Static Analysis Tool Comparison with Respect to C++

Jacob Cox

NASA IV&V

September 2013

Introduction

- This presentation is of the analysis of one MPCV build with both Klocwork and Flexelint.
- The objective was to determine the value of using Flexelint in addition to Klocwork
- This is not a general comparison.
- This is not a theoretical comparison.
- All ITAR data has been scrubbed.

Comparison

- FSW with
  - 1215 Files
  - 831061 lines of C++ and C source (as reported by Klocwork)
- Tools
  - Klocwork Review Release 9.5.3 by Klocwork Inc.
  - Flexelint Version 9.00h by Gimpel Software

Comparing Apples to Apples

- flexelintFiles.txt : files Flexelint analyzed
- klocworkFiles.txt : files Klocwork analyzed

- diff flexelintFiles.txt klocworkFiles.txt
- 1194a1195
- > directory path/fileName.CPP

- The perl script recursively running Flexelint does not recognize ‘*.CPP’ as a source file (the perl script needs modified to be case insensitive)

Files with Warnings

- pluto:FswVersion24> diff flexelintResultsFiles.txt klocworkResultsFiles.txt | grep '^<' | wc
-     516   1032   46992
- **516 files in Flexelint results not in Klocwork results**

- pluto:FswVersion24> diff flexelintResultsFiles.txt klocworkResultsFiles.txt | grep '^>' | wc
-      79   160   5917
- **79 files in Klocwork results not in Flexelint results**

Additional Flexelint Filter Items

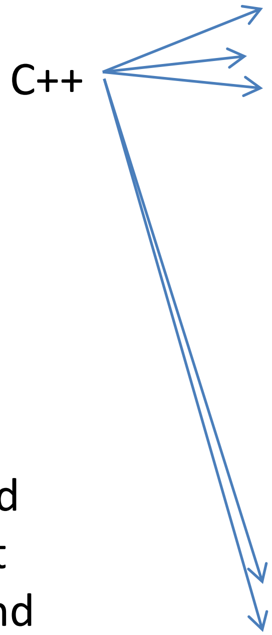
Error Code	Description from the Flexelint manual	Rationale
745	function 'Name' has no explicit type or class, int assumed	would result in a compiler warning
818	Pointer parameter 'Symbol' (Location) could be declared ptr to const	large number of warnings and unlikely to write issues
1001	Scope 'Name' must be a struct or class name	would result in a compiler error
1013	Symbol 'Name' not a member of class 'Name'	would result in a compiler error
1015	Symbol 'Name' not found in class	would result in a compiler error
1025	No function matches invocation 'Name' on arg no. Integer	would result in a compiler error
1039	Symbol 'Symbol' is not a member of class 'String'	would result in a compiler error
1055	Symbol 'Symbol' undeclared, assumed to return int	would result in a compiler warning
1401	member symbol 'Symbol' (Location) not initialized by constructor	large number of warnings and unlikely to write issues (no issues created based on the equivalent Klocwork warning)
1502	defined object 'Symbol' of type Name has no non-static data members	not an issue to report; informational
1540	pointer member 'Symbol' (Location) neither freed nor zero'ed by destructor	no issue would be written based on previous responses by the project
1762	Member function 'Symbol' could be made const	large number of warnings and unlikely to write issues
1764	Reference parameter could be declared const reference	large number of warnings and unlikely to write issues
1904	Old-style C comment	not an issue to report; informational
1927	Symbol 'Symbol' was not initialized in the constructor initializer list	large number of warnings and unlikely to write issues (no issues created based on the equivalent Klocwork warning)
1928	Symbol 'Name' did not appear in the constructor initializer list	large number of warnings and unlikely to write issues (no issues created based on the equivalent Klocwork warning)

Note: this list was approved by the NASA IV&V PM

Warning Comparison

- Klocwork: 4088 warnings (656 analyzed, “New”)
- Flexelint: 13567 warnings
- 137 Flexelint warnings duplicated by Klocwork
- 121 Klocwork warnings duplicated by Flexelint **(13 issues were in this set)**
- 71 Flexelint warning types not mapped to Klocwork
- 17 Klocwork warning types not mapped to Flexelint

