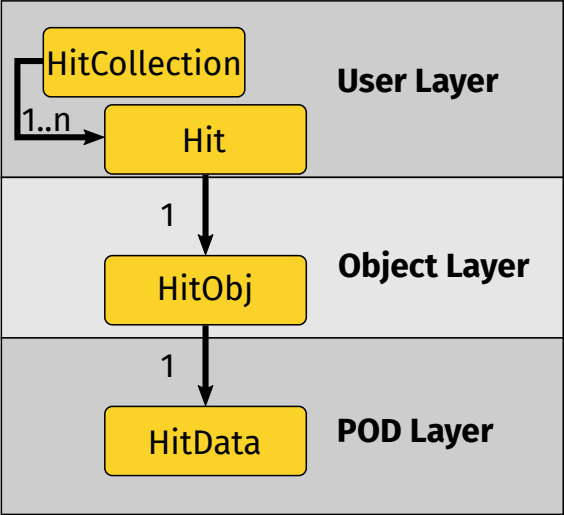


podio basics



Fundamental Problem?

- See [AIDASoft/podio#174](#)
- Seems to usually run fine when compiled with gcc, trips more often when compiled with clang
- AddressSanitizer quickly shows the problem for both

The problematic pieces:

```
auto clusters = ExampleClusterCollection();  
auto cluster = clusters.create();  
clusters.clear(); // remove this and everything works
```

The problem

```
struct Data; // POD with all the data

// Obj, handling lifetime, etc.
struct Obj : public podio::ObjBase {
    Data data;
};

class Object { // User facing object
    // this gets called on leaving scope
    ~Object() { m_obj->release(); }
    Obj* m_obj;
};

// User facing collection
struct Collection {
    Object create();
    void clear();

private:
    deque<Obj*> m_entries;
};
```

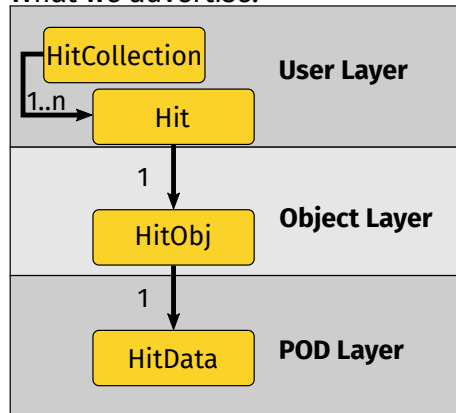
```
int podio::ObjBase::release(){
    // use-after-free here
    if (id.index != ObjectID::untracked){
        return 1;
    }
    if (--ref_counter == 0) {
        delete this;
    }
    return 0;
}

// Collection.cc =====
Object Collection::create() {
    Obj* obj = new Obj();
    m_entries.push_back(obj);
    return Object(obj);
}

void Collection::clear() {
    for (auto& obj : m_entries) delete obj;
    m_entries.clear();
}
```

What we do vs. what we claim we do

What we advertise:



What we implement:

