DC Lab2 Report

Team 04

B10901163 張顥譽 B10901176 蔡弘祥 B10901179 鄭承瑞

File Structure

team04_lab2

|- team04_lab2_report

|- src

|- Rsa256Wrapper.sv

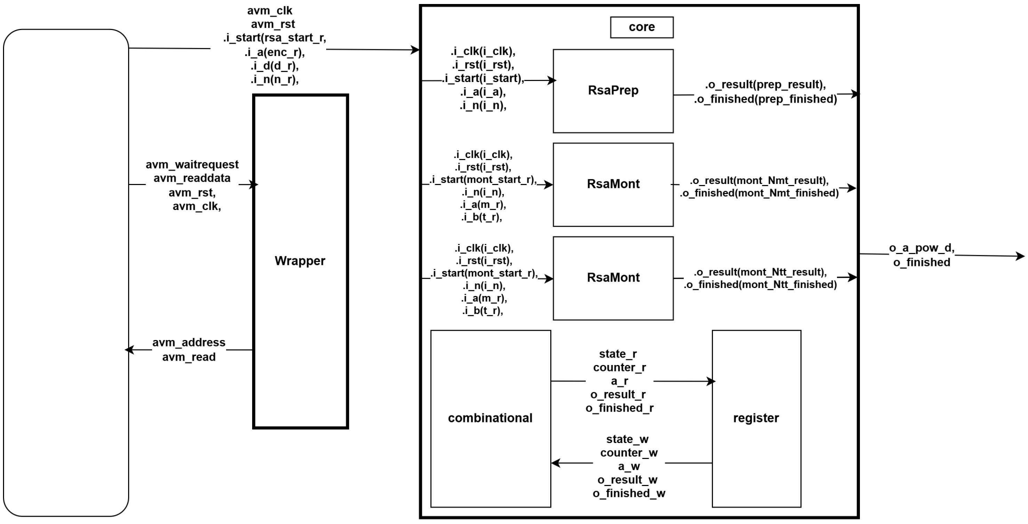
|- Rsa256core.sv

|- DE2_115.qsf

|- DE2_115.sv

|- DE2_115.sdc

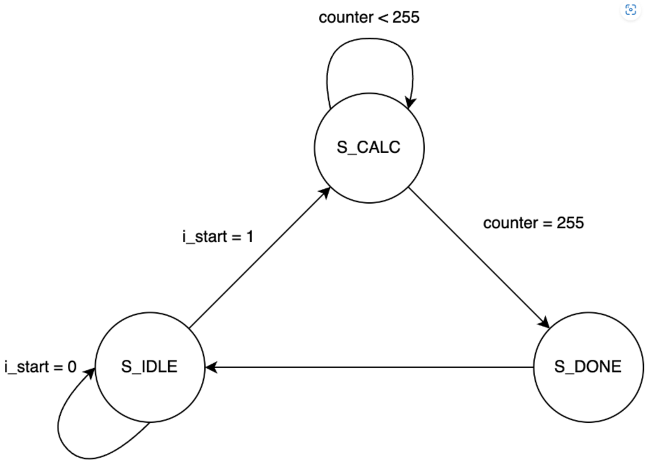
System Architecture



Hardware Scheduling

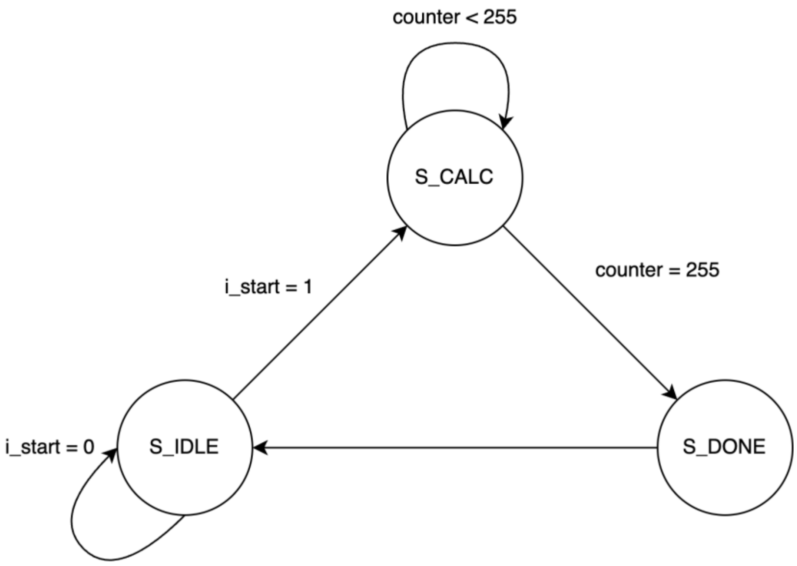
Modules / Submodules

1. **RsaPrep:** Do modulo_product(N, a)



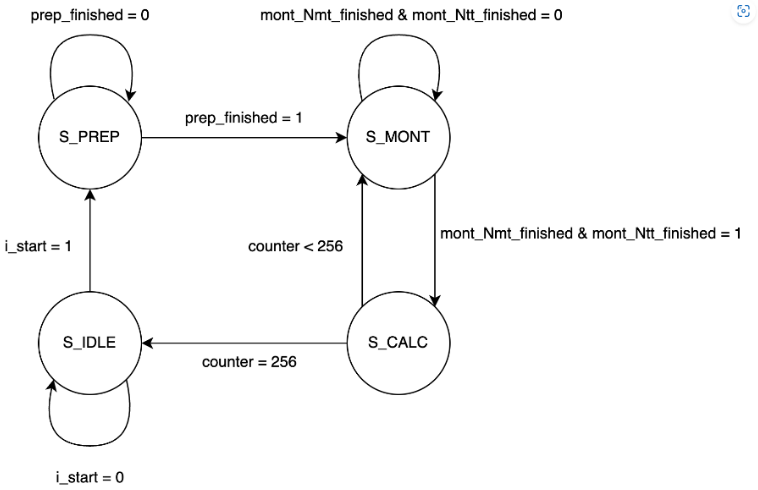
- S_IDLE: wait for master module call
- S_CALC: do the for-loop in the pseudocode, need 256 cycles
- S_DONE: output the result and set the finish signal to 1

2. **RsaMont:** Do montgomery_algorithm(N, a, b)



- S_IDLE: wait for master module call
- S_CALC: do the for-loop in the pseudocode, need 256 cycles
- S_DONE: output the result and set the finish signal to 1

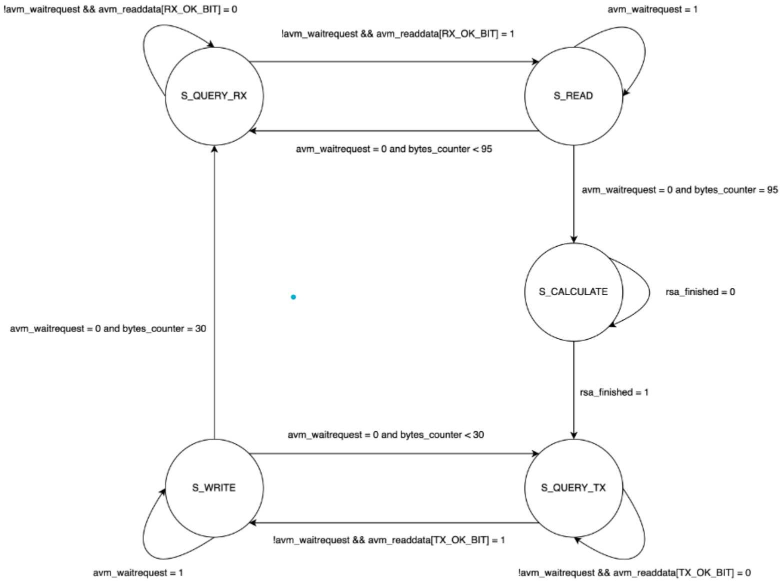
3. **Rsa256Core: D**o rsa256_mont(N, y, d)



- S_IDLE: wait for master module call
- S_PREP: do modulo_product(N, a). if done, go to S_MONT
- S_MONT: do montgomery_algorithm(N, m, t) and montgomery_algorithm(N, t, t) parallelly. if both done, go to S_MONT

