

# Update on software quality tools

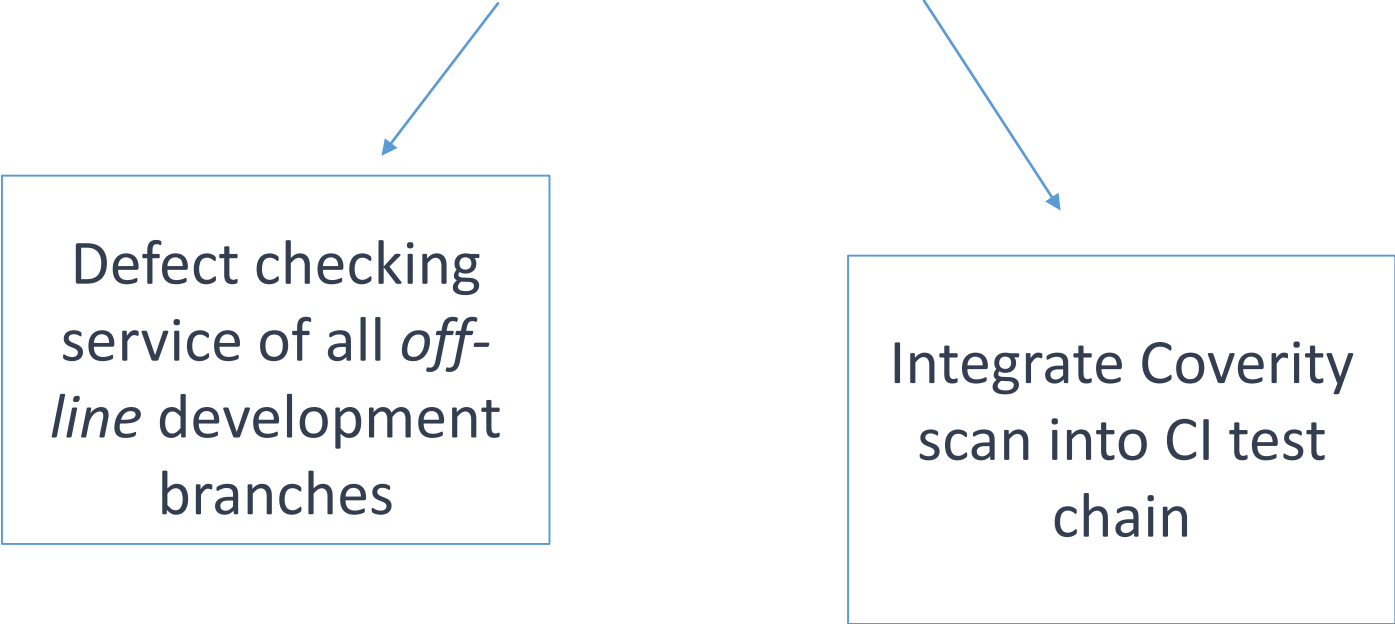
SHARMAZANASHVILI Alexander  
Georgian Technical University

PIRTSKHALAVA Mariam  
Georgian Technical University



## WP3: “Improve ATLAS software quality”

- The purpose of this working package is to promote software quality evaluation as an integral part of the ATLAS software development process. This will require the development of tools and practices in two key areas:



Defect checking  
service of all *off-line* development  
branches

Integrate Coverity  
scan into CI test  
chain

# Defect Checking Service

- Weekly activities of Georgian Team:
  1. Analyze status of Scan on voatlas405
  2. Preparation of Jira Ticket for scan
  3. Getting defects from voatlas405
  4. Finding authors on Git
  5. Grouping defects
  6. Preparation of Jira Tickets for defects
- Since June 2018 Georgian team provide Jira Tickets every week
- We have problem with Jira Tickets while it belongs just to SQ group and authors cannot respond to our tickets. We need conceptual solution here.

