

Obfuscation of function block diagrams: Annex

Antti Pakonen

VTT Technical Research Centre of Finland Ltd., Espoo, Finland

Email: antti.pakonen@vtt.fi

I. INTRODUCTION

This is the annex to my publication [1] on obfuscation of IEC 61131-3 [2] function block diagram (FBD) programs.

II. OBFUSCATION TECHNIQUES FOR FBD

A. Non-Latin characters in identifiers

Table I
POTENTIAL SIMULACRA FOR LATIN LETTERS IN ISO/IEC 10646

Letter	Potential simulacrum	Code point
A	GREEK CAPITAL LETTER ALPHA	0391
A	CYRILLIC CAPITAL LETTER A	0410
B	GREEK CAPITAL LETTER BETA	0392
B	CYRILLIC CAPITAL LETTER VE	0412
C	CYRILLIC CAPITAL LETTER ES	0421
C	ROMAN NUMERAL ONE HUNDRED	216D
D	ROMAN NUMERAL FIVE HUNDRED	216E
E	GREEK CAPITAL LETTER EPSILON	0395
E	CYRILLIC CAPITAL LETTER IE	0415
F	–	–
G	–	–
H	GREEK CAPITAL LETTER ETA	0397
H	CYRILLIC CAPITAL LETTER EN	041D
I	GREEK CAPITAL LETTER IOTA	0399
I	CYRILLIC CAPITAL LETTER BYELORUSSIAN-UKRAINIAN I	0406
J*	CYRILLIC CAPITAL LETTER JE	0408
K*	GREEK CAPITAL LETTER KAPPA	039A
K*	CYRILLIC CAPITAL LETTER KA	041A
K*	KELVIN SIGN	212A
L	ROMAN NUMERAL FIFTY	216C
M	GREEK CAPITAL LETTER MU	039C
M	CYRILLIC CAPITAL LETTER EM	041C
M	ROMAN NUMERAL ONE THOUSAND	216C
N	GREEK CAPITAL LETTER NU	039D
O	GREEK CAPITAL LETTER OMICRON	039F
O	CYRILLIC CAPITAL LETTER O	041E
P	GREEK CAPITAL LETTER RHO	03A1
P	CYRILLIC CAPITAL LETTER ER	0420
Q	–	–
R	–	–
S	CYRILLIC CAPITAL LETTER ZHE	0405
T	GREEK CAPITAL LETTER TAU	03A4
T	CYRILLIC CAPITAL LETTER TE	0422
U	–	–
V	ROMAN NUMERAL FIVE	2164
W*	–	–
X	GREEK CAPITAL LETTER CHI	03A7
X	ROMAN NUMERAL TEN	2169
Y*	GREEK CAPITAL LETTER UPSILON	03A5
Z*	GREEK CAPITAL LETTER ZETA	0396

* Character is not used in any name listed in Table III.

Consulting the ISO/IEC 10646 [3], we can find simulacra for almost the all Latin characters (see Table I for select examples), only lacking suitable replacements for F, G, Q, R, U, and W. Since no function defined in IEC 61131-3 is spelled

using only those characters, we can create a simulacrum block for every default function there is.

For an identifier with n characters $c_1 \dots c_n$, if, for every c_n we have s_n possible simulacra in Table I, then we can count the number of possible ways we can rewrite the identifier (not including the original form) as:

$$\left[\prod_{i=1}^n (s_i + 1) \right] - 1$$

This is the number shown as “possible simulacra” in Table III.

B. Logic hidden in execution control parameters

We can use the NuSMV [4] model checker to prove that our MUX (Fig. 5 in the paper) is correctly implemented in the execution control variable processing logic.

See the file: Obf_MUX.smv

C. Clutter logic

We can also use the NuSMV model checker that the patterns in Section IV-C effectively block the superfluous “fake” logic from having an effect on the actual intended functionality.

The NuSMV input files for each pattern in the paper are listed in Table II.

Table II
NUSMV INPUT FILES FOR THE “FAKE” LOGIC PATTERNS

NuSMV file	Figure in paper
Obf_SR.smv	Fig. 6
Obf_TP_TON.smv	Fig. 7
Obf_MINMAX.smv	Fig. 8

REFERENCES

- [1] A. Pakonen, “Obfuscation of function block diagrams,” in *ETFA 2023*, IEEE, Sept. 2023.
- [2] IEC, “Programmable controllers – part 3: Programming languages,” International Electrotechnical Commission, IEC Standard 61131-3:2013, 2013.
- [3] ISO/IEC, “Information technology – Universal coded character set (UCS),” International Organization for Standardization / International Electrotechnical Commission, ISO/IEC Standard 10646:2020, 2020.
- [4] A. Cimatti, E. Clarke, E. Giunchiglia, F. Giunchiglia, M. Pistore, M. Roveri, R. Sebastiani, and A. Tacchella, “NuSMV version 2: An opensource tool for symbolic model checking,” in *International Conference on Computer-Aided Verification (CAV 2002)*, ser. LNCS, vol. 2404. Springer, 2002.

Table III
NUMBER OF POSSIBLE SIMULACRA FOR DEFAULT IEC 61131-3
FUNCTIONS / BLOCKS

Function / block	Can be replaced	Cannot be replaced	Possible simulacra
REPLACE	A,C,E,L,P	R	1457
CONCAT	A,C,N,O,T		485
DELETE	D,E,L,T		323
LIMIT	I,L,M,T		215
EXPT	E,P,T,X		107
INSERT	E,I,N,S,T	R	107
SPLIT	I,L,P,S,T		107
MOVE	E,M,O,V		71
ACOS	A,C,O,S		53
ATAN	A,N,T		53
MAX	A,M,X		35
ASIN	A,I,N,S		35
EXP	E,P,X		35
RIGHT	I,G,H	G,R	26
MID	D,I,M		23
MIN	I,M,N		23
MOD	D,M,O		23
ABS	A,B,S		17
COS	C,O,S		17
CTD	C,D,T		17
CTUD	C,D,T	U	17
LEFT	E,L,T	F	17
NOT	N,O,T		17
TAN	A,N,T		17
TON	N,O,T		17
TRUNC	C,N,T	R,U	17
MUX	M,X	U	15
ADD	A,D		11
AND	A,D,N		11
DIV	D,I,V		11
FIND	D,I,V	F	11
LEN	E,L,N		11
SEL	E,L,S		11
SHL	H,L,S		11
SIN	I,N,S		11
XOR	O,X	R	11
CTU	C,T	U	8
F_TRIG	I,T	F,G,R	8
R_TRIG	I,T	G,R	8
TOF	O,T	F	8
TP	P,T		8
MUL	L,M	U	7
LE	E,L		5
LOG	L,O	G	5
LT	L,T		5
NE	E,N		5
ROL	L,O	R	5
SHR	H,S	R	5
SQRT	S,T	Q,R	5
SUB	B,S	U	5
LN	L,N		3
EQ	E	Q	2
GE	E	G	2
GT	T	G	2
OR	O	R	2
ROR	O	R	2
RS	S	R	1
SR	S	R	1