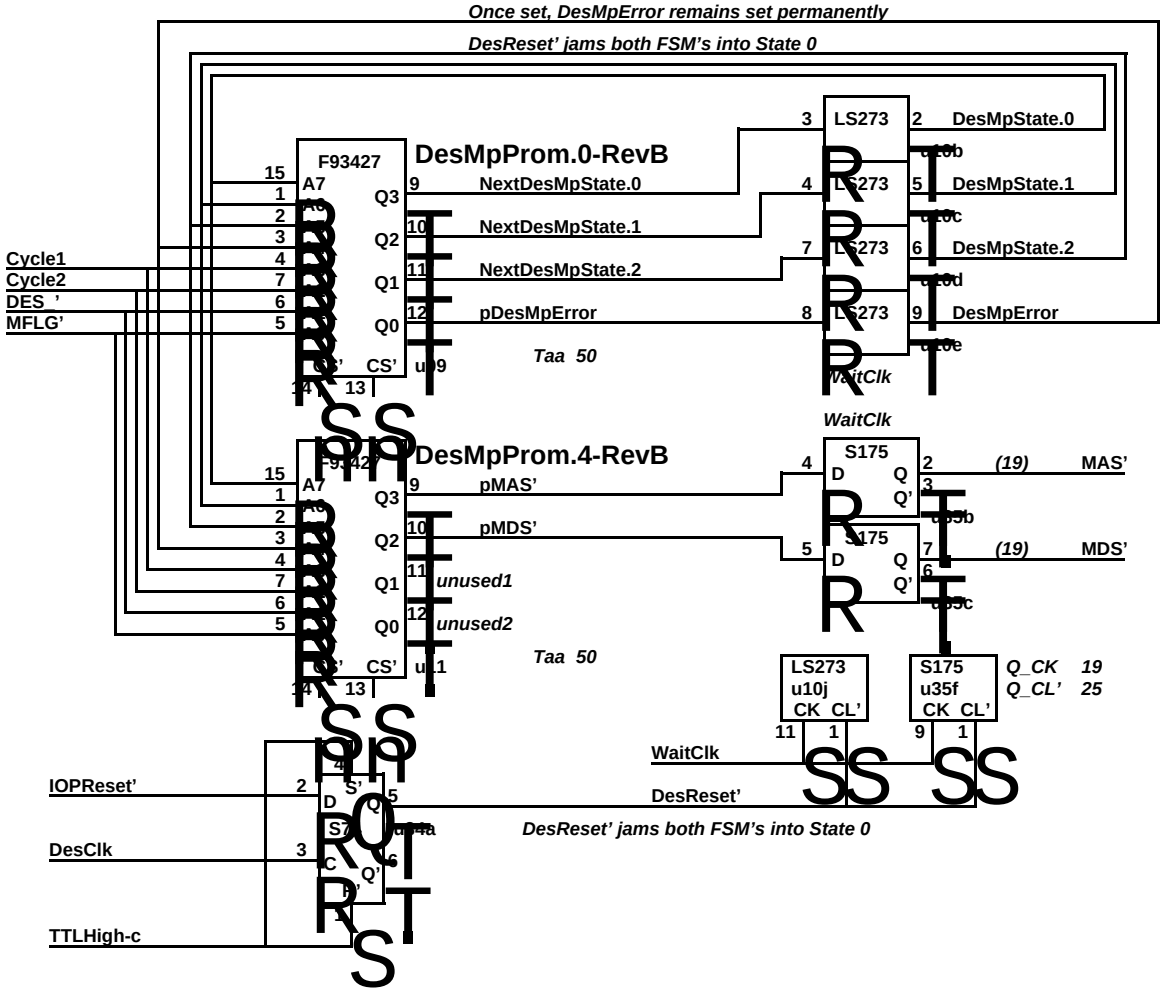
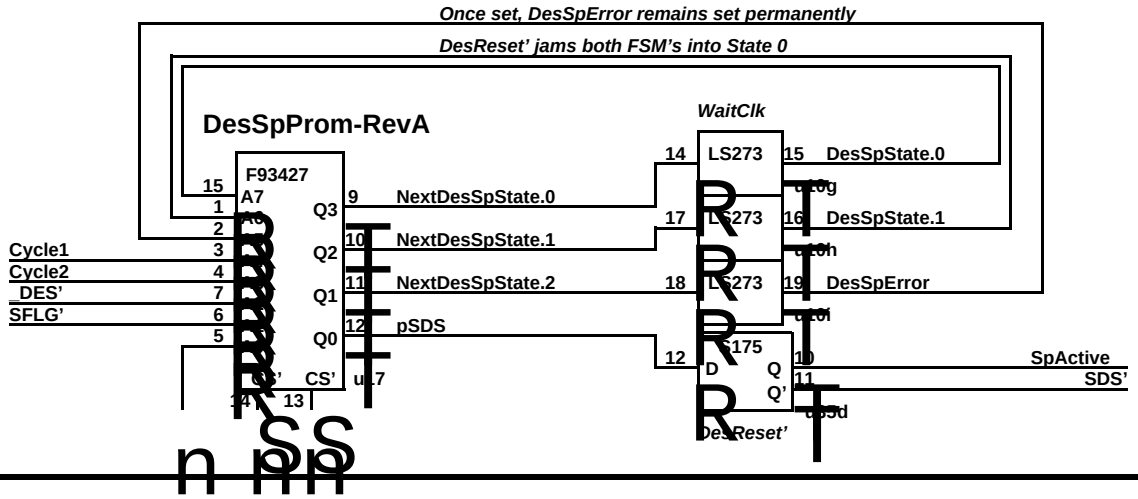
