1
DilationFactor	1,1
Padding	0,0,0,0
PaddingValue	0
Weights	[]
Bias	[]
WeightLearnRateFactor	1
WeightL2Factor	1
BiasLearnRateFactor	1
BiasL2Factor	0
WeightsInitializer	glorot
BiasInitializer	zeros

```
numClasses = numel(classNames);
layers = [
    imageInputLayer(imageSize,Normalization="none")
    convolution2dLayer(7,64,Padding=0)
    batchNormalizationLayer()
    reluLayer()
    dropoutLayer(0.5)
    averagePooling2dLayer(2,Stride=2)
    convolution2dLayer(7,128,Padding=0)
    batchNormalizationLayer()
    reluLayer()
    dropoutLayer(0.5)
    averagePooling2dLayer(2,Stride=2)
    fullyConnectedLayer(numClasses)
    softmaxLayer
    classificationLayer(Classes=classNames,ClassWeights=classWeights)];
```

```
options = trainingOptions("adam", ...
    ExecutionEnvironment="auto", ...
    InitialLearnRate=0.001, ...
    MaxEpochs=50, ...
    MiniBatchSize=256, ...
    Shuffle="every-epoch",...
    LearnRateSchedule="piecewise", ...
    LearnRateDropPeriod=30, ...
    LearnRateDropFactor=0.1, ...
    Plots="training-progress", ...
    ValidationData={XVal,TVal}, ...
    ValidationPatience=10, ...
    OutputNetwork="best-validation-loss");
```


(Sub)system requirements & design
Requirements allocated to ML component management
Data management
Learning process management
Model training
Learning process verification
Model implementation
Inference model verification & integration
Independent data and learning verification
ML requirements verification
(Sub)system requirements verification

使用 Experiment Manager 优化模型架构



Mode: Sequential
Cluster:
Pool Size: 0
EXECUTION

Exhaustive Sweep Result

Experiment_pneumonia_CNN
(View Experiment Source)
Image Classification by Parameter Sweeping of Hyperparameters

Start: 3/17/2023, 5:50:38 AM

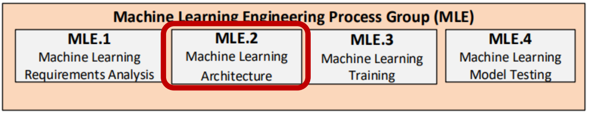
16/16 Trials

Complete	16	Stopped	0	Error	0
Running	0	Queued	0	Canceled	0
Discarded	0				

Progress	Elapsed Time	solver	filterSize	numFilters1	numFilters2	dropoutProba...	initialLearnRate	miniBatchSize	Training Accu...	Training Loss	Validation Acc...	Validation Loss
100.0%	0 hr 0 min 25 sec	adam	5.0000	16.0000	32.0000	0.5000	0.0010	256.0000	95.7031	80.3711	96.5649	71.7652
100.0%	0 hr 0 min 26 sec	adam	7.0000	16.0000	32.0000	0.5000	0.0010	256.0000	95.7031	104.2054	93.8931	86.6424
100.0%	0 hr 0 min 27 sec	adam	5.0000	32.0000	32.0000	0.5000	0.0010	256.0000	96.4844	87.8010	95.9924	77.1358
100.0%	0 hr 0 min 26 sec	adam	7.0000	32.0000	32.0000	0.5000	0.0010	256.0000	95.7031	96.4919	96.3740	80.0187
100.0%	0 hr 0 min 27 sec	adam	5.0000	16.0000	64.0000	0.5000	0.0010	256.0000	95.7031	76.1400	96.1832	73.7988
100.0%	0 hr 0 min 25 sec	adam	7.0000	16.0000	64.0000	0.5000	0.0010	256.0000	94.5313	86.4628	95.8015	76.8764
100.0%	0 hr 0 min 29 sec	adam	5.0000	32.0000	64.0000	0.5000	0.0010	256.0000	94.9219	105.4229	96.3740	67.1370
100.0%	0 hr 0 min 25 sec	adam	7.0000	32.0000	64.0000	0.5000	0.0010	256.0000	96.4844	56.4471	95.4198	78.0972
100.0%	0 hr 0 min 25 sec	adam	5.0000	16.0000	32.0000	0.5000	0.0100	256.0000	95.7031	68.6924	94.4656	79.5324
100.0%	0 hr 0 min 24 sec	adam	7.0000	16.0000	32.0000	0.5000	0.0100	256.0000	94.9219	114.2560	93.8931	92.0040
100.0%	0 hr 0 min 25 sec	adam	5.0000	32.0000	32.0000	0.5000	0.0100	256.0000	95.7031	113.6935	95.2290	87.8737
100.0%	0 hr 0 min 28 sec	adam	7.0000	32.0000	32.0000	0.5000	0.0100	256.0000	94.9219	108.4328	94.8473	92.4369
100.0%	0 hr 0 min 25 sec	adam	5.0000	16.0000	64.0000	0.5000	0.0100	256.0000	94.1406	90.0234	95.9924	75.7485
100.0%	0 hr 0 min 28 sec	adam	7.0000	16.0000	64.0000	0.5000	0.0100	256.0000	92.1875	125.3804	94.6565	93.3567
100.0%	0 hr 0 min 24 sec	adam	5.0000	32.0000	64.0000	0.5000	0.0100	256.0000	94.1406	122.7316	95.4198	80.0752
100.0%	0 hr 0 min 24 sec	adam	7.0000	32.0000	64.0000	0.5000	0.0100	256.0000	97.2656	70.4008	94.8473	86.6711

Confusion Matrix for Validation Data (Trial 1, Result1, Experiment_pneumonia_CNN)

True Class \ Predicted Class	normal	pneumonia		
normal	130	5	96.3%	3.7%
pneumonia	13	376	96.7%	3.3%
	90.9%	98.7%		
	9.1%	1.3%		



Machine Learning Engineering Process Group (MLE)

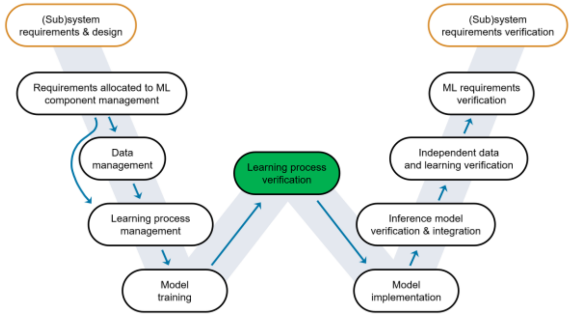
MLE.1 Machine Learning Requirements Analysis