Klocwork All Warnings



Row Labels	Category
ABR	130
ABV.MEMBER	1
ABV.STACK	16
CL.ASSIGN.NON_CONST_ARG	6
CL.MLK	30
CWARN.DTOR.NONVIRT.NOTEMPTY	2
CWARN.NOEFFECT.UCMP.GE	1
INCONSISTENT.LABEL	1
INFINITE_LOOP.LOCAL	6
LV_UNUSED.GEN	12
MLK.MUST	1
NPD.CHECK.CALL.MIGHT	1
NPD.CHECK.MIGHT	5
NPD.CHECK.MUST	15
NPD.FUNC.MIGHT	2
NPD.FUNC.MUST	26
PRECISION.LOSS	74
SV.STRBO.BOUND_COPY	3
SV.STRBO.UNBOUND_COPY	7
UNINIT.CTOR.MIGHT	11
UNINIT.CTOR.MUST	3421
UNINIT.STACK.ARRAY.MIGHT	4
UNINIT.STACK.ARRAY.MUST	69
UNINIT.STACK.MIGHT	4
UNINIT.STACK.MUST	83
UNREACH.GEN	80
UNREACH.RETURN	3
VA_UNUSED.GEN	63
VA_UNUSED.INIT	11
Grand Total	**4088**

Note: these totals were for Build 9.0 Version 24. Counts were not maintained for prior versions and there would be a small amount of fluctuation from build to build

Note: 76 IV&V TIMs were written

Flexelint All Warnings

Warning	Desc	Count
7	Unable to open include file	4
24	Expected an expression, found 'String'	7
31	Redefinition of symbol 'Symbol'	5
36	Redefining the storage class of 'Symbol'	1
42	Expected a statement	6
92	Negative array dimension	1
110	Attempt to assign to void	17
115	Struct/union not defined	41
118	Too few arguments (Integer) for prototype	6
128	Pointer to function not allowed	4
142	The following option has too many elements	2
150	Token 'String' unexpected	2
416	creation of out-of-bounds pointe	1
423	Creation of memory leak in assignment to variable	14
427	// comment terminates in \	1
435	integral constant 'String' has precision Integer, use +fll to enable long long	31
438	Last value assigned to variable 'Symbol' not used	29
440	for clause irregularity: variable 'Symbol' tested in 2nd expression does not match 'Symbol' modified in 3rd	36
442	for clause irregularity: testing direction inconsistent with increment direction	45
520	Highest String ’Name’ lacks side-effects	1
522	Highest String ’Name’ lacks side-effects	122
570	Loss of sign (Context) (Type to Type)	27
587	Predicate 'String' can be pre-determined and always evaluates to String	4
603	Symbol 'Symbol' (Location) not initialized	2

Warning	Desc	Count
613	Possible use of null pointer 'Symbol'	1028
647	Suspicious truncation	1
685	Relational operator 'String,' always evaluates to 'String'	18
694	The type of constant 'String' (precision Integer) is dialect dependent	28
701	Shift left of signed quantity (int)	73
702	Shift right of signed quantity (int)	11
712	Loss of precision (Context) (Type to Type)	3
713	Loss of precision (Context) (Type to Type)	315
734	**Loss of precision (Context) (Integer bits to Integer bits)**	**244**
736	**Loss of precision (Context) (Integer bits to Integer bits)**	**1505**
737	Loss of sign in promotion from Type to Type	149
740	Unusual pointer cast (incompatible indirect types)	668
747	Significant prototype coercion (Context) Type to Type	246
761	Redundant typedef 'Symbol' previously declared at Location	1
776	Possible truncation of addition	1
794	Conceivable use of null pointer 'Symbol' in [left/right] argument to operator 'String’ Reference	46
826	Suspicious pointer-to-pointer conversion (area too small)	203
835	A zero has been given as [left/right] argument to operator 'Name'	6
838	Previously assigned value to variable 'Symbol' has not been used	285
840	Use of nul character in a string literal	189
843	Variable 'Symbol' (Location) could be declared as const	29
845	The [left/right] argument to operator 'Name' is certain to be 0	17
864	Expression involving variable 'Symbol' possibly depends on order of evaluation	56
866	Unusual use of 'String' in argument to sizeof	2

Flexelint All Warnings

All C++

Warning	Desc	Count
1018	Expected a type after 'new'	3
1032	Member 'String' cannot be called without object	2
1046	member 'Symbol', referenced in a static function, requires an object	2
1054	template variable declaration expects a type, int assumed	18
1057	member 'Symbol' cannot be used without an object	13
1058	Initializing a non-const reference 'Symbol' with a non-lvalue	20
1072	Reference variable 'Symbol' must be initialized	2
1080	Definition for class ’Name’ is not in scope	1
1402	member 'Symbol' (Location) not initialized	1
1415	Pointer to non-POD class 'Name' passed to function 'Symbol'	74
1417	An uninitialized reference ’Symbol’ is being used to initialize reference ’Symbol’	1
1506	Call to virtual function 'Symbol' within a constructor or destructor	2
1514	Creating temporary to copy 'Type' to 'Type' (context: Context)	10
1524	new in constructor for class 'Name' which has no explicit destructor	11
1529	Symbol 'Symbol' not first checking for assignment to this	5
1536	Exposing low access member 'Symbol'	753
1541	member 'Symbol' (Location) possibly not initialized by constructor	5
1551	function 'Symbol' may throw an exception in destructor 'Symbol'	44
1566	member ’Symbol’ (Location) might have been initialized by a separate function but no ’-sem(Name,initializer)’ was seen	84
1579	Pointer member ’Symbol’ (Location) might have been freed by a separate function but no ’-sem(Name,cleanup)’ was seen	100
1702	operator 'Name' is both an ordinary function 'String' and a member function 'String'	37
1703	Function 'Name' arbitrarily selected.	11
1705	static class member may be accessed by the scoping operator	75
1713	Parentheses have inconsistent interpretation	1

Also All C++

Flexelint All Warnings

Warning	Desc	Count
1729	Initializer inversion detected for member 'Symbol'	164
1744	member 'Symbol' (Location) possibly not initialized by private constructor	49
1746	parameter 'Symbol' of function 'Symbol' could be made const reference	127
1757	Discarded instance of post decrement/increment	6
1763	Member function 'Symbol' marked as const indirectly modifies class	272
1773	Attempt to cast away const (or volatile)	181
1774	Could use dynamic_cast to downcast ptr to polymorphic type 'Symbol'	15
1776	Converting a string literal to char * is not const safe (Context)	3
1780	Returning address of reference parameter 'Symbol'	4
1784	Symbol 'Symbol' previously declared as "C", compare with Location	21
1785	Implicit conversion from Boolean (Context) (Type to Type)	1
1786	Implicit conversion to Boolean (Context) (Type to Type)	919
1791	No token on this line follows the 'return' keyword	1
1924	C-style cast	4513
1926	Symbol 'Symbol's default constructor implicitly called	483
Grand Total		**13567**

Flexelint Warnings with the same Title

734; Loss of precision (*Context) (Integer bits to Integer bits)* – *An* assignment is being made into an object smaller than an int. The information being assigned is derived from another object or combination of objects in such a way that information could potentially be lost. The number of bits given does not count the sign bit.

735; Loss of precision (*Context) (Integer bits to Integer bits)* – *An* assignment (or implied assignment, see *Context) is made from a long double to a* double. Using a cast will suppress the message. The number of bits includes the sign bit.

736; Loss of precision (*Context) (Integer bits to Integer bits)* – *An* assignment (or implied assignment, see *Context) is being made to a float from a value* or combination of values that appear to have higher precision than a float. You may suppress this message by using a cast. The number of bits includes the sign bit.

