



# Using Static Analysis Within the Application Lifecycle

APRIL 2020

Requirement: "The product should be ISO26262 ASIL B compliant"

Sub-requirement:

Table 8 - Design principles for software unit design and implementation

Methods		ASIL			
		A	B	C	D
1c	Initialization of variables	++	++	++	++

Requirement Violations

<input type="checkbox"/>	Number	Summary	Type	Klocwork State
<a href="#">Clear</a>	(All)	(All)	(All)	(All)
<input type="checkbox"/>	96	Uninitialized Variable	Static Analysis	New

Project Configuration

C and C++

- Use of Uninitialized Data
- UNINIT.STACK.MUST: Uninitialized Variable

Pre-Commit Analysis

Post-Commit Analysis



# Provides Visibility of Product 'Release Blockers'

The screenshot shows the HelixALM interface for the 'Sample Project 907Perforce'. The left sidebar contains navigation options: Dashboards, Issues (selected), Test Cases, Test Runs, Documents, Requirements, Folders, Reports, and Administration. The main content area is titled 'Issues' and shows a table of issues. The table has columns for Num..., Summary, Type, Priority, and Status. The 'Type' column is filtered to 'Static Analysis'. The 'Status' column shows 'Open, not assigned' for all items. A red circle highlights the 'Klocwork Issues' filter in the top right of the table area.

Num...	Summary	Type	Priority	Status
(All)	(All)	(All)	(All)	(All)
97	This function has been declared with a non-void 'return' typ...	Static Analysis		Open, not assigned
96	Uninitialized Variable	Static Analysis		Open, not assigned
95	Non-void function does not return value	Static Analysis		Open, not assigned
94	Uninitialized Heap Use	Static Analysis		Open, not assigned
93	Uninitialized Array	Static Analysis		Open, not assigned
92	Uninitialized Array	Static Analysis		Open, not assigned
91	Buffer Overflow - Array Index Out of Bounds	Static Analysis		Open, not assigned
90	Uninitialized Array	Static Analysis		Open, not assigned
89	Result of function that may return NULL will be dereferenced	Static Analysis		Open, not assigned
88	Null pointer may be dereferenced	Static Analysis		Open, not assigned
87	Pointer will be dereferenced after it was positively checked f...	Static Analysis		Open, not assigned
86	Null pointer will be dereferenced	Static Analysis		Open, not assigned
85	Result of function that may return NULL will be dereferenced	Static Analysis		Open, not assigned
84	Memory Leak - possible	Static Analysis		Open, not assigned
83	Memory Leak	Static Analysis		Open, not assigned
82	Freeing Unallocated Memory	Static Analysis		Open, not assigned
81	Freeing Freed Memory	Static Analysis		Open, not assigned

# Extended and Filterable Violation Data

The screenshot displays the HelixALM interface for viewing a specific issue. The left sidebar contains navigation options: Dashboards, Issues, Test Cases, Test Runs, Documents, Requirements, Folders, Reports, and Administration. The main content area is titled 'Issues > Viewing Issue 91' and shows the issue details for 'Buffer Overflow - Array Index Out of Bounds'. The issue is currently 'Open, not assigned' and is a 'Static Analysis' type. The product is 'Klocwork' and it was entered on 3/26/2020 by 'Baron, Michael DEMO186'. The description states: 'Array 'str' of size 20 may use index value(s) 20..24'. The file path is 'C:\Users\mbaron\Downloads\qac\workspace\cxxx\_testsuite\uninitialized\_array\_001.cpp', method is 'uninitialized\_array\_001\_N', line is 19, code is 'ABV.GENERAL', and severity is 'Critical'. A 'Klocwork Issue Link' is provided. The 'Custom Fields' section includes 'Days in Current State' (0.99), 'Risk Score' (0), 'Fix Churn' (Low), 'Klocwork Id' (20), 'Klocwork Status' (Analyze), and 'Klocwork State' (Existing). The 'Computer Config' is 'User's Test Config'. Annotations include a purple circle around the 'Type' field, a light blue circle around the 'Description' field, and another purple circle around the 'Klocwork Id', 'Klocwork Status', and 'Klocwork State' fields.

