

Ghosts and Demons: Undefined Behavior in C2Y (Status 2026-08-23)

N3957, Martin Uecker, Graz University of Technology, uecker@tugraz.at

This is a preliminary analysis of all UB in the core language listed as item 1 to 87, as 88 to 98 for the preprocessor, and as items 99 to 221 for the standard library in Annex J.2 according to N3220 (corresponding to C23). The list also includes some items which were not classified in Annex J.2 or are new in C2Y. The color in the left column has the following meaning: **Green** are items which could be defined or made a constraint violation. For **45 items** a change that removes the UB was voted into C2Y as of 2026/08. **Light green** items require (type) checking across translation units which is not currently done by most implementations. **Orange** items can be detected at runtime for existing code. **Red** items refer to memory safety issues that are difficult or expensive to detect without breaking existing ABIs. Those will require new annotations or an opt-in memory safety mode. **Blue** are items that can be rules out by maintaining type safety in an opt-in memory safety mode. The right column proposes solutions and lists related documents. The color indicates where mainstream compilers already provide a (partial) implementation of well-defined safe behavior. On the index it indicates **removed** (proposed), **memory-safety mode**, **type safety**, **dynamic checking**, or **work needed**.

	Undefined Behavior	Status / Plan
1	Shall outside of constraints	
	Attribute appear but member declarator list is omitted	constraint
	Type compatibility uses shall in definition	ghost (N3484, 2025/02)
	Floating expressions evaluated in translation	ghost (N3732, 2026/03), see #54 and N3447
	static assert, constant expr. is not an integer constant expr	constraint (N3525, 2025/08)
	a non-value representation shall not be generated	ghost (N3700, 2026/03)
2	Does not end with newline	defined behavior (N3411, 2025/02)
3	Token concat produces universal character name	constraint (N3418, 2025/02)
4	Non-standard or missing main FREESTANDING	constraint (N3623, 2025/08)
5	Data race	opt-in memory safety (lifetime)
6	Character not in base source char set	(N3571, N3807, N3866 , target: ??)
7	Invalid multibyte character in source	(N3572, N3808 , target: ??)
8	Both internal and external linkage	constraint (N3410, 2025/02)
9	Access outside life-time	opt-in memory safety (lifetime), Annex L
10	Value of pointer outside life-time	opt-in memory safety (lifetime)
none	Modification of object with temporary lifetime	(6.2.4§8 in N3685), (see #36)
11	Automatic object is used which has indet. representation	obsolete entry in J2 (N3714 2026/03)
12	A non-value representation is read via non-char. lvalue	in opt-in memory safety mode
13	A non-value representation produced via non-char. lvalue	ghost?
14	Declarations which are not compatible	linker constraint
15	Composite type with unevaluated sizes	constraint / defined (N3652, 2025-07, online)
16	Range error in conversion from to integer	trap (floating point exception)
17	Range error floating point	trap (floating point exception)
18	Lvalue does not designate object	ghost (N3882, 2026/08), Annex L
19	Conversion of incomplete lvalues	constraint (N3481, 2025/02)
20	Automatic not address taken.	opt-in memory safety mode (initialization)
21	Pointer conversion of arrays with register	implementation-defined (N3244, 2024/06) CV?
22	Use of void expression	ghost (N3409, 2025/02)
23	Range, conversion pointer to integer	(N3712, WIP ...)
24	Conversion pointers, alignment	trap (UBSan: alignment)
25	Function call via incompat. pointer	in opt-in memory safety mode
26	Unmatched single or double quote	(N3570, N3806, wording group : 2026/08)
27	Reserved keyword used incorrectly	constraint
28	Invalid character in identifier	constraint (N3904, 2026/08)
29	Identifier starts with digit	constraint (N3904, 2026/08)
30	Two identifier differ only in non-significant character	constraint (N3911, 2026/08)
31	__func__ explicitly declared	special case of #27

