The first law of defensive programming:

When you have to defend, You have already lost هنگامی که شما باید دفاع کنید، قبلا از دست داده اید

* **Consistent objects**
  + Create consistent and complete objects ایجاد اشیاء سازگار و کامل
* Consistent mutations
  + All transitions must lead to complete and consistent state تمام گذرها باید به حالت کامل و سازگار منجر شوند
* **No primitive types**
  + Avoid excessive use of primitive types اجتناب از استفاده بیش از حد از انواع ابتدایی
  + Replace primitive types with custom domain types
  + Consequence : no defense
* **Function domains**
  + Satisfy mandatory conditions before making a function call رعایت شروط اجباری قبل از اجرای توابع

Try{

doSomethings();

}catch(InvalidOperationException){ 🡨 **Defensive code**

…

}

* Defensive design starts after this point
* **Defensive design**
  + Encapsulate state and operations
  + Unify positive and negative execution flows متحد کردن جریان های مثبت و منفی اجرا
* **Objects, not nulls**
  + Do not use null references
  + Without null : no defense
* **Rich domain models**
  + Immutability: Good servant, bad master تغییر ناپذیری : کلاینت خوب ، سرور بد
  + Restricted mutability for the best of both worlds تغییر پذیری محدود برای هر دو جهان
  + Historical modeling for powerful features
* **No exceptions**
  + Do not introduce alternate execution paths with exceptions
  + Do not use exceptions as just another heavyweight if-else
  + Better approach : pass either the result or the error in a discriminated union رویکرد بهتر: نتیجه یا خطای یک یونیون تبعیض آمیز را منتقل کنید

**Defensive code is a matter of choice**

**Cheap features: defined in code**

**Expensive features: defined in design**

**Traditional defensive techniques**

|  |  |
| --- | --- |
| Predictability پیش بینی پذیری | Reveal intention افشای قصد   * Method name * Argument name * Return value |
| **Certainty** یقین | Do not pass switches to a method   * No Boolean arguments * No enum arguments   Switches introduce uncertainty  Method should do one thing with absolute certainty متد باید یک چیز را با اطمینان مطلق انجام دهد |
| **Simplicity** سادگی | * Keep small number of method arguments * Keep the code short * Avoid branching when possible * Avoid code repetition |
| **Completeness** تکمیل | * **If** instruction should have a reasonable **else** branch * **Switch** instruction should have a reasonable **default** case |
| **Failing fast** شکست سریع | Do not let bad data propagate اجازه ندهید اطلاعات بد منتشر شود |
| **Handling errors** رسیدگی به خطاها | * Handle errors when day happen * Assert preconditions, postconditions and invariants * Add global exception handler to keep the application running |

**An experiment**

bool Contains(int[] arr, int srch)

{

for (int i = 0 ; i< arr.length(); i++)

{

if(arr[i] == srch)

{

return true;

}

}

return false;

}

-🡪

bool Contains(int[] arr, int srch)

{

Int end = ar.length-1;

Int last = ar[end];

Arr[end] = srch;

Int index = 0;

While(ar[index] != search)

{

Index = index +1;

}

Ar[end] = last;

Return index < end || last == srch;

}

Proactive caller: if(valid(x)) obj.Dosomethings(x);

