Recategorization Plan Guidelines for MISRA Compliance using Polyspace

Contents

Table of figures

Introduction

The goal of this document is to provide a process of a complete Polyspace Bug Finder R2022a workflow that supports the MISRA compliance 2020 document edited by the MISRA Consortium "Achieving compliance with MISRA Coding Guidelines"[1].

Inside this document, you will find an example Guidelines Recategorization Plan (GRP) that defines the outset of a development project between an Acquirer and a Supplier. GRP determines how the Coding Guidelines are to be applied, including:

1. The set of rules to be checked.
2. The category associated with each rule if that is not the recommended category of the Standard.

[1] MISRA Compliance:2020: Achieving compliance with MISRA Coding Guidelines - February 2020 – www.misra.org.uk

3. The action behind each category. For instance, below are examples of actions to take associated with each category of guidelines provided from the MISRA C:2012 Standard:
    - *Mandatory Guidelines – Guidelines for which violation is never permitted.*
    - *Required Guidelines – Guidelines which can only be violated when supported by a deviation defining a set of clear restrictions, requirements, and precautions.*
    - *Advisory Guidelines – Recommendations to be followed as far as is reasonably practical. Violations are identified but are not required to be supported by a deviation.*

This document describes how to support a workflow in Polyspace requesting a MISRA compliance and necessitating a recategorization plan, as well as where to add the revised categories.

Note: This process can be extended to SEI CERT C Coding Standard or any other guidelines Standard as soon as you want to apply the same recategorization process.

Process within Polyspace

This section describes the steps necessary to follow a recategorization process. Later in the document, you can find an in-depth explanation for each step.

These steps require the use of Polyspace Bug finder (desktop or server) to launch an analysis on the set of rules selected. Additionally, a Polyspace Access repository is required where runs will be stored and from where the MISRA compliance is checked.

Below, a broad overview of each step:

1. Create an XML file (later referred to as `GRP.xml`) compatible with the Polyspace Bug Finder launching option that checks only the guidelines (MISRA C:2012 directives, rules, and CERT-C) necessary for the project (see documentation on option -checkers-selection-file). The file includes comments about categories and the matching requirements of recategorization described in the GRP document.
   Note: A `GRP.xml` example has been shipped with this document (see in report section *The shipped `GRP.xml` file*).

2. In Polyspace Access, create a new Software Quality Objective setting (see documentation) to align the developed code with the MISRA/CERT-C compliance requested recategorization (later referred to as `SQO-GRP`):
    a. SQO Level 1 contains all MISRA/CERT-C **revised** rules with a category '`Mandatory`'.
    b. SQO Level 2 contains all MISRA/CERT-C **revised** rules with a category '`Required`'.
    c. SQO level 3 contains all MISRA/CERT-C **revised** rules with a category '`Advisory`'.

   Associating a SQO level by category allows user to check the overall quality and effort to reach 100% MISRA compliance of the project along its development. 100% Compliance to a SQO level means 100% compliance to a lower SQO level.
   Note: All rules that have been disabled will not appear in the SQO settings.

3. Launch Polyspace Bug Finder analysis with `GRP.xml` file and upload the results to a project in Polyspace Access.

4. Set your Polyspace Access project's SQO settings to the SQO settings `SQO-GRP` you created at step 2 (see documentation).

5. Review results of the uploaded run in Polyspace Access. Follow the requirements for each category and fix or justify the violation. A violation will be considered as fixed when one of the following is true:
    a. The violation is not raised by Polyspace Bug Finder.
    b. The violation is raised and has been justified with an annotation in the source code (see documentation).
    c. The violation is raised and has been justified with a Status '`Justified`', '`No action planned`' or '`Not a defect`' in Polyspace Access.

6. Generate a report on the project which contains a `PASS`/`FAIL` value according to the Software Quality Objective level selected in Polyspace Access.

Adding a revised category mode in Polyspace

The main purpose of achieving MISRA compliance in Polyspace is to select the rules that will be checked in a Polyspace analysis and to associate the revised category associated with each rule.

Create a `GRP.xml` file

The first step (see item 1 in section Process within Polyspace) is to create the `GRP.xml` file that will be used as the custom set of guidelines.

To do so, you can use the Polyspace UI 'Checker Selection' in the 'Coding Standards & Coding Metrics' section within the Configuration Window in Polyspace UI or create XML file directly (**Erreur ! Source du renvoi introuvable.** 1).

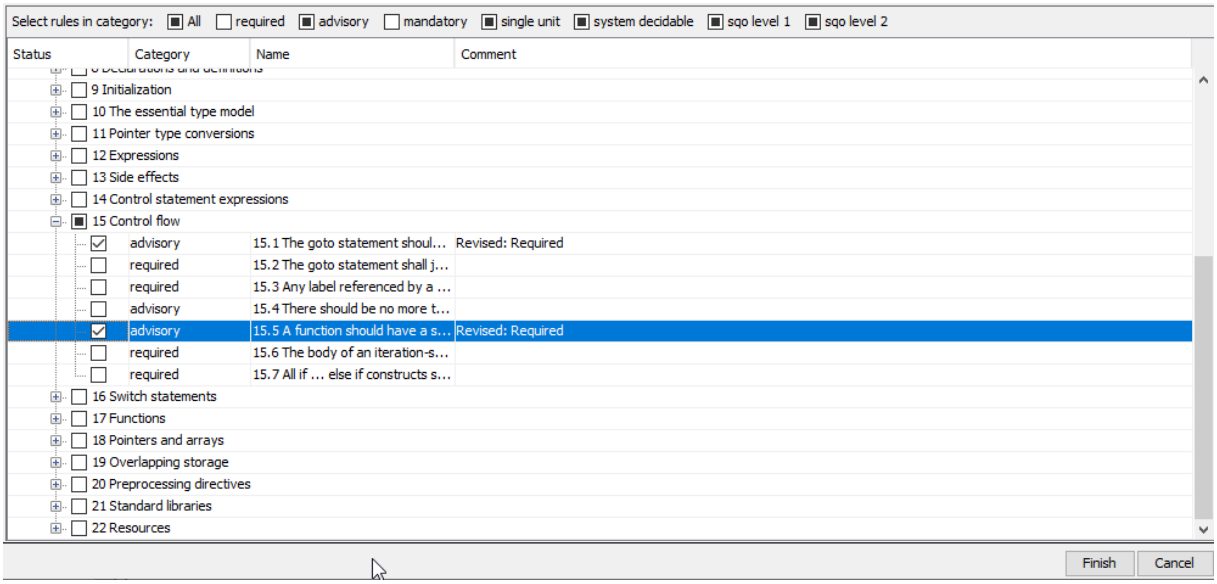

Figure 1 - Set revised mode in Polyspace UI.

The `GRP.xml` file will contain the list of all MISRA C:2012 and CERT-C guidelines enabled `state="on"` with a comment containing the revised mode:

- MISRA (Example with D4.6 revised as 'Required')

```
<section>
…
<check id="D4.6" state="on">
```

```
    <comment>Revised: Required</comment>
  </check>
…
</section>
```

- CERT-C (Example with INT35 revised as ‘Mandatory’)

```
  <section>
  …
  <check id="INT35-C" state="on">
    <comment>Revised: Mandatory</comment>
  </check>
…
</section>
```

All guidelines considered will have a state of “**on**” and a revised comment, or not listed and be considered as “**off**”.

Launching

Below an example with the minimum options required to launch an analysis that follows the recategorization plan set with `GRP.xml` file containing a set of MISRA/CERT-C revised rules:

```
polyspace-bug-finder-server -checkers-selection-file <pathto>/GRP.xml
-misra3 from-file -cert-c from-file …
```

SQO settings in Polyspace Access

Step 2 is to create a SQO list of rules to get the PASS/FAIL status to check if at least all required/mandatory and advisory rules are compliant with the GRP.