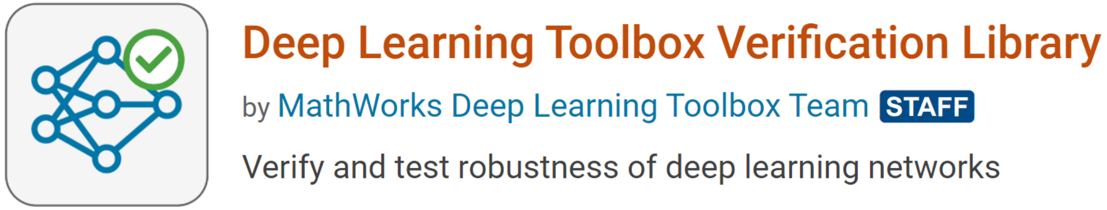
MLE.2 Machine Learning Architecture

MLE.3 Machine Learning Training

MLE.4 Machine Learning Model Testing

验证深度学习网络的鲁棒性

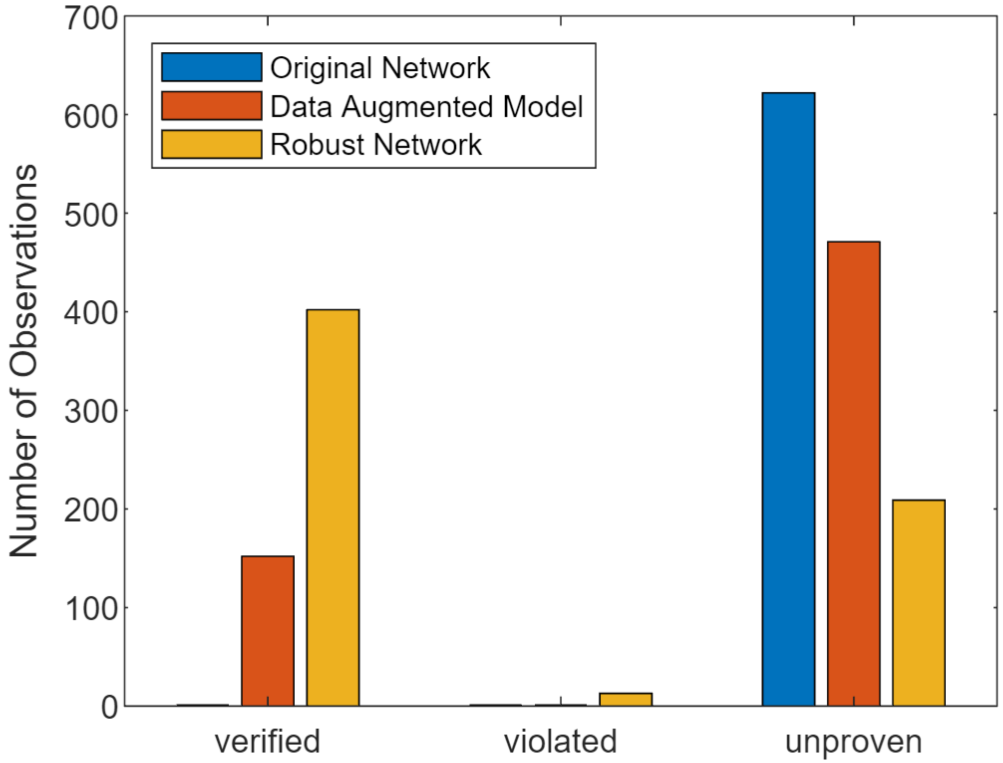

(Sub)system requirements & design
Requirements allocated to ML component management
Data management
Learning process management
Model training
Learning process verification
Model implementation
Inference model verification & integration
Independent data and learning verification
ML requirements verification
(Sub)system requirements verification

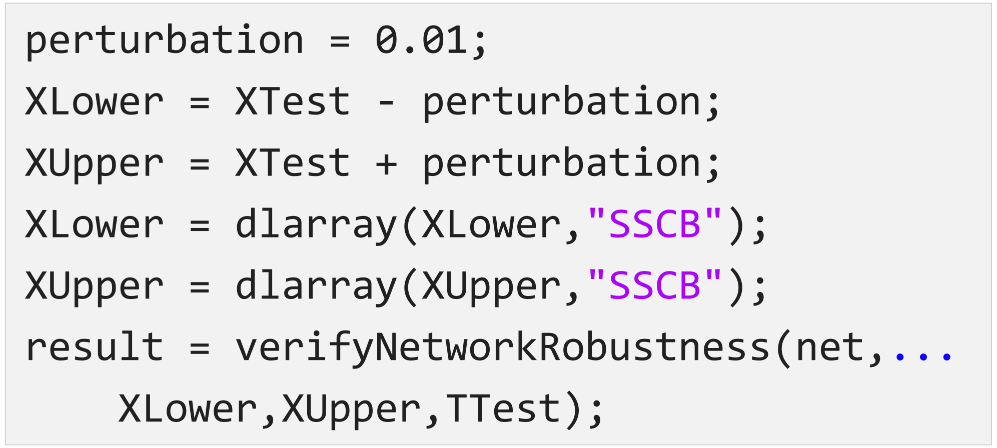


Deep Learning Toolbox Verification Library

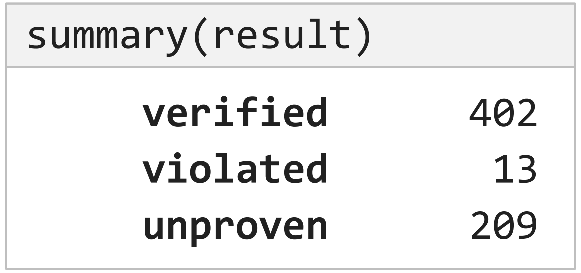
by MathWorks Deep Learning Toolbox Team STAFF