- Example of Jira Ticket for Unsuccessful Scan

## Coverity Scan Report 21/06/2018

Name	Status	Size	Items
Main folder	Not Complete	7.0Gb	163'932
Coverity Build	Not Done		
Coverity Analyze	Not Done		

Build History:					
Name	Instalation	Faults	File		
Status	Strings	Status	Strings		
Athena Build			Configuring incomplete, errors occurred!	#35	/main/build_athena.out
External Build			CMake Error at Coin3D-stamp/download-Coin3D.cmake:159 (message): make[2]: *** [src/Coin3D-stamp/Coin3D-download] Error 1 make[2]: Target `External/Coin3D/CMakeFiles/Coin3D.dir/build' not remade because of errors. make[1]: *** [External/Coin3D/CMakeFiles/Coin3D.dir/all] Error 2	#7'607	/main/build_externals.out
		[ 94%] Built target Package_Gdb make[1]: Target `all' not remade because of errors. make: *** [all] Error 2 make: Target `default_target' not remade because of errors.	#247'771	/main/build_externals.out	

Analyze history:	
Status	Not Done
Files Analyzed	0
Defects Found	0
Analyze Time	-

# Defect Checking Service

- Example of Jira Ticket for Successful Scan

Coverity Scan Report	24/09/2018			
	Overall:			
	Name	Status	Size	Items
	Main folder	Complete	210,5 GB	417'81
	Coverity Build	Done		
	Coverity Analyze	Done		

Build History:					
Name	Instalation	Faults	File		
Status	Strings	Status	Strings		
Athena Build			Completed Successfully		/main/build_athena.out
External Build			Completed Successfully		/main/build externals.out

Analyze history:	
Status	Done
Files Analyzed	35788
Defects Found	60084
Analyze Time	13h00

# Defect Checking Service

## ■ Example of Jira Ticket for Defects

<https://atlas-coverity.cern.ch/reports.htm#v22539/p10017/fileInstanceId=21160233&defectInstanceId=11675880&mergedDefectId=118843>

Open issues Switch filter

Order by Actual Start

ATLASSQ-5  
Coverity Scan Report 11/07/2018

ATLASSQ-2  
Coverity full scan report 11/06/2018

ATLASSQ-4  
Coverity Scan Report 29/06/2018

ATLASSQ-3  
Coverity Scan Report 21/06/2018

ATLASSQ-9  
Coverity Defects Report 29/07/2018

ATLASSQ-11  
Coverity Defects Report Calorimeter ...

ATLASSQ-93  
Coverity Defects Report Simulation P...

ATLASSQ-92  
Coverity Scan Report 26/11/2018

ATLASSQ-91  
Coverity Scan Report 15/11/2018

ATLASSQ-84  
Coverity Scan Report 28.10.2018

ATLASSQ-29  
Coverity Defects Report 26/09/2018

ATLASSQ-28  
Coverity Scan Report 24/09/2018

ATLASSQ-27  
Coverity Defect #118887

ATLASSQ-26  
Coverity Defect #118888

ATLAS Software Quality / ATLASSQ-9  
Coverity Defects Report 29/07/2018

Details

Type: Bug  
Priority: Major  
Labels: None

Status: TO DO  
Resolution: Unresolved

Description

Coverity Defects Report #003/29-07-2018

#	CID	Defect Type	Date	Defect File	Author	e-mail
1	118843	Wrapper object use after free	29/07/2018	/Simulation/ISF/ISF_Fatras/ISF_FatrasTools/src/PhotonConversionTool.cxx	Vincent R. Pascuzzi	vpascuzzi@cern.ch
2	118842	Wrapper object use after free	29/07/2018	/Simulation/ISF/ISF_Fatras/ISF_FatrasTools/src/PhotonConversionTool.cxx	Vincent R. Pascuzzi	vpascuzzi@cern.ch
3	118841	Uninitialized scalar field	29/07/2018	/PhysicsAnalysis/RingerSelectorTools/Root/AsgElectronRingerSelector.cxx	Werner Spolidoro Freund	werner.spolidoro.freund@cern.ch
4	118840	Uninitialized pointer field	29/07/2018	/Reconstruction/RecoTools/CaloRingerTools/src/CaloRingerReaderUtils.h	Werner Spolidoro Freund	werner.spolidoro.freund@cern.ch
5	118839	Not restoring ostream format	29/07/2018	/PhysicsAnalysis/RingerSelectorTools/Root/AsgElectronRingerSelector.cxx	Werner Spolidoro Freund	werner.spolidoro.freund@cern.ch
		Unsafe		/PhysicsAnalysis/RingerSelectorTools	Werner	