HelixALM Sample Project 907Perforce Add Item Recent Items Baron, Michael DEMO186

Issues > Viewing Issue 91 Watch 0

Buffer Overflow - Array Index Out of Bounds

Edit Assign Estimate Accept Force Close Release Notes Comment Actions

**General**

Status Open, not assigned

Type Static Analysis

Product Klocwork

Date Entered 3/26/2020

Entered By Baron, Michael DEMO186 (mbaron@perforce.com)

**Custom Fields**

Days in Current State 0.99

Risk Score 0

Fix Churn Low

Klocwork Id 20

Klocwork Status Analyze

Klocwork State Existing

Overview \* Detail \* Workflow \* Files Email Traceability Folders History \*

Report 1 of 1

Baron, Michael DEMO186 (mbaron@perforce.co... < >

Found by Baron, Michael DEMO186 (mbaron@perforce.com) Date Found 3/26/2020

Description

Array 'str' of size 20 may use index value(s) 20..24

File: C:\Users\mbaron\Downloads\qac\workspace\cxxx\_testsuite\uninitialized\_array\_001.cpp

Method: uninitialized\_array\_001\_N

Line: 19

Code: ABV.GENERAL

Severity: Critical

[Klocwork Issue Link](#)

Computer Config User's Test Config

# Issue Link Back

## Description

Array 'str' of size 20 may use index value(s) 20..24

File: C:\Users\mbaron\Downloads\qac\workspace\cxx\_testsuite\uninitialized\_a

Method: uninitialized\_array\_001\_N

Line: 19

Code: ABV.GENERAL

Severity: Critical

[Klocwork Issue Link](#)

The screenshot displays the Klocwork IDE interface. At the top, there are navigation tabs for 'Projects', 'Users', and 'Roles'. Below this, the project name 'cxx\_testsuite' is shown along with filters '\*default\*' and 'no constraints'. A blue navigation bar contains tabs for 'Issues', 'Reports', 'XRef', 'Views', 'Modules', 'Configuration', and 'Builds'. The main area is split into two panes. The left pane shows the details of a specific issue: 'Array 'str' of size 20 may use index value(s) 20..24'. The issue metadata includes ID 32, code ABV.GENERAL, name 'Buffer Overflow - Array Index Out of Bounds', location 'uninitialized\_array\_001.cpp: 19', build 'build\_9', severity 'Critical (1)', owner 'no owner\*', state 'Existing', and status 'Analyze'. A 'Klocwork Issue Link' is circled in blue on the left side of the image, with a blue arrow pointing from it to the 'no owner\*' field in the issue details. The right pane shows the source code for 'C:\Users\mbaron\Downloads\qac\workspace\cxx\_testsuite\uninitialized\_array\_001.cpp (build\_9)'. The code includes headers for <stdio.h> and <string.h>, and defines two functions: 'uninitialized\_array\_001\_P()' and 'uninitialized\_array\_001\_N()'. In the 'uninitialized\_array\_001\_N()' function, line 19 contains the code 'strcat(str, "world");', which is highlighted in red to indicate the location of the issue.

# Product SCA Overview

HelixALM Sample Project 907Perforce Add Item Recent Items Baron, Michael DEMO186 ?

Issues > Viewing Issue 72 Watch 0

### Klocwork Static Analysis Results

Edit Assign Estimate Accept Force Close Release Notes Comment Actions Bar Mail

Overview \* **Detail \*** Workflow Files Email Traceability Folders History \*

**Report 1 of 1**  
Baron, Michael DEMO186 (mbaron@perforce.co...)

**Found by** Baron, Michael DEMO186 (mbaron@perforce.com) **Date Found** 3/26/2020

**Description**

Severity	Violations	Deviations	Total
Critical	19	1	20
Error	3	2	5
Warning	0	0	0
Review	0	0	0
Severity 6	1	0	1
<b>Total</b>	<b>23</b>	<b>3</b>	<b>26</b>


Code	Violations	Deviations	Total
ABV.GENERAL	4	0	4
ABV.STACK	1	0	1
FNH.MUST	1	2	3

**General**

Status: Open, not assigned  
Type: Static Analysis  
Product: Klocwork  
Date Entered: 3/26/2020  
Entered By: Baron, Michael DEMO186 (mbaron@perforce.com)

**Custom Fields**

Days in Current State: 25.27  
Risk Score: 0  
Fix Churn: Low  
Klocwork Id: SUMMARY



# Full Summary Linking

Projects Users Roles About Help English mbaron

cxx\_testsuite \*default\* no constraints

Issues Reports XRef Views Modules Configuration Builds

Search for:  Search SmartRank Sort by: id

SEARCHES

- status:Analyze
- state:Existing
- category:"Suspicious Code Practices"
- code:NPE,NPD
- entity:main

Print Edit All 1 to 3 of 3

#7: Freeing of non-heap memory from 'localArray'. Memory referenced by 'localArray' is illegally freed by passing argument 1 to function 'delete[]' at line 9  
C:\Users\mbaron\Downloads\lqac\workspace\cxx\_testsuite\freeing\_non\_heap\_memory\_001.cpp:9 | freeing\_non\_heap\_memory\_001\_P()  
Code: FNH.MUST | Severity: Error(2) | State: Existing | Status: Fix | Taxonomy: C and C++ | Reference: none | Owner: unowned

#12: Memory leak. Dynamic memory stored in 'x' allocated through function 'malloc' at line 34 is lost at line 38  
C:\Users\mbaron\Downloads\lqac\workspace\cxx\_testsuite\freeing\_unallocated\_memory\_001.cpp:38 | a6()  
Code: MLK.MUST | Severity: Error(2) | State: Existing | Status: Fix | Taxonomy: C and C++ | Reference: none | Owner: unowned

#13: Possible memory leak. Dynamic memory stored in 'foo' allocated through function 'memory\_leak\_001\_assign' at line 15 can be lost at line 15  
C:\Users\mbaron\Downloads\lqac\workspace\cxx\_testsuite\memory\_leak\_001.cpp:15 | memory\_leak\_001()  
Code: MLK.MIGHT | Severity: Error(2) | State: Existing | Status: Analyze | Taxonomy: C and C++ | Reference: none | Owner: unowned

Severity	Violations
Critical	<a href="#">19</a>
Error	<a href="#">3</a>
Warning	<a href="#">0</a>
Review	<a href="#">0</a>
Severity 6	<a href="#">1</a>
Total	<a href="#">23</a>

# Summary of features

- Import issues from a Klocwork project into a HelixALM project, this can be filtered on a Klocwork view to restrict the issues imported
  - Added ALM issue fields include Klocwork ID, Klocwork State and Klocwork Status
  - Issue description including message, severity, checker code, location data and a hyperlink to the issue on the Klocwork server
- Updates existing ALM issue fields and description on script re-run
- Option to raise a single summary issue providing a breakdown of the Klocwork projects issues in addition to the individual issues being raise or instead of.
  - Includes a table of the checker codes, number of open issues, number of deviated issues and totals.