Reactive caller : try{

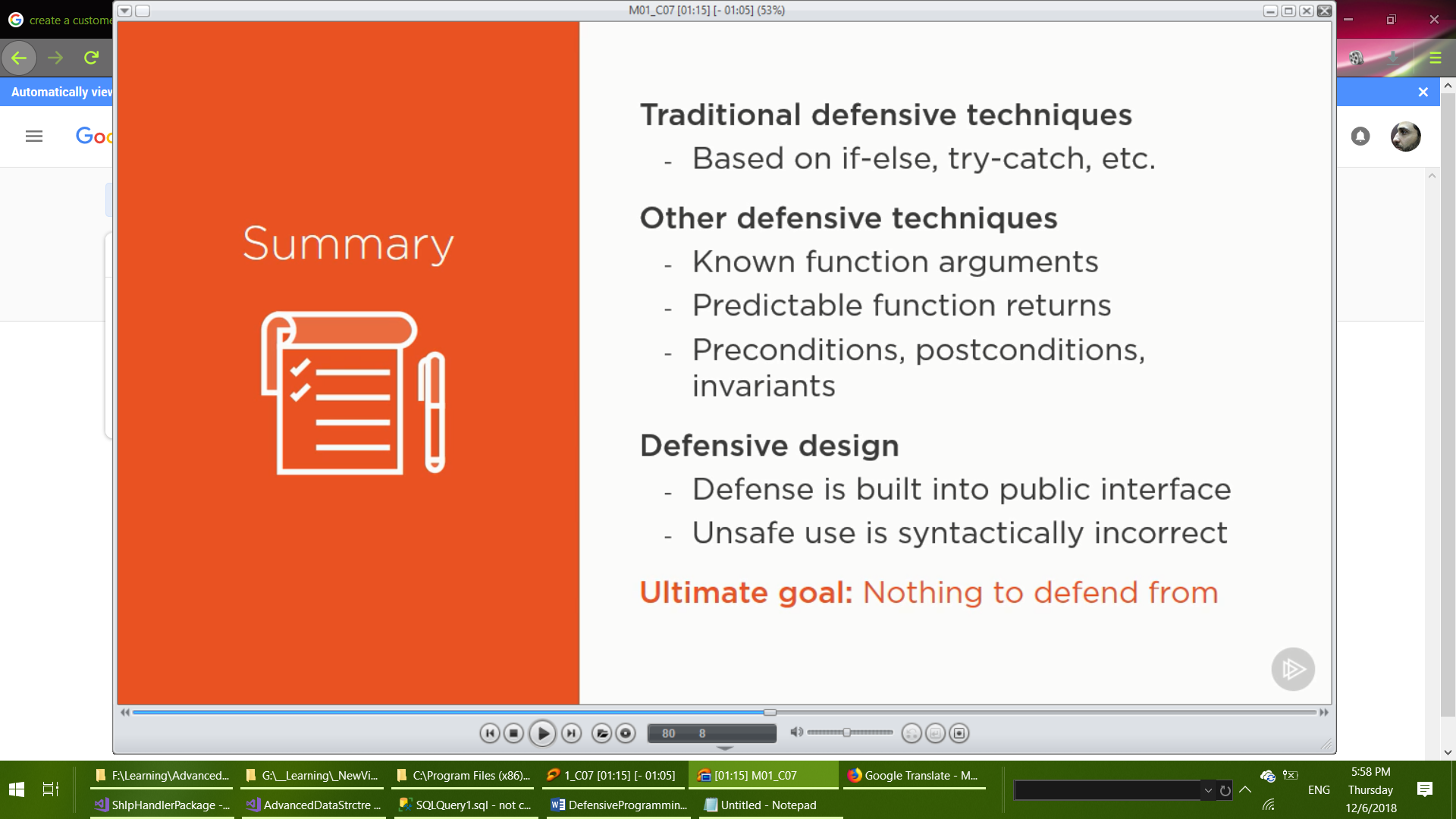
obj.Dosomethings(x);