	Undefined Behavior	Status / Plan
32	Program attempts to modify string literal	opt-in memory safety, Annex L, N3860
33	Various token issues	constraint / defined behavior
34	Sequencing of side effects	defined order, N3203, N3585
35	Exceptional condition during evaluation	trap (UBSan: signed-integer-overflow)
36	Object accessed via wrong type	opt-in memory safety, Annex L, ty-alloc
37	Function call via wrong type	opt-in memory safety, Annex L, CFI
none	OOB array subscription (non-pointer)	trap (UBSan: bounds)
none	No object designated by → operator	related to #39 and effective types, N3740
38	Member of atomic structure or union	constraint (N3653, 2026/02)
none	Member access of an incomplete object	constraint (N3532, 2025/08)
none	Another storage class specifier is present	constraint (6.5.3.6§7 in N3685), (N3871 2026/08)
39	Operand of * has invalid value: null pointer Operand of * has invalid value: one-after Operand of * has invalid value: not correctly aligned Operand of * has invalid value: insufficient space	trap (UBSan: null) opt-in memory-safety #44 Annex L N3711, N3741 (strong support 2026/03)
40	Weird pointer conversion	constraint (N3340, 2024/10)
41	Division / modulo by zero	trap (UBSan: integer/float-divide-by-zero), #35
42	Non-reprs. Result for division / modulo	trap (UBSan: signed-integer-overflow), #35
43	OOB pointer arithmetic	constraint / trap, opt-in memory safety, Annex L
44	Indirection of one-after pointer	constraint / trap, opt-in memory safety
45	Subtraction of unrelated pointers	implementation-defined behavior
46	OOB array subscription	trap (UBSan: bounds), N3395
47	Pointer subtraction not representable in ptrdiff	trap (implementation-defined?), WIP
48	Shift by neg. our too much	trap (UBSan: shift-exponents)
49	Signed left shift	trap (UBSan: shift), N2161
50	Relative comparison of unrelated pointers	implementation-defined behavior
51	Overlapping assignment	
none	Mismatched constexpr union access	defined
52	Integer constant expression	ghost (N3447, 2025/02)
53	Constant expression in initializer	ghost (N3447, 2025/02)
54	Arithmetic constant expression	ghost (N3447, 2025/02)
55	Object accessed in address constant	ghost (N3447, 2025/02)
56	Completeness after declaration for an object with no linkage	constraint (N3244, 2024/06)
57	Block scope function decl. with storage class	constraint (N3244, option 1, 2024/06)
58	Structure / union with no named members	implementation-defined (N3341, 2024/10)
59	OOB FAM access or pointer arithmetic	constraint in opt-in memory safety mode
60	Tagged type not completed when needed.	ghost (N3244, 2024/06)
61	Modification of const-qualified object	(see #36), Annex L
62	Access to volatile object via non-volatile lvalue	(see #36)
63	Function types includes qualifier	implementation-defined (N3342, 2024/10)
64	Two qualified types	ghost (N3484, 2025/02)
65	Restrict, access rules	constraint in opt-in memory safety mode
66	Restrict, assignment	constraint?
67	Inline function not also defined.	constraint (N3244, 2024/10)
none	Inconsistent _Noreturn (same TU) Inconsistent _Noreturn (across TUs)	6.7.13.7§3 (N3685), trap
68	_Noreturn function returns	trap (UBSan: unreachable)
69	Inconsistency of alignment specifiers (same TU) Inconsistency of alignment specifiers (across TUs)	constraint (N3244, alternative, 2024/10) linker constraint
70	Different alignment across TU	linker constraint
71	Pointers required to be compatible	ghost (N3881 2026/08)
72	VLA with non-positive size	trap (UBSan: vla-bound)

Undefined Behavior		Status / Plan
73	Arrays not compatible at run-time	trap (GCC patch exists)
74	Static in array parameter	trap + opt-in memory safety (bounds) , N3395
75	Storage classifier or qual. for void as parameter	constraint (N3344, alternative 1, 2024/10)
76	Incompatible function types	ghost (N3484, 2025/02)
77	Inferred type extensions	moved to J.3
78	Inferred type extensions	moved to J.3
79	Value of unnamed member used	ghost (N3245, 2024/10)
80	Initializer UB	constraint (N3346, 2024/10)
81	Initializer UB	constraint (N3346, 2024/10)
82	Initializer UB	constraint (N3346, 2024/10)
83	Call of function via unsequenced etc.	unspecified result
84	Unequal to one external definitions	linker constraint
none	Inferred identifier in an enclosed block	6.7.9§3 (N3685), constraint
85	A function with variable type without ...	ghost (N3482, 2025/02)
86	Function reaches } and return value is used	constraint / trap N3483
87	Tentative def. with internal linkage and incomplete type	constraint (N3347 + RM 26758, 2024/10)
88	non-preprocessor directive	preprocessor, alx-0013
89	token defined issues	preprocessor
90	#include preprocessing issues	preprocessor, N3710
91	character sequence in an #include does not start with letter	preprocessor
92	directives in macro argument	preprocessor
93	result of operator # is not a valid character string literal	preprocessor
94	result of the preprocessing operator ## is not a valid token	preprocessor
95	#line preprocessing directive	preprocessor
96	non-STD C #pragma preprocessing directive	preprocessor
97	invalid #pragma STD C preprocessing directive	preprocessor
98	name of a predefined macro or defined in #define / #undef	preprocessor (see #27)
99	Move overlapping object with library function	memory S
100	file with std name placed in standard include path	preprocessor, out-of-scope
101	header included in external definition or declaration	
102	function, object, type, macro before inclusion of std header	(see #27)
103	std header included while a macro is defined for keyword	(see #27)
104	program declares library function without external linkage	(see #27)
105	declaration of reserved identifier not allowed by 7.4.3/4	(see #27)
106	removal of macro with underscore + capital or underscore	(see #27)
107	Invalid type to library function	Annex L
108	Oob in library function	memory S
109	Macro assert suppressed	#109, #113, #122, #124, #138 (also see #27)
110	Macro assert has non-scalar argument	
111	Floating point pragma used outside specified contexts	constraint / implementation-defined
112	Invalid value as argument to character-handling function	
113	Macro errno suppressed, or identifier declared.	#109, #113, #122, #124, #138 (also see #27)
...	(floating point environment / exceptions)	
118	Result of integer arithmetic / conversion function not representable	trap
...	(locale related)	
122	Macro math_errhandling suppressed, or identifier declared	#109, #113, #122, #124, #138 (also see #27)
123	Argument to floating-pointer classification / comparison function is not real float type	
124	Setjmp suppressed, or identifier declared	#109, #113, #122, #124, #138 (also see #27)
125	Setjmp wrong context	Annex L
126	Uninitialized longjmp	memory I, Annex L