Verify and test robustness of deep learning networks



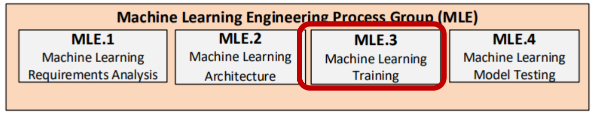


```
perturbation = 0.01;
XLower = XTest - perturbation;
XUpper = XTest + perturbation;
XLower = dlarray(XLower,"SSCB");
XUpper = dlarray(XUpper,"SSCB");
result = verifyNetworkRobustness(net,...
    XLower,XUpper,TTest);
```



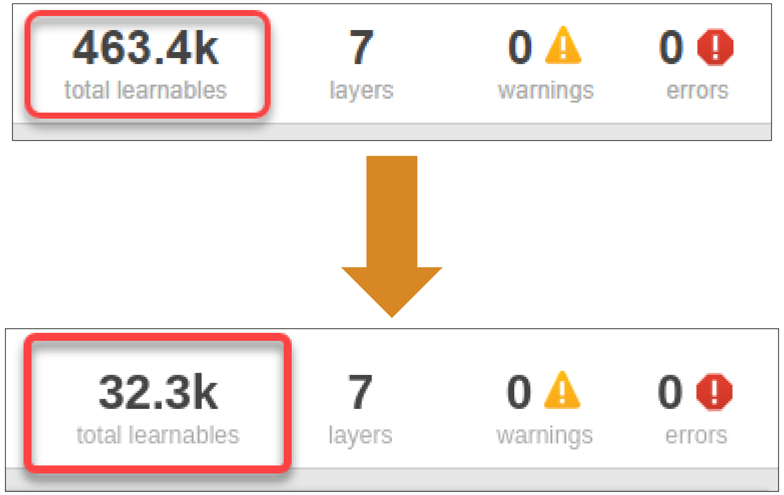
```
summary(result)

      verified      402
      violated       13
      unproven      209
```


Machine Learning Engineering Process Group (MLE)
MLE.1
Machine Learning Requirements Analysis
MLE.2
Machine Learning Architecture
MLE.3
Machine Learning Training
MLE.4
Machine Learning Model Testing

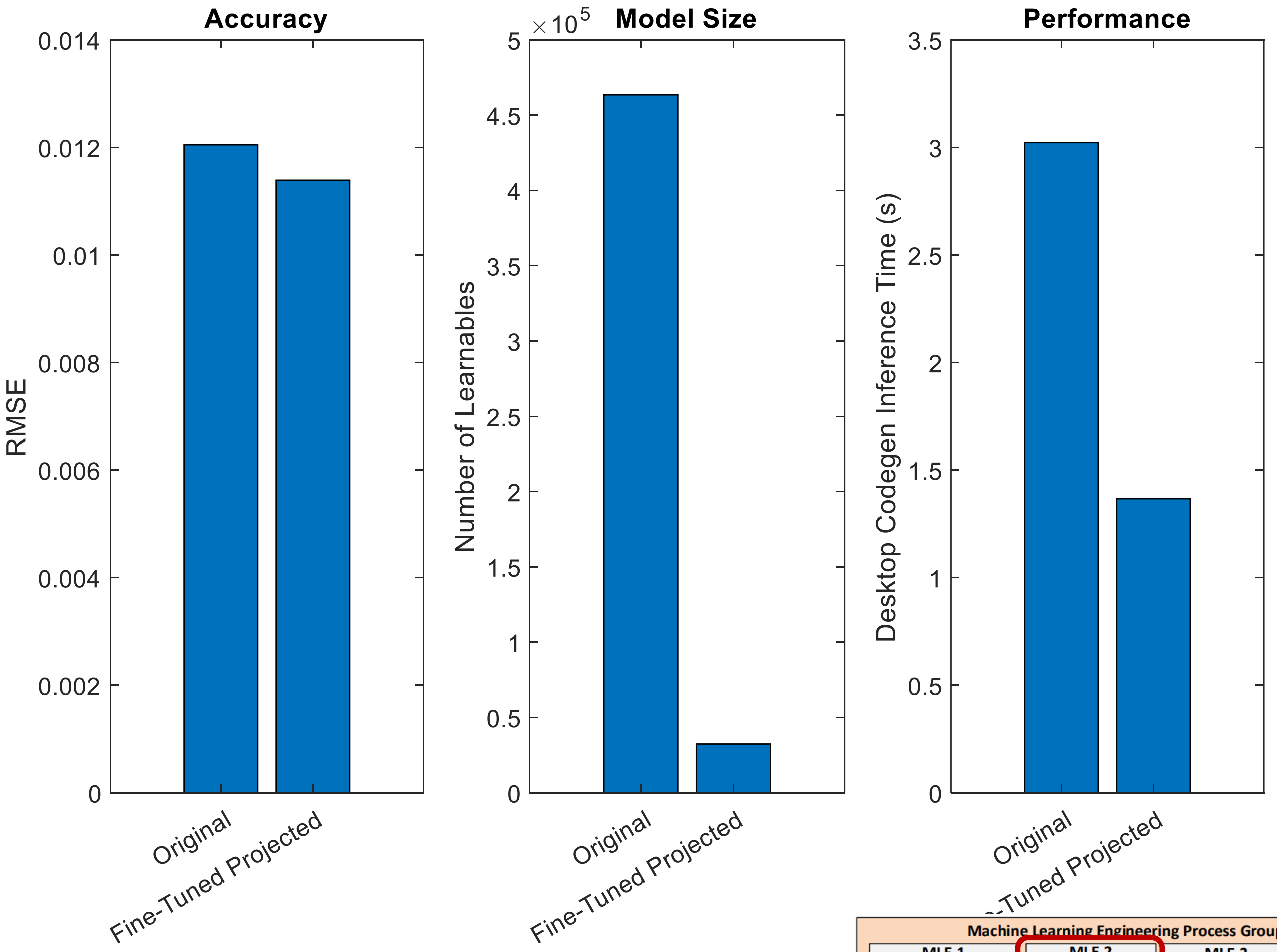
网络压缩

体积减小 93%，速度提升 2 倍



463.4k total learnables | 7 layers | 0 warnings | 0 errors

32.3k total learnables | 7 layers | 0 warnings | 0 errors



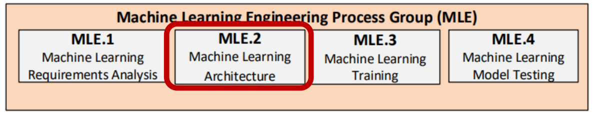
Machine Learning Engineering Process Group (MLE)