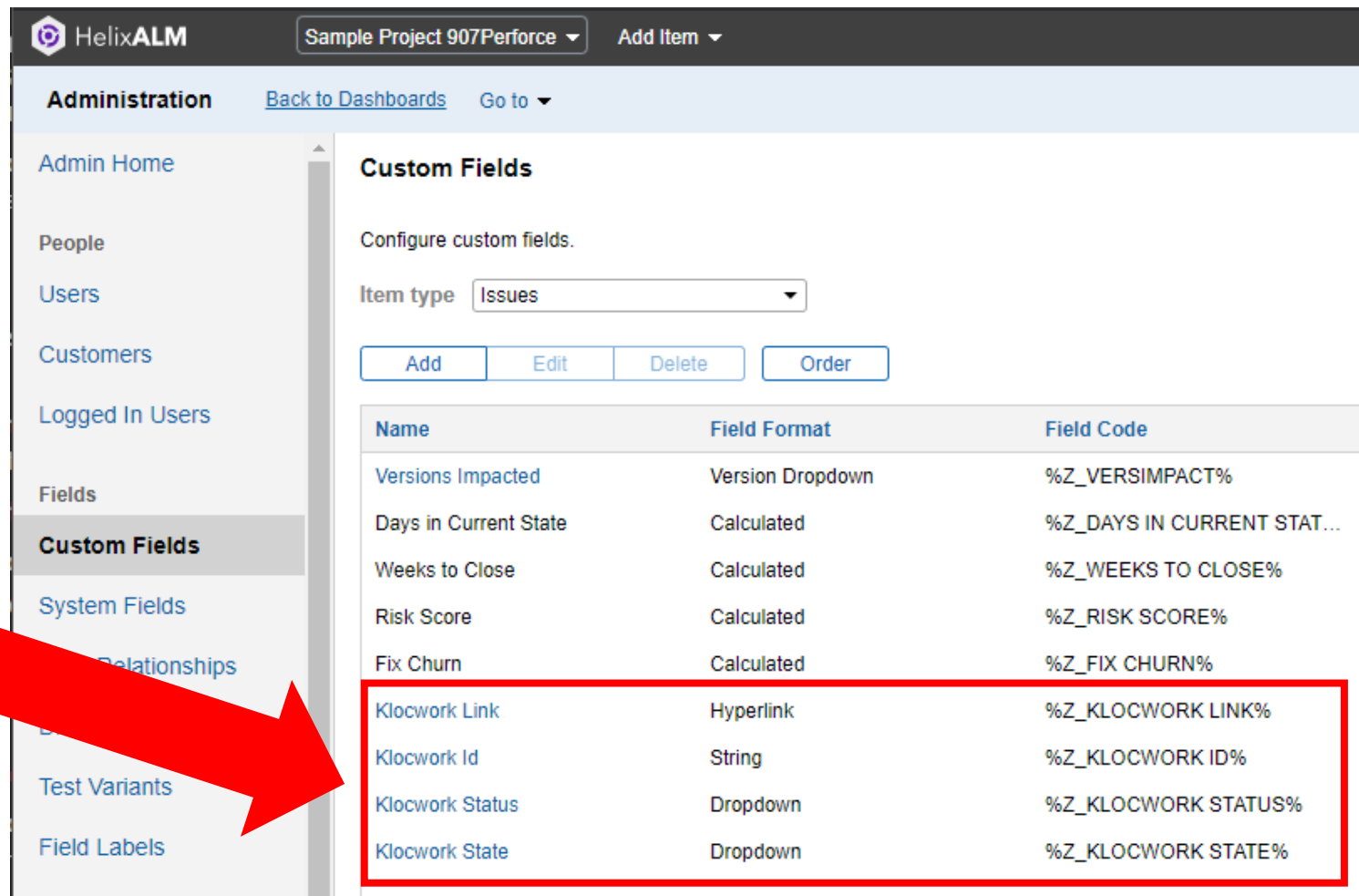


# Setup

CONFIGURATION

# Configuring Custom Fields

The plugin requires some additional custom fields adding to the issue type. These need to be named the same for the script to work.



The screenshot shows the HelixALM Administration interface. The top navigation bar includes the HelixALM logo, the current project 'Sample Project 907Perforce', and an 'Add Item' dropdown. The left sidebar contains navigation links: Admin Home, People, Users, Customers, Logged In Users, Fields, Custom Fields (highlighted), System Fields, Relationships, Test Variants, and Field Labels. The main content area is titled 'Custom Fields' and includes the instruction 'Configure custom fields.' Below this is an 'Item type' dropdown menu set to 'Issues'. There are four buttons: 'Add', 'Edit', 'Delete', and 'Order'. A table lists the configured custom fields:

Name	Field Format	Field Code
Versions Impacted	Version Dropdown	%Z_VERSIMPACT%
Days in Current State	Calculated	%Z_DAYS IN CURRENT STAT...
Weeks to Close	Calculated	%Z_WEEKS TO CLOSE%
Risk Score	Calculated	%Z_RISK SCORE%
Fix Churn	Calculated	%Z_FIX CHURN%
Klocwork Link	Hyperlink	%Z_KLOCWORK LINK%
Klocwork Id	String	%Z_KLOCWORK ID%
Klocwork Status	Dropdown	%Z_KLOCWORK STATUS%
Klocwork State	Dropdown	%Z_KLOCWORK STATE%

A large red arrow points from the text on the left to the 'Custom Fields' section in the sidebar and the table of fields.