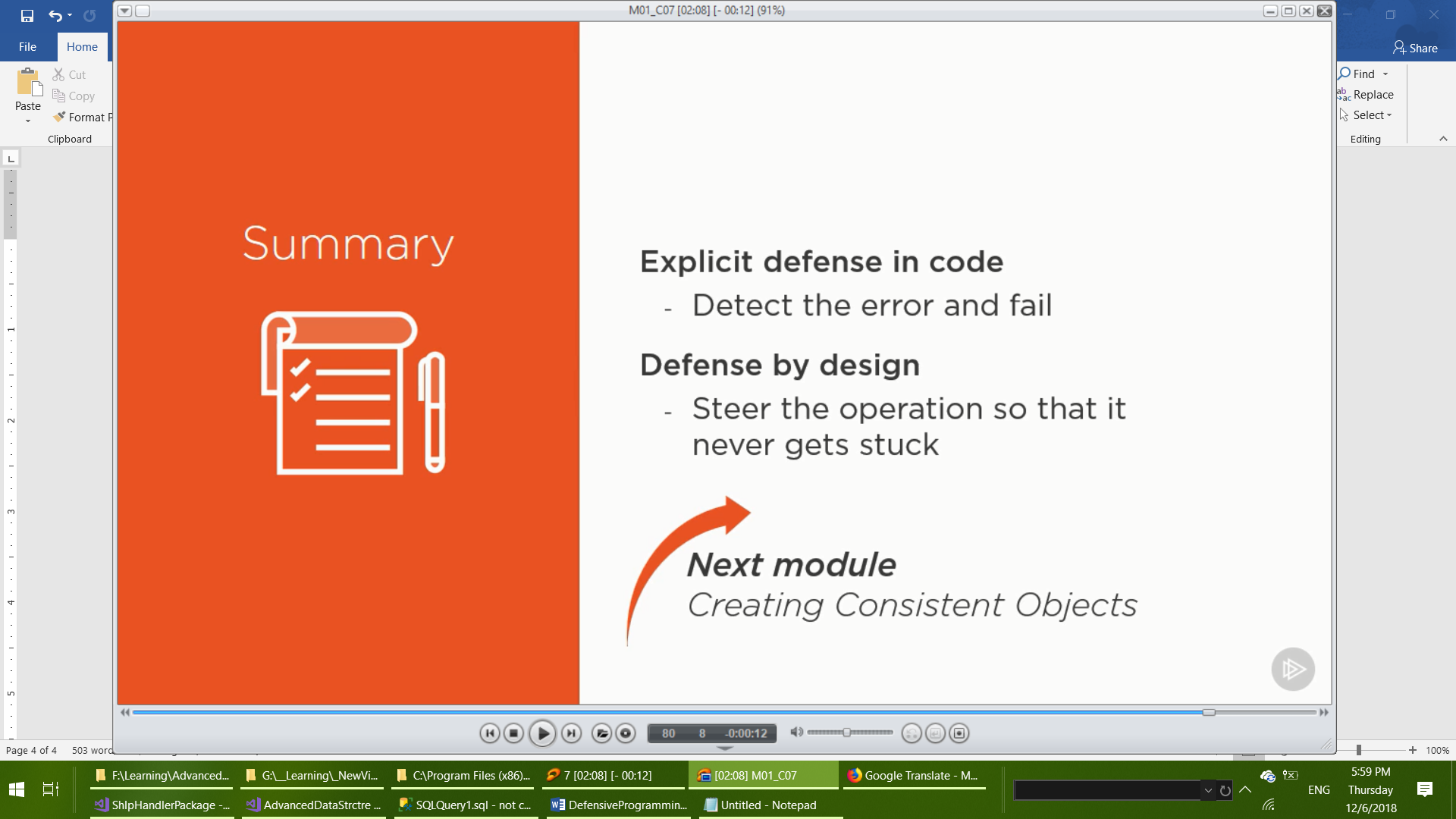
}catch…

Want to avoid error conditions

Produce design in which they can’t appear

**Software which repeatedly transforms one system state into the next system state**





Implicit parameter less constructor is the built-in factory function

Set numeric fields to zero, Boolean to false, references to null

In customized constructor: when invalid data are received new object must **not** constructed.

Constructor must ensure that only valid objects can be created.

The customized constructor caller will never be able to obtain an inconsistent object.