MLE.1 Machine Learning Requirements Analysis | MLE.2 Machine Learning Architecture | MLE.3 Machine Learning Training | MLE.4 Machine Learning Model Testing

示例：使用深度神经网络设计 SOC 估计器

	EKF Extended Kalman Filter	**Tree** Fine Regression Tree	**FFN** 1-hidden layer Feedforward Network	**LSTM** Stacked Long Short-Term Memory Network	**LSTM*** * Compressed Stacked Long Short-Term Memory Network
预处理工作量	🔵	🟡	🟡	🔵	🔵
训练速度	N/A	🔵	🟡	🔴	🔴
可解释性	🔵	🔵	🔴	🔴	🔴
推理速度	🟡	🔵	🔵🔵	🔴	🟡
模型尺寸	🔵	🟡	🔵	🔴	🔵
准确度 （RSME）	🔵	🟡	🔵	🔵🔵	🔵🔵

Much Better 🔵🔵 Better 🔵 Okay 🟡 Worse 🔴


Machine Learning Engineering Process Group (MLE)

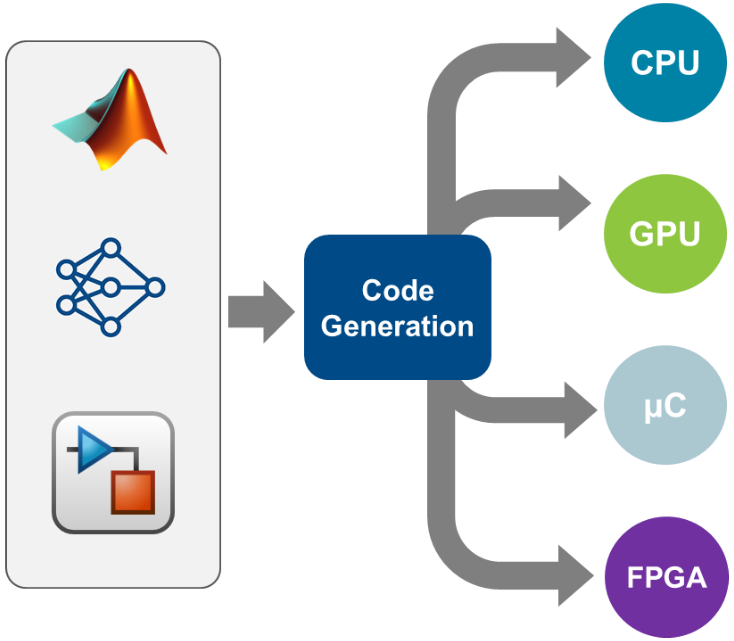
MLE.1 Machine Learning Requirements Analysis

MLE.2 Machine Learning Architecture

MLE.3 Machine Learning Training

MLE.4 Machine Learning Model Testing

零编码错误部署到目标硬件



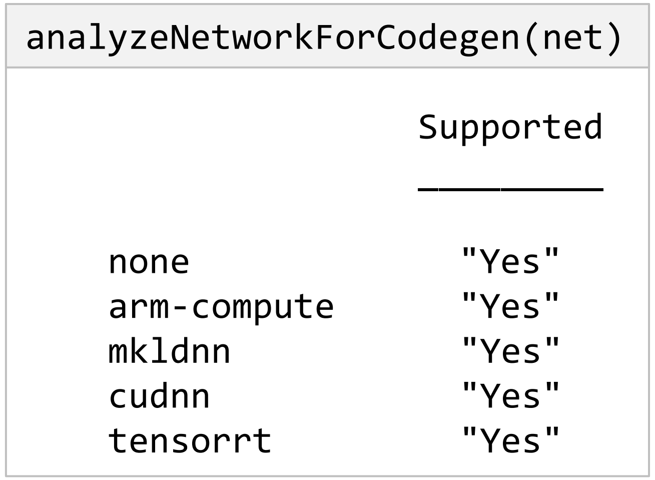
Code Generation

CPU

GPU

μC

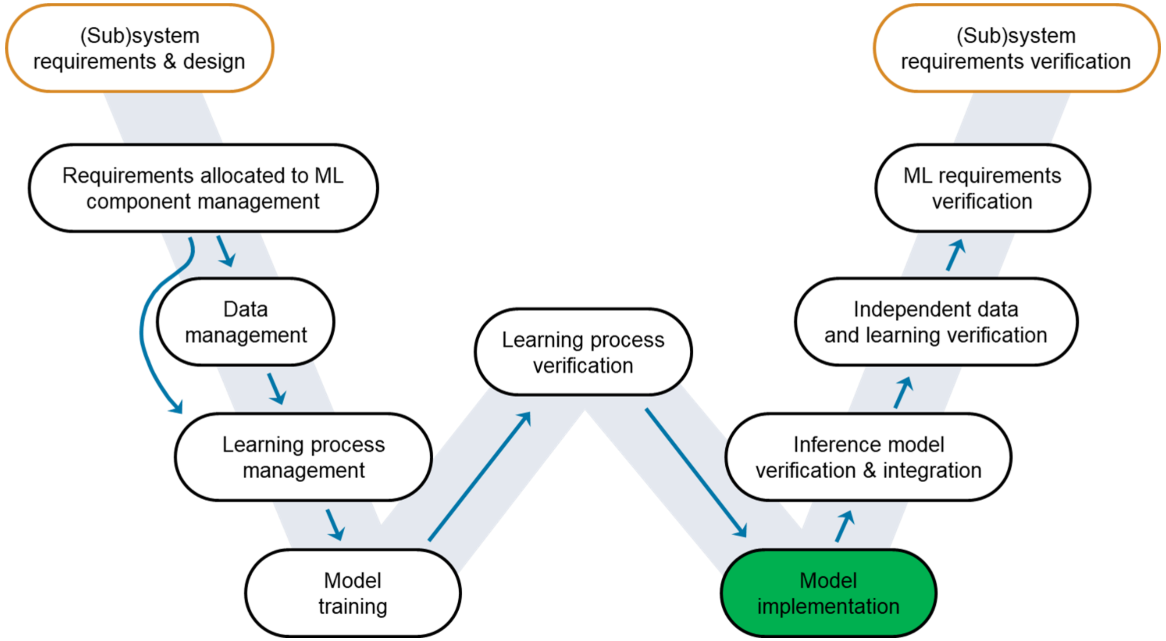
FPGA



```
analyzeNetworkForCodegen(net)

                        Supported
                        _________

     none               "Yes"
     arm-compute        "Yes"
     mkldnn             "Yes"
     cudnn              "Yes"
     tensorrt           "Yes"
```