# Custom Field - Klocwork Status Dropdown

The screenshot displays the HelixALM Administration interface. The top navigation bar includes the HelixALM logo, 'Sample Project 907Perforce', 'Add Item', 'Recent Items', and the user 'Baron, Michael DEMO186'. The left sidebar lists various administration options, with 'Dropdown Field Values' selected. The main content area is titled 'Dropdown Field Values' and contains an 'Item type' dropdown set to 'All Types' and an 'Edit' button. A search bar is also present. A modal window titled 'Configure List Values | Klocwork Status Field' is open, showing a list of values for the 'Klocwork Status' field. The list includes 'Analyze', 'Ignore', 'Not a Problem', 'Fix', 'Fix in Next Release', 'Fix in Later Release', 'Defer', and 'Filter'. The 'Analyze' through 'Fix in Later Release' items are highlighted with a red box. The modal also features an 'Add' button, an 'Order' button, a search bar, a help icon, and a 'Close' button.

HelixALM Sample Project 907Perforce Add Item Recent Items Baron, Michael DEMO186

Administration Back to Dashboards Go to

Admin Home  
People  
Users  
Customers  
Logged In Users  
Fields  
Custom Fields  
System Fields  
Field Relationships  
**Dropdown Field Values**  
Test Variants  
Field Labels  
Import and Export  
Microsoft Word Import  
Text Import  
XML Import  
XML Export  
Types

**Dropdown Field Values**

Configure the list of values a dropdown field uses.

Item type All Types

Edit Search for an item

**Configure List Values | Klocwork Status Field**

List name  
Klocwork Status

Add Order Search for a value

- Analyze
- Ignore
- Not a Problem
- Fix
- Fix in Next Release
- Fix in Later Release
- Defer
- Filter

Close

# Custom Field - Klocwork State Dropdown

The screenshot shows the HelixALM administration interface. The top navigation bar includes the HelixALM logo, the current project 'Sample Project 907Perforce', and an 'Add Item' button. The left sidebar contains a navigation menu with categories like 'Administration', 'People', 'Users', 'Customers', 'Logged In Users', 'Fields', 'Custom Fields', 'System Fields', 'Field Relationships', 'Dropdown Field Values', 'Test Variants', 'Field Labels', 'Import and Export', 'Microsoft Word Import', 'Text Import', 'XML Import', 'XML Export', and 'Types'. The 'Dropdown Field Values' section is active, showing a list of fields. The 'Klocwork State' field is selected and highlighted in blue. A modal window titled 'Configure List Values | Klocwork State Field' is open, displaying the configuration for this field. The modal shows the 'List name' as 'Klocwork State' and a search box for values. A red box highlights the list of values: 'New', 'Existing', and 'Fixed'. The modal also includes 'Add' and 'Order' buttons and a 'Close' button at the bottom right.

Administration [Back to Dashboards](#) Go to ▾

Admin Home

People

Users

Customers

Logged In Users

Fields

Custom Fields

System Fields

Field Relationships

**Dropdown Field Values**

Test Variants

Field Labels

Import and Export

Microsoft Word Import

Text Import

XML Import

XML Export

Types

**Dropdown Field Values**

Configure the list of values a dropdown field uses.

Item type

**Field**

- Issue Version Found
- Issue Component
- Issue Severity
- Issue Disposition
- Versions Impacted
- Klocwork Status
- Klocwork State**
- Estimate Version
- Fix Resolution
- Fix Version
- Verify Version
- Force Close Resolution
- Release Notes Release Version
- Test Type
- Product
- Component
- Assign Priority

**Configure List Values | Klocwork State Field**

**List name**  
Klocwork State

- New
- Existing
- Fixed

# Configure System Field Values Pt1

The screenshot displays the HelixALM Administration interface. The top navigation bar includes the HelixALM logo, the current project 'Sample Project 907Perforce', and user information 'Baron, Michael DEMO186'. The left sidebar shows the 'Administration' menu with 'System Fields' selected. The main content area is titled 'System Fields > Editing Product Field' and contains a 'Save' button and a 'Cancel' button. A red box highlights the field configuration details: 'Field name' is 'Product' with a 'Rename Field' link; 'Long label' is 'Issue Product'; 'Field code' is '%PROD%'; 'Field type' is 'Dropdown'; and 'Properties' shows 'Value list' as 'Issue Product' with a 'Configure List Values' link. To the right, the 'Configure List Values' section shows the 'List name' as 'Issue Product', 'Add' and 'Order' buttons, a search box, and a list of values including 'Wysi CRM', 'Activity Professional Suite (APS)', and 'Klocwork'. A red box highlights the 'Klocwork' value, and a large red arrow points from the text below to this value.