Integer is referring to the number of bits not the type

Klocwork warnings not mapped to Flexelint

ABV.MEMBER
ABV.STACK
CL.ASSIGN.NON_CONST_ARG
CWARN.DTOR.NONVIRT.NOTEMPTY
INCONSISTENT.LABEL
INFINITE_LOOP.LOCAL
NPD.CHECK.CALL.MIGHT
NPD.FUNC.MIGHT
NPD.FUNC.MUST

SV.STRBO.BOUND_COPY
SV.STRBO.UNBOUND_COPY
UNINIT.STACK.ARRAY.MIGHT
UNINIT.STACK.ARRAY.MUST
UNINIT.STACK.MIGHT
UNINIT.STACK.MUST
UNREACH.GEN
UNREACH.RETURN

Flexelint warnings not mapped to Klocwork

Subcategory	Warning
7	Unable to open include file
24	Expected an expression, found 'String'
31	Redefinition of symbol 'Symbol'
36	Redefining the storage class of 'Symbol'
42	Expected a statement
92	Negative array dimension
110	Attempt to assign to void
115	Struct/union not defined
118	Too few arguments (Integer) for prototype
128	Pointer to function not allowed
142	The following option has too many elements
150	Token 'String' unexpected
416	**creation of out-of-bounds pointer** (1 high severity issue)
427	**// comment terminates in \** (1 issues which was low severity since the next line was also a comment)
435	integral constant 'String' has precision Integer, use +fll to enable long long
440	for clause irregularity: variable 'Symbol' tested in 2nd expression does not match 'Symbol' modified in 3rd
442	for clause irregularity: testing direction inconsistent with increment direction
520	Highest String ’Name’ lacks side-effects
522	Highest String ’Name’ lacks side-effects
570	Loss of sign (Context) (Type to Type)

Bold warnings resulted in submitted issues

Flexelint warnings not mapped to Klocwork

Subcategory	Warning
587	Predicate 'String' can be pre-determined and always evaluates to String
603	Symbol 'Symbol' (Location) not initialized
647	Suspicious truncation
694	The type of constant 'String' (precision Integer) is dialect dependent
701	**Shift left of signed quantity (int)**
702	**Shift right of signed quantity (int)**
712	Loss of precision (Context) (Type to Type)
713	Loss of precision (Context) (Type to Type)
737	Loss of sign in promotion from Type to Type
740	Unusual pointer cast (incompatible indirect types)
761	Redundant typedef 'Symbol' previously declared at Location
776	Possible truncation of addition
794	Conceivable use of null pointer 'Symbol' in [left/right] argument to operator 'String’ Reference
835	A zero has been given as [left/right] argument to operator 'Name'
838	Previously assigned value to variable 'Symbol' has not been used
840	Use of nul character in a string literal
843	Variable 'Symbol' (Location) could be declared as const
845	The [left/right] argument to operator 'Name' is certain to be 0
864	Expression involving variable 'Symbol' possibly depends on order of evaluation
866	Unusual use of 'String' in argument to sizeof

Flexelint warnings not mapped to Klocwork (C++)

Subcategory	Warning
1018	Expected a type after 'new'
1032	Member 'String' cannot be called without object
1046	member 'Symbol', referenced in a static function, requires an object
1054	template variable declaration expects a type, int assumed
1057	member 'Symbol' cannot be used without an object
1058	Initializing a non-const reference 'Symbol' with a non-lvalue
1072	Reference variable 'Symbol' must be initialized
1080	Definition for class ’Name’ is not in scope
1402	member 'Symbol' (Location) not initialized
1415	Pointer to non-POD class 'Name' passed to function 'Symbol'
1417	An uninitialized reference ’Symbol’ is being used to initialize reference ’Symbol’
1506	Call to virtual function 'Symbol' within a constructor or destructor
1514	Creating temporary to copy 'Type' to 'Type' (context: Context)
1529	**Symbol 'Symbol' not first checking for assignment to this** (5 issues all low severity)
1536	Exposing low access member 'Symbol'
1551	function 'Symbol' may throw an exception in destructor 'Symbol'
1702	operator 'Name' is both an ordinary function 'String' and a member function 'String'

Bold warning resulted in a submitted issue

Flexelint warnings not mapped to Klocwork (C++)

Subcategory	Warning
1703	Function 'Name' arbitrarily selected.
1705	static class member may be accessed by the scoping operator
1713	Parentheses have inconsistent interpretation
1746	parameter 'Symbol' of function 'Symbol' could be made const reference
1757	Discarded instance of post decrement/increment
1763	Member function 'Symbol' marked as const indirectly modifies class
1773	Attempt to cast away const (or volatile)
1774	Could use dynamic_cast to downcast ptr to polymorphic type 'Symbol'
1776	Converting a string literal to char * is not const safe (Context)
1780	Returning address of reference parameter 'Symbol'
1784	Symbol 'Symbol' previously declared as "C", compare with Location
1785	Implicit conversion from Boolean (Context) (Type to Type)
1786	Implicit conversion to Boolean (Context) (Type to Type)
1791	No token on this line follows the 'return' keyword
1924	C-style cast
1926	Symbol 'Class's default constructor implicitly called