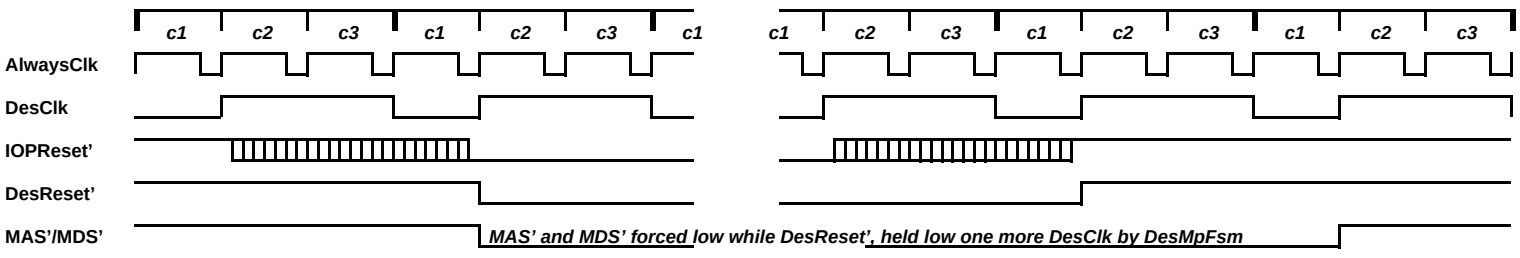