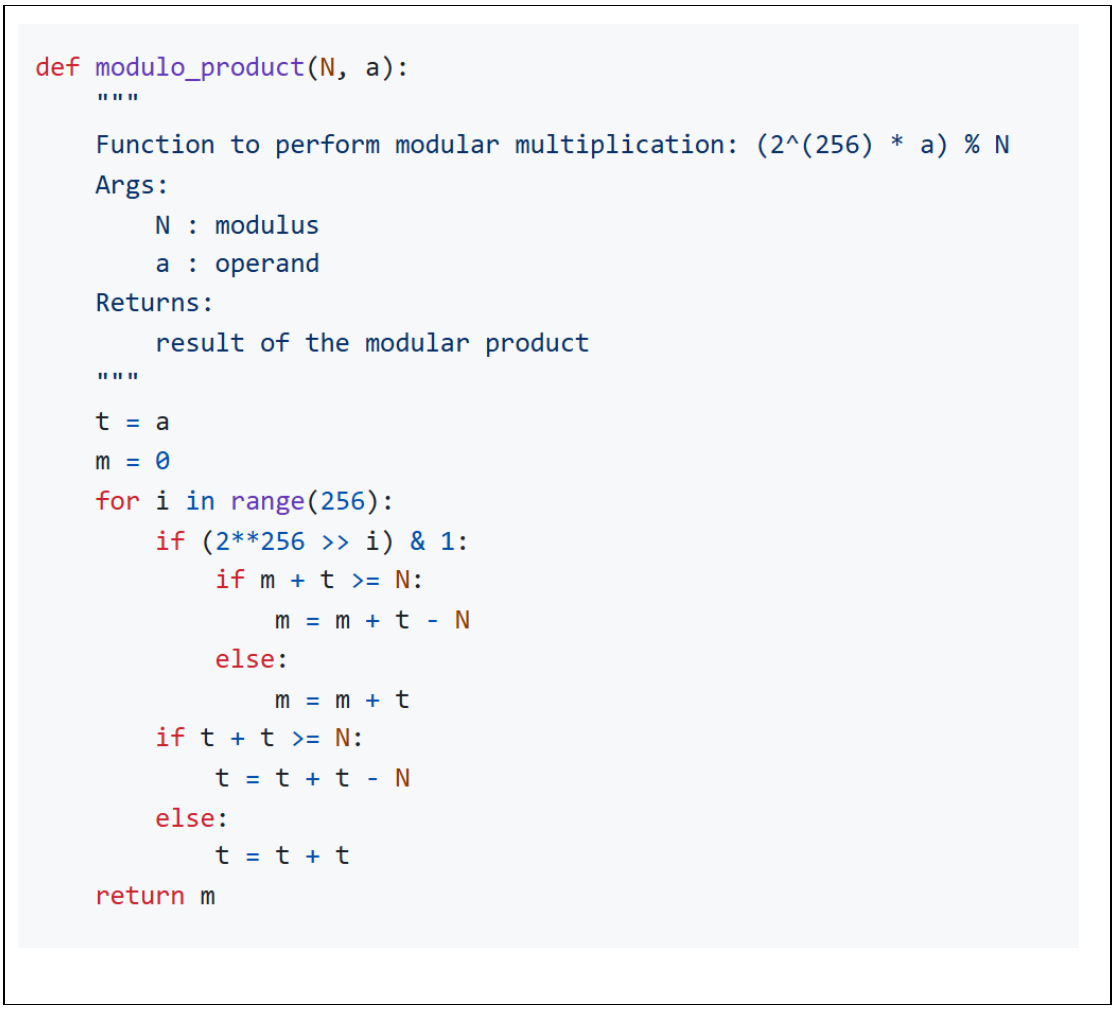
- S_CALC: do the for-loop in the pseudocode, need 256 cycles. output the result and set the finish signal to 1 in the last cycle

4. Wrapper

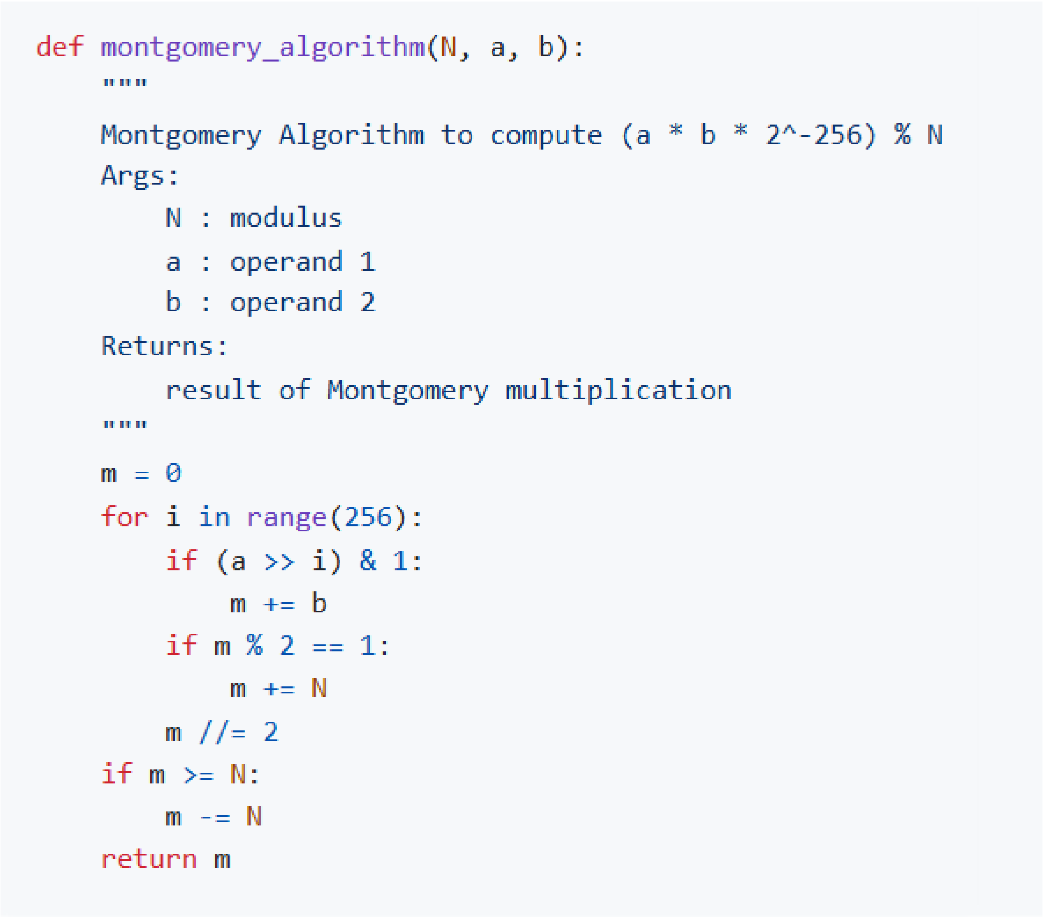

!avm_waitrequest && avm_readdata[RX_OK_BIT] = 0
!avm_waitrequest && avm_readdata[RX_OK_BIT] = 1
avm_waitrequest = 1
S_QUERY_RX
S_READ
avm_waitrequest = 0 and bytes_counter < 95
avm_waitrequest = 0 and bytes_counter = 95
S_CALCULATE
rsa_finished = 0
avm_waitrequest = 0 and bytes_counter = 30
rsa_finished = 1
avm_waitrequest = 0 and bytes_counter < 30
S_WRITE
S_QUERY_TX
!avm_waitrequest && avm_readdata[TX_OK_BIT] = 1
avm_waitrequest = 1
!avm_waitrequest && avm_readdata[TX_OK_BIT] = 0

Algorithm

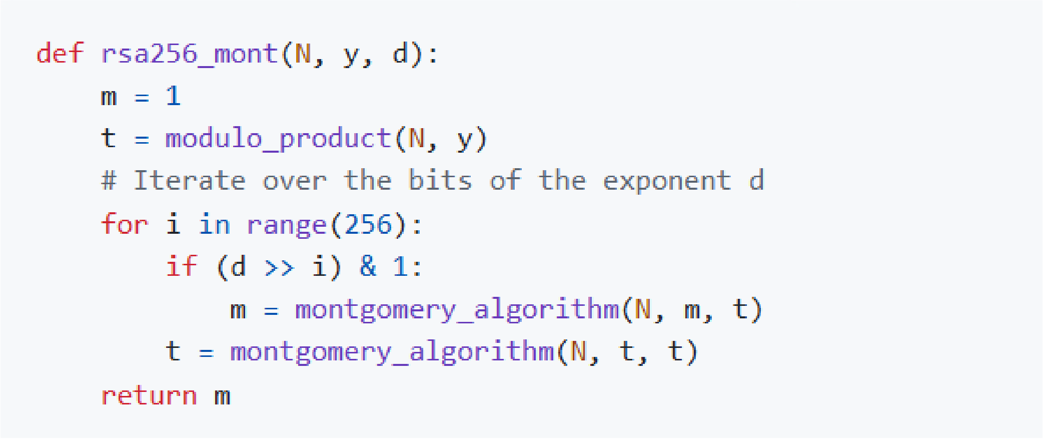
below algorithm is pseudocode,



```python
def modulo_product(N, a):
    """
    Function to perform modular multiplication: (2^(256) * a) % N
    Args:
        N : modulus
        a : operand
    Returns:
        result of the modular product
    """
    t = a
    m = 0
    for i in range(256):
        if (2**256 >> i) & 1:
            if m + t >= N:
                m = m + t - N
            else:
                m = m + t
        if t + t >= N:
            t = t + t - N
        else:
            t = t + t
    return m
```