Warning to Warning Map

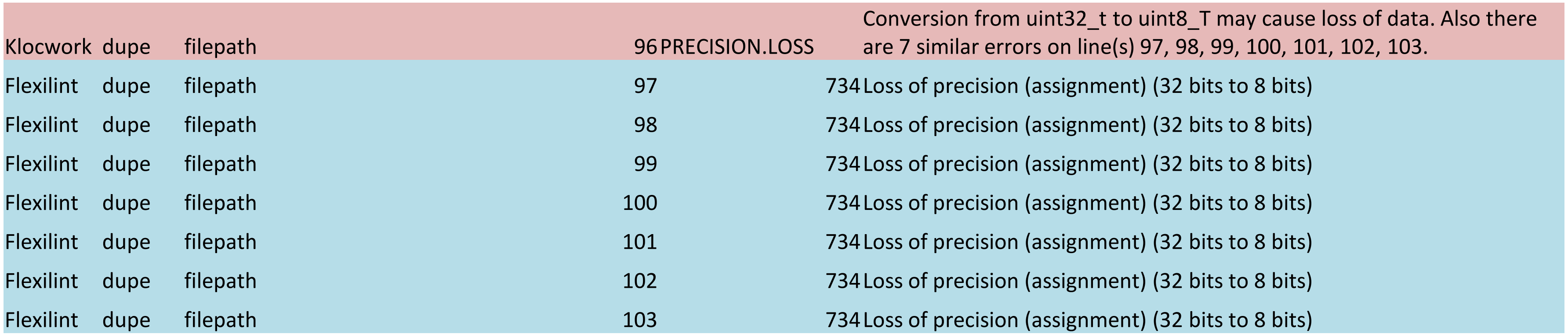
PRECISION.LOSS	Conversion from uint32_t to uint16_t may cause loss of data	734	Loss of precision (assignment) (32 bits to 16 bits)
		736	Loss of precision (assignment) (64 bits to 32 bits)
		747	Significant prototype coercion (arg. no. 1) float to double
UNINIT.CTOR.MUST	'this->member is not initialized in this constructor.	1566	member ‘Class::member' (line #, file) might have been initialized by a separate function but no '-sem(Class::member)' was seen
		1729	Initializer inversion detected for member ‘Class::member'
UNINIT.CTOR.MIGHT	'this->member' might not be initialized in this constructor.	1541	Member 'Base::member' (line #, file) possibly not initialized by constructor
		1744	member ‘Child::Child' (line #, file) possibly not initialized by private constructor
ABR	Buffer overflow, array index of ‘location' may be out of bounds. Array ‘location' of size 0 may use index value(s) 0	826	Suspicious pointer-to-pointer conversion (area too small)
CL.MLK	Possible memory leak in class 'BaseClass'. Memory referenced by ‘member' allocated in constructor at line # is not deallocated in destructor. Also there is one similar error on line #	1524	new in constructor for class ‘Class' which has no explicit destructor
		423	Creation of memory leak in assignment to ‘Class::member'
		1579	Pointer member 'Class::member' (line #, file) might have been freed by a separate function but no '-sem(Class::member)'' was seen
VA_UNUSED.GEN	Value of 'result' is never used after assignment. Also there is one similar error on line #.	838	Previously assigned value to variable 'result' has not been used
MLK.MUST	Memory leak. Dynamic memory stored in 'pointer’ allocated through function 'new[]' at line # is lost at line #	1524	new in constructor for class ‘Class' which has no explicit destructor
NPD.CHECK.MIGHT	Pointer ‘ptr' checked for NULL at line # may be dereferenced at line #. Also there are 4 similar errors on line(s) #, #, #, #.	613	Possible use of null pointer 'unknown-name' in argument to operator 'unary *'
NPD.CHECK.MUST	Pointer ‘ptr' checked for NULL at line # will be dereferenced at line #. Also there is one similar error on line #		
LV_UNUSED.GEN	Local variable ‘var' is never used	438	Last value assigned to variable ‘var' (defined at line #) not used
VA_UNUSED.INIT	Value of ‘var' is never used after initialization		
CWARN.NOEFFECT.UCMP.GE	Comparison of unsigned value against 0 is always true	685	Relational operator '>=' always evaluates to 'true'