Des Master Port FSM

Des Slave Port FSM



Reset Des Chip and FSM's with IOPReset'

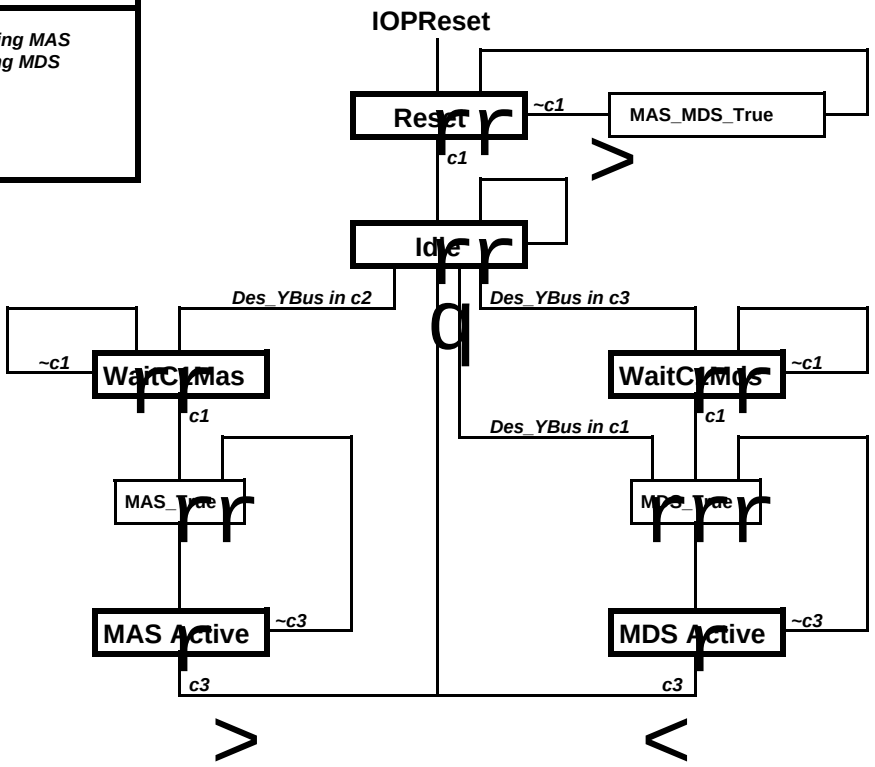


XEROX PARC	Project	Drawing	File	Designer	Rev	Date	Page
	CPE	DES Finite-State Machines	CPE31.sil	Tony West	Ba	5/30/83	32

Note on semantics of Master Port Writes

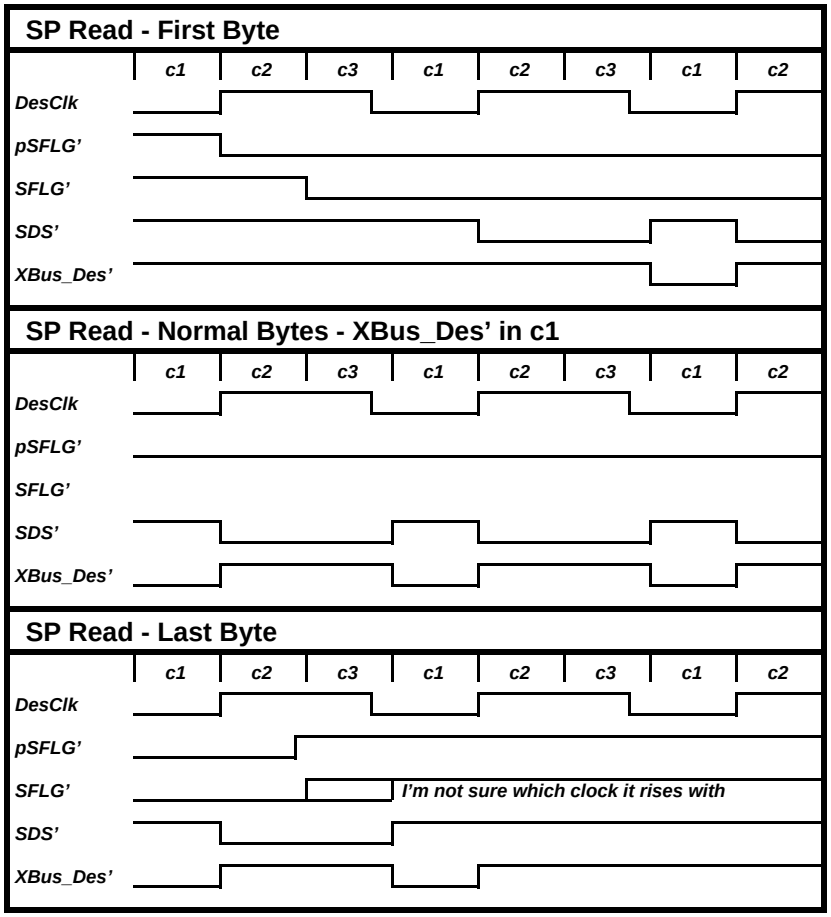
If you write to the Des chip in c2, it means write an address using MAS
If you write to the Des chip in c1 or c3, it means write data using MDS
You may have to wait for c1 in some of these cases.