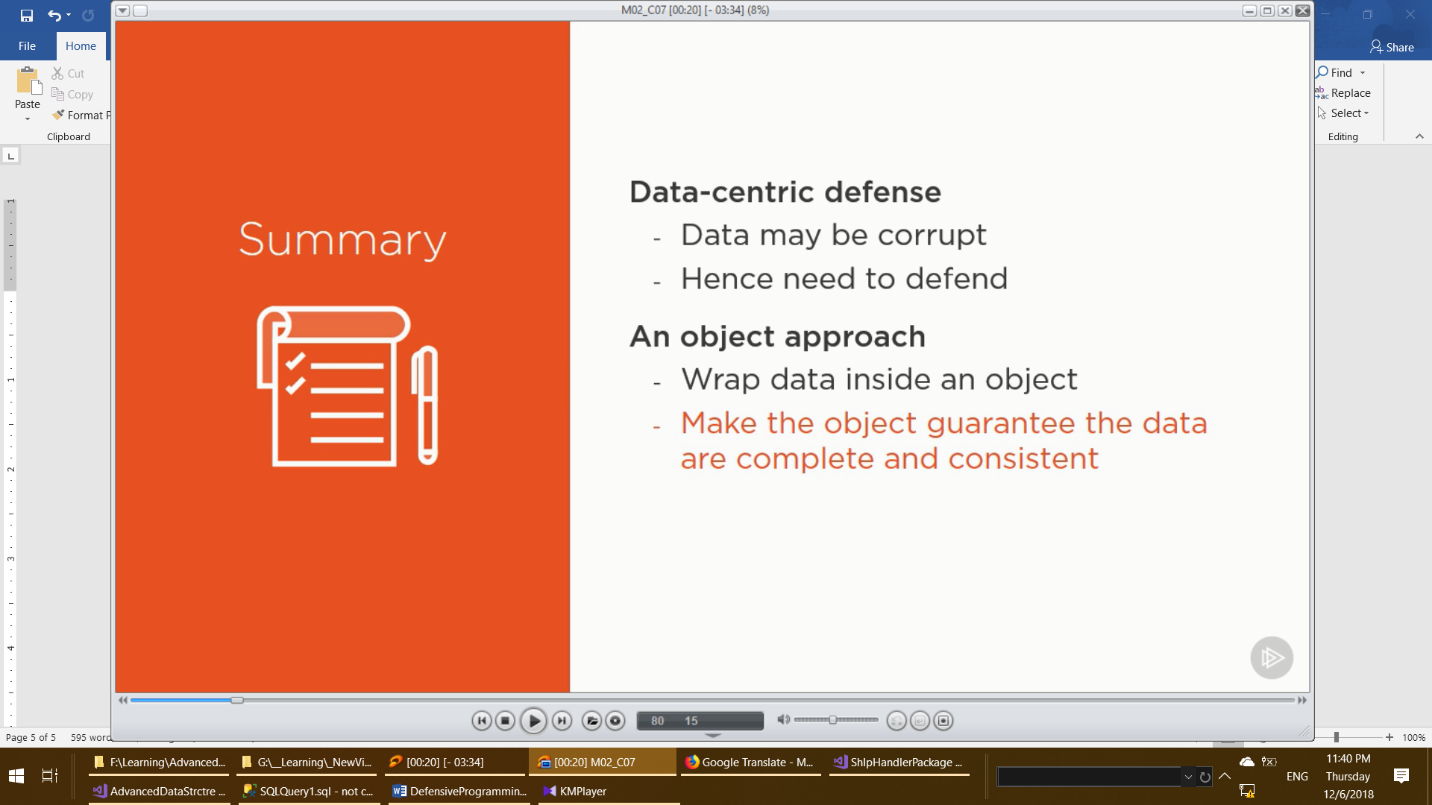
Provide your own factory function for every stateful objects.