To do so, you must manually create a SQO GRP setting in Polyspace Access (Figure 2).

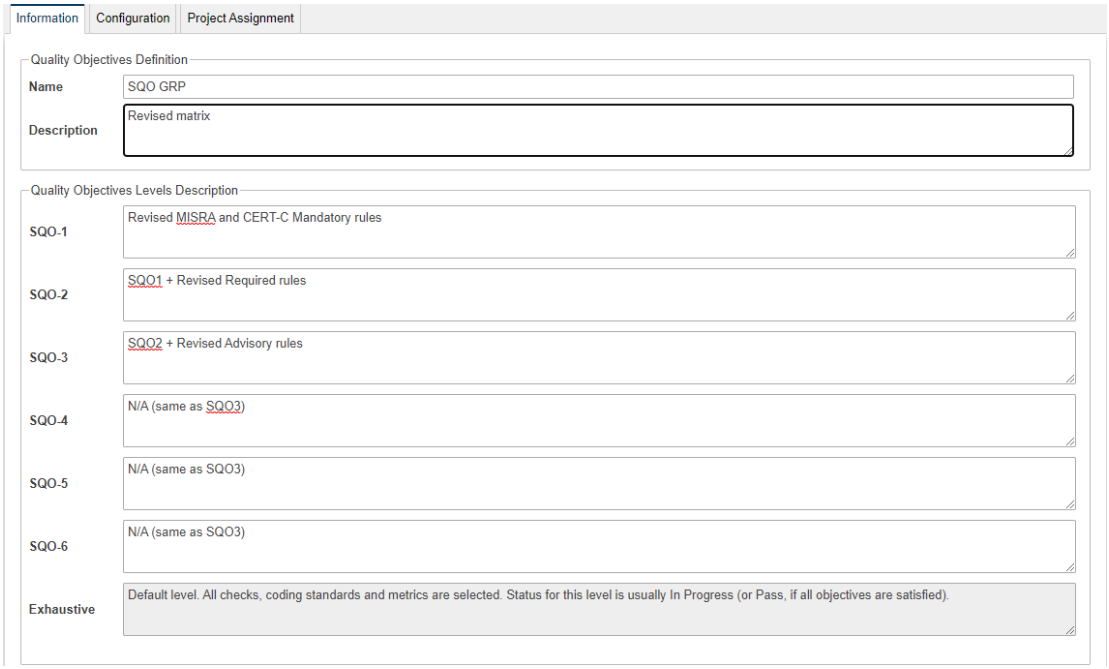

Figure 2 - Example of Quality Objectives Setting in Polyspace Access

Each SQO level will contain the list of guidelines associated with one revised category.

- If a guideline is revised as Mandatory, it will be set in SQO-1 bucket (Figure 33).

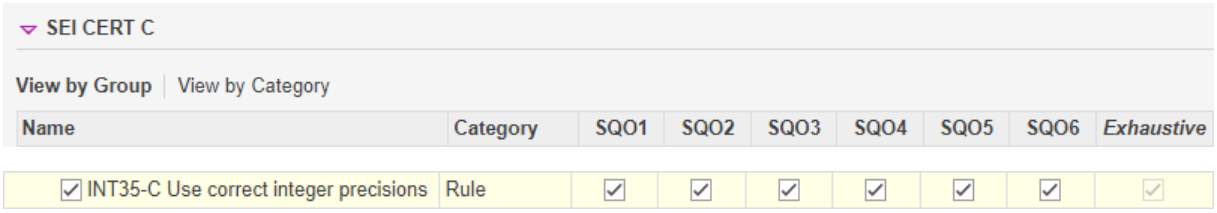

Figure 3 - Example with CERT-C INT35-C rule revised as Mandatory in SQO-1 bucket

- If a guideline is revised as Required, it will be set in SQO-2 bucket (Figure 44).