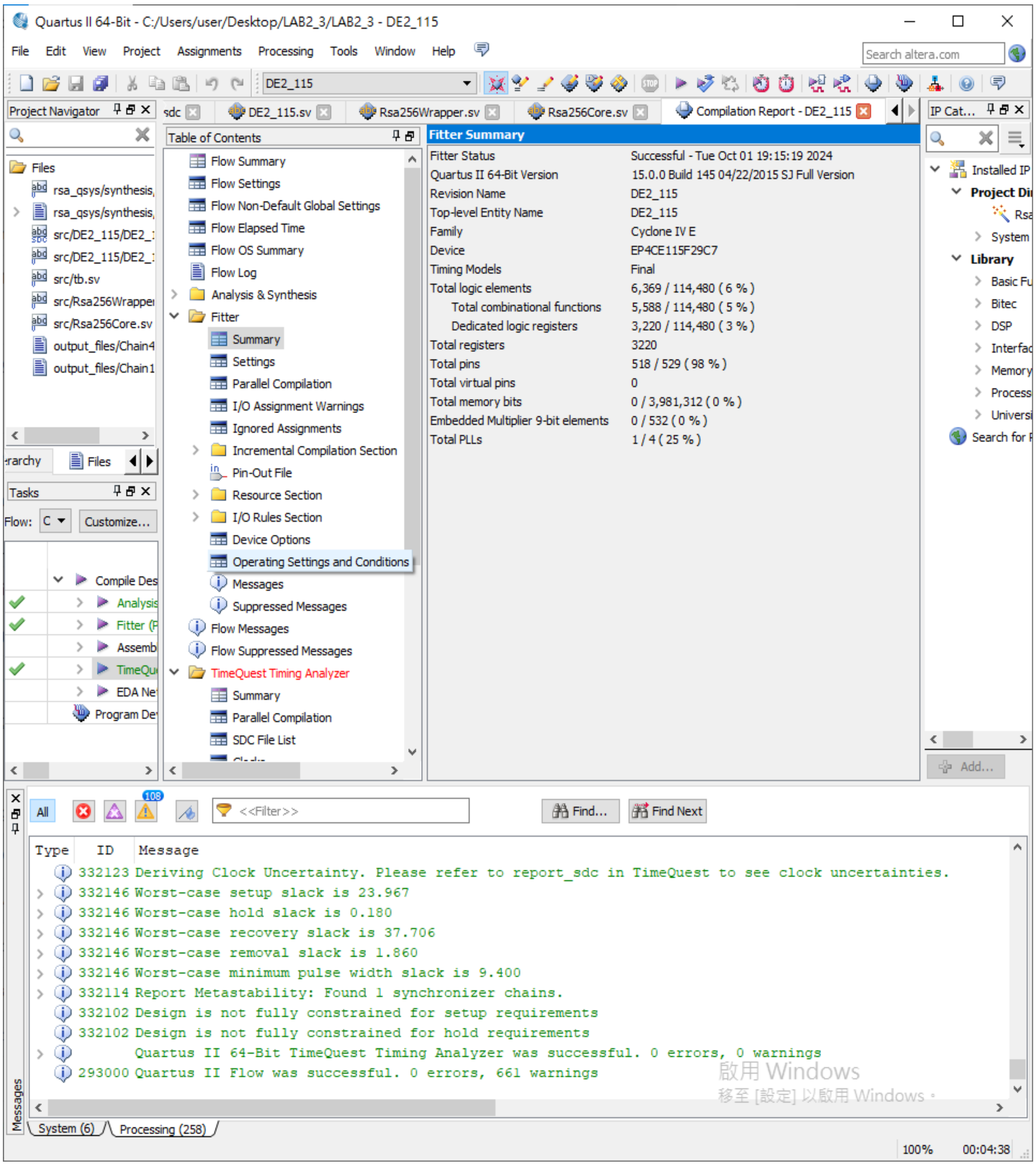


```python
def montgomery_algorithm(N, a, b):
    """
    Montgomery Algorithm to compute (a * b * 2^-256) % N
    Args:
        N : modulus
        a : operand 1
        b : operand 2
    Returns:
        result of Montgomery multiplication
    """
    m = 0
    for i in range(256):
        if (a >> i) & 1:
            m += b
        if m % 2 == 1:
            m += N
        m //= 2
    if m >= N:
        m -= N
    return m
```



```python
def rsa256_mont(N, y, d):
    m = 1
    t = modulo_product(N, y)
    # Iterate over the bits of the exponent d
    for i in range(256):
        if (d >> i) & 1:
            m = montgomery_algorithm(N, m, t)
        t = montgomery_algorithm(N, t, t)
    return m
```

Fitter Summary



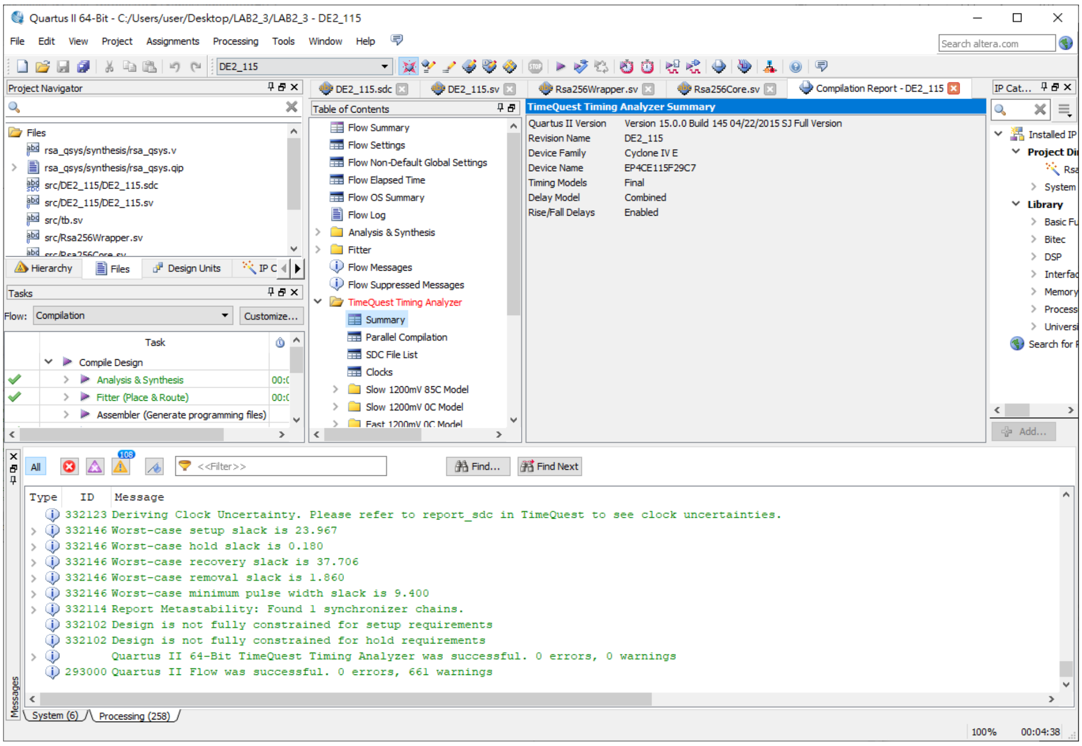
Fitter Summary

Fitter Status	Successful - Tue Oct 01 19:15:19 2024
Quartus II 64-Bit Version	15.0.0 Build 145 04/22/2015 SJ Full Version
Revision Name	DE2_115
Top-level Entity Name	DE2_115
Family	Cyclone IV E
Device	EP4CE115F29C7
Timing Models	Final
Total logic elements	6,369 / 114,480 (6 %)
Total combinational functions	5,588 / 114,480 (5 %)
Dedicated logic registers	3,220 / 114,480 (3 %)
Total registers	3220
Total pins	518 / 529 (98 %)
Total virtual pins	0
Total memory bits	0 / 3,981,312 (0 %)
Embedded Multiplier 9-bit elements	0 / 532 (0 %)
Total PLLs	1 / 4 (25 %)

```
Type  ID     Message
      332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
      332146 Worst-case setup slack is 23.967
      332146 Worst-case hold slack is 0.180
      332146 Worst-case recovery slack is 37.706
      332146 Worst-case removal slack is 1.860
      332146 Worst-case minimum pulse width slack is 9.400
      332114 Report Metastability: Found 1 synchronizer chains.
      332102 Design is not fully constrained for setup requirements
      332102 Design is not fully constrained for hold requirements
             Quartus II 64-Bit TimeQuest Timing Analyzer was successful. 0 errors, 0 warnings
      293000 Quartus II Flow was successful. 0 errors, 661 warnings
```

Timing Analyzer

summary

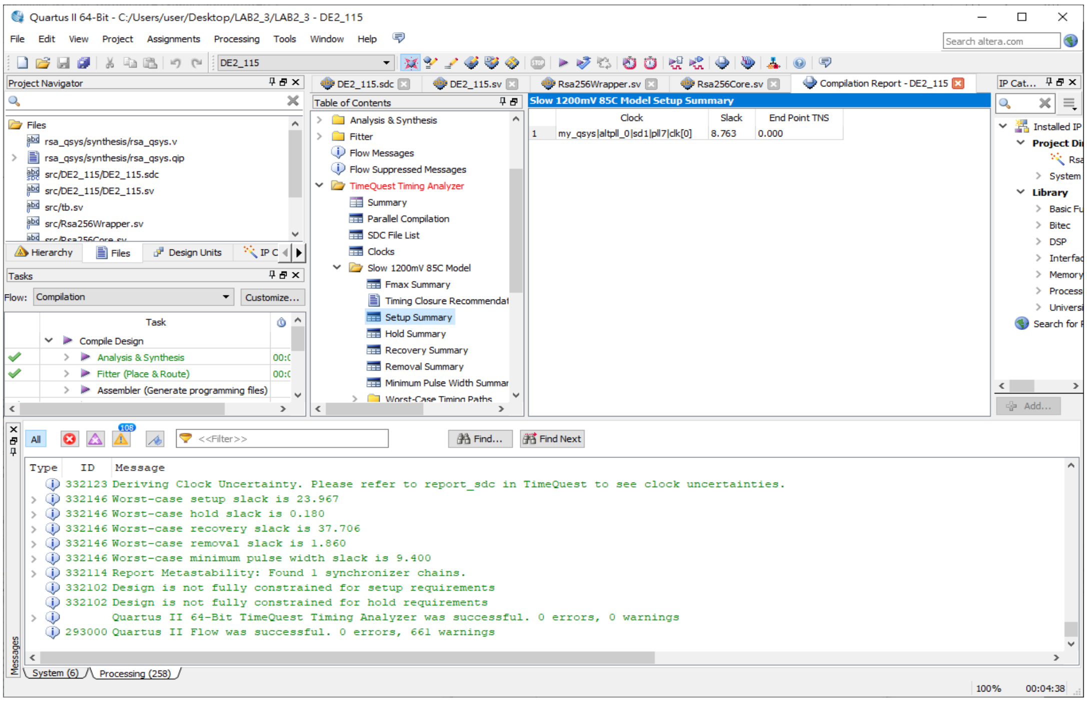


TimeQuest Timing Analyzer Summary

Quartus II Version	Version 15.0.0 Build 145 04/22/2015 SJ Full Version
Revision Name	DE2_115
Device Family	Cyclone IV E
Device Name	EP4CE115F29C7
Timing Models	Final
Delay Model	Combined
Rise/Fall Delays	Enabled

```
Type  ID    Message
      332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
      332146 Worst-case setup slack is 23.967
      332146 Worst-case hold slack is 0.180
      332146 Worst-case recovery slack is 37.706
      332146 Worst-case removal slack is 1.860
      332146 Worst-case minimum pulse width slack is 9.400
      332114 Report Metastability: Found 1 synchronizer chains.
      332102 Design is not fully constrained for setup requirements
      332102 Design is not fully constrained for hold requirements
             Quartus II 64-Bit TimeQuest Timing Analyzer was successful. 0 errors, 0 warnings
      293000 Quartus II Flow was successful. 0 errors, 661 warnings
```

setup summary

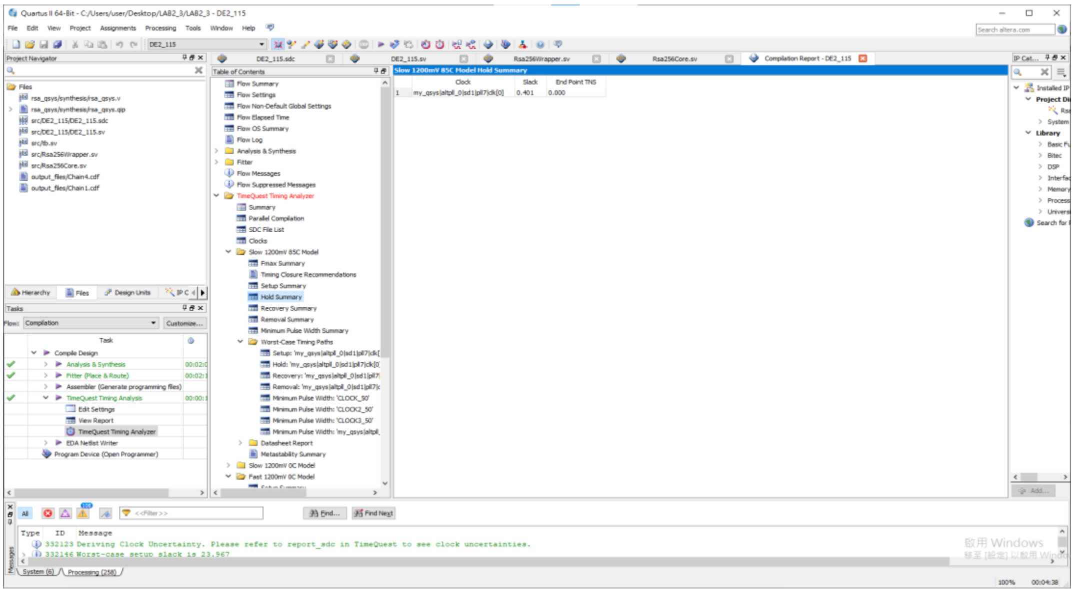


Slow 1200mV 85C Model Setup Summary

	Clock	Slack	End Point TNS
1	my_qsys|altpll_0|sd1|pll7|clk[0]	8.763	0.000

```
Type  ID    Message
      332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
      332146 Worst-case setup slack is 23.967
      332146 Worst-case hold slack is 0.180
      332146 Worst-case recovery slack is 37.706
      332146 Worst-case removal slack is 1.860
      332146 Worst-case minimum pulse width slack is 9.400
      332114 Report Metastability: Found 1 synchronizer chains.
      332102 Design is not fully constrained for setup requirements
      332102 Design is not fully constrained for hold requirements
             Quartus II 64-Bit TimeQuest Timing Analyzer was successful. 0 errors, 0 warnings
      293000 Quartus II Flow was successful. 0 errors, 661 warnings
```

hold

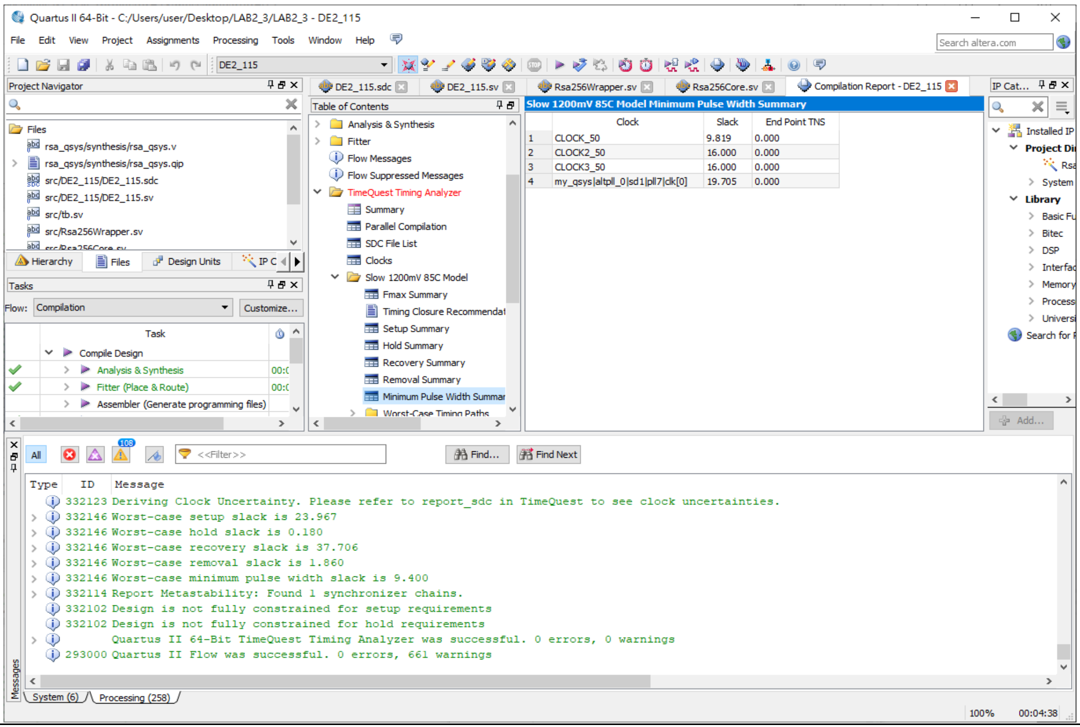


Quartus II 64-Bit - C:/Users/user/Desktop/LAB2_3/LAB2_3 - DE2_115

Slow 1200mV 85C Model Hold Summary

	Clock	Slack	End Point TNS
1	my_qsys|altpll_0|sd1|pll7|clk[0]	0.401	0.000

```
Type  ID     Message
      332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
>     332146 Worst-case setup slack is 23.967
```