(Sub)system requirements & design

Requirements allocated to ML component management

Data management

Learning process management

Model training

Learning process verification

Model implementation

Inference model verification & integration

Independent data and learning verification

ML requirements verification

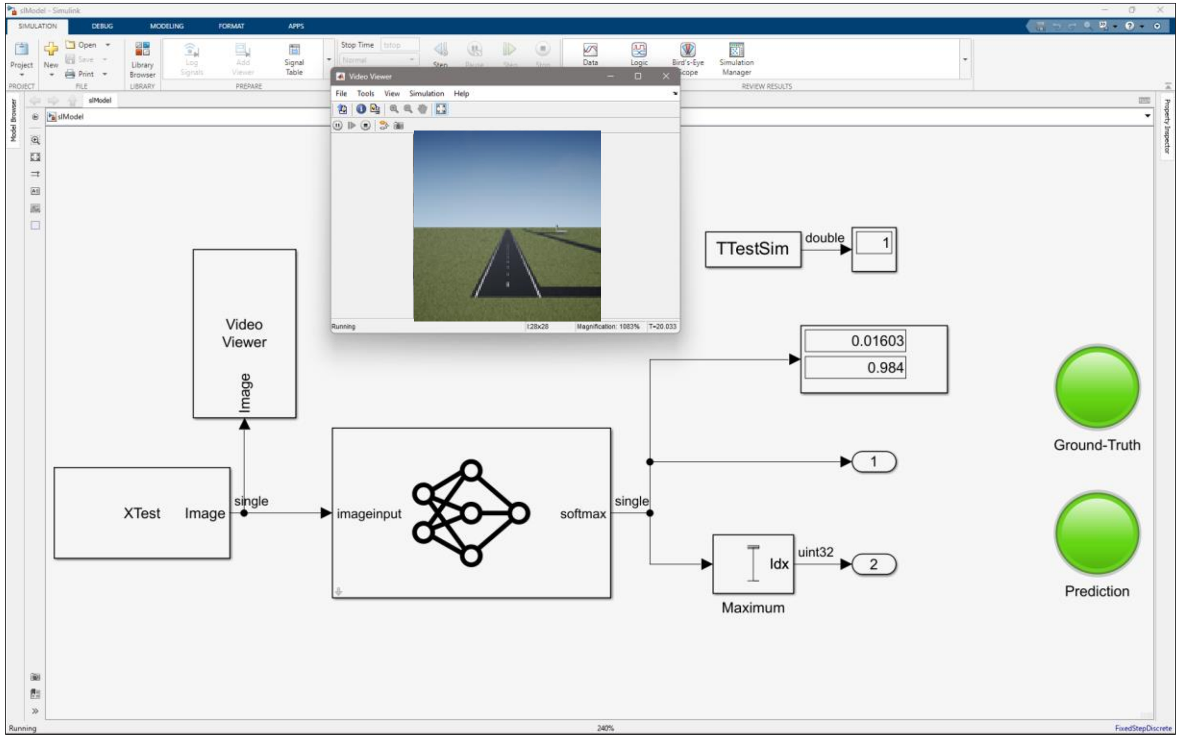
(Sub)system requirements verification

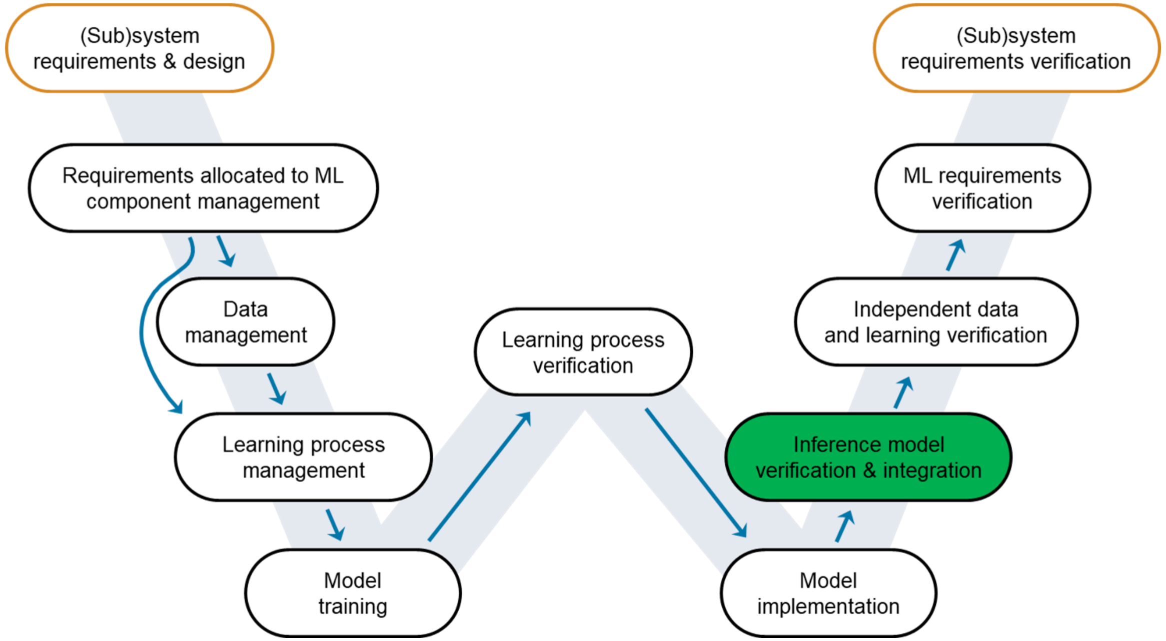
Machine Learning Engineering Process Group (MLE)