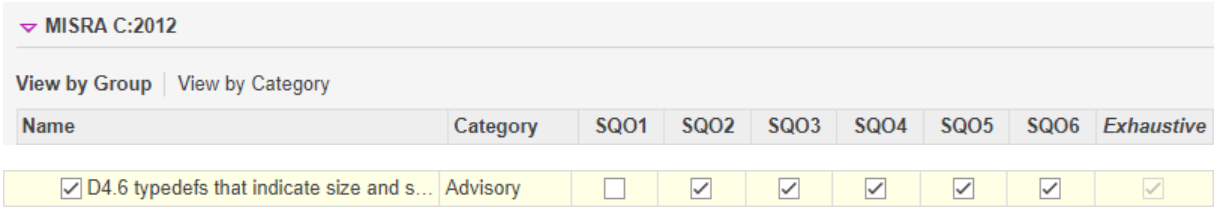

Figure 4 - Example with MISRA C:2012 D4.6 directive revised as Required in SQO-2 bucket

- If a guideline is revised as Advisory, it will be set in SQO-3 bucket (Figure 55).

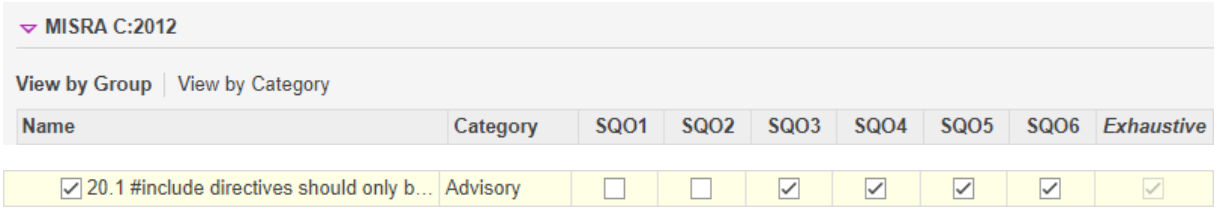

Figure 5 - Example with MISRA C:2012 20.1 rule revised as Advisory in SQO-3 bucket

Display of revised categories

Comments about revised categories are only visible in a report generated (see in report section Generate a report) within a section called '*Coding Standard configuration*'.

In Polyspace Access, the revised categories can be visible from the menu `Review>Window>Configuration Settings>Checkers configuration`.

Checking MISRA compliance through a generated report

You can generate a report to receive `PASS`/`FAIL` information which helps you understand if the analysis is MISRA compliant based on the recategorization matrix.

Generate a report

From the Polyspace desktop UI, you can open results from the repository and generate a report by selecting template `'SoftwareQualityObjective.rpt'`. The template `SoftwareQualityObjective.rpt` (see documentation) is shipped with Polyspace and available in folder `polyspaceroot/toolbox/polyspace/psrptgen/templates/metrics`

This process can be done using the command line once you have obtained the `ID` of the results in the repository (see documentation).

Contents

The report contains information which allows you to check MISRA compliance. For instance:

a. The SQO setting list selected for the compliance and the SQO level chosen to generate the report is at the top of the generated report.
b. A `PASS` value is assigned that depends on the SQO level selected and if all violations have been fixed (see in report section Fixed violations).
   If at least one violation has not been fixed or justified, a result of `FAIL` will show.
c. At the end of the report, a paragraph contains the list of all rules that have been enabled and the revised category associated with each rule when the comment has been enabled in `GRP.xml`.

Fixed violations

It is not possible to force a violation to be fixed in the source code. A violation that has a `PASS` status in the report has been justified via an annotation in the source code or within Polyspace Access with an adequate status (see available status in report section *Process within Polyspace – item 4.c*).

The shipped `GRP.xml` file

An example of a `GRP.xml` file has been shipped that can be used with this document. It contains a set of MISRA directives, MISRA rules, and a small set of CERT-C rules where we have applied a recategorization. This GRP file is given only as an example and should be updated with the set of rules that you want to apply for your own recategorization plan.