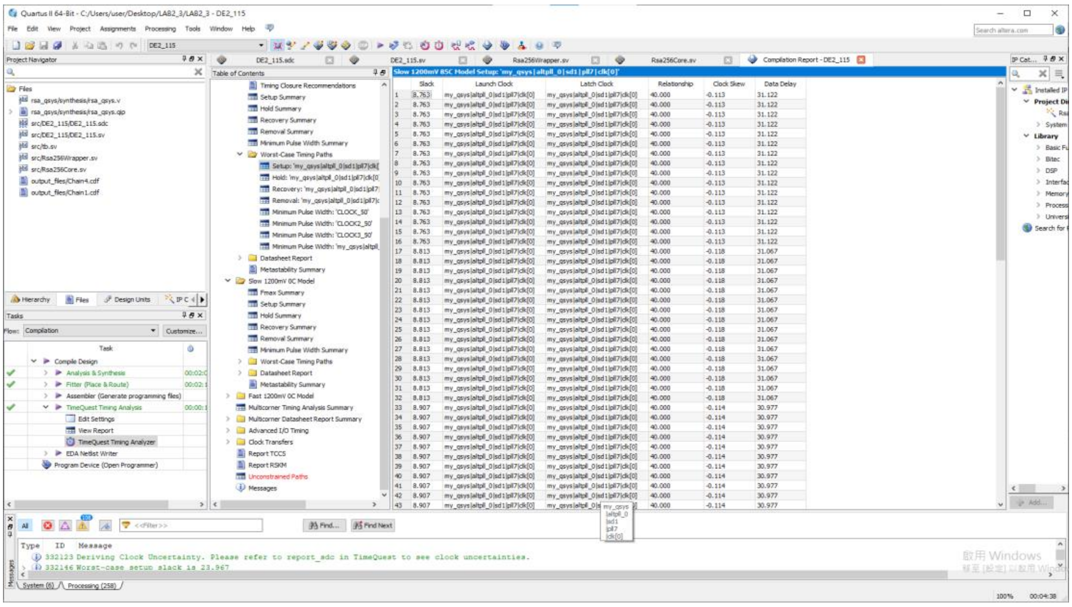


Quartus II 64-Bit - C:/Users/user/Desktop/LAB2_3/LAB2_3 - DE2_115

Slow 1200mV 85C Model Minimum Pulse Width Summary

	Clock	Slack	End Point TNS
1	CLOCK_50	9.819	0.000
2	CLOCK2_50	16.000	0.000
3	CLOCK3_50	16.000	0.000
4	my_qsys|altpll_0|sd1|pll7|clk[0]	19.705	0.000

```
Type  ID     Message
      332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
>     332146 Worst-case setup slack is 23.967
>     332146 Worst-case hold slack is 0.180
>     332146 Worst-case recovery slack is 37.706
>     332146 Worst-case removal slack is 1.860
>     332146 Worst-case minimum pulse width slack is 9.400
>     332114 Report Metastability: Found 1 synchronizer chains.
      332102 Design is not fully constrained for setup requirements
      332102 Design is not fully constrained for hold requirements
>            Quartus II 64-Bit TimeQuest Timing Analyzer was successful. 0 errors, 0 warnings
      293000 Quartus II Flow was successful. 0 errors, 661 warnings
```

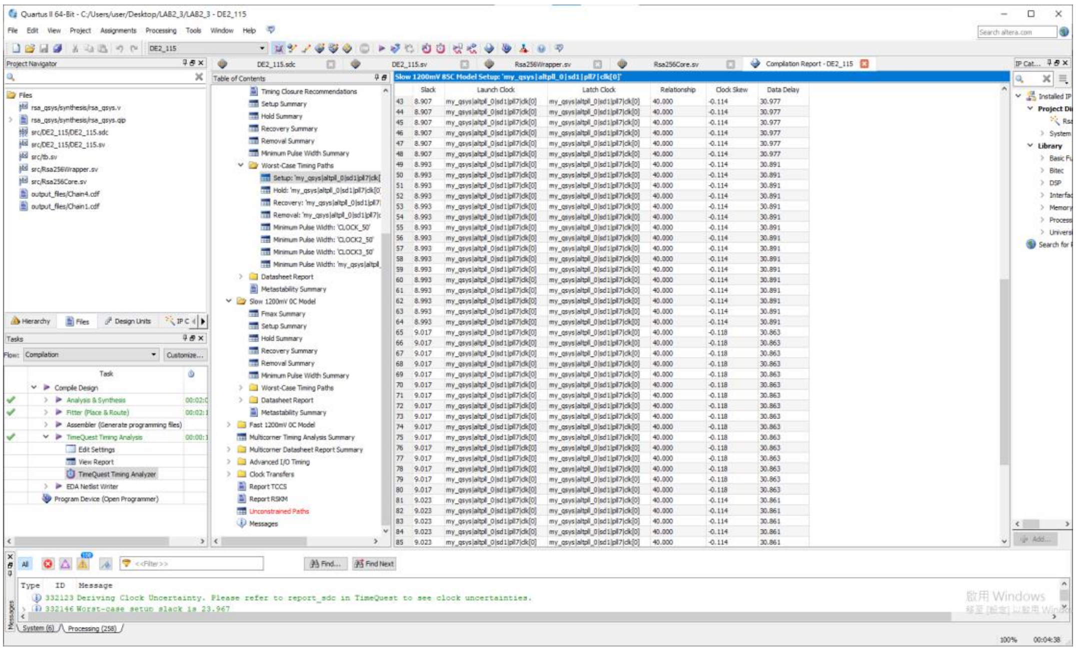


Quartus II 64-Bit - C:/Users/user/Desktop/LAB2_3/LAB2_3 - DE2_115

Slow 1200mV 85C Model Setup: 'my_qsys|altpll_0|sd1|pll7|clk[0]'

	Slack	Launch Clock	Latch Clock	Relationship	Clock Skew	Data Delay
1	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
2	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
3	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
4	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
5	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
6	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
7	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
8	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
9	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
10	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
11	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
12	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
13	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
14	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
15	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
16	8.763	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.113	31.122
17	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
18	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
19	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
20	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
21	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
22	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
23	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
24	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
25	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
26	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
27	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
28	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
29	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
30	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
31	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
32	8.813	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	31.067
33	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
34	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
35	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
36	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
37	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
38	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
39	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
40	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
41	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
42	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
43	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977

```
Type  ID     Message
      332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
      332146 Worst-case setup slack is 23.967
```

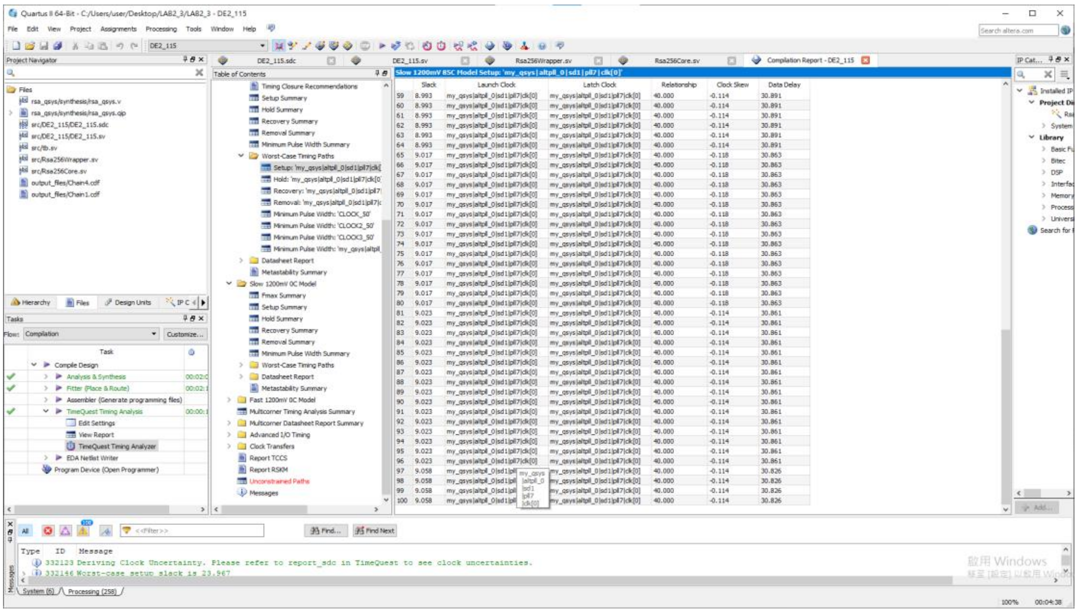


Quartus II 64-Bit - C:/Users/user/Desktop/LAB2_3/LAB2_3 - DE2_115

Slow 1200mV 85C Model Setup: 'my_qsys|altpll_0|sd1|pll7|clk[0]'

	Slack	Launch Clock	Latch Clock	Relationship	Clock Skew	Data Delay
43	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
44	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
45	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
46	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
47	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
48	8.907	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.977
49	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
50	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
51	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
52	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
53	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
54	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
55	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
56	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
57	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
58	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
59	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
60	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
61	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
62	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
63	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
64	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
65	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
66	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
67	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
68	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
69	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
70	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
71	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
72	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
73	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
74	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
75	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
76	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
77	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
78	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
79	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
80	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
81	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
82	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
83	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
84	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
85	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861

```
Type  ID     Message
      332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
      332146 Worst-case setup slack is 23.967
```