Issues: By Snapshot | Outstanding Defects

Filters: Issue Kind, Classification

ID	Type	Impact	Status	First Detected	Owner	Classification	Severity	Action	Component	Category	File
121403	Parse recovery warning	Low	New	04/12/2018	Unassigned	Unspecified	Unspecified	Undecoded	Other	Parse warnings	/Trigger
121402	Parse recovery warning	Low	New	04/12/2018	Unassigned	Unspecified	Unspecified	Undecoded	Other	Parse warnings	/Control
121401	Parse recovery warning	Low	New	04/12/2018	Unassigned	Unspecified	Unspecified	Undecoded	Other	Parse warnings	/Control
121400	Explicit null dereference	Medium	New	04/12/2018	Unassigned	Unspecified	Unspecified	Undecoded	Other	Null pointer dereference	/Control
121399	Explicit null dereference	Medium	New	04/12/2018	Unassigned	Unspecified	Unspecified	Undecoded	Other	Null pointer dereference	/Control
121398	Unchecked dynamic cast	Medium	New	04/12/2018	Unassigned	Unspecified	Unspecified	Undecoded	Other	Null pointer dereference	/Database
121395	Not restoring ostream	Medium	New	27/11/2018	Unassigned	Unspecified	Unspecified	Undecoded	Other	API usage errors	/HLT/Event
121394	Parse recovery warning	Low	New	27/11/2018	Unassigned	Unspecified	Unspecified	Undecoded	Other	Parse warnings	/HLT/Event
121393	Parse recovery warning	Low	New	27/11/2018	Unassigned	Unspecified	Unspecified	Undecoded	Other	Parse warnings	/Calorim

42 issues match

PhotonConversionTool.cxx

Historical version of the file displaying the issue before it was in the Fixed state. To see the latest version, click here.

```
1 p1*childDirection,
2 mass,
3 charge1,
4 pdg1,
5 time,
6 *parent));
7
8 std::vector<ISF::ISFParticle> ch2(new ISF::ISFParticle(vertex,
9 p2*childDirection,
10 mass,
11 charge2,
12 pdg2,
13 time,
14 *parent));
15
16 // Since ISF::ISFParticleVector is just a std::vector, do not "release" since
17 // then we need to manage the memory (could have just used raw pointers).
18 CID 118842: Wrapper object use after free (WRAPPER_ESCAPE) [selected issue]
19 children[0] = ch1.get();
20 CID 118843 (R1 of 1): Wrapper object use after free (WRAPPER_ESCAPE)
21 3 escape: The internal representation of local ch2 escapes into children[0], but is destroyed when it exits scope
22 children[1] = ch2.get();
23
24 // register TruthIncident
25 ISF::ISFTruthIncident truth( const_cast<ISF::ISFParticle>(&parent),
26 children,
27 m_processCode,
28 parent->nextGeoID(),
29 ISF::kIsPrimary);
30 m_truthRecordSvc->registerTruthIncident( truth);
31
32 //Make sure the conversion products get a chance to have correct truth info before pushing into the particle broker
33 if (ichildren[0]->getTruthBinding()) {
34 children[0]->setTruthBinding(new ISF::TruthBinding(&parent->getTruthBinding()));
35 }
36 if (ichildren[1]->getTruthBinding()) {
37 children[1]->setTruthBinding(new ISF::TruthBinding(&parent->getTruthBinding()));
38 }
```

118843 Wrapper object use after free

A use after free bug would occur if the internal pointer is used.