Comparison of Flexelint to Klocwork for Uninitialized Class Members

Flexilint	dupe	filepath	80	1744	member 'Class::member1’ possibly not initialized by private constructor
Flexilint	dupe	filepath	80	1744	member 'Class::member2’ possibly not initialized by private constructor
Flexilint	dupe	filepath	80	1744	member 'Class::member3’ possibly not initialized by private constructor
Flexilint	dupe	filepath	80	1744	member 'Class::member4’ possibly not initialized by private constructor
Flexilint	dupe	filepath	80	1744	member 'Class::member5’ possibly not initialized by private constructor
Flexilint	dupe	filepath	80	1744	member 'Class::member6’) possibly not initialized by private constructor
Flexilint	dupe	filepath	80	1744	member 'Class::member7) possibly not initialized by private constructor
Flexilint	dupe	filepath	80	1744	member 'Class::member8’) possibly not initialized by private constructor
Flexilint	dupe	filepath	80	1744	member 'Class::member9’) possibly not initialized by private constructor
Klocwork	dupe	filepath	80	UNINIT.CTOR.MIGHT	'this->member1' might not be initialized in this constructor.
Klocwork	dupe	filepath	80	UNINIT.CTOR.MIGHT	'this->member2' might not be initialized in this constructor.
Klocwork	dupe	filepath	80	UNINIT.CTOR.MIGHT	'this->member3' might not be initialized in this constructor.
Klocwork	dupe	filepath	80	UNINIT.CTOR.MUST	'this->member4' is not initialized in this constructor.
Klocwork	dupe	filepath	80	UNINIT.CTOR.MUST	this->member5’ is not initialized in this constructor.
Klocwork	dupe	filepath	80	UNINIT.CTOR.MUST	'this->member6' is not initialized in this constructor.
Klocwork	dupe	filepath	80	UNINIT.CTOR.MUST	'this->member7' is not initialized in this constructor.
Klocwork	dupe	filepath	80	UNINIT.CTOR.MUST	'this->member8' is not initialized in this constructor.
Klocwork	dupe	filepath	80	UNINIT.CTOR.MUST	'this->member9' is not initialized in this constructor.

Same number of warnings for both tools

Comparing Precision Loss



Klocwork	dupe	filepath	96	PRECISION.LOSS		Conversion from uint32_t to uint8_T may cause loss of data. Also there are 7 similar errors on line(s) 97, 98, 99, 100, 101, 102, 103.
Flexilint	dupe	filepath	97		734	Loss of precision (assignment) (32 bits to 8 bits)
Flexilint	dupe	filepath	98		734	Loss of precision (assignment) (32 bits to 8 bits)
Flexilint	dupe	filepath	99		734	Loss of precision (assignment) (32 bits to 8 bits)
Flexilint	dupe	filepath	100		734	Loss of precision (assignment) (32 bits to 8 bits)
Flexilint	dupe	filepath	101		734	Loss of precision (assignment) (32 bits to 8 bits)
Flexilint	dupe	filepath	102		734	Loss of precision (assignment) (32 bits to 8 bits)
Flexilint	dupe	filepath	103		734	Loss of precision (assignment) (32 bits to 8 bits)

One warning in Klocwork but multiple warnings in Flexelint.