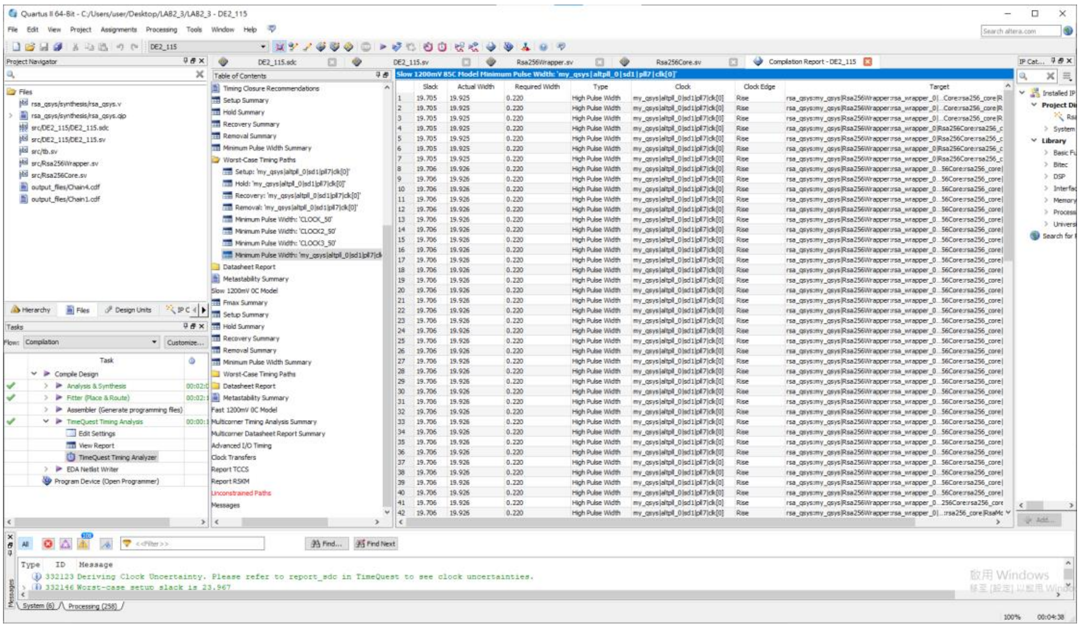


Quartus II 64-Bit - C:/Users/user/Desktop/LAB2_3/LAB2_3 - DE2_115

Slow 1200mV 85C Model Setup: 'my_qsys|altpll_0|sd1|pll7|clk[0]'

	Slack	Launch Clock	Latch Clock	Relationship	Clock Skew	Data Delay
59	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
60	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
61	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
62	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
63	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
64	8.993	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.891
65	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
66	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
67	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
68	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
69	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
70	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
71	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
72	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
73	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
74	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
75	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
76	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
77	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
78	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
79	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
80	9.017	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.118	30.863
81	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
82	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
83	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
84	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
85	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
86	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
87	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
88	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
89	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
90	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
91	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
92	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
93	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
94	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
95	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
96	9.023	my_qsys|altpll_0|sd1|pll7|clk[0]	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.861
97	9.058	my_qsys|altpll_0|sd1|pl	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.826
98	9.058	my_qsys|altpll_0|sd1|pl	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.826
99	9.058	my_qsys|altpll_0|sd1|pl	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.826
100	9.058	my_qsys|altpll_0|sd1|pl	my_qsys|altpll_0|sd1|pll7|clk[0]	40.000	-0.114	30.826

```
Type   ID     Message
       332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
       332146 Worst-case setup slack is 23.967
```

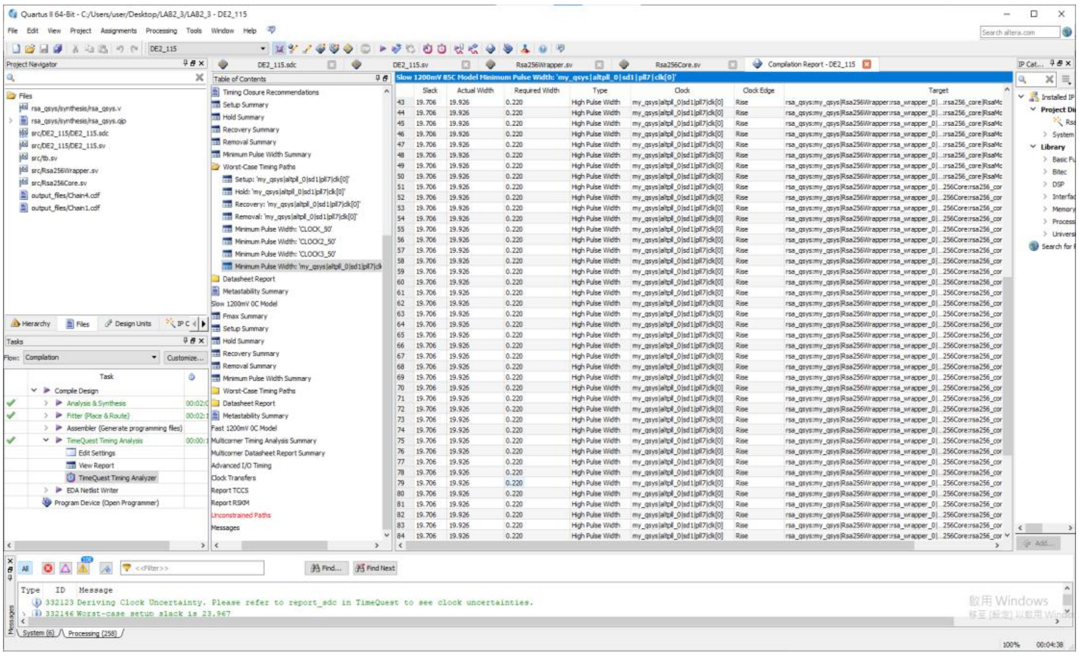


Quartus II 64-Bit - C:/Users/user/Desktop/LAB2_3/LAB2_3 - DE2_115

Slow 1200mV 85C Model Minimum Pulse Width: 'my_qsys|altpll_0|sd1|pll7|clk[0]'

	Slack	Actual Width	Required Width	Type	Clock	Clock Edge	Target
1	19.705	19.925	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...Core:rsa256_core|R
2	19.705	19.925	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...Core:rsa256_core|R
3	19.705	19.925	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...Core:rsa256_core|R
4	19.705	19.925	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|Rsa256Core:rsa256_c
5	19.705	19.925	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|Rsa256Core:rsa256_c
6	19.705	19.925	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|Rsa256Core:rsa256_c
7	19.705	19.925	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|Rsa256Core:rsa256_c
8	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
9	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
10	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
11	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
12	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
13	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
14	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
15	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
16	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
17	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
18	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
19	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
20	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
21	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
22	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
23	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
24	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
25	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
26	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
27	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
28	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
29	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
30	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
31	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
32	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
33	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
34	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
35	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
36	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
37	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
38	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
39	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
40	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...56Core:rsa256_core|
41	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0...256Core:rsa256_core
42	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...:rsa256_core|RsaMc

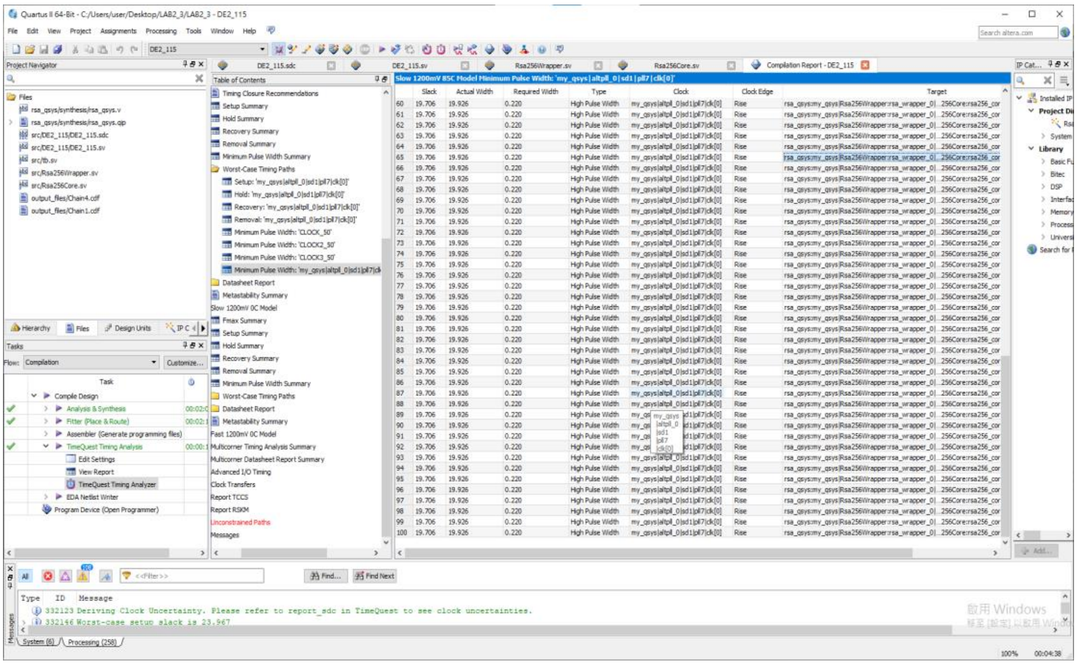
```
Type   ID     Message
       332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
       332146 Worst-case setup slack is 23.967
```


Quartus II 64-Bit - C:/Users/user/Desktop/LAB2_3/LAB2_3 - DE2_115
File Edit View Project Assignments Processing Tools Window Help
DE2_115
Project Navigator
Files
rsa_qsys/synthesis/rsa_qsys.v
rsa_qsys/synthesis/rsa_qsys.qip
src/DE2_115/DE2_115.sdc
src/DE2_115/DE2_115.sv
src/tb.sv
src/Rsa256Wrapper.sv
src/Rsa256Core.sv
output_files/Chain4.cdf
output_files/Chain1.cdf
Hierarchy Files Design Units IP C
Tasks
Flow: Compilation Customize...
Task
Compile Design
Analysis & Synthesis
Fitter (Place & Route)
Assembler (Generate programming files)
TimeQuest Timing Analysis
Edit Settings
View Report
TimeQuest Timing Analyzer
EDA Netlist Writer
Program Device (Open Programmer)
Table of Contents
Timing Closure Recommendations
Setup Summary
Hold Summary
Recovery Summary
Removal Summary
Minimum Pulse Width Summary
Worst-Case Timing Paths
Setup: 'my_qsys|altpll_0|sd1|pll7|clk[0]'
Hold: 'my_qsys|altpll_0|sd1|pll7|clk[0]'
Recovery: 'my_qsys|altpll_0|sd1|pll7|clk[0]'
Removal: 'my_qsys|altpll_0|sd1|pll7|clk[0]'
Minimum Pulse Width: 'CLOCK_50'
Minimum Pulse Width: 'CLOCK2_50'
Minimum Pulse Width: 'CLOCK3_50'
Minimum Pulse Width: 'my_qsys|altpll_0|sd1|pll7|clk
Datasheet Report
Metastability Summary
Slow 1200mV 0C Model
Fmax Summary
Setup Summary
Hold Summary
Recovery Summary
Removal Summary
Minimum Pulse Width Summary
Worst-Case Timing Paths
Datasheet Report
Metastability Summary
Fast 1200mV 0C Model
Multicorner Timing Analysis Summary
Multicorner Datasheet Report Summary
Advanced I/O Timing
Clock Transfers
Report TCCS
Report RSKM
Unconstrained Paths
Messages
DE2_115.sdc
DE2_115.sv
Rsa256Wrapper.sv
Rsa256Core.sv
Compilation Report - DE2_115
IP Cat...
Installed IP
Project Di
System
Library
Basic Fu
Bitec
DSP
Interfac
Memory
Process
Univers
Search for
Add...
All
<<Filter>>
Find...
Find Next
System (6)
Processing (258)
啟用 Windows
移至 [設定] 以啟用 Windows
100%
00:04:38

Slow 1200mV 85C Model Minimum Pulse Width: 'my_qsys|altpll_0|sd1|pll7|clk[0]'

	Slack	Actual Width	Required Width	Type	Clock	Clock Edge	Target
43	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...:rsa256_core|RsaMc
44	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...:rsa256_core|RsaMc
45	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...:rsa256_core|RsaMc
46	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...:rsa256_core|RsaMc
47	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...:rsa256_core|RsaMc
48	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...:rsa256_core|RsaMc
49	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...:rsa256_core|RsaMc
50	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...:rsa256_core|RsaMc
51	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
52	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
53	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
54	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
55	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
56	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
57	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
58	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
59	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
60	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
61	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
62	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
63	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
64	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
65	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
66	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
67	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
68	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
69	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
70	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
71	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
72	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
73	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
74	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
75	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
76	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
77	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
78	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
79	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
80	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
81	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
82	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
83	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
84	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor

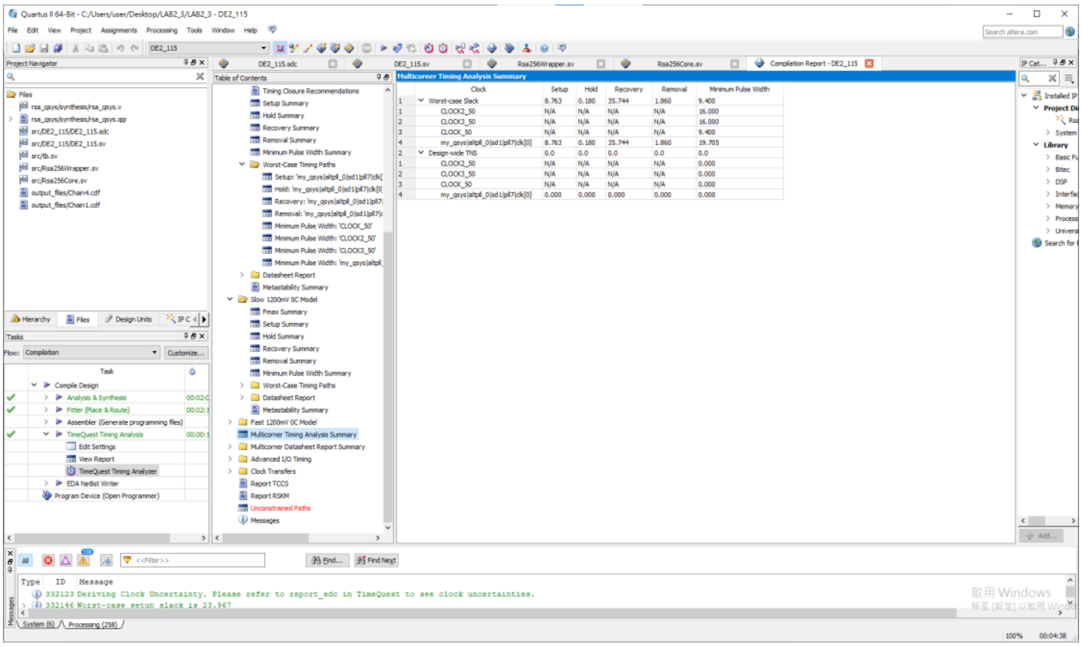
```
Type  ID   Message
   332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
>  332146 Worst-case setup slack is 23.967
```


Quartus II 64-Bit - C:/Users/user/Desktop/LAB2_3/LAB2_3 - DE2_115
File Edit View Project Assignments Processing Tools Window Help
DE2_115
Project Navigator
Files
Table of Contents
Minimum Pulse Width: 'my_qsys|altpll_0|sd1|pll7|clk
Compilation Report - DE2_115
IP Cat...
my_qsys
|altpll_0
|sd1
|pll7
|clk[0]
System (6)
Processing (258)
啟用 Windows
移至 [設定] 以啟用 Windows
100%
00:04:38

Slow 1200mV 85C Model Minimum Pulse Width: 'my_qsys|altpll_0|sd1|pll7|clk[0]'

	Slack	Actual Width	Required Width	Type	Clock	Clock Edge	Target
60	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
61	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
62	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
63	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
64	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
65	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
66	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
67	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
68	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
69	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
70	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
71	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
72	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
73	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
74	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
75	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
76	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
77	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
78	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
79	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
80	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
81	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
82	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
83	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
84	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
85	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
86	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
87	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
88	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
89	19.706	19.926	0.220	High Pulse Width	my_qs d1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
90	19.706	19.926	0.220	High Pulse Width	my_qs d1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
91	19.706	19.926	0.220	High Pulse Width	my_qs d1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
92	19.706	19.926	0.220	High Pulse Width	my_qs d1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
93	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
94	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
95	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
96	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
97	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
98	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
99	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor
100	19.706	19.926	0.220	High Pulse Width	my_qsys|altpll_0|sd1|pll7|clk[0]	Rise	rsa_qsys:my_qsys|Rsa256Wrapper:rsa_wrapper_0|...256Core:rsa256_cor

```
Type  ID   Message
   332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
>  332146 Worst-case setup slack is 23.967
```

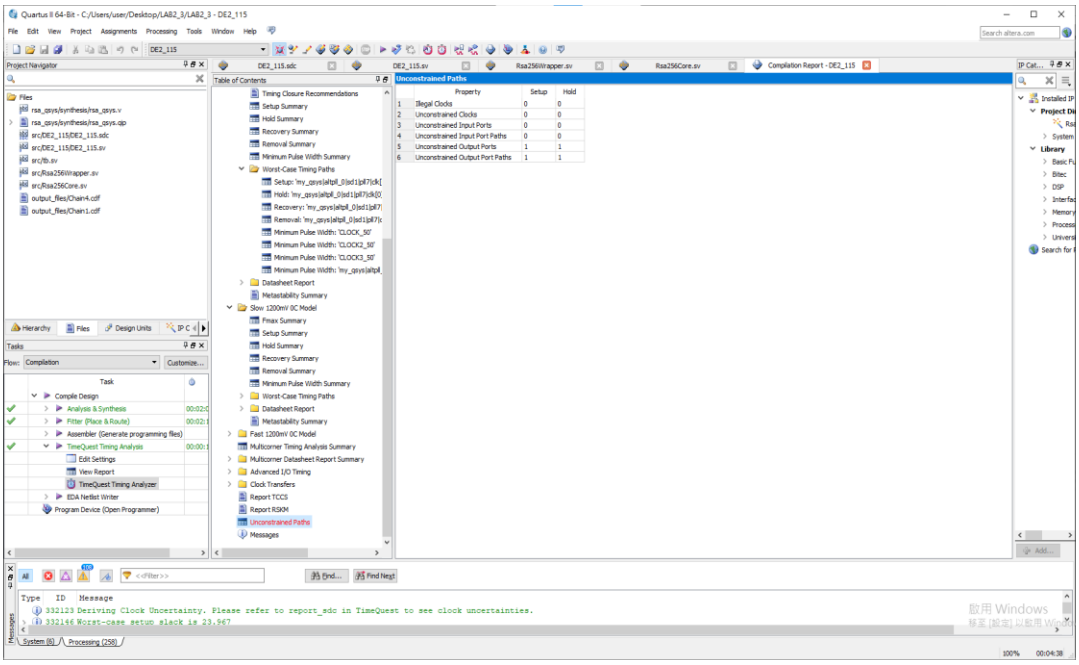


Quartus II 64-Bit - C:/Users/user/Desktop/LAB2_3/LAB2_3 - DE2_115

Multicorner Timing Analysis Summary

	Clock	Setup	Hold	Recovery	Removal	Minimum Pulse Width
1	Worst-case Slack	8.763	0.180	35.744	1.860	9.400
1	CLOCK2_50	N/A	N/A	N/A	N/A	16.000
2	CLOCK3_50	N/A	N/A	N/A	N/A	16.000
3	CLOCK_50	N/A	N/A	N/A	N/A	9.400
4	my_qsys|altpll_0|sd1|pll7|clk[0]	8.763	0.180	35.744	1.860	19.705
2	Design-wide TNS	0.0	0.0	0.0	0.0	0.0
1	CLOCK2_50	N/A	N/A	N/A	N/A	0.000
2	CLOCK3_50	N/A	N/A	N/A	N/A	0.000
3	CLOCK_50	N/A	N/A	N/A	N/A	0.000
4	my_qsys|altpll_0|sd1|pll7|clk[0]	0.000	0.000	0.000	0.000	0.000

```
Type  ID     Message
      332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
      332146 Worst-case setup slack is 23.967
```

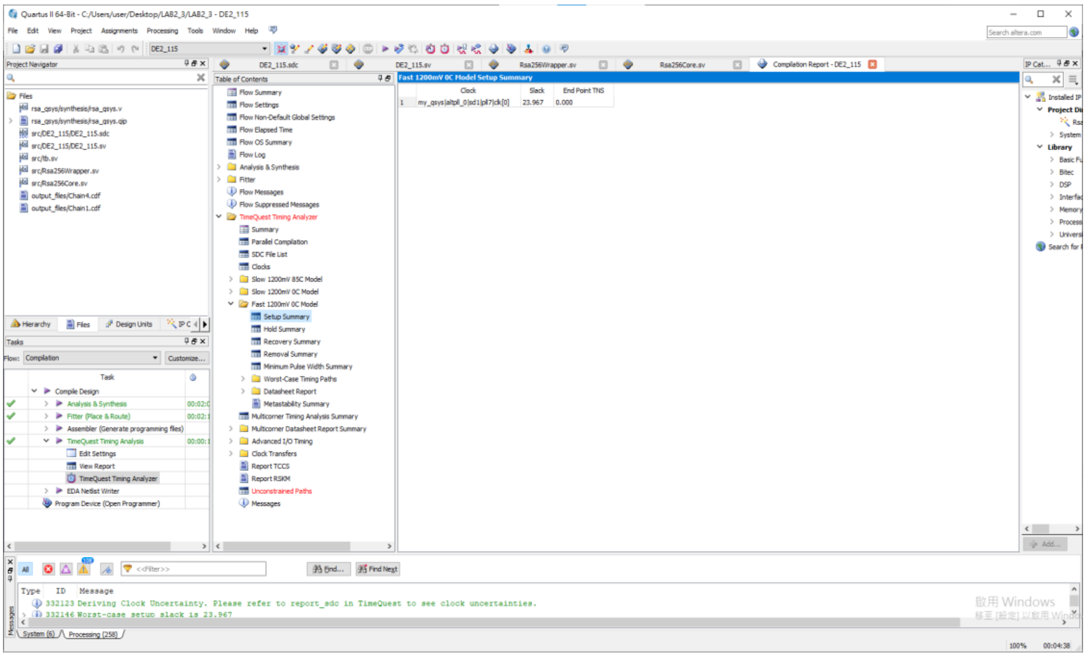


Quartus II 64-Bit - C:/Users/user/Desktop/LAB2_3/LAB2_3 - DE2_115

Unconstrained Paths

	Property	Setup	Hold
1	Illegal Clocks	0	0
2	Unconstrained Clocks	0	0
3	Unconstrained Input Ports	0	0
4	Unconstrained Input Port Paths	0	0
5	Unconstrained Output Ports	1	1
6	Unconstrained Output Port Paths	1	1

```
Type  ID     Message
      332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
      332146 Worst-case setup slack is 23.967
```

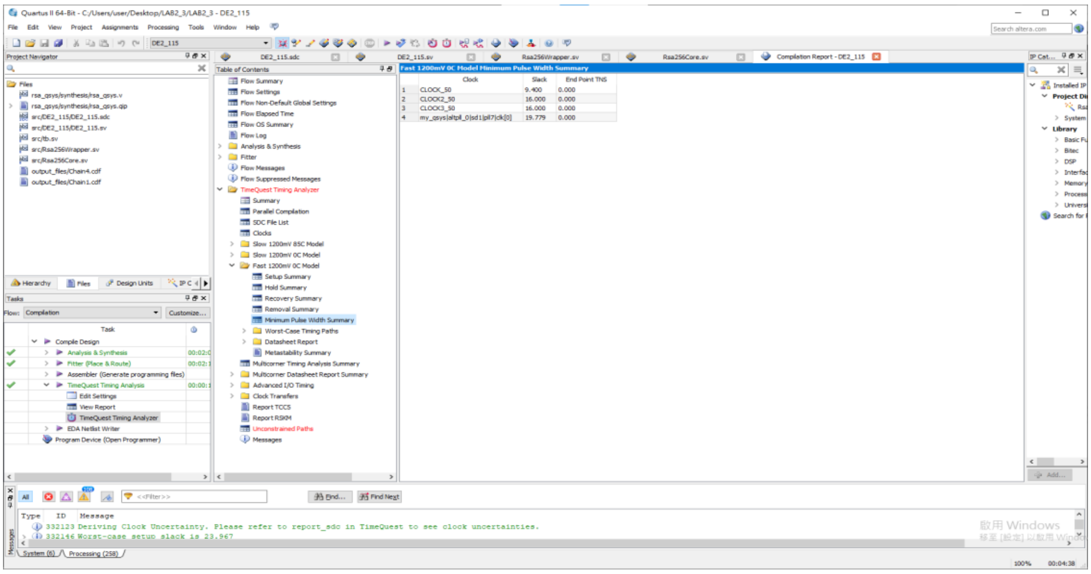


Quartus II 64-Bit - C:/Users/user/Desktop/LAB2_3/LAB2_3 - DE2_115

Fast 1200mV 0C Model Setup Summary

	Clock	Slack	End Point TNS
1	my_qsys|altpll_0|sd1|pll7|clk[0]	23.967	0.000

```
Type  ID     Message
      332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
      332146 Worst-case setup slack is 23.967
```



Quartus II 64-Bit - C:/Users/user/Desktop/LAB2_3/LAB2_3 - DE2_115

Fast 1200mV 0C Model Minimum Pulse Width Summary

	Clock	Slack	End Point TNS
1	CLOCK_50	9.400	0.000
2	CLOCK2_50	16.000	0.000
3	CLOCK3_50	16.000	0.000
4	my_qsys|altpll_0|sd1|pll7|clk[0]	19.779	0.000

```
Type  ID     Message
      332123 Deriving Clock Uncertainty. Please refer to report_sdc in TimeQuest to see clock uncertainties.
      332146 Worst-case setup slack is 23.967
```

遇到的問題與解決辦法，心得與建議

遇到的問題：很多簡報的部分沒有寫清楚，例如輸入格式，還有一個是 **Rsa256Core** 不能用 **always comb(**會報錯，助教可以補充在 **slide** 上**)**，以及一個是 **rst** 要改成 **reset**，還有一個是 **S_Write** 結束時，**bytecounter** 要設成 **64(**因為他沒有要再讀 **n,d)**，坑太多，族繁不及備載。

好險我們不會屈服於困難，和第二組並肩作戰，最後在實驗室搞了 **5** 個小時終於完成。

心得：做出來的那瞬間就是 **decipher 3** 的輸出值。