MLE.1	**MLE.2**	**MLE.3**	**MLE.4**
Machine Learning Requirements Analysis	Machine Learning Architecture	Machine Learning Training	Machine Learning Model Testing

系统级仿真和测试

将 AI 模型集成到 Simulink

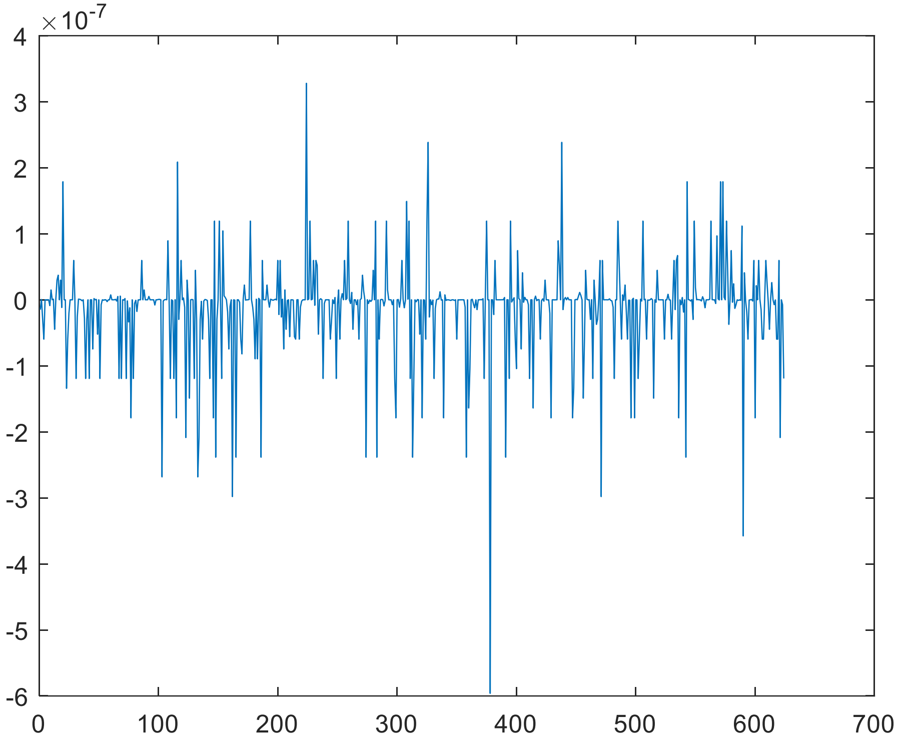


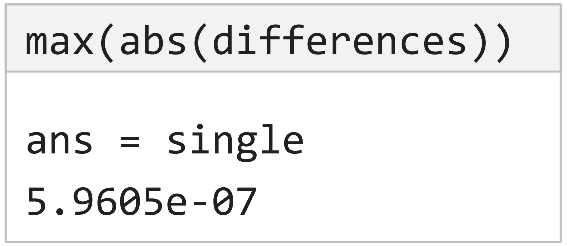

(Sub)system requirements & design
Requirements allocated to ML component management
Data management
Learning process management
Model training
Learning process verification
Model implementation
Inference model verification & integration
Independent data and learning verification
ML requirements verification
(Sub)system requirements verification

Machine Learning Engineering Process Group (MLE)

MLE.1	MLE.2	MLE.3	MLE.4
Machine Learning Requirements Analysis	Machine Learning Architecture	Machine Learning Training	Machine Learning Model Testing

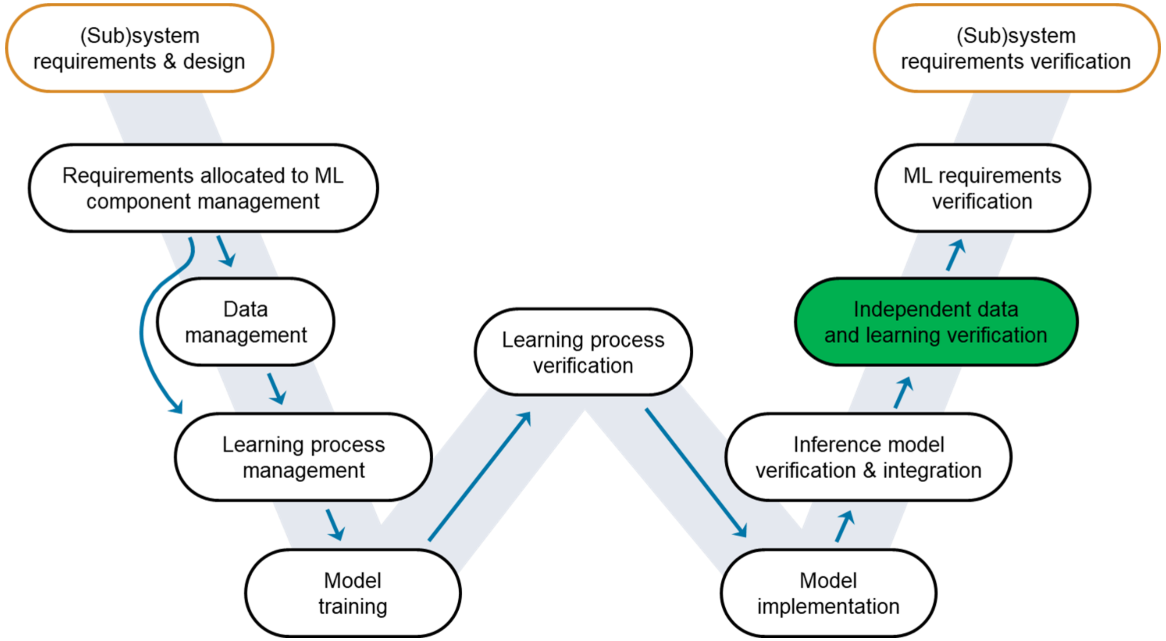
开发模型和推理模型完全一致





```
max(abs(differences))

ans = single
5.9605e-07
```