Compare Null Pointer Dereferences

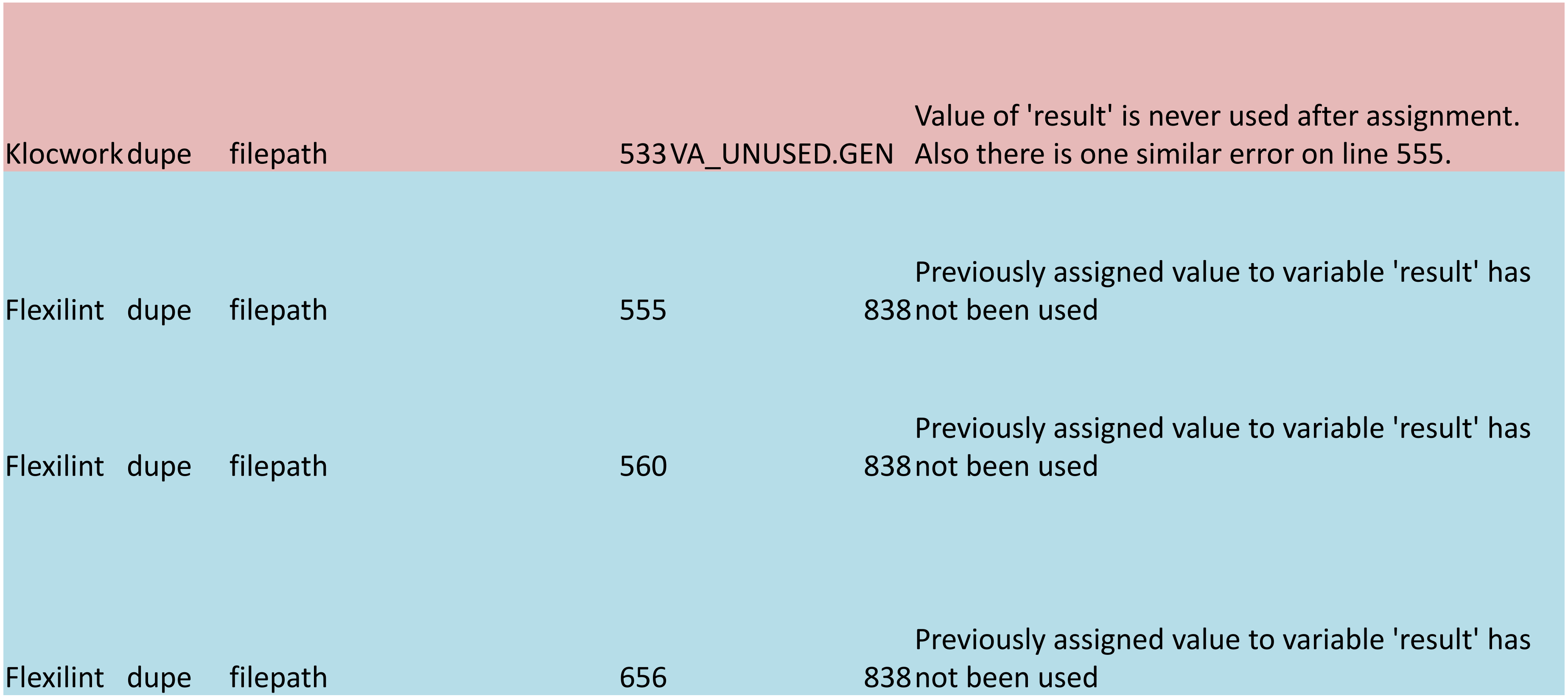
Klocwork	dupe	filepath	290	NPD.CHECK.MIGHT	Pointer ‘ptr' checked for NULL at line 273 may be dereferenced at line 290. Also there are 4 similar errors on line(s) 296, 302, 308, 314.
Flexilint	dupe	filepath	291	613	Possible use of null pointer 'unknown-name' in argument to operator 'unary *'
Flexilint	dupe	filepath	297	613	Possible use of null pointer 'unknown-name' in argument to operator 'unary *'
Flexilint	dupe	filepath	303	613	Possible use of null pointer 'unknown-name' in argument to operator 'unary *'
Flexilint	dupe	filepath	309	613	Possible use of null pointer 'unknown-name' in argument to operator 'unary *'
Flexilint	dupe	filepath	315	613	Possible use of null pointer 'unknown-name' in argument to operator 'unary *'

Comparing Precision Loss

Flexilint	dupe	filepath	174	736	Loss of precision (assignment) (64 bits to 32 bits)
Flexilint	dupe	filepath	174	747	Significant prototype coercion (arg. no. 1) float to double
Klocwork	dupe	filepath	174	PRECISION.LOSS	Conversion from double to real32_T may cause loss of data. Also there are 107 similar errors on line(s) 178, 179, 180, 184, 185, 186, 190, 191, 198, 199, ...