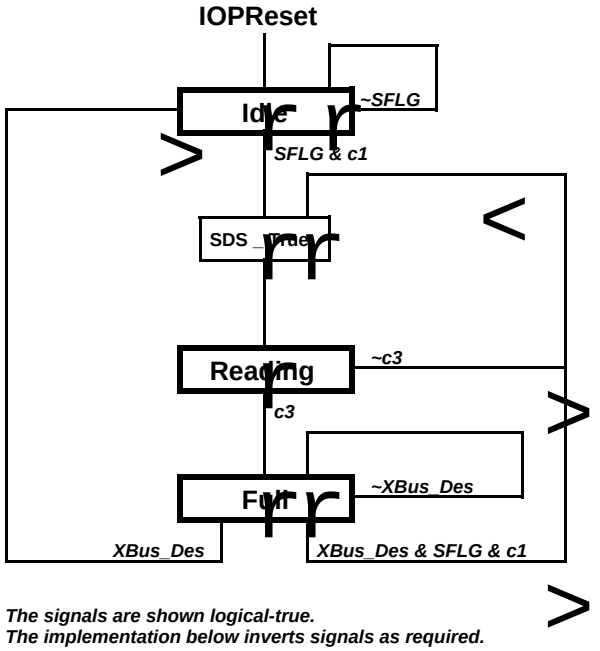
The signals are shown logical-true.
The implementation below inverts signals as required.



Master Port Finite-State Machine - Error handling of DesMpError signal is not shown

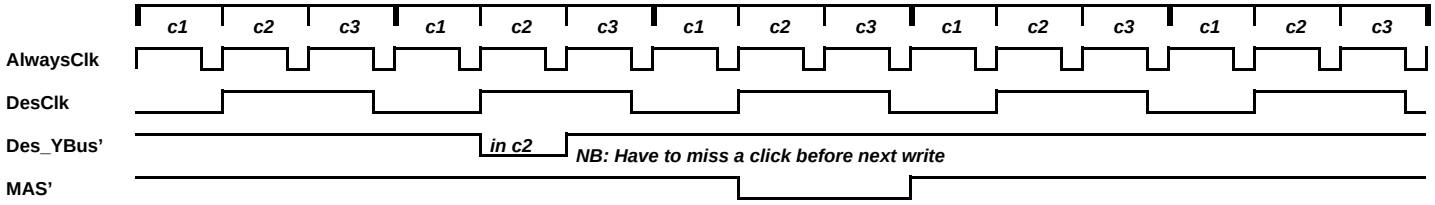
Slave Port Finite-State Machine - Error handling of DesSpError signal is not shown



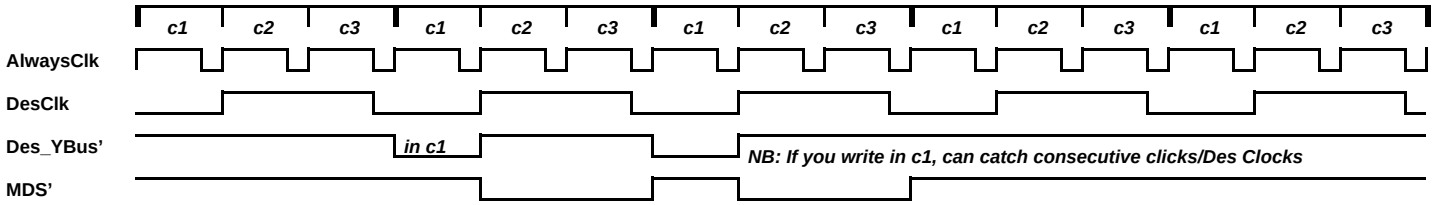


The signals are shown logical-true.
The implementation below inverts signals as required.