(Sub)system requirements & design

Requirements allocated to ML component management

Data management

Learning process management

Model training

Learning process verification

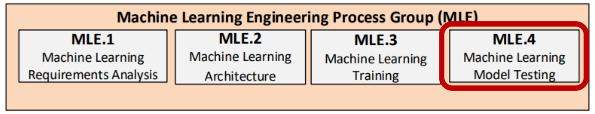
Model implementation

Inference model verification & integration

Independent data and learning verification

ML requirements verification

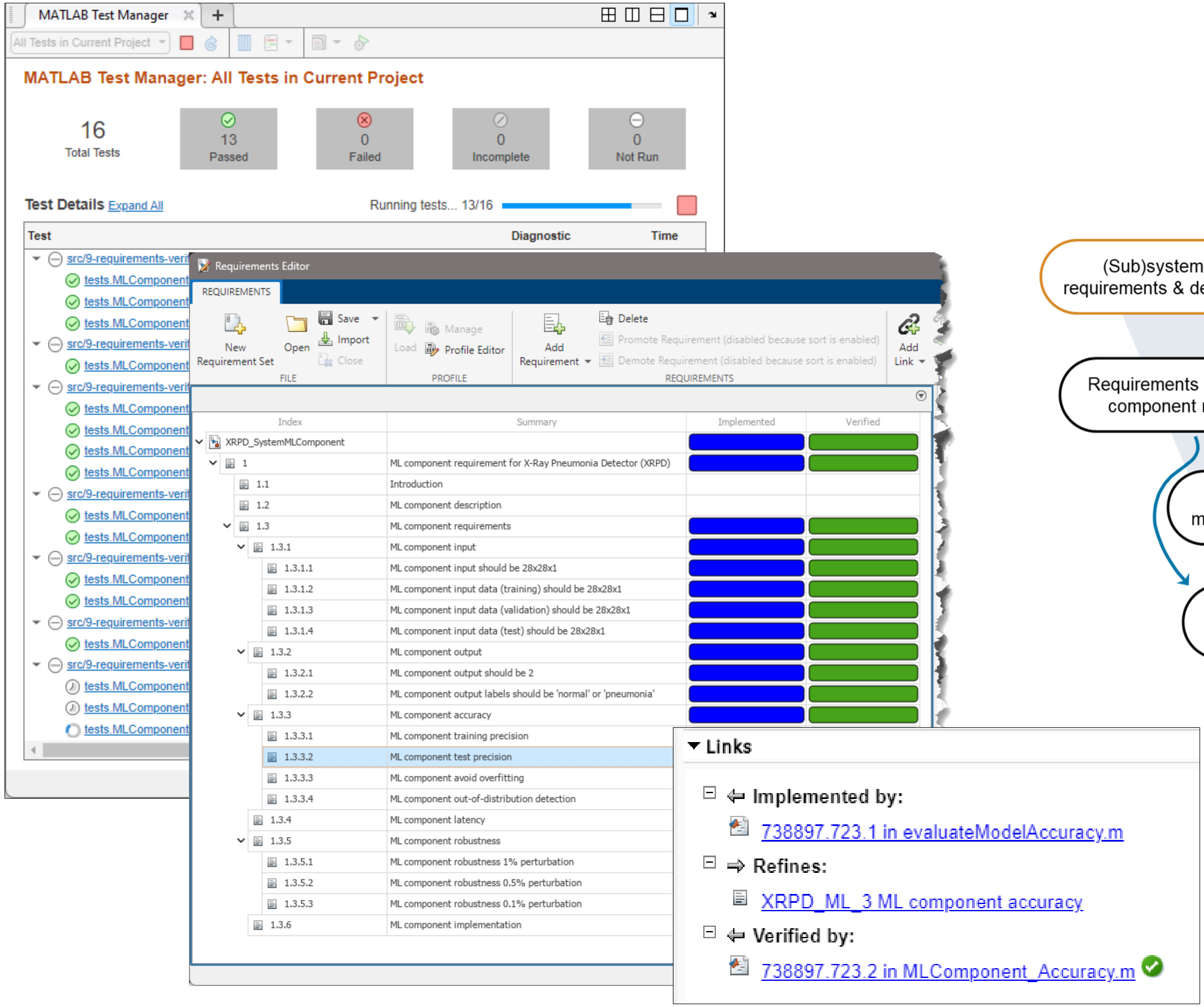
(Sub)system requirements verification



Machine Learning Engineering Process Group (MLE)

MLE.1 Machine Learning Requirements Analysis	**MLE.2** Machine Learning Architecture	**MLE.3** Machine Learning Training	**MLE.4** Machine Learning Model Testing

验证需求通过全面测试



MATLAB Test Manager: All Tests in Current Project

16 Total Tests | 13 Passed | 0 Failed | 0 Incomplete | 0 Not Run

Test Details Expand All — Running tests... 13/16

Test	Diagnostic	Time
src/9-requirements-verif		
✓ tests.MLComponent		
✓ tests.MLComponent		
✓ tests.MLComponent		
src/9-requirements-verif		
✓ tests.MLComponent		
src/9-requirements-verif		
✓ tests.MLComponent		
✓ tests.MLComponent		
✓ tests.MLComponent		
✓ tests.MLComponent		
src/9-requirements-verif		
✓ tests.MLComponent		
✓ tests.MLComponent		
src/9-requirements-verif		
✓ tests.MLComponent		
✓ tests.MLComponent		
src/9-requirements-verif		
✓ tests.MLComponent		
src/9-requirements-verif		
tests.MLComponent		
tests.MLComponent		
tests.MLComponent		

Index	Summary	Implemented	Verified
XRPD_SystemMLComponent		🟦	🟩
1	ML component requirement for X-Ray Pneumonia Detector (XRPD)	🟦	🟩
1.1	Introduction		
1.2	ML component description		
1.3	ML component requirements	🟦	🟩
1.3.1	ML component input	🟦	🟩
1.3.1.1	ML component input should be 28x28x1	🟦	🟩
1.3.1.2	ML component input data (training) should be 28x28x1	🟦	🟩
1.3.1.3	ML component input data (validation) should be 28x28x1	🟦	🟩
1.3.1.4	ML component input data (test) should be 28x28x1	🟦	🟩
1.3.2	ML component output	🟦	🟩
1.3.2.1	ML component output should be 2	🟦	🟩
1.3.2.2	ML component output labels should be 'normal' or 'pneumonia'	🟦	🟩
1.3.3	ML component accuracy	🟦	🟩
1.3.3.1	ML component training precision		
1.3.3.2	ML component test precision		
1.3.3.3	ML component avoid overfitting		
1.3.3.4	ML component out-of-distribution detection		
1.3.4	ML component latency		
1.3.5	ML component robustness		
1.3.5.1	ML component robustness 1% perturbation		
1.3.5.2	ML component robustness 0.5% perturbation		
1.3.5.3	ML component robustness 0.1% perturbation		
1.3.6	ML component implementation		