float(32 bits) = float(32 bits) + double(64 bits)

Unused value



Klocwork	dupe	filepath	533	VA_UNUSED.GEN	Value of 'result' is never used after assignment. Also there is one similar error on line 555.
Flexilint	dupe	filepath	555	838	Previously assigned value to variable 'result' has not been used
Flexilint	dupe	filepath	560	838	Previously assigned value to variable 'result' has not been used
Flexilint	dupe	filepath	656	838	Previously assigned value to variable 'result' has not been used

Klocwork issues warning at assignment;
Flexelint issues warning at **re**assignment.

Issues from Flexelint

Sub-category	Description	Priority	Severity	Analysis	Issue Count
427	// comment terminates in \	3	4	issue:	1
416	Likely creation of out-of-bounds pointer (4 beyond end of data) by operator 'ptr+int'	3	3	Issue; appears getting memory outside the struc.	1
613	Possible use of null pointer ‘Class::member' in left argument to operator	3	4	ftn doesn't guard as others do	1
613	Possible use of null pointer ‘Class::member' in left argument to operator	3	3	log is initialized if the value of Number is greater than zero. There is no check on this condition or the validity of the variable prior to use on line # nor on line #.	7
613	Possible use of null pointer 'buf' in left argument to operator	3	3	recast of the member 'buf' which is initialized to zero. It is set by a call to the method setBuf. This method does not check that a client has set the buffer.	2
747	Significant prototype coercion (arg. no. 2) float to int	1	4	float to int to float	2
747	Significant prototype coercion (arg. no. 3) long long to unsigned int	1	3	The long long is used in a less than test	1
1529	Symbol ‘Class::operator=(Class &)' not first checking for assignment to this	3	4	correct	4
1529	Symbol 'BaseClass::operator=(const BaseClass &)' not first checking for assignment to this	3	4	correct	189

Issues (count) Submitted vs Issues Analyzed

Flexelint Warnings		Severity			Grand Total
		3	4	NAI	
416	Likely creation of out-of-bounds pointer	1			**1**
427	// comment terminates in \		1		**1**
613	Possible use of null pointer	4	6	1018	**1028**
747	Significant prototype coercion	3		243	**246**
840	Use of nul character in a string literal		188	1	**189**
1529	operator=(const Class &) not first checking for assignment to this		5		**5**
Total		8	200	1262	1470

Issues from Klocwork

Category	Description	Severity
UNREACH.GEN	Code is unreachable	3
PRECISION.LOSS	Conversion from uint32_t to uint8_t may cause loss of data. Also there are 3 similar errors on line(s) 161, 163, 164.	4
PRECISION.LOSS	Conversion from uint32_t to uint8_t may cause loss of data	4
PRECISION.LOSS	Conversion from uint32_t to uint16_t may cause loss of data. Also there is one similar error on line 340.	4
PRECISION.LOSS	Conversion from uint32_t to uint8_T may cause loss of data. Also there are 7 similar errors on line(s) 97, 98, 99, 100, 101, 102, 103.	4
PRECISION.LOSS	Conversion from uint32_t to uint16_t may cause loss of data	5
PRECISION.LOSS	Conversion from unsigned int to uint16_t may cause loss of data	5
LV_UNUSED.GEN	Local variable 'id' is never used	5
PRECISION.LOSS	Conversion from uint32_t to uint16_t may cause loss of data	5
PRECISION.LOSS	Conversion from uint32_t to uint16_t may cause loss of data	5
PRECISION.LOSS	Conversion from uint32_t to uint16_t may cause loss of data	5
PRECISION.LOSS	Conversion from unsigned int to uint8_t may cause loss of data	5

Recommendations

- Though the tools find many of the same issues, each finds issues the other does not.
- The integrated user interface makes Klocwork easier to use.

- If schedule and resources permit use both. The MPCV IV&V Team uses Flexelint to supplement Klocwork.

Challenges

- Identifying the warnings in one tool that are also in the set of warnings from the other. This would prevent duplicate analysis of intersection of the warnings.