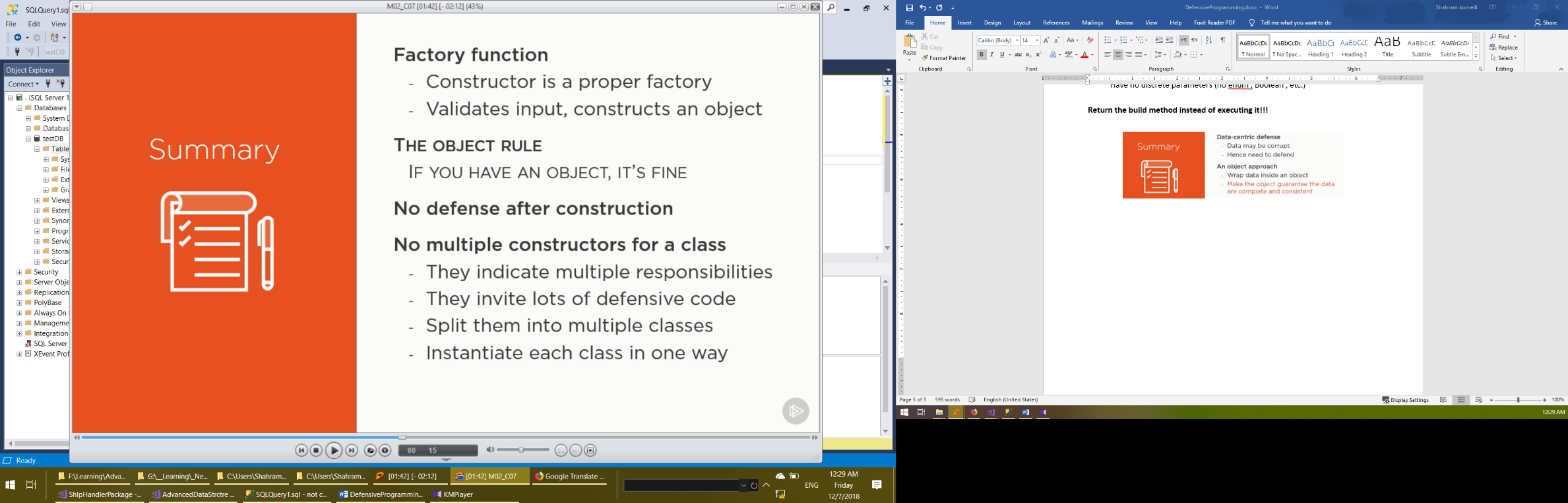
**Rules of thumb:**

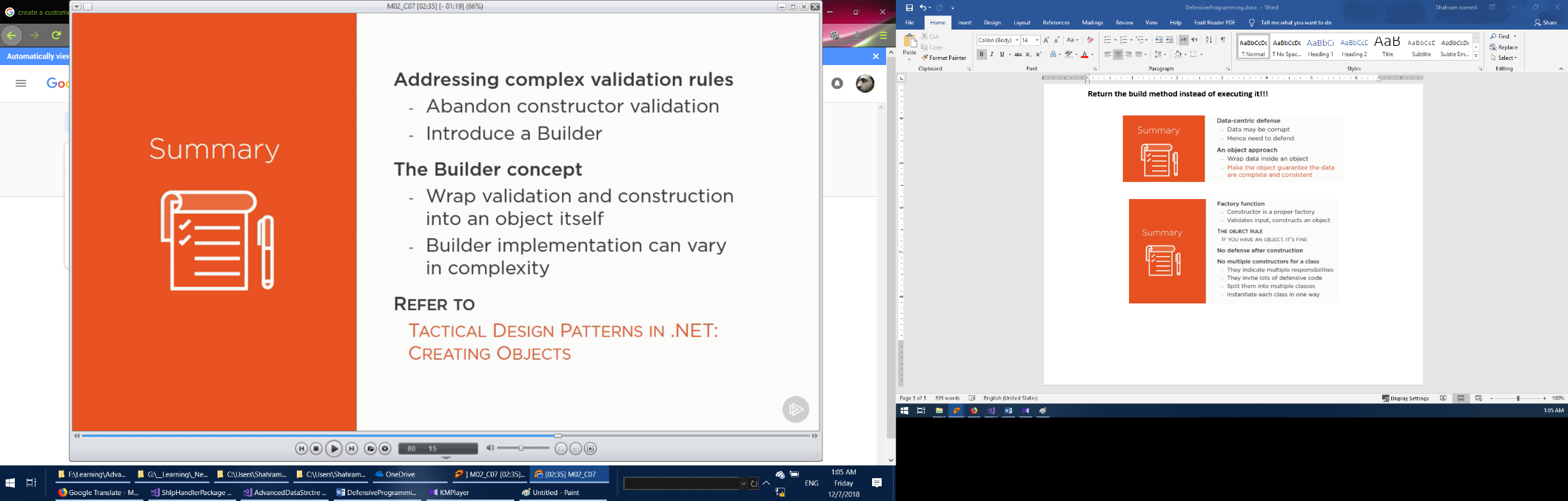
Define one factory function per class