	Undefined Behavior	Status / Plan
127	Longjmp / setjmp use of cached value	Annex L
...	(signal handling)	
136	Variadic function accesses args differently	
137	Incorrect va_arg use	
138	va_start / va_copy / va_end suppressed	#109, #113, #122, #124, #138 (also see #27)
139	va_start / va_copy without va_end or vv	
140	va_arg no next arg, or incompatible type	Annex L
141	va_arg argument not an object	
142	Integer null pointer to va_arg	
143	Incorrect va_copy / va_start	
144	va_start, syntax	syntax
145	Generic function suppressed	(wording fix N3918, 2026/08)
146	Offsetof comma	syntax
147	unreachable	trap (UBSan: unreachable)
148	Bytes of nullptr_t	special case of 12
149	Offset of invalid member	
150	Invalid argument to integer-constant macro	
...	(formatted I/O)	
182	Zero-sized allocation is used (malloc, ...)	memory S
183	Freed pointer value used	memory T, Annex L
184	Invalid use of free (or realloc)	memory T, Annex L
185	Values-bytes-malloc	unspecified, N3448, 2025/02
186	Values-bytes-realloc	unspecified, N3448, 2025/02
none	stdc_rotate_{left,right} second argument	N3593
..195	(stdlib.h)	
..201	(string.h)	
..207	(tgmath.h)	
..213	(threads.h)	
..215	(time.h)	
..218	(wchar.h)	
..221	(wctype.h)	

Acknowledgments: The Undefined Behavior Study Group for discussions and help. Dr. Philipp Klaus-Krause for pointing out errors in previous versions of this document. All remaining or new errors are my own.

Appendix: Remaining UB in the Core Language (1-87)

N3220	N3886	Undefined Behavior
4	2	Non-standard or missing main FREESTANDING ONLY
5	3	Data race
6	4	Character not in base source char set
7	5	Invalid multibyte character in source
9	6	Access outside life-time
10	7	Value of pointer outside life-time
none	none	Modification of object with temporary lifetime
12	8	A non-value representation is read via non-char. lvalue
13	9	A non-value representation produced via non-char. lvalue
14	10	Declarations which are not compatible
16	12	Range error in conversion from to integer
17	13	Range error floating point
20	15	Automatic not address taken.
23	16	Range, conversion pointer to integer
24	17	Conversion pointers, alignment
25	18	Function call via incompat. pointer
26	19	Unmatched single or double quote
27	20	Reserved keyword used incorrectly
31	24	<code>__func__</code> explicitly declared
32	25	Program attempts to modify string literal
33	26	Various token issues
34	27	Sequencing of side effects
35	28	Exceptional condition during evaluation
36	29	Object accessed via wrong type
37	30	Function call via wrong type
none	none	OOB array subscription (non-pointer)
none	none	No object designated by <code>→</code> operator
39	32	Operand of * has invalid value
41	33	Division / modulo by zero
42	34	Non-reprs. Result for division / modulo
43	35	OOB pointer arithmetic
44	36	Indirection of one-after pointer
45	37	Subtraction of unrelated pointers
46	38	OOB array subscription
47	39	Pointer subtraction not representable in <code>ptrdiff</code>
48	40	Shift by neg. our too much
49	41	Signed left shift
50	42	Relative comparison of unrelated pointers
51	43	Overlapping assignment
none	44	Mismatched <code>constexpr</code> union access
59	45	OOB FAM access or pointer arithmetic
61	46	Modification of const-qualified object
62	47	Access to volatile object via non-volatile lvalue
65	48	Restrict, access rules
66	49	Restrict, assignment
none	none	Inconsistent <code>_Noreturn</code> (same TU / across TUs)
68	50	<code>_Noreturn</code> function returns
69	51	Inconsistency of alignment specifiers across TUs
70	52	Different alignment across TU
72	54	VLA with non-positive size
73	55	Arrays not compatible at run-time
74	56	Static in array parameter
83	57	Call of function via unsequenced etc.
84	58	Unequal to one external definitions
none	none	Inferred identifier in an enclosed block
86	59	Function reaches <code>}</code> and return value is used