Links

⇐ **Implemented by:**

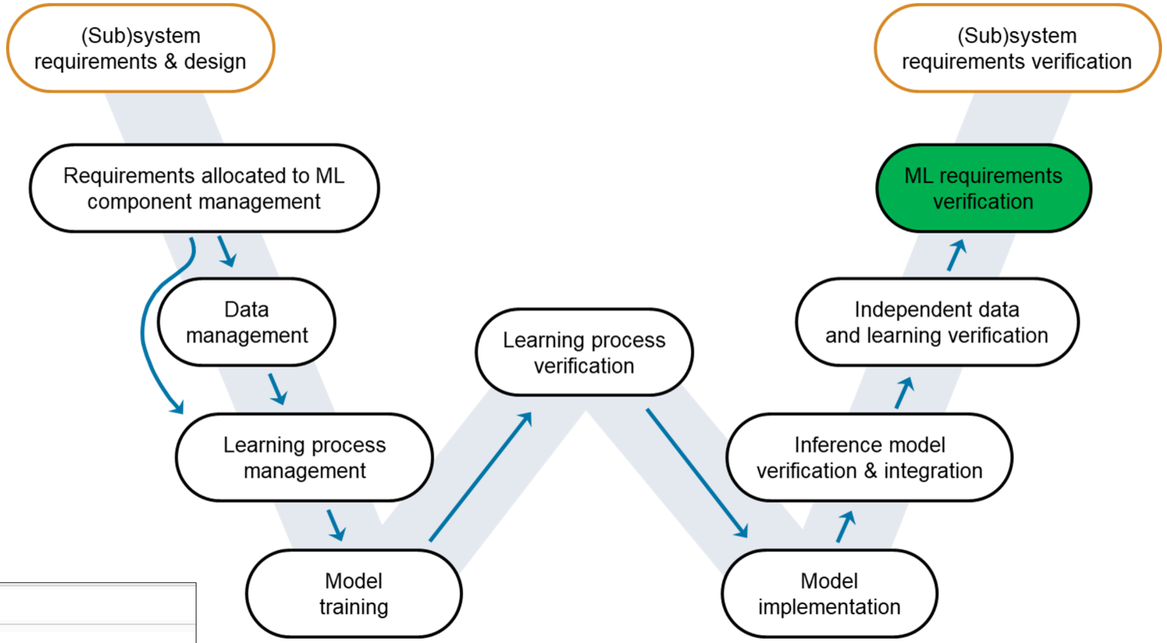
738897.723.1 in evaluateModelAccuracy.m

⇒ **Refines:**

XRPD_ML_3 ML component accuracy

⇐ **Verified by:**

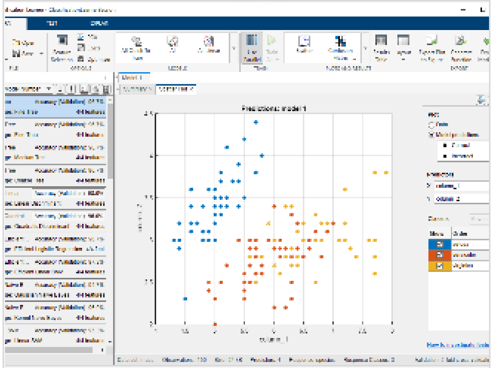
738897.723.2 in MLComponent_Accuracy.m ✓


(Sub)system requirements & design
Requirements allocated to ML component management
Data management
Learning process management
Model training
Learning process verification
Model implementation
Inference model verification & integration
Independent data and learning verification
ML requirements verification
(Sub)system requirements verification

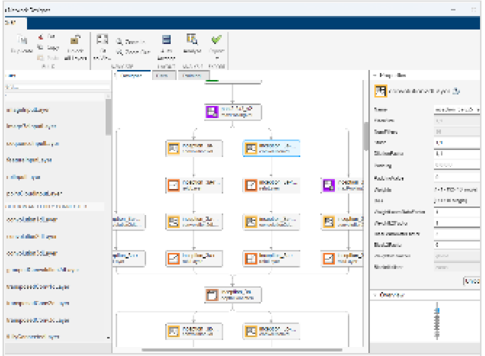
Machine Learning Engineering Process Group (MLE)			
MLE.1 Machine Learning Requirements Analysis	**MLE.2** Machine Learning Architecture	**MLE.3** Machine Learning Training	**MLE.4** Machine Learning Model Testing

关键要点

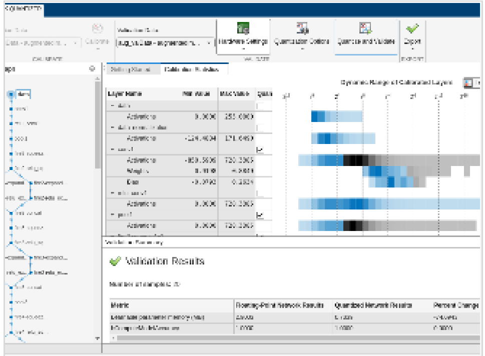
- ASPICE 4.0 中引入了机器学习
- MATLAB 机器学习/深度学习应用简化了 ML 设计、训练、部署和测试



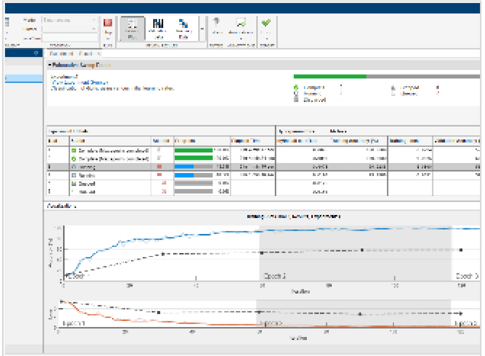
Classification Learner



Deep Network Designer



Deep Network Quantizer



Experiment Manager

2024 MathWorks 中国汽车年会

Thank you