Direct / indirect addressing

Addressing methods are mostly tied to variable types, not areas, so the following procedures apply to both DB and Tag variables.

Direct addressing

Direct addressing in Simatic is typically symbolic addressing, meaning in the simplest case we correspond two variables of the same type to each other:

```
fromReal : Real;
fromInt : Int;
toReal : Real;
toInt : Int;
…

#toInt := #fromInt;
#toReal := #fromReal;
```

If the types do not match, conversion will help us:

```
#toInt := REAL_TO_INT(IN := #fromReal);
```

It is crucial to understand that conversion can lead to data loss. In the example above, the REAL type can store much larger numbers and fractional parts, while the INT only handles smaller integers and rounds off fractions. When converting between variables with different ranges, all values outside the smaller range should be considered. In this case, rather than using an INT, a variable with a broader range should be selected (example DINT, LINT).

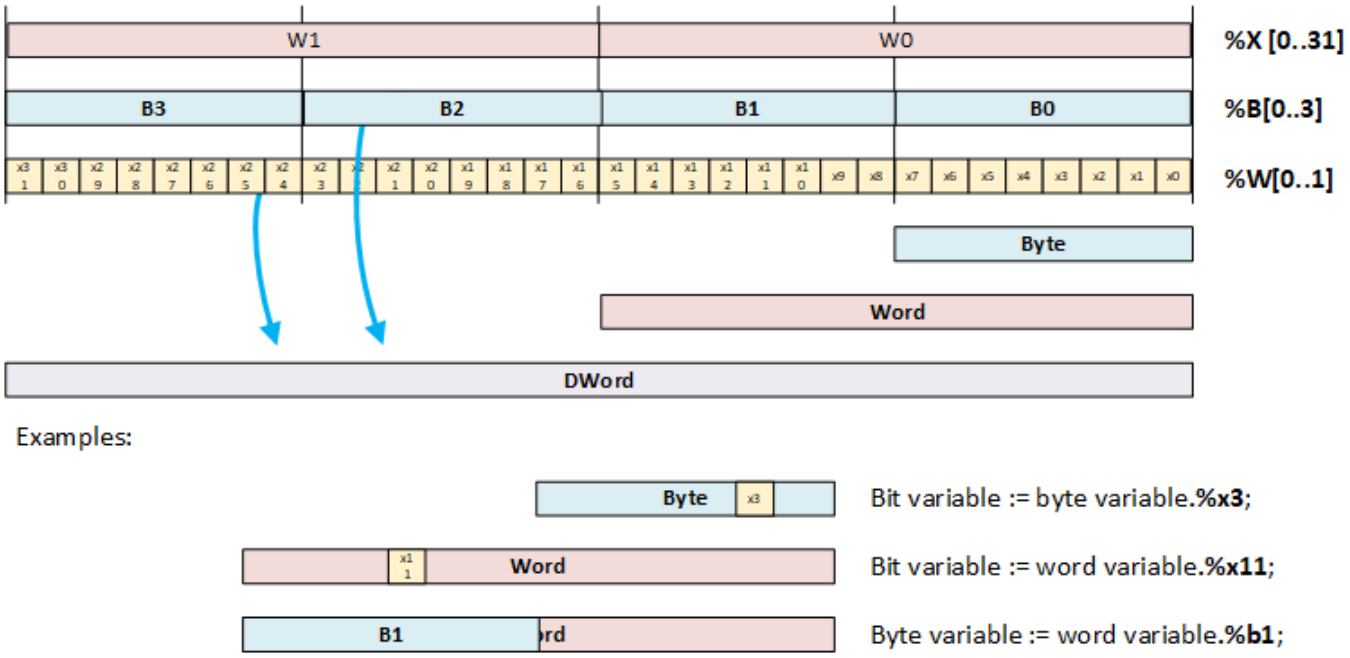
Direct addressing is also applicable to STRUCTURE and ARRAY types, as long as both sides have identical structures.

Another approach is direct addressing, which involves referring to sub-elements of a variable. Although this method applies to a limited range of variables, it is a simple form of assignment. While it isn't as straightforward as the S7-Classic AT command that many programmers prefer, it is at least available:

Slice addressing

Slice addressing involves dividing a memory region, such as a byte or word, into smaller segments like booleans. With S7-1200 and S7-1500, you can target specific parts within declared variables

(**only by byte, word, dword**) and access segments of 1, 8, 16, or 32 bits.



The following example is a SPLIT function that splits a WORD Input variable into bits:

```
// FC Input : inWord (Word)
// FC output: 16 variable bit0..bit15 (Bool)
// splitting
#bit0 := #inWord.%X0;
#bit1 := #inWord.%X1;
#bit2 := #inWord.%X2;
#bit3 := #inWord.%X3;
#bit4 := #inWord.%X4;
#bit5 := #inWord.%X5;
#bit6 := #inWord.%X6;
#bit7 := #inWord.%X7;
#bit8 := #inWord.%X8;
#bit9 := #inWord.%X9;
#bitA := #inWord.%X10;
#bitB := #inWord.%X11;
#bitC := #inWord.%X12;
#bitD := #inWord.%X13;
#bitE := #inWord.%X14;
#bitF := #inWord.%X15;
```

Pointer; indirect addressing

In the TIA Portal, there are two ways to perform indirect addressing or pointer referencing: the ANY and the VARIANT. However, it is important to note that the S7-1200 series PLCs do not support the ANY method. Using a pointer essentially involves moving a data block of a specific size to a memory

area of the same size. This operation ignores the structure and variables within the data area, making it a quick and useful method when applied carefully. **However, careless use of this tool can be very risky.**

A key issue is that it doesn't handle the variables within the data being pointed to; for example, when searching for errors with xref, these procedures are not visible to the compiler, which can lead to difficult-to-detect errors caused by improper pointer use.

ANY type

Structure of the ANY Pointer (**10 Bytes**):

Name	Length	Description
Syntax ID	1 byte	Always 16#10 for S7
Data Type	1 byte	Code for the type of data being pointed to (e.g., 16#02 for Byte, 16#04 for Word
Repetition Factor	2 bytes	Number of elements of the specified data type
DB Numbe	2 bytes	The number of the data block (0 if not in a DB)
Memory Area	1 byte	Code for the memory area (e.g., 16#84 for DB, 16#81 for Input)
Address	3 bytes	The start address of the data (bit and byte address)

TIA Coding of data types

The following table lists the coding of data types for the ANY pointer:

Hexadecimal code	Data type	Description
B#16#00	NIL	Null pointer
B#16#01	BOOL	Bits
B#16#02	BYTE	bytes, 8 bits
B#16#03	CHAR	8-bit characters
B#16#04	WORD	16-bit words
B#16#05	INT	16-bit integers
B#16#06	DWORD	32-bit words
B#16#07	DINT	32-bit integers
B#16#08	REAL	32-bit floating-point numbers
B#16#0B	TIME	Time duration
B#16#0C	S5TIME	Time duration
B#16#09	DATE	Date
B#16#0A	TOD	Date and time
B#16#0E	DT	Date and time
B#16#13	STRING	Character string
B#16#17	BLOCK_FB	Function block
B#16#18	BLOCK_FC	Function
B#16#19	BLOCK_DB	Data block
B#16#1A	BLOCK_SDB	System data block
B#16#1C	COUNTER	Counter

Hexadecimal code	Data type	Description
B#16#1D	TIMER	Timer

2026/01/16 12:40 · vamsan