In /Fatras/PhotonConversionTool.getCh2(ISF::ISFParticle const\*, double, Eigen::Matrix<double, 3, 1, 0, 3, 1> const&, Eigen::Matrix<double, 3, 1, 0, 3, 1> const&, double, Eigen::Matrix<double, 3, 1, 0, 3, 1> const&, Trx::ParticleHypothesis&). An internal pointer of a wrapper object remains available after the object is freed (CVE-416).

▼ Triage

Classification: Unspecified

Severity: Unspecified

Action: Undecoded

Ext Reference: <https://its.cern.ch/jira/browse/ATLASSQ-3808>

Owner: Unassigned

Enter comments (See the Triage History section below for previous comments)

Apply Next Apply

▼ Projects & Streams

▼ Defect History

▼ Triage History

▼ Occurrences

1: Athena

Events contributing to issue:

3 escape PhotonConversionTool.cxx:367

<https://its.cern.ch/jira/projects/ATLASSQ/issues/ATLASSQ-9?filter=allopenissues&orderby=cf%5B13000%5D+ASC%2C+priority+DESC%2C+updated+DESC>

# Defect Checking Service

- We have positive feedback from authors

Hi Mariam,

Thanks for the report - we already have a ticket open on the new PixelFastDigitizationTool defects here:

<https://its.cern.ch/jira/browse/ATLASSIM-3826>

Automating the creation of JIRA tickets for new defects is a great improvement though! Thanks for doing this.

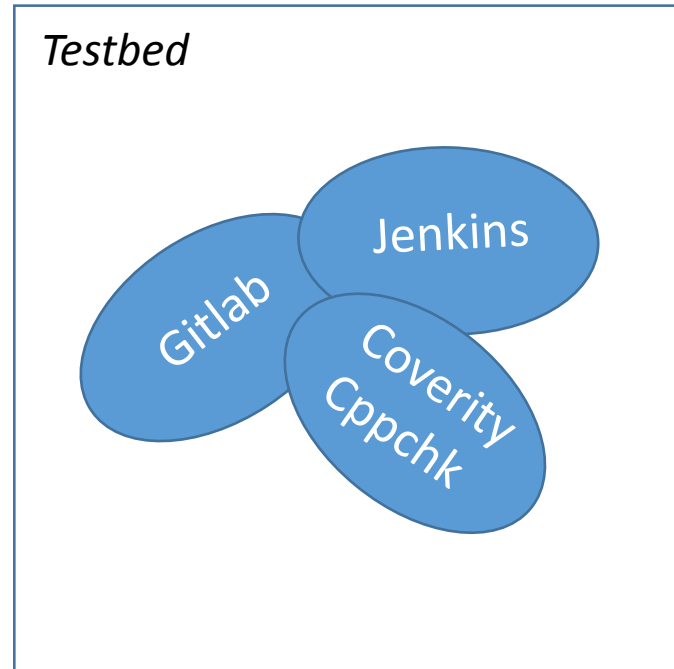
Cheers,

John

- Also from Shaun, Jochen, Andy

## Integrate Coverity Scan into CI test chain

- In 2017 we did hard attempts to create so call Testbed server at Georgian Technical University



- However we met with technical problems with network administration. We cannot serve merge requests in Jenkins. Work was postponed.



- Now we start playing with CPPCHECK

## General Objectives:

- Run CPPCHECK for regular scanning
- Get CPPCHECK defects
- Finding authors on Gitlab
- Grouping defects
- Preparation of Jira Ticket for defects

# CPPCheck Scan

- Recently usage of Coverity in ATLAS is temporarily stopped. So we move to CPPCHECK application and start investigation of Scan and defects
- First we try run application locally
- We try different settings and this one make results:

```
cppcheck --template="{file}:{line}:{severity}:{id}:{message}" <folder name> --xml 2> <file name>
```

- It took 1h25 for scanning full Athena repository and 35min for scanning just SIMULATION folder
- We have got 519 defects for Simulation folder

- Defects list for Simulation folder

[illegible]

## Future Steps:

- Selection of scanning method
- Run application from Server (we need authorizations)
- Get defects and parsing
- Finding authors on Gitlab
- Grouping defects
- Preparation of Jira Ticket for defects



Thanks for attention