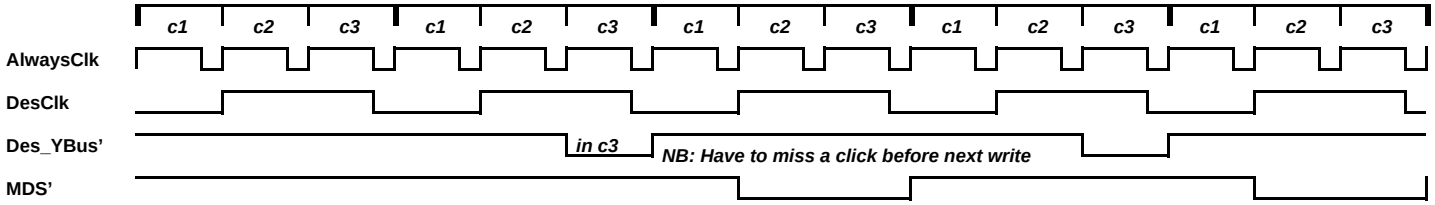
Write address into Des Master Port in C2



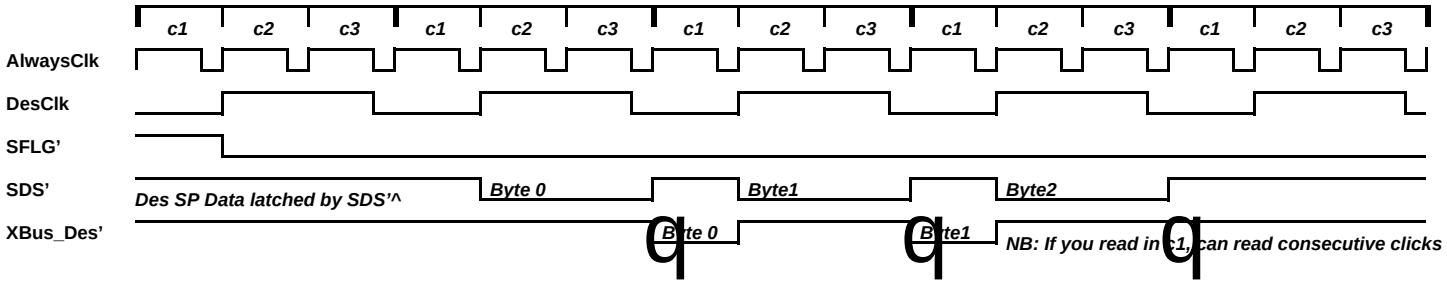
Write data into Des Master Port in C1



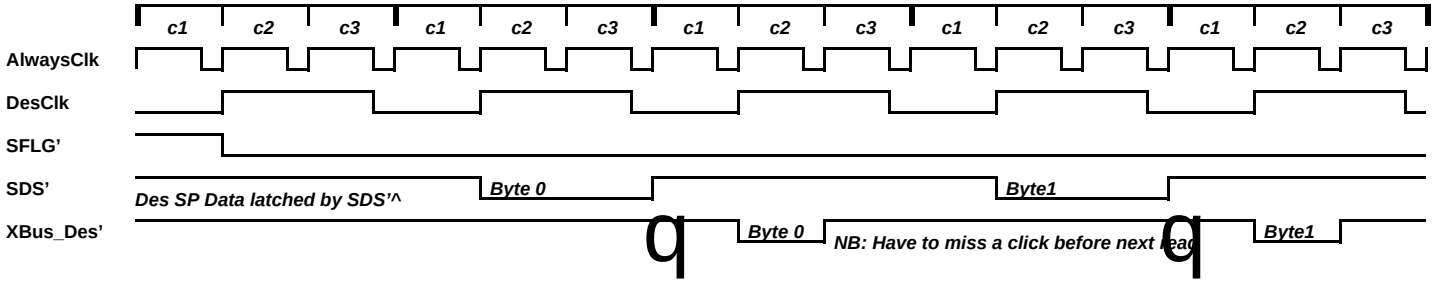
Write data into Des Master Port in C3