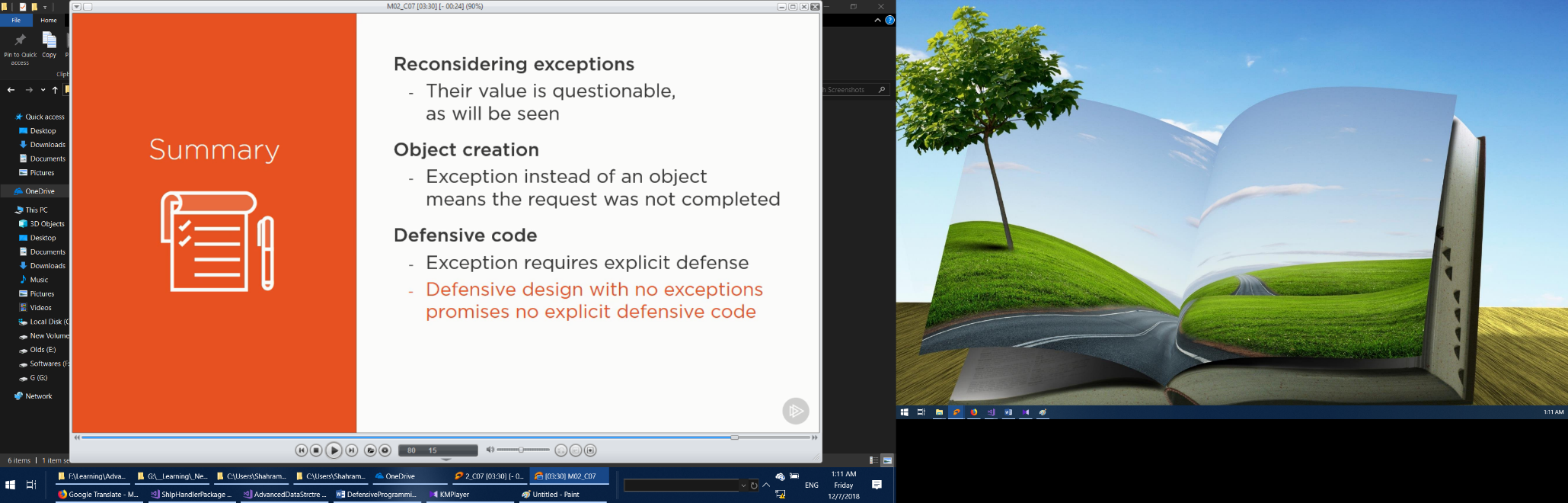
Have no discrete parameters (no enum , Boolean , etc.)

**Return the build method instead of executing it!!!**

****

****

****

****