Configure the system field “Issue Product” to add “Klocwork” to the list of items.

# Configure System Field Values Pt2

The screenshot shows the HelixALM Administration interface. The left sidebar contains navigation options: Admin Home, People, Users, Customers, Logged In Users, Fields, Custom Fields, System Fields (highlighted), Field Relationships, Dropdown Field Values, Test Variants, Field Labels, Import and Export, and Microsoft Word Import. The main content area is titled 'System Fields > Editing Type Field' and includes 'Save' and 'Cancel' buttons. A red box highlights the 'Field name' section, which includes 'Type' (Rename Field), 'Long label' (Issue Type), 'Field code' (%TYPE%), 'Field type' (Dropdown), and 'Properties' (Value list: Issue Type, Configure List Values). A large red arrow points from the 'Configure List Values' link to the 'Configure List Values' dialog box. The dialog box has a title bar 'Configure List Values' and a 'List name' of 'Issue Type'. It features 'Add' and 'Order' buttons and a search input field. A list of values is displayed, including 'Crash - Data Loss', 'Crash - No Data Loss', 'Incorrect Functionality', 'Cosmetic', 'Feature Request', 'Question', and 'Static Analysis'. The 'Static Analysis' item is highlighted with a red box. A 'Close' button is at the bottom right.

Configure the system field “Issue Type” to add “Static Analysis” to the list of items.

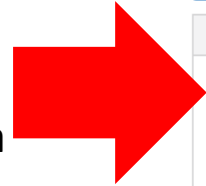
# Configure System Field Values Pt2

The screenshot displays the HelixALM Administration interface. The left sidebar shows the navigation menu with 'System Fields' selected. The main content area is titled 'System Fields > Editing Type Field' and contains a 'Configure List Values' dialog box. The dialog box has a 'List name' of 'Issue Type' and a search bar. A list of values is shown, including 'Crash - Data Loss', 'Crash - No Data Loss', 'Incorrect Functionality', 'Cosmetic', 'Feature Request', 'Question', and 'Static Analysis'. The 'Static Analysis' value is highlighted with a red box. A red arrow points from the 'Static Analysis' value to the 'Value list' section of the 'Editing Type Field' panel, which shows 'Issue Type' is configured to use 'Configure List Values'.

Configure the system field “Issue Type” to add “Static Analysis” to the list of items.

# Custom Issue List Filter

The script uses a pre-defined custom issue list filter to obtain only the Klocwork issues currently raised in the ALM project. Create a filter with the same name and options as this



### Edit Issue Filter

**Name**

Description

Share with  Owner: Baron, Michael DEMO186 (mbaron@perforce.com)

[Delete All](#)

NOT (	Criteria	)	AND/OR
	Klocwork Id is not blank		

No filter restriction criteria selected

[Klocwork Id]





# Setup

USAGE

# General Requirements

- The script is written in Python and tested using Python 3.6
- The script connects to the Klocwork API, which has been included since v9.5
  - The script will use a Klocwork authentication token to connect to the database, please make sure one has been created by using the kwauth tool
- The script connects to the HelixALM API and takes a token and secret key as arguments. These must be created first through the web interface to work
  - <https://help.perforce.com/alm/helixalm/2020.1.0/web/Content/User/AddingAPIKeys.htm>
- The script can be run manually however its best use is in an automated fashion at the end of a CI system build, after the Klocwork integration analysis has been performed

# Basic Usage

```
python ALMxKW.py --kw-url http(s)://<host>:<port>/<project> --alm-url https://<host>:<port> --alm-project <project> --alm-key <key> --alm-secret <secret-key>
```

Breakdown:

`--kw-url http(s)://<host>:<port>/<project>` : The Klocwork server url and project name to get issues from

`--alm-url https://<host>:<port>` : The HelixALM server to connect to

`--alm-project <project>` : The HelixALM project name to import issues into

`--alm-key <key>` : The HelixALM user API key created

`--alm-secret <secret-key>` : The matching secret key to the API key used

# Extra Options

`--kw-view <Klocwork View Name>` : Specify the name of the Klocwork view to filter results on

`--kw-grouping` : Turn issue grouping: on

`--summary` : Submit one issue with a summary



Working together to provide a scalable  
DevOps solution