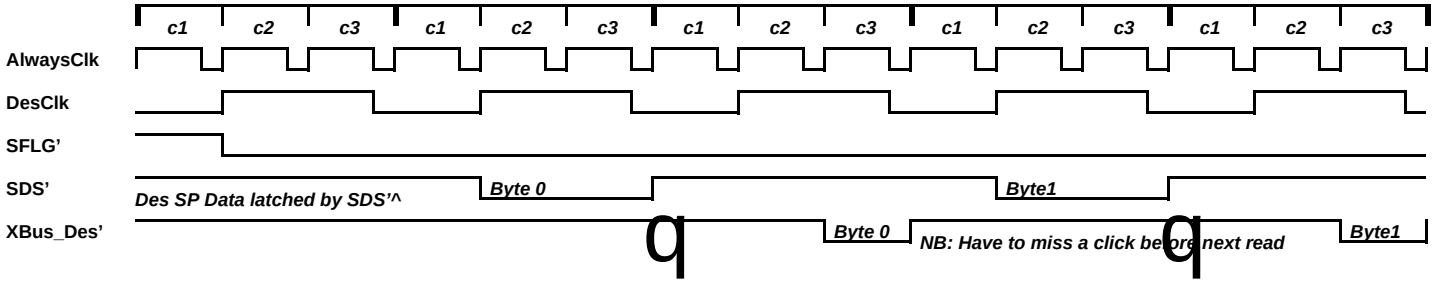
Read Data from Des Slave Port in C1

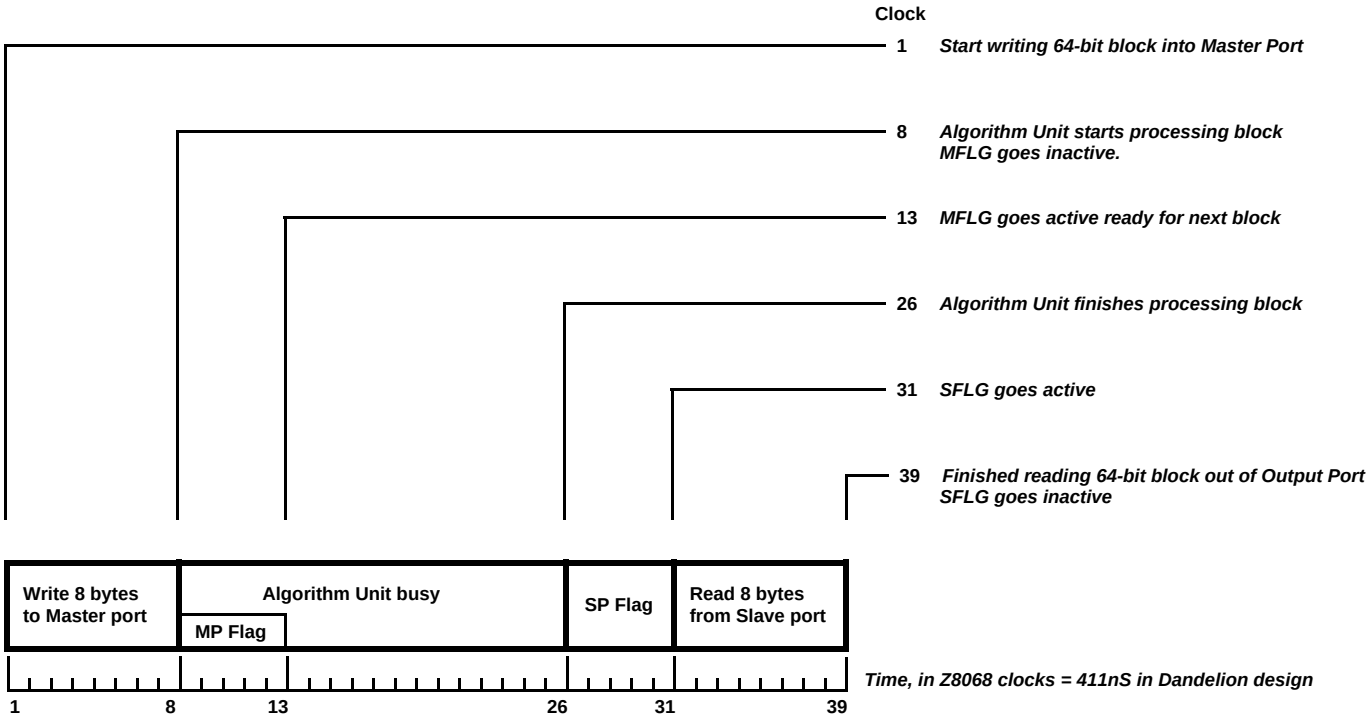


Read Data from Des Slave Port in C2



Read Data from Des Slave Port in C3





WARNING! This data is not guaranteed to be correct!

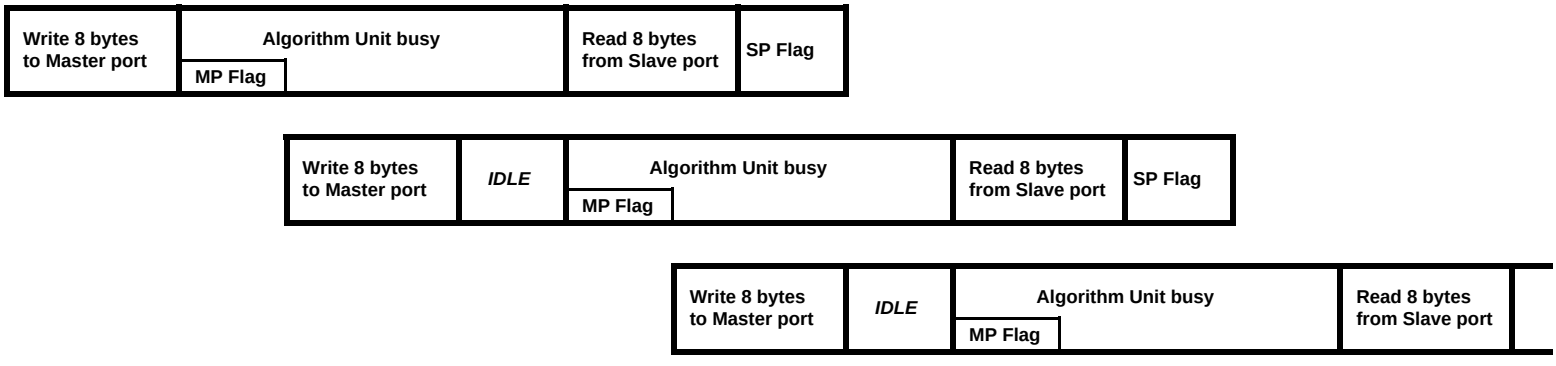
NOTES:

The longest operation in encrypting a block is the time it takes to get the data through the algorithm unit, 18 clocks. Therefore, this is the bottleneck in the pipelining scheme, and the software must aim to keep the Algorithm unit fully busy.

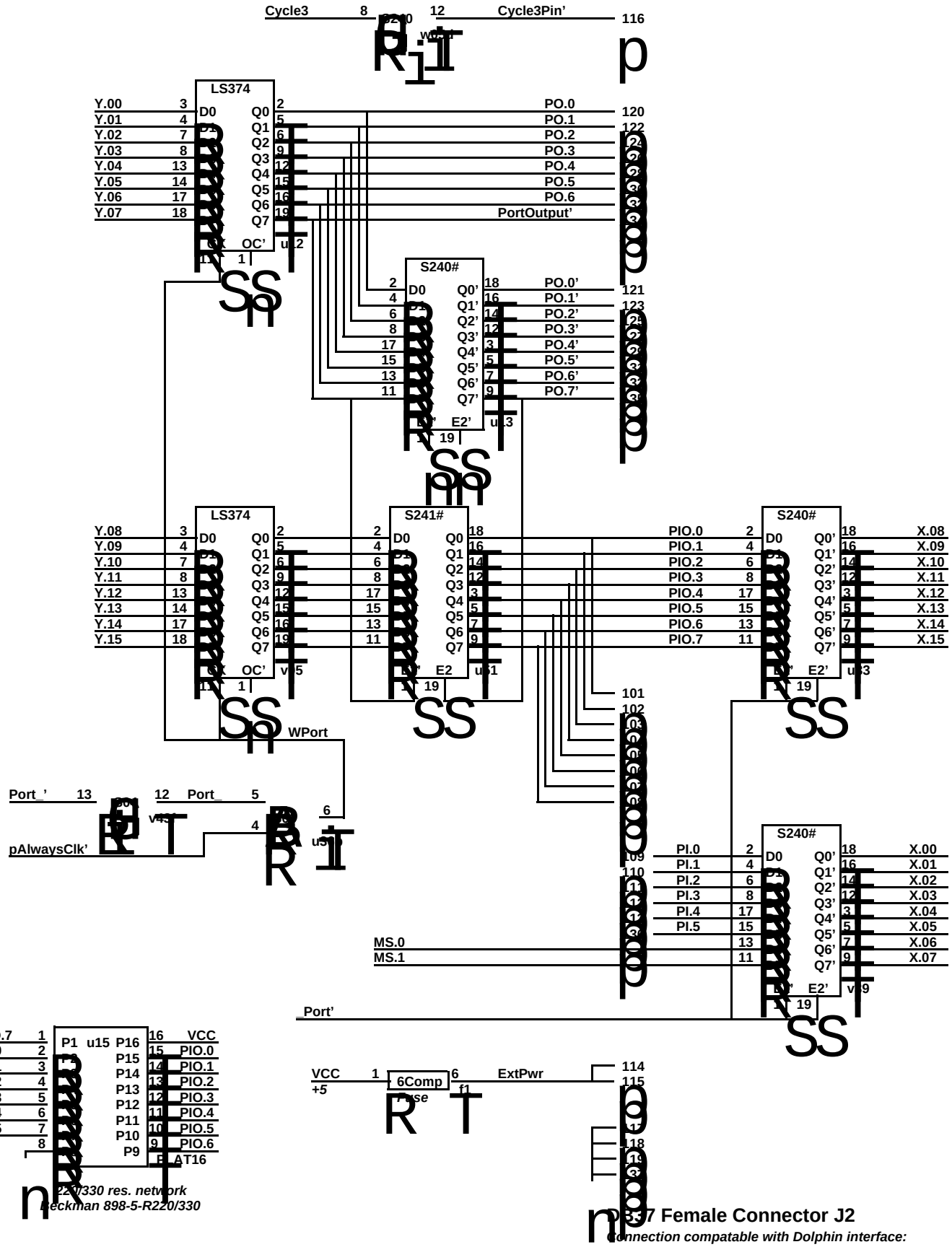
Apart from the first and last blocks, the time taken to encrypt the middle blocks is 18 clocks.

One possible pipelining scheme

WARNING! This data is not guaranteed to be correct!



WARNING! This data is not guaranteed to be correct!



XEROX PARC	Project	Drawing	File	Designer	Rev	Date	Page
	CPE	General Purpose 8-bit Port	CPE35.sil	Bob Garner	Ba	